PCT Patent Application No. WO 2006/083063 to Park, for a system and method for mediating and conducting peer-to-peer electronic commerce, discloses a method of allowing people who don't have a commercial website to have their product details spidered and sold on a regular website.

U.S. Patent Publication No. 2006/0068785 to Kamijo et al., for a secure communication over a medium, discloses a process to assist in securing insecure communications using a cell phone.

U.S. Patent Publication No. 2005/0209876 to Linlor, for a secure money transfer between hand-held devices, discloses a method of storing a clients billing information in a database and then making a purchase from their computer using a Personal Identification Number (PIN) or biometrics to identify themselves.

BRIEF SUMMARY OF THE INVENTION

What is needed is a system that is pre-emptive and uses technology already available on every computer that accesses the Internet; so that additional software may not be required on the client computer operated by the account user. The system according to the invention preferably uses a database independent of the client computer, and works in conjunction with traditional authentication systems, or optionally without traditional authentication at all (such as with standard online credit card transactions).

The system according to the invention includes a method to determine the MAC address of a computer and other identifying details from outside the local area network (e.g., via the Internet) using common online scripting languages.

Authentication is not required for the system according to the invention to function; instead the system assists in securing existing authentication systems and online credit card transactions. The system is also comprehensive and complete, actually offering an automated security solution when suspicious transactions are made. In addition to specifying the computer used in any online transaction using the MAC address of the computer, the system according to the invention may also show the IP address of the connecting computers between the client computer and the receiving server. This allows administrators to determine if the alleged account user is using spoofing

technology to try and hide their identity. The system according to the invention may be used for law enforcement, by discreetly capturing significant data from online criminals and terrorists.

For an additional level of security, more stringent computer identification may be implemented and biometrics may be integrated with the system according to the invention to gain access to highly sensitive online accounts for government and law enforcement.

The security system according to the invention is a companion for existing authentication and processing systems. The system may provide for:

1. a reduction in hacking, fraudulent charges, and staff needed to administer a current security system;

2. an improvement in client/merchant satisfaction, and the ability to use the effectiveness of the system as selling point;

3. revenue potential (for payment processors and publishers) for the enhanced security services;

4. creation of highly secure authentication systems for federal or law enforcement applications accessible via the Internet;

5. elimination of the threat of fraudsters or hackers using IP spoofing to hide their identities and commit fraud; and

6. Provision of a system useful for espionage and for law enforcement to collect data from online criminals or terrorists.

A system for enhancing security between a client and a server is provided, including: a database, accessible by the server, the database having a record associated with an account, the account associated with a MAC address; wherein when the client accesses the account, the server receives the MAC address associated with the client and compares the MAC address associated with the client to the MAC address associated with the account, and if the MAC address associated with the client is the same as the MAC address associated with the account, permits access to the account.

If the MAC address associated with the client is not the same as the MAC address associated with the client, the server communicates with said client to determine if access to the account should be permitted.

The account may associated with a geographic area, and the server receives an IP address associated with the client, and if the geographic area associated with the IP address is not the same as the geographic area associated with the account or the MAC address of the client is not the same as the MAC address associated with the account, the server denies access to the account. If the geographic area associated with the IP address is not the same as the geographic area associated with the account and the MAC address of the client is not the same as the MAC address associated with the account, the server may notify law enforcement of the IP address and MAC address of the client.

The account may be associated with biometric information related to a user, and the server receives the biometric information from the client.

DESCRIPTION OF THE FIGURES

Exemplary embodiments are illustrated in referenced figures of the drawings. It is intended that the embodiments and figures disclosed herein are to be considered illustrative rather than restrictive.

Figure 1 is a block diagram of a system according to the invention;

Figure 2 is a flow chart showing the process by which an account is opened according to the invention;

Figure 3 is a flow chart showing the process by which an account is accessed according to the invention;

Figure 4 is a block diagram showing the interaction between an ActiveX Control Container and a Windowed ActiveX Control;

Figure 5 is a block diagram showing communication between an ActiveX Control Container and an ActiveX Control; and

Figure 6 is a block diagram showing a Java security architecture.

DETAILED DESCRIPTION OF THE INVENTION

Throughout the following description specific details are set forth in order to provide a more thorough understanding to persons skilled in the art. However, well known elements may not have been shown or described in detail to avoid unnecessarily obscuring the disclosure. Accordingly, the description and drawings are to be regarded as being illustrative and not restrictive.

The system, according to the invention, restricts access to an account (or a credit card) based on the MAC address of the network card 30 in client computer 20 used by the account user 10. Each network card 30 is identifiable by a unique MAC address.

A typical system incorporating the invention is shown in Figure 1. Account user 10, accesses the Internet 50 via client computer 20 to communicate with a server 70 operated by account provider 80. Server 70 may be a single computer, software running on a computer, or a plurality of computers. Server 70 communicates with database 90 which may be within server 70 or one or more computers in communication with server 70. Account provider 80 also has access to database 90. Client computer 20 includes a network card 30 for communications, network card 30 having a MAC address.

To use the secure account, the MAC address of the client computer must be registered with the server permitting access to the account. If client computer 20 tries to access an account or use a credit card via an unregistered computer (and therefore unregistered MAC address), then the registered account user 10 may be notified by e-mail and/or by phone, and the account, transaction or credit card can be suspended due to the suspicious action until the account user 10 verifies the transaction. If account user 10 was just using a different, unregistered computer, account user 10 can respond to the notification and the account can be re-activated without intervention from a "live" person.

The MAC address of a particular computer is positioned one level below an IP address, and within a local network it can be determined by sending an "arp –a" request. MAC addresses of computers accessing the Internet are determined and used by ISPs routinely to restrict or allow access to the

Internet by sending a Dynamic Host Configuration Protocol (DHCP) request or an Address Resolution Protocol (ARP) request to the client computer. These requests involve sending a message to the client computer 20 with the request, which in turn responds with the MAC address.

Communications sent through the Internet only retain the MAC address of the last IP/Hop in the transmitted packet, meaning that the MAC address of the original client computer 20 is not usually preserved as the packet goes from router to router throughout the Internet. However, there are several ways of determining the MAC address of client computer 20, including the following:

1. Capturing the MAC address from the first router or hop receiving the packet from client computer 20. Such a method requires a series of queries of previous routers and requires cooperation from the ISPs involved.

2. "Spoofing" a DHCP packet or ARP request with the connecting computer (as sent from the local subnet) and storing the resulting MAC address in a text file to be sent back to the requesting server 70.

3. Using a script that reports the MAC address and may also report the IP address and/or host name of client computer 20 for a message received from a connecting computer. For the purposes of law enforcement, additional details could be determined for investigation of criminals or terrorists. A secure script, digitally signed by a well-known and secure source, will allow users to run the script without security warnings. Such a script can be created using commonly used Internet scripting languages, or the script can be included as an application add-on or plug-in for computer programs or websites that use authentication; or the script may be a small stand alone application distributed by credit card issuers or payment processors.

In a preferred embodiment of the invention, more than one of these means for obtaining a MAC address may be used.

Microsoft™ or Java™ software may be used to implement the system in order to provide scripts with compatibility with most systems. The system is designed for maximum compatibility and discreet operation. In a preferred embodiment, code implementing the method according to the

invention is downloaded from a web server and then executed on client computer 20 and account provider server

Embodiment using ActiveX™ Controls

The system and method according to the invention may be implemented using ActiveX controls, which are software components based on the Component Object Model (COM™) environment provided by Microsoft™. Like Java applets, ActiveX controls 100 can be used to add rich content to web pages. Unlike applets, ActiveX controls 100 are limited to use in Microsoft's Internet Explorer™ web browser.

In the context of this document, the term "ActiveX" is used to refer to the technology that downloads and runs controls in one of the formats supported by the "Authenticode" code signing system, and corresponds to controls that can be declared from a web page using an OBJECT tag. Such controls include: COM controls (filetypes .DLL and .OCX); Win32 executable files (filetype .EXE); INF set-up files, used to specify locations and versions for a collection of other files (filetype .INF); and "cabinet" files that are referred to by an OBJECT tag (filetype .CAB). These controls are all treated in a very similar way by web-enabled ActiveX container 120 applications, including in the use of the same caching and versioning mechanisms.

ActiveX controls 100 are highly portable COM objects, and are used extensively throughout Microsoft Windows platforms and, especially, in web-based applications. COM objects, including ActiveX controls 100, can invoke each other locally and remotely through interfaces defined by the COM architecture. The COM architecture allows for interoperability among binary software components produced in disparate ways.

If an ActiveX control 100 is not installed locally, it is possible to specify a URL where the control can be obtained by account user 10. Once obtained, the control 100 installs itself on client computer 20 automatically if permitted by the browser. Once it is installed, it can be invoked without the need to be downloaded again.

ActiveX controls 100 can be signed or unsigned. A signed control provides a high degree of verification that the control was produced by the signer and has not been modified. As ActiveX

controls 100 do not run in a limited environment or "sandbox", it is important to have a high degree of trust in the author of the control.

The system and method according to the invention may be implemented using an ActiveX control 100, herein referred to as an "secureIDx control". The secureIDx control uses several programmatic elements to interact efficiently with a control container and with account user 10. These programming elements may be: class ColeControl 130; a set of event-firing functions; and a dispatch map.

The secureIDx control object inherits a set of features from its MFC base class, ColeControl 130. These features include in-place activation and Automation logic. COleControl can provide the control object with the same functionality as an MFC window object and the ability to fire events. COleControl can also provide windowless controls, which rely on their container 120 for some of the functionality a window otherwise provides, but offers faster display than windows. The fired events are used to notify the control container when something important happens in the control. The automatic logic in the secureIDx control interacts with client computer 20 and creates a unique signature for client computer 20. This unique identity of client computer 20 works as an authentication token in addition to the existing authentication systems, or as an identity token itself. SecureIDx is derived from client computer 20's MAC Address and may also be derived from the client computer's IP Address or the account user's biometrics.

When a control 100 is used within a control container 120, it uses two mechanisms to communicate: it exposes properties and methods, and it fires events. Figures 4 and 5 demonstrate how these two mechanisms are implemented.

ActiveX controls 100 are an integral part of systems and applications, and they are required for essential functions in many environments. Though priorities many change from organization to organization and user to user, it is important to understand the tradeoffs between functionality and security and to make informed decisions about the appropriate level of risk.

Authenticode and Software Signing

Software downloaded from the Internet to client computers 20 may contain unauthorized programs or viruses intended to cause damage or provide clandestine network access for malicious users. As networks become more interconnected, the threat of malicious software and viruses has extended. To counter this growing threat, Microsoft developed Authenticode™ technology to enable developers to digitally sign software using standard X.509 public key certificates. Account users can verify the publisher of digitally signed software as well as verify that the software has not been tampered with, because the publisher has signed the code. For software distributed on the Internet, most users are more likely to trust software signed by certificates issued by a reputable commercial certification authority. Therefore, if software is distributed via the Internet, it is useful to obtain the services of a commercial certification authority to issue digital signing certificates to sign the application.

Java Embodiment

The system and method according to the invention can also be implemented using Java. Java refers to a programming language; a virtual machine designed to run that language (also known as the "JVM"); and a set of APIs and libraries. The libraries are written in a combination of Java and other programming languages, for example C and C++.

The Java language is object-oriented, with all code defined as part of a class. When the software is implemented using a JVM, these classes are dynamically loaded as modules of code that can be separately compiled. Classes are stored and represented as a sequence of bytes in a standard format, called the classfile format. (They need not be stored in files as such - it is possible to create and load classfiles on the fly, for example by downloading them from a network.)

Java's security model is based on several layers of verification, including: checking the structure of each classfile to make sure that it conforms to the classfile format; checking the sequence of instructions within each method to make sure that each instruction is valid, that there are no invalid jumps between instructions, and the arguments to each instruction are of the correct type. The JVM instruction set is designed to allow this analysis to be tractable; as classes are dynamically linked, consistency checks make sure that each class is consistent with its superclasses, e.g. that final

methods are not overridden, and that access permissions are preserved; security restrictions are imposed on which packages can be accessed which can be used to prevent access to implementation classes that would not normally be needed by applets, for example; and runtime checks are performed by some instructions. For example, when an object is stored in an array, the interpreter (or compiled code) checks that the object to be stored is of the correct type, and the array index is not out of bounds.

This security scheme does not depend on the trustworthiness of the compiler that produced the classfiles (or on whether the code was compiled from source in the Java language or from another language). The compiler for the standard API libraries must be trustworthy, but this can be ensured because the standard libraries are provided by the JVM implementation. However, the scheme is complicated, and quite difficult to implement correctly. The presence of several layers increases the potential for error; a flaw in any layer may cause the whole system to collapse. This is offset against the increased efficiency over a fully interpreted language implementation where all checking is done at run-time (such as the current implementations of JavaScript and VBScript, or of Safe-Tcl and Safe-Perl).

An applet is a software component that runs within a larger application. Java applets run in the context of a Java-enabled web browser. The web browser is responsible for maintaining the environment or "sandbox" that manages the applet's resource access. In practice, this usually serves to prevent the applet from accessing the local filesystem on client computer. The browser downloads the applet code from a web server and either embeds the applet into an HTML page or opens a new browser window to show the applet user interface. The default security manager denies applets all access to the filesystem and all network access except to the web host that supplied the applet.

The method and system may be incorporated into an applet, referred to herein as secureBox. The secureBox applet is a signed applet that once trusted by a client computer runs harmlessly on the client computer with a strict security policy. The applet securely enumerates the user's computer identity by recording the MAC address and optionally the client computer 20's IP address and/or the account user's biometric information and posts such identity to server 70 which authenticates or generates alerts based on submitted identification.

Applets do have several disadvantages. For example, applets require a Java plug-in, which is not always available. Some organizations do not permit users to install software, so these users might not view applets by default. There are also performance issues. The applet cannot run until the Java Virtual Machine is initialized, and this delay can be significant. Applets usually execute at a speed that is comparable to, but slower than, compiled applications. Finally, Java applets are considered more difficult and expensive to develop than html based pages.

The JAR file format is a convention for using PKWARE™'s ZIP format to store Java classes and resources that may be signed. All JAR files are ZIP files, containing a standard directory called "/META-INF/". The META-INF directory includes a "manifest file", with name "MANIFEST.MF", that stores additional property information about each file (this avoids having to change the format of the files themselves). It also contains "signature files", with filetype ".SF", that specify a subset of files to be signed by a given principal, and detached signatures for the .SF files. A typical Java security architecture is shown in Figure 6.

Deploying Downloadable Code

Both Java and ActiveX authenticate code by signing it using a digital signature scheme. Digital signatures use public-key cryptography; each signer has a private key, and there is a corresponding public key that can be used to verify signatures by the signing party. Assuming that the digital signature algorithm is secure and is used correctly, it prevents anyone but the owner of a private key from signing a piece of data or code.

An alternative approach to signing for authenticating controls, would be to secure the connection between the web site and the browser, using a transport protocol such as SSL 3.0 (or secure IP) that ensures the integrity of the transmitted information. The site certificate would be shown when a control runs or requests additional privileges. This would have several advantages over code signing, including: in cases where the web pages also need to be authenticated, it is much simpler than requiring two separate mechanisms, and the account user 80 sees a single, consistent certificate; it is common for controls that need extra privileges, beyond the default environment or "sandbox" permissions for Java or scripts, to also require a secure (i.e. authenticated, and optionally private) connection back to the site that served them; it simplifies creating secure systems of co-

operating controls and scripts that can span pages; individual controls can be revoked at any time, by removing them from all web sites; and an malicious user cannot reuse a signed control maliciously, because the controls themselves are never signed.

It is not difficult to spoof a MAC address, however, it is extremely difficult for a malicious user, such as a hacker or fraudster, to know what the MAC address is in the first place. In order to determine the MAC address, the malicious user would have to know specifically which client computer 20 was used to access the account, which is only really possible if they have direct access to the client computer 20 being used. Further security can be provided by checking the region of the IP address and verifying the IP addresses of the connecting computers to determine if attempts have been made to hide a computer's identity.

Given the above, fraud/hacking becomes possible only by malicious users who have physical access to the client computer 20 used to access the account or credit card. If this were to happen, a report can be provided showing exactly which MAC address and IP address was used to access the account, making it easy for a particular case to be disputed by a merchant.

The system according to the invention provides both convenience and security, and fraud prevention measures/actions to prevent access/purchases from unauthorized computers. The system is practical to implement and can compliment existing online authentication checks and/or purchases.

The system may be viewed as an online computer registry and fraud/hack prevention system. The system would be queried for any publisher or merchant that wants a significant security improvement with their system.

The logic follows:

New Account / Account Creation

As seen in Figure 2, an embodiment of the process by which a new account is created includes the steps:

1. In step 210, an account user 10 using a client computer 20 logs into an online account provided by an account provider 80 for the first time, or purchases a good or service online with their credit card provided by a account provider 80, such as a credit card provider for the first time.

2. In step 220, database 90 at server 70 hosting the account or used by the credit card provider to maintain the credit card account is queried, and the system determines that this is the first time the particular account or credit card has been used online.

3. In step 230, the account is registered and verified. Depending on the security level selected by the administrator of the account provider 80, client computer 20 will either:

(a) Automatically have its MAC address and IP address registered to the account or credit card and stored in database 90;

(b) Receive an e-mail automatically emailed to the e-mail address provided to the account provider, to confirm that the account user 10 has made the request. If the account user 10 confirms the request, the MAC address and IP address of client computer 20 are registered with the account or credit card. If the account user 10 does not confirm the request, the account or credit card may automatically be suspended, and an administrator notified; or

(c) Receive a phone call using the phone number provided to the account provider 80, to confirm that they have made the request. If the account user 10 confirms the request, the MAC address and IP address of the client computer 20 are registered with the account or credit card. If the account user 10 does not confirm the request, the account or credit card may be suspended, and an administrator notified. Optionally, an additional automated check could be made by an administrator using the account user's registered phone number to test the type of phone being used (PSTN line, cell phone, or VOIP). If the phone type is not appropriate (i.e. VOIP instead of a cell phone), the administrator could be notified for review and the account suspended.

Current Account / Fraud Prevention

The system according to the invention can also be used to protect accounts by preventing unauthorized access to such accounts. In such a use, the following steps, as seen in Figure 3, may occur:

1. In step 310, account user 10 logs into their existing online account, or makes a purchase with their credit card.

2. In step 320, database 90 is queried, and determines that the account accessed is an existing account.

3. In step 330, depending on the security level selected by the administrator, server 70 queries to the client computer 20 for verification purposes, specifically to determine if:

(a) The MAC address of client computer 20 matches the account;

(b) The MAC address of client computer 20 matches the account and the IP address of the client computer 20 is from the appropriate geographical region; and/or

(c) The IP address is accurate and is not being spoofed.

4. In step 340, if the database query is successful, the authentication process or purchase continues as intended.

5. In step 350, if the database query is NOT successful, depending on the security level selected by the administrator, the following may happen:

(a) Client computer 20 is automatically e-mailed (to the e-mail address provided to the administrator), to confirm that they have made the request. If client computer 20 confirms the request, the new MAC address and IP address are registered to the account or credit card. This automatically registers the additional computer for use with the account. If the client computer 20 does not confirm the request, the account or credit card may automatically be suspended, and an administrator notified; or

(b) The account user 10 is automatically phoned (at the phone number provided to the administrator), to confirm that they have made the request. If the account user 10 confirms

the request, the new MAC address and IP address are registered to the account or credit card. This automatically registers the additional client computer 20 for use with the account. If the account user 10 does not confirm the request, the account or credit card may automatically be suspended, and an administrator notified.

For investigative purposes, the system is able to provide the true IP address and MAC address of attempted frauds or hacks, thus allowing investigators to track down fraudsters or hackers, even if they are using proxy servers. Additional information could also be used by law enforcement to help gather information regarding online criminals and terrorists.

The system is automated and has significant revenue potential by having multiple database servers (co-located or licensed) to meet demand, and charge per usage fees for database queries and automated e-mail/call services. The system according to the invention thereby may save the online industry significant amounts of time and money.

Using the system, the only fraud/hacks possible are by people who have physical access to the client computer 20. Although it is possible to spoof IP and MAC addresses, it is virtually impossible to know (or find out) which MAC address is registered with the account, unless the malicious user knows which client computer 20 was used to register the account in the first place. The true IP address functionality also eliminates the risk of IP address spoofing by showing the true IP address used by each client computer in every online transaction. The system thereby can determine which client computer was used for the transaction, which would greatly limit a merchant's liability by proving that the transaction was completed at an authorized location.

Profiling

The system according to the invention can be used for anti-fraud / profiling purposes to allow users to look for and be notified of suspicious credit card activity. This additional protection helps make credit card transactions even more secure for online purchases.

At present credit card companies look for suspicious activity on their own. However, each credit card company sets its own criteria, which may not be suitable for every card user. The system according to the invention allows clients to determine themselves the types of purchases they want

to allow with a particular credit card. For example, a card user may want to be notified if a purchase over $100 is made on their card, or if there is a purchase overseas, etc. The card users themselves know exactly how they plan on using their card, while the credit card providers do not.

If a suspicious transaction occurs, the card user can preselect to have the card immediately suspended or they can be sent an automated e-mail or phone call to confirm authorization of the purchase.

In this embodiment of the system, card users need be able to change their profile settings. For additional security, the system may require an automated confirmation e-mail or phone call to the account holder when any profile change is made.

Revenue Model.

An operator of the system using graduated licensing and usage fees may generate revenue. For example:

1. Co-located solution - the publisher, payment processor, or other party pays the operator a monthly fee for a fixed amount of queries to a database hosted on the operator's servers. This could be done on a shared server or a dedicated server (at an additional cost). The information stored may only be for the purpose of account verification, so that personal information would not have to be stored in the database. For example, the database may just have to store the account name, or the last digits of a credit card, and the MAC address of the client computer 20.

2. Local solution - the publisher, payment processor, etc. pays a license fee to run the software and database on their own server (this may be restricted by usage, but at a lower fee than as indicated above).

3. Security notifications – a charge per usage fee for automated security notifications to the account user by e-mail (if their account or credit card is being used on an additional computer), a higher fee may be charged for automated notifications by telephone.

4. Payment processors or credit card companies may offer these enhanced services to their merchants. Game publishers, etc., may consider the system to release resources otherwise tied up dealing with hacking/security issues.

In an alternative embodiment, payment processors may access a consolidated credit card security database for each transaction, so that no password would be required. This system would offer the convenience of not having to use a password, and complete peace of mind for the cardholder and the merchant, knowing that it is not possible to place an order from a computer that has not been authorized to do so.

The invention encompasses all modifications, permutations, additions and sub-combinations of the features described herein. Although the exemplary aspects and embodiments of the invention have been disclosed in detail for illustrative purposes, it will be recognized that permutations, additions, variations, sub-combinations or modifications of the disclosed apparatus lie within the scope of the present invention.

CLAIMS

The invention claimed is:

1. A system for enhancing security between a client and a server, comprising:

a database, accessible by the server, said database having a record associated with an account, said account associated with a MAC address;

wherein when said client accesses said account, said server receives said MAC address associated with said client and compares said MAC address associated with said client to said MAC address associated with said account, and if said MAC address associated with said client is the same as said MAC address associated with said account, permits access to said account.

2. The invention of claim 1 wherein if said MAC address associated with said client is not the same as said MAC address associated with said client, communicating with said client to determine if access to said account should be permitted.

3. The invention of claim 1 wherein said account is associated with a geographic area, and said server receives an IP address associated with said client.

4. The invention of claim 3 wherein if said geographic area associated with said IP address is not the same as said geographic area associated with said account or said MAC address of said client is not the same as said MAC address associated with said account, said server denying access to said account.

5. The invention of claim 4 wherein if said geographic area associated with said IP address is not the same as said geographic area associated with said account and said MAC address of said client is not the same as said MAC address associated with said account, said server notifies law enforcement of the IP address and MAC address of said client.

6. The invention of claim 4 wherein said account is associated with biometric information related to a user.

7. The invention of claim 6 wherein said server receives said biometric information from said client.

8. A method of allowing a client computer to access an account, comprising:

(a) said client computer requesting access to an account at a server;

(b) said server determining a MAC address associated with said client computer;

(c) said server accessing a database, said database having a MAC address associated with said account;

(d) comparing said MAC address associated with said account and said MAC address associated with said client computer;

(e) if said MAC address associated with said account and said MAC address associated with said client computer are the same, permitting access to said account.

9. The method of claim 3 further comprising the step of:

(f) if said MAC address associated with said account and said MAC address associated with said computer are different, contacting a user associated with said account.

10. The invention of claim 8 wherein a geographic area is associated with said account, and said server determining an IP address associated with said client computer.

11. The invention of claim 10 wherein if said geographic area associated with said IP address is not the same as said geographic area associated with said account, or said MAC address of said client is not the same as said MAC address associated with said account, said server denying access to said account.

12. The invention of claim 11 wherein if said geographic area associated with said IP address is not the same as said geographic area associated with said account and said MAC address of said client is not the same as said MAC address associated with said account, said server notifying law enforcement of the IP address and MAC address of said client computer.

13. The invention of claim 11 wherein said account is associated with biometric information related to a user.

14. The invention of claim 13 wherein said server receives said biometric information from said client.

5

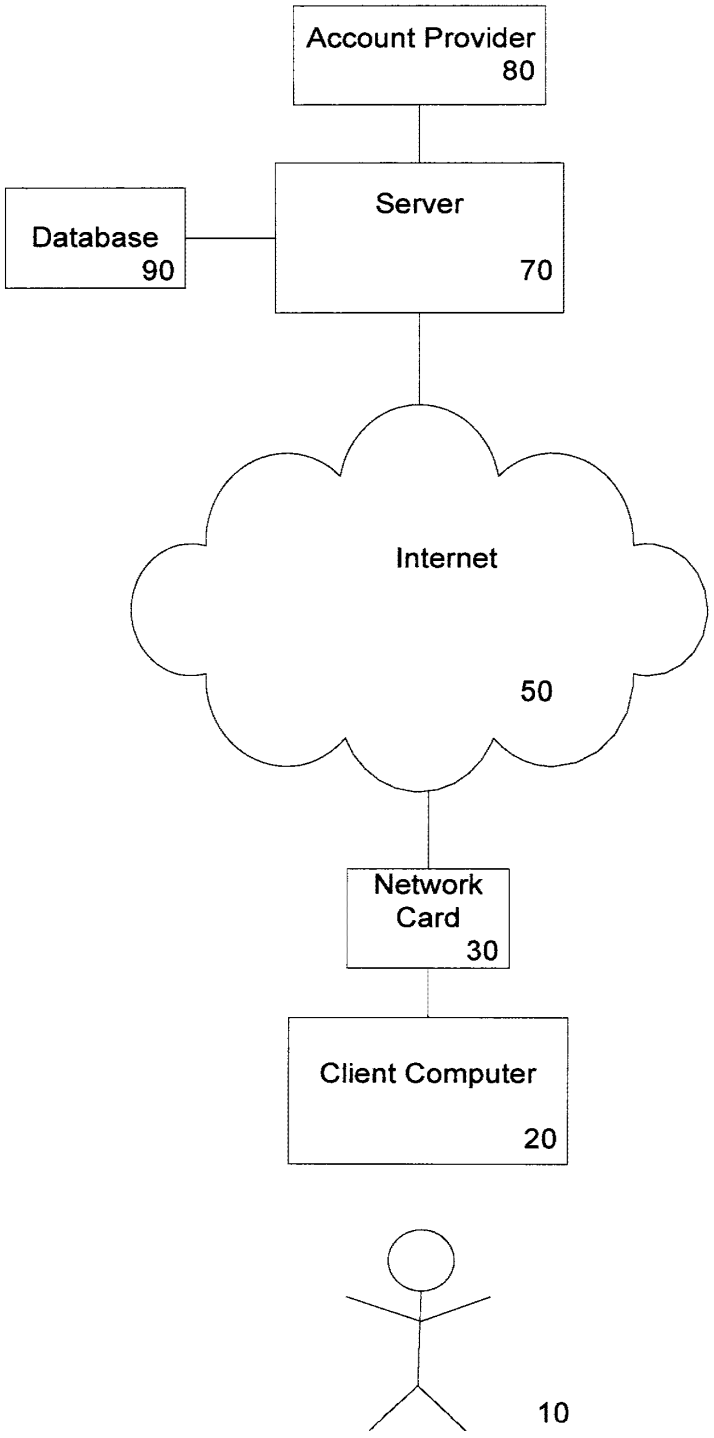

Account Provider
80
Server
70
Database
90
Internet
50
Network
Card
30
Client Computer
20
10

Fig 1

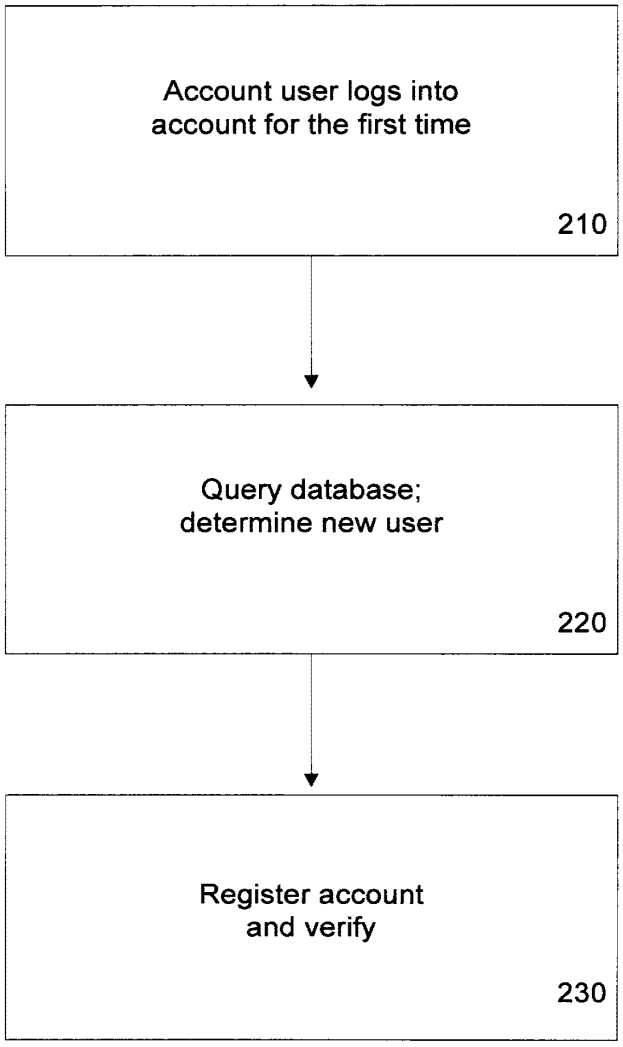

Account user logs into account for the first time
210
Query database; determine new user
220
Register account and verify
230

Fig 2

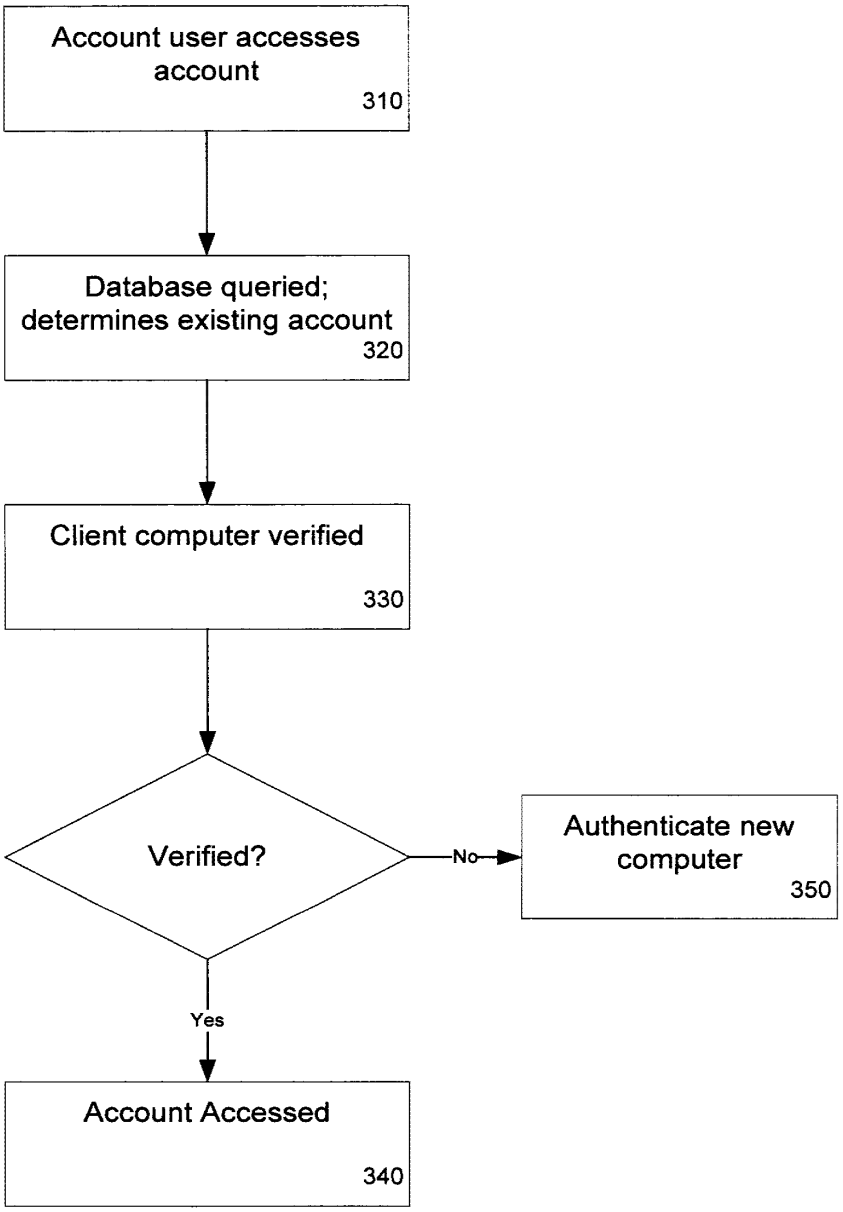

Account user accesses account
310
Database queried; determines existing account
320
Client computer verified
330
Verified?
No
Authenticate new computer
350
Yes
Account Accessed
340

Fig 3

Figure 4

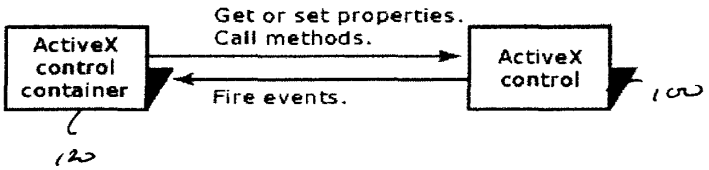
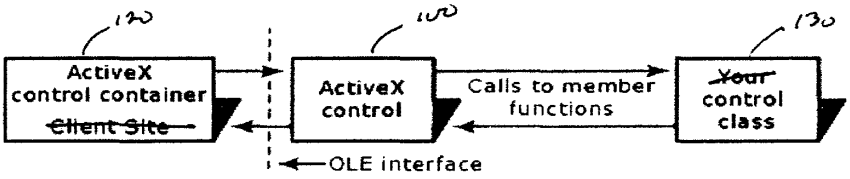
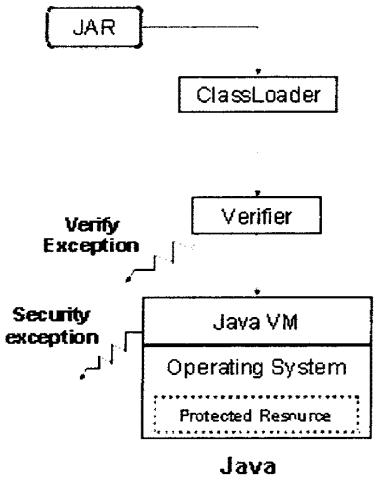


Figure 5



5/5

Figure 6


JAR
ClassLoader
Verifier
Verify Exception
Security exception
Java VM
Operating System
Protected Resource
Java

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2007/001767

A. CLASSIFICATION OF SUBJECT MATTER
IPC: ***H04L 9/32*** (2006.01) , ***G06Q 20/00*** (2006.01)
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC (2006.01) : ***H04L 9/32***, ***G06Q 20/00*** using keywords

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)
Delphion, Canadian Patent Database, WEST
Keywords:authentication, MAC, account, database, ActiveX, Java, COM, control container, SecureIDx, computer registry, hack/fraud, client, server, IP address, geographic area

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US2003/0014368 A1; "Systems, Methods and Apparatus for Secure Printing of Negotiable Instruments"; LEURIG et al; 16 January 2003 (16-01-2003) [Abstract], [0016] - [0040]	1-14
A	US2004/0097217 A1; "System and Method for Providing Authentication and Authorization Utilizing a Personal Wireless Communication Device"; McCAIN et al: 20 May 2004 (20-05-2004) [Abstract], [0036], [0159]	1-14
A	US2004/0098620 A1; "System, Apparatuses, Methods, and Computer-Readable Media Using Identification Data in Packet Communications"; SHAY, A. D.; 20 May 2004 (20-05-2004) ** whole document **	1-14
A	US2006/0212407 A1: "User Authentication and Secure Transaction System"; LYON, D. B.; 21 September 2006 (21-09-2006) ** whole document **	1-14

[ ] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 January 2008 (14-01-2008)	24 January 2008 (24-01-2008)
Name and mailing address of the ISA/CA Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001-819-953-2476	Authorized officer Lawrence J. Engel 819- 997-2936

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CA2007/001767

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US 2003014368A1	16-01-2003	None	
US 2004097217A1	20-05-2004	WO 2005015485A1	17-02-2005
		WO 2005015485A9	28-07-2005
US 2004098620A1	20-05-2004	AU 2003294304A1	15-06-2004
		CA 2506418A1	03-06-2004
		EP 1574009A1	14-09-2005
		JP 2006510328T	23-03-2006
		US 2004098619A1	20-05-2004
		US 2005160289A1	21-07-2005
		WO 2004047407A1	03-06-2004
US 2006212407A1	21-09-2006	WO 2006101684A2	28-09-2006
		WO 2006101684A3	06-12-2007

Electronic Acknowledgement Receipt

EFS ID:	16536991
Application Number:	13734178
International Application Number:	
Confirmation Number:	3155
Title of Invention:	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES
First Named Inventor/Applicant Name:	Craig S. ETCHEGOYEN
Customer Number:	96051
Filer:	Sean Dylan Burdick/Amanda Ivey
Filer Authorized By:	Sean Dylan Burdick
Attorney Docket Number:	UN-NP-SC-085
Receipt Date:	08-AUG-2013
Filing Date:	04-JAN-2013
Time Stamp:	14:28:15
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	SC-085_IDS_Transmittal_Letter.pdf	30860 be456f389963eca6246ed77bed8deb83cfdf790b	no	2

Warnings:	
Information:	

2	Information Disclosure Statement (IDS) Form (SB08)	SC-085_IDS_List.pdf	66895 9030eecb7e71788c22301c8460bd52c45d11916d	no	5
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Foreign Reference	JP19924117548A.pdf	293119 3dc34901cceaf5bc1536fd8cbcb17461dab8d683	no	6
Warnings:					
Information:					
4	Foreign Reference	JP19924117548A_Abstract_English.pdf	41922 9999ea28e5af44941f3d16a4a9d42610ddbe76b8	no	1
Warnings:					
Information:					
5	Foreign Reference	WO_01-09756_SAFEWWW.pdf	1713984 938450bb8f859ba7f32f7b3693d93cfb6839ec11	no	50
Warnings:					
Information:					
6	Foreign Reference	WO_2008_034900_Boesgaard_Sorenson.pdf	3109330 c634bbd28958579a01cd2c60b2f4910f5cb19b86	no	87
Warnings:					
Information:					
7	Foreign Reference	WO08052310_PGMX_Inc.pdf	1188134 c8da1e27055978067a524f44bfd1783e626f82b8	no	31
Warnings:					
Information:					
8	Non Patent Literature	Eisen_Catching_Fraudulent_Man_MIddle.pdf	47602 d20534aa08bf39d10e0efa5fd3801556fe9b7c40	no	2
Warnings:					
Information:					
9	Non Patent Literature	RFC_2459.pdf	474755 3bb0063429c8f12b7307ff00b9c049de3a4169ff	no	75
Warnings:					
Information:					
10	Non Patent Literature	XP002604710_Wiki_Software_Extension.pdf	112965 b25cd933c2b3161b7cf0624769e31b02e0194a83	no	2

Warnings:					
Information:					
11	Non Patent Literature	XP002603488_Database_Appls_and_the_Web.pdf	324904 ac39dbd53e422150fe261bd5ba732442910f3eed	no	3
Warnings:					
Information:					
12	Non Patent Literature	Zhu_Yunpu_New_Architecture_Secure_Two_Party.pdf	6939907 57b754b0a26378167b3058fae5ac79ebc2f7c4fc	no	240
Warnings:					
Information:					
13	Non Patent Literature	RFC-4252.pdf	643898 3e4c3b0eb023b7a005be5223b99137f67891aeeb	no	16
Warnings:					
Information:					
14	Non Patent Literature	Nesi_Protection_Processor_MPEG-21.pdf	22417802 c80ccb4460289c637a61b9de7f0f12ae590b5282	no	5
Warnings:					
Information:					
		Total Files Size (in bytes):	37406077		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. no.:	13/734,178	Conf. no.	3155
Applicant:	UNILOC LUXEMBOURG, S. A.	Art Unit:	2649
Filed:	January 4, 2013	Examiner:	Yuwen Pan

Title: NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENLCOSED CONTENT SOUND WAVES

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicant hereby submits, without admission of prior art effect thereof, form(s) PTO/SB/08 pursuant to the duty of disclosure requirements of 37 CFR §§ 1.56, 1.97 and 1.98.

Applicant has listed publication dates on the attached form(s) PTO/SB/08 based on information presently available to the undersigned. However, the listed publication dates should not be construed as an admission that the information was actually published on the date indicated.

It is respectfully requested that the Examiner initial and return a copy of the enclosed forms PTO/SB/08, and to indicate in the official file wrapper of this patent application that the documents have been considered.

This Information Disclosure Statement is being filed within three months of the U.S. filing date, before the mailing date of a first Office Action on the merits, or before the mailing of a first Office Action after the filing of a request for continued examination, therefore no statement under 37 CFR § 1.97(e) or fee is required.

Respectfully Submitted,

Sean D. Burdick
Reg. No. 51,513

Uniloc USA, Inc.
7160 N. Dallas Parkway, Suite 380
Plano, TX 75024
972-905-9580x227

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

UNILOC USA, INC.
LEGACY TOWN CENTER
7160 DALLAS PARKWAY
SUITE 380
PLANO, TX 75024

MAILED

AUG 13 2013

OFFICE OF PETITIONS

In re Application of
Craig S. Etchegoyen, et al.
Application No.: 13/734,178
Filed: 04 January 2013
Attorney Docket No.: UN-NP-SC-085
For: NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES

: DECISION ON REQUEST TO
: PARTICIPATE IN THE PATENT
: PROSECUTION HIGHWAY
: PROGRAM AND PETITION
: TO MAKE SPECIAL UNDER
: 37 CFR 1.102(a)

This is a decision on the request to participate in the Patent Prosecution Highway (PPH) pilot program and the petition under 37 CFR 1.102(a), filed 08 January 2013 and renewed 09 May 2013, to make the above-identified application special.

The request and petition are **GRANTED**.

DISCUSSION

A grantable request to participate in the PPH program and petition to make special require:

(1) The U.S. application must validly claim priority under 35 U.S.C. 119(a) to one or more applications filed in the IPAU;

(2) Applicant must submit a copy of the allowable/patentable claim(s) from the IPAU application(s);

(3) All of the claims in the U.S. application must sufficiently correspond or be amended to sufficiently correspond to the allowable/patentable claim(s) in the IPAU application(s); and

(4) Examination of the U.S. application has not begun;

(5) Applicant must submit a copy of all of the Office actions from each of the IPAU application(s);

(6) Applicant must submit:

a. An IDS listing the documents cited by the IPAU examiner in the IPAU Office action(s) (unless already submitted in this application)
b. Copies of documents except U.S. patents or U.S. patent application publications (unless already submitted in this application); and

The request to participate in the PPH pilot program and petition comply with the above requirements. Accordingly, the above-identified application has been accorded "special" status.

Telephone inquiries concerning this decision should be directed to April M. Wise at (571) 272-1642.

All other inquiries concerning the examination or status of the application is accessible in the PAIR system at http://www.uspto.gov/ebc.index.html.

This application will be forwarded to the examiner for action on the merits commensurate with this decision.

/dab/
David Bucci
Petitions Examiner
Office of Petitions

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/734,178	01/04/2013	Craig S. ETCHEGOYEN	UN-NP-SC-085

CONFIRMATION NO. 3155

96051
Uniloc USA Inc.
Legacy Town Center
7160 Dallas Parkway
Suite 380
Plano, TX 75024

POA ACCEPTANCE LETTER

OC000000063237706

Date Mailed: 08/19/2013

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 08/08/2013.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/zabraha/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/734,178	01/04/2013	Craig S. ETCHEGOYEN	UN-NP-SC-085	3155

96051 7590 09/06/2013

Uniloc USA Inc.
Legacy Town Center
7160 Dallas Parkway
Suite 380
Plano, TX 75024

EXAMINER	
AKINYEMI, AJIBOLA A	
ART UNIT	PAPER NUMBER
2649	

NOTIFICATION DATE	DELIVERY MODE
09/06/2013	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

sean.burdick@unilocusa.com
sbaker@unilocusa.com

Office Action Summary	Application No. 13/734,178	Applicant(s) ETCHEGOYEN ET AL.	
	Examiner AJIBOLA AKINYEMI	Art Unit 2649	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03/22/2013*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-8* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-8* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *01/04/2013* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some * c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

1) The present application is being examined under the pre-AIA first to invent provisions.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

2. The following is a quotation of the appropriate paragraphs of pre-AIA 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claim 1 is rejected under pre-AIA 35 U.S.C. 102(b) as being anticipated by Gass (Pub. No.: US 2004/0038716A1).

With respect to claim 1:

Gass discloses a method for near field authentication of a source the source using an audio transceiver computing device comprising scanning a plurality of predetermined frequencies for a free frequency **(parag,0016 discloses scanning plurality of predetermined frequency for a free frequencies);** selecting the free frequency from the plurality of predetermined frequencies **(parag.0016 also discloses selecting free frequency from plurality of frequencies);** generating a periodic enclosed content

message; generating a modulated carrier wave representing the periodic enclosed content message and transmitting the modulated carrier wave at the free frequency **(Parag. 0015 also discloses the RDS encoder encodes said frequency or channel information generating a corresponding RDS signal 5 modulated on the RDS sub carrier at 57 KHz).**

Claim Rejections - 35 USC § 103

4. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained through the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under pre-AIA 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.

2. Ascertaining the differences between the prior art and the claims at issue.

3. Resolving the level of ordinary skill in the pertinent art.

4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

6. Claim 2 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Gass (Pub. No.: US 2004/0038716A1) and further in view of Martin (Pub. No.: US 2007/0198850A1).

With respect to claim 2:

The rejection of claim 1 is incorporated; Gass does not explicitly disclose the method further comprising displaying a user interface on the audio transceiver computing device requesting the biometric data from a user; and responsive to receiving the biometric data, generating the periodic enclosed content message, wherein the content in each period of the periodic enclosed content message includes the biometric data.

Martin discloses this limitation (parag. 0062-0063 discloses a user interface on the audio transceiver computing device requesting the biometric data from a user). It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the teaching of Martin into the teaching of Gass in order to provide a security system wherein the user is provided with dual layered verification system in addition to a unique identifier given to the user.

7. Claims 3-5 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Gass (Pub. No.: US 2004/0038716A1) and further in view of Kip (Patent No.: US 5019813).

With respect to claim 3:

The rejection of claim 1 is incorporated; Gass does not explicitly disclose wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

Kip discloses this above limitations (col.5, line 39-44). It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the teaching of Kip into the teaching of Gass in order to provide a universally applicable data exchange system operating in a contactless manner.

With respect to claim 4:

Kip discloses the method wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user (fig.5b, col.5, line 39-44).

With respect to claim 5:

Gass discloses the method wherein the modulated carrier wave comprises a sound wave (parag. 0016).

8. Claims 6-8 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Gass (Pub. No.: US 2004/0038716A1), Martin (Pub. No.: US 2007/0198850A1) as applied to claim 2 above and further in view of Kip (Patent No.: US 5019813).

With respect to claim 6:

The rejection of claim 2 is incorporated; Gass and Martin do not disclose wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

Kip discloses this above limitations (col.5, line 39-44). It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the teaching of Kip into the teaching of Gass in view of Martin in order to provide a universally applicable data exchange system operating in a contactless manner.

With respect to claim 7:

Kip discloses the method wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user (fig.5b, col.5, line 39-44).

With respect to claim 8:

Gass discloses the method wherein the modulated carrier wave comprises a sound wave (parag. 0016).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to AJIBOLA AKINYEMI whose telephone number is (571)270-1846. The examiner can normally be reached on monday- friday (8.30-5pm) Est.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, YUWEN PAN can be reached on (571) 272-7855. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Ajibola Akinyemi/
Primary Examiner, Art Unit 2649

Notice of References Cited	Application/Control No. 13/734,178	Applicant(s)/Patent Under Reexamination ETCHEGOYEN ET AL.	
	Examiner AJIBOLA AKINYEMI	Art Unit 2649	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-5,019,813 A	05-1991	Kip et al.	340/10.51
*	B	US-2004/0038716 A1	02-2004	Gass, Vincent	455/569.1
*	C	US-2007/0198850 A1	08-2007	Martin et al.	713/186
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13734178	ETCHEGOYEN ET AL.
	Examiner	**Art Unit**
	AJIBOLA AKINYEMI	2649

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	08/30/2013								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13734178	ETCHEGOYEN ET AL.
	Examiner	Art Unit
	AJIBOLA AKINYEMI	2649

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
455	41.1	8/30/2013	AA

SEARCH NOTES		
Search Notes	Date	Examiner
455/11.1,569.1	8/30/2013	AA

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L3	2488	455/41.1.ccls.	US-PGPUB; USPAT	OR	OFF	2013/08/30 11:09
L4	61	scan$4 same free adj frequency	US-PGPUB; USPAT	OR	OFF	2013/08/30 11:11
L5	1283727	scan$4	US-PGPUB; USPAT	OR	OFF	2013/08/30 11:11
L6	452	3 and 5	US-PGPUB; USPAT	OR	OFF	2013/08/30 11:12
L7	382	6 and select$3	US-PGPUB; USPAT	OR	OFF	2013/08/30 11:12
L8	15	scan$3 same select$3 same free adj frequency	US-PGPUB; USPAT	OR	OFF	2013/08/30 11:14

8/30/2013 11:14:44 AM
C:\Users\aakinyemi\Documents\EAST\Workspaces\12645007.wsp

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 3155

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/734,178	01/04/2013 RULE	455	2649	UN-NP-SC-085

APPLICANTS

Craig S. ETCHEGOYEN, Newport Beach, CA;
Dono HARJANTO, Irvine, CA;
Sean D. BURDICK, Dallas, TX;
UNILOC LUXEMBOURG S.A., Luxembourg, LUXEMBOURG

**** CONTINUING DATA ***************************

This appln claims benefit of 61/595,599 02/06/2012

**** FOREIGN APPLICATIONS ***************************

AUSTRALIA 2012100462 04/24/2012

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
01/31/2013

Foreign Priority claimed	35 USC 119(a-d) conditions met	Verified and Acknowledged		STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
☑ Yes ☐ No	☑ Yes ☐ No	/AJIBOLA A AKINYEMI/ Examiner's Signature	☐ Met after Allowance AA Initials	CA	9	8	1

ADDRESS

Uniloc USA Inc.
Legacy Town Center
7160 Dallas Parkway
Suite 380
Plano, TX 75024
UNITED STATES

TITLE

NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES

FILING FEE RECEIVED		
603	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

BIB (Rev. 05/07).

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO
(modified by Applicant)

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	13/734,178
Filing Date	January 4, 2012
First Named Inventor	Craig S. ETCHEGOYEN
Art Unit	2649
Examiner Name	/Ajibola Akinyemi/
Attorney Docket Number	UN-NP-SC-085

U. S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-5,239,648	08/24/1993	Nukui, Harumi	
		US-5,313,637	05/17/1994	Rose, David K.	
		US-6,098,106	08/01/2000	Philyaw et al.	
		US-2004/0187018	09/23/2004	Owen et al.	
		US-2006/0130135	06/15/2006	Krstulich et al.	
		US-2010/0281261	11/04/2010	Razzell, Charles	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code – Number – Kind Code	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date page(s), volume-issue number(s), publisher, city and/or country where published.	T

Examiner Signature	/Ajibola Akinyemi/	Date Considered	08/30/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A./

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO
(modified by Applicant)

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 5

Complete if Known	
Application Number	13/734,178
Filing Date	January 4, 2013
First Named Inventor	Craig S. ETCHEGOYEN
Art Unit	2649
Examiner Name	~~Yuwen Pan~~ /Ajibola Akinyemi/
Attorney Docket Number	UN-NP-SC-085

U. S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-4,200,770	04/29/1980	Hellman et al.	
		US-4,218,582	08/19/1980	Hellman et al.	
		US-4,323,921	04/06/1982	Guillou	
		US-4,337,483	06/29/1982	Guillou	
		US-4,405,829	09/20/1983	Rivest et al.	
		US-4,450,535	05/22/1984	de Pommery et al.	
		US-4,633,036	12/30/1986	Hellman et al.	
		US-4,652,990	03/24/1987	Pailen et al.	
		US-4,672,572	06/09/1987	Alsberg, Peter	
		US-4,747,139	05/24/1988	Taafe, James L.	
		US-4,868,877	09/19/1989	Fischer, Addison M.	
		US-4,977,594	12/11/1990	Shear, Victor H.	
		US-5,005,200	04/02/1991	Fischer, Addison M.	
		US-5,048,085	09/10/1991	Abraham et al.	
		US-5,050,213	09/17/1991	Shear, Victor H.	
		US-5,123,045	06/16/1992	Ostrovsky et al.	
		US-5,144,667	09/01/1992	Pogue, Jr. et al.	
		US-5,148,481	09/15/1992	Abraham et al.	
		US-5,155,680	10/13/1992	Wiedemer, John D.	
		US-5,162,638	11/10/1992	Diehl et al.	
		US-5,191,611	03/02/1993	Lang, Gerald s.	
		US-5,204,901	04/20/1993	Hershey et al.	
		US-5,231,668	07/27/1993	Kravitz, David W.	
		US-5,349,643	09/20/1994	Cox et al.	

Examiner Signature		Date Considered	08/30/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A./

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO
(modified by Applicant)

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 5

Complete if Known	
Application Number	13/734,178
Filing Date	January 4, 2013
First Named Inventor	Craig S. ETCHEGOYEN
Art Unit	2649
Examiner Name	~~Yuwen Pan~~ /Ajibola Akinyemi/
Attorney Docket Number	UN-NP-SC-085

U. S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-5,418,854	05/03/1995	Kaufman et al.	
		US-5,606,614	02/25/1997	Brady et al.	
		US-6,098,053	08/01/2000	Slater, Alan	
		US-6,163,843	12/09/2000	Inoue et al.	
		US-6,681,017	01/20/2004	Matias et al.	
		US-6,880,079	04/12/2005	Kefford et al.	
		US-7,032,110	04/18/2006	Su et al.	
		US-7,032,242	04/18/2006	Grabelsky et al.	
		US-7,310,813	12/18/2007	Lin et al.	
		US-7,444,508	10/28/2008	Karjala et al.	
		US-7,506,056	03/17/2009	Satish et al.	
		US-7,599,303	10/06/2009	Nadeau et al.	
		US-7,739,401	06/15/2010	Goyal, Pawan	
		US-7,739,402	06/15/2010	John Roese	
		US-7,852,861	12/14/2010	Wu et al.	
		US-2002/0010864	01/24/2002	Safa, John Aram	
		US-2002/0099952	07/25/2002	Lambert et al.	
		US-2002/0112171	08/15/2002	Ginter et al.	
		US-2003/0063750	04/03/2003	Medvinsky et al.	
		US-2003/0149777	08/07/2003	Adler, Micah	
		US-2003/0190046	10/09/2003	Kamerman et al.	
		US-2003/0204726	10/30/2006	Kefford et al.	
		US-2003/0212892	11/13/2003	Oishi, Kazuomi	
		US-2003/0217263	11/20/2003	Sakai, Tsutomu	

Examiner Signature	/Ajibola Akinyemi/	Date Considered	08/30/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A./

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO
(modified by Applicant)

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 3 of 5

Complete if Known	
Application Number	13/734,178
Filing Date	January 4, 2013
First Named Inventor	Craig S. ETCHEGOYEN
Art Unit	2649
Examiner Name	~~Yuwen Pan~~ /Ajibola Akinyemi/
Attorney Docket Number	UN-NP-SC-085

U. S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-2003/0237004	12/25/2003	Okamura, Mine	
		US-2004/0030912	02/12/2004	Merkle et al.	
		US-2004/0143746	07/22/2004	Ligeti et al.	
		US-2004/0145773	07/29/2004	Oakeson et al.	
		US-2005/0033957	02/10/2005	Enokida, Tomoaki	
		US-2005/0169271	08/04/2005	Janneteau et al.	
		US-2005/0187890	08/25/2005	Sullivan, Bryan	
		US-2006/0095454	05/04/2006	Shankar et al.	
		US-2006/0161914	07/20/2006	Morrison et al.	
		US-2006/0271485	11/30/2006	McKenzie et al.	
		US-2006/0280207	12/14/2006	Guarini et al.	
		US-2007/0005974	01/04/2007	Kudou, Yoshiyuki	
		US-2007/0055853	03/08/2007	Hatasaki et al.	
		US-2007/0079365	04/05/2007	Ito et al.	
		US-2007/0219917	09/20/2007	Liu et al.	
		US-2008/0022103	01/24/2008	Brown et al.	
		US-2008/0028114	01/31/2008	Mun, Kui-Yon	
		US-2008/0040785	02/14/2008	Shimada, Katsuhiko	
		US-2008/0049779	02/28/2008	Hopmann et al.	
		US-2008/0052775	02/28/2008	Sandhu et al.	
		US-2008/0076572	03/27/2008	Nguyen et al.	
		US-2008/0082813	04/03/2008	Chow et al.	
		US-2008/0098471	04/24/2008	Ooi et al.	
		US-2008/0244739	10/02/2008	Liu et al.	

Examiner Signature	/Ajibola Akinyemi/	Date Considered	08/30/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A./

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO
(modified by Applicant)

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 4 of 5

Complete if Known	
Application Number	13/734,178
Filing Date	January 4, 2013
First Named Inventor	Craig S. ETCHEGOYEN
Art Unit	2649
Examiner Name	~~Yuwen Pan~~ /Ajibola Akinyemi/
Attorney Docket Number	UN-NP-SC-085

U. S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-2008/0298595	12/04/2008	Narayanan et al.	
		US-2008/0311994	12/18/2008	Amaitis et al.	
		US-2009/0003600	01/01/2009	Chen et al.	
		US-2009/0006861	01/01/2009	ven Bemmel, Jeroen	
		US-2009/0016264	01/15/2009	Hirano et al.	
		US-2009/0113088	04/30/2009	Illowsky et al.	
		US-2009/0158426	06/18/2009	Yoon et al.	
		US-2010/0034207	02/11/2010	Mcgrew et al.	
		US-2010/0164720	07/01/2010	Kore, Vinayak	
		US-2010/0211795	08/19/2010	Brown et al.	
		US-2011/0026529	02/03/2011	Majumdar et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code – Number – Kind Code	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T
		JP 4 117 548	04/17/1992	Fujitsu Ltd		
		WO 2001/009756	02/08/2001	Safewww, Inc.		
		WO 2008/034900	03/27/2008	Boesgaard Sorensen		
		WO 2008/052310	05/8/2008	PGMX, Inc.		

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date page(s), volume-issue number(s), publisher, city and/or country where published.	T
		Eisen, Ori, "Catching the Fraudulent Man-in-the-Middle and Man-in-the-Browser," Network Security, April 2010, pp. 11-12.	

Examiner Signature	/Ajibola Akinyemi/	Date Considered	08/30/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A./

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO
(modified by Applicant)

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	13/734,178
Filing Date	January 4, 2013
First Named Inventor	Craig S. ETCHEGOYEN
Art Unit	2649
Examiner Name	~~Yuwen Pan~~ /Ajibola Akinyemi/
Attorney Docket Number	UN-NP-SC-085

Sheet 5 of 5

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date page(s), volume-issue number(s), publisher, city and/or country where published.	T
		Housley et al., "Internet x.509 Public Key Infracstructure Certificate and CRL Profile," The Internet Society, Network Working Group, Sept. 1999, 75 pages. [RFC 2459]	
		Wikipedia: "Software Extension," May 28, 2009, Internet Article retrieved on October 11, 2010. XP002604710	
		H. Williams, et al., "Web Database Applications with PHP & MySQL", Chapter 1, "Database Applications and the Web", ISBN 0-596-00041-3, O'Reilly & Associates, Inc., March 2002, avail. at: http://docstore.mik.ua/orelly/webprog/webdb/ch01_01.htm. XP002603488	
		Zhu, Yunpu, "A New Architecture for Secure Two-Party Mobile Payment Transactions," Submitted to the School of Graduate Studies of the University of Lethbridge, Master of Science, 2010, 240 pages.	
		Ylonen et al., "The Secure Shell (SSH) Authentication Protocol," Network Working Group, January 2006, 17 pages. RFC-4252.	
		Nesi, et al., "A Protection Processor for MPEG-21 Players," In Proceedings of ICME, 2006, pp.1357-1360.	

Examiner Signature	/Ajibola Akinyemi/	Date Considered	08/30/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A./

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

PRIORITY DOCUMENT EXCHANGE

FAILURE STATUS REPORT

An attempt by the Office to electronically retrieve, under the Priority Document Exchange programs (PDX and DAS), 2012100462 to which priority is claimed has FAILED on 10/02/2013.

For further questions or assistance, please contact our EBC Customer Support Center at

1-866-217-9197 (toll-free)

571-272-4100 (local)

M-F 6AM - Midnight (Eastern Time)

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

PRIORITY DOCUMENT EXCHANGE

FAILURE STATUS REPORT

An attempt by the Office to electronically retrieve, under the Priority Document Exchange programs (PDX and DAS), 2012100462 to which priority is claimed has FAILED on 10/04/2013.

For further questions or assistance, please contact our EBC Customer Support Center at

1-866-217-9197 (toll-free)

571-272-4100 (local)

M-F 6AM - Midnight (Eastern Time)

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

PRIORITY DOCUMENT EXCHANGE

FAILURE STATUS REPORT

An attempt by the Office to electronically retrieve, under the Priority Document Exchange programs (PDX and DAS), 2012100462 to which priority is claimed has FAILED on 10/08/2013.

For further questions or assistance, please contact our EBC Customer Support Center at

1-866-217-9197 (toll-free)

571-272-4100 (local)

M-F 6AM - Midnight (Eastern Time)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. no.:	13/734,178	Conf. no.	3155
Applicant:	Craig S. ETCHEGOYEN	Art Unit:	2649
Filed:	January 4, 2013	Examiner:	Ajibola A. Akinyemi

Title: NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES

TRANSMITTAL LETTER

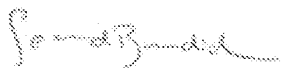
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir,

Pursuant to verbal instructions from the Application Assistance Unit, Applicant hereby files this general transmittal letter and accompanying foreign priority document, AU 2012100462, to cure the priority document retrieval failure as noticed in the patent application's image file wrapper.

Should you have any questions, please feel free to contact the undersigned directly.

Respectfully Submitted,



Sean D. Burdick
Reg. No. 51,513

Uniloc USA, Inc.
7160 N. Dallas Parkway, Ste. 380
Plano, TX 75024
972 905 9580 x227

Electronic Acknowledgement Receipt	
EFS ID:	17285745
Application Number:	13734178
International Application Number:	
Confirmation Number:	3155
Title of Invention:	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES
First Named Inventor/Applicant Name:	Craig S. ETCHEGOYEN
Customer Number:	96051
Filer:	Sean Dylan Burdick
Filer Authorized By:	
Attorney Docket Number:	UN-NP-SC-085
Receipt Date:	31-OCT-2013
Filing Date:	04-JAN-2013
Time Stamp:	19:04:56
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Interim Copy of the Foreign Priority Document	AU_2012100462.pdf	3251218 012474993571616288895a3019e2859631a536bd9	no	29
Warnings:					
Information:					

2	Transmittal Letter	UN-NP-SC-085_Transmittal_Form_re_Priority_Doc_Retrieval.pdf	29095 8d8cfad76499e624d04bee3fe37d9d9c2afb1a82	no	1
Warnings:					
Information:					
			Total Files Size (in bytes):	3280313	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

(12) CERTIFIED INNOVATION PATENT (11) Application No. **AU 2012100462 B4**
(19) AUSTRALIAN PATENT OFFICE

(54) Title
Near field authentication through communication of enclosed content sound waves

(51) International Patent Classification(s)
H04L 9/28 (2006.01) ***H04L 29/06*** (2006.01)

(21) Application No: **2012100462** (22) Date of Filing: **2012.04.24**

(30) Priority Data

(31) Number	(32) Date	(33) Country
61/595,599	**2012.02.06**	**US**

(45) Publication Date: **2012.05.24**
(45) Publication Journal Date: **2012.05.24**
(45) Granted Journal Date: **2012.05.24**
(45) Certified Journal Date: **2012.11.08**

(71) Applicant(s)
Uniloc USA, Inc.

(72) Inventor(s)
Etchegoyen, Craig S.;Harjanto, Dono;Burdick, Sean D.

(74) Agent / Attorney
Madderns Patent & Trade Mark Attorneys, GPO Box 2752, Adelaide, SA, 5001

(56) Related Art
US 2010/0281261 A1

20121004624 24 Apr 2012

ABSTRACT

A method for near field authentication of sources using an audio transceiver computing device includes scanning a plurality of predetermined frequencies for a free frequency, selecting the free frequency from the plurality of predetermined frequencies, generating a periodic enclosed content message, generating a modulated carrier wave representing the periodic enclosed content message, and transmitting the modulated carrier wave at the free frequency. A method for near field authentication of sources using a microphone input of a receiving computing device includes scanning a plurality of predetermined frequencies to detect a signal using the microphone input, verifying, responsive to detecting the signal, that the signal includes at least one enclosed content message, and extracting a content from the enclosed content message.

2012100462 24 Apr 2012

Regulation 3.2

AUSTRALIA
PATENTS ACT 1990

COMPLETE SPECIFICATION

FOR AN INNOVATION PATENT

ORIGINAL

Name of Applicant:	Uniloc USA, Inc.
Actual Inventors:	Craig S Etchegoyen Dono Harjanto Sean D Burdick
Address for Service:	C/- MADDERNS, GPO Box 2752, Adelaide, South Australia, Australia

Invention title: NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES

The following statement is a full description of this invention, including the best method of performing it known to us.

20121100462 24 Apr 2012

NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES

BACKGROUND

1. Field of the Invention

[0001] The present invention relates generally to technology for near field authentication of users and their computing devices. More specifically, the invention relates to effecting near field authentication for digital communications by means of encoded sound waves.

2. Description of the Related Art

[0002] The use of a user's electronic device to complete a purchase has been suggested, for example, utilizing Bluetooth technology or a WiFi Internet connection to transmit the data to the register. However, such technology requires a transactional device such as a register or ATM machine to be upgraded and retrofitted with expensive equipment and software to securely receive the data and authenticate the user's electronic device. Thus, while it may be desirable for the user, it could be prohibitively expensive for the commercial entity utilizing the transactional device, especially for small businesses.

[0003] The use of other technology aside from the Internet or the Bluetooth may also require not only that the transactional device be upgraded and retrofitted, but also that the user's electronic device be similarly modified. In addition, alternative technology may also have range limitations which can degrade the user's experience when performing a transaction. For example, in a conventional near field communication, radio communication is utilized to facilitate transactions. However, the conventional near field communication requires that the two transacting devices be in extremely close proximity to each other, i.e., within about 4 centimeters from each other to ensure reliable communication. This requirement for close proximity places a very restrictive limitation on practical applications for near field transactions in the real world. If one of the transacting devices is a cash register, and the other transacting device is a customer's mobile phone, the customer would need to extend the phone to within centimeters of the register and risk dropping the phone. The proximity limitation may also prevent the user from making further use of the phone while the transaction is taking place and while the phone is extended away from the customer. For example, should complications in the transaction arise, or if the user is required to provide a manual input, the customer may not be able to complete the transaction.

[0004] Another drawback of the conventional near field communication is the lack of security, despite the close proximity of the two devices. That is, the conventional near field communication offers no

20121100462 03 Jul 2012

protection against eavesdropping and can be vulnerable to data modifications. Needless to say, this is undesirable for financial transactions and other confidential communications.

[0005] Thus, there is a need for improved technology for effecting near field communications.

SUMMARY

[0006] The present invention provides a method for source authentication in network communications. A source such as a mobile computing device transmits an authentication request by executing the following salient steps using an audio transceiver: scanning a plurality of predetermined frequencies for a free frequency, selecting the free frequency from the plurality of predetermined frequencies, generating a periodic enclosed content message, encoding a carrier wave with the periodic enclosed content message, and transmitting the modulated carrier wave at the free frequency. The audio transceiver, in one example, may be a mobile phone having both a speaker and a microphone.

[0007] The periodic enclosed content message includes an enclosed content message at each period. The enclosed content message comprises a beginning indication, a content, and an ending indication. The beginning indication indicates when the enclosed content message begins, while the ending indication indicates when the enclosed content ends. This allows for verification that the enclosed content message is completely instead of partially received. Furthermore, the content includes biometric data or device identification data, or both, which can be used to authenticate the user or the mobile computing device. Furthermore, the content may also include financial information for the user, or other data which might be used for gaining access to a secure network for facilitating a transaction once the user or the mobile computing device, or both, have been authenticated.

[0008] In another form, the method further comprises displaying a user interface on the audio transceiver computing device requesting the biometric data from a user; and

responsive to receiving the biometric data, generating the periodic enclosed content message, wherein the content in each period of the periodic enclosed content message includes the biometric data.

[0009] In another form, the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

[0010] In another form, the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.

[0011] In another form, the modulated carrier wave comprises a sound wave.

Paragraphs [0012] and [0013] have been intentionally deleted.

20121100462 03 Jul 2012

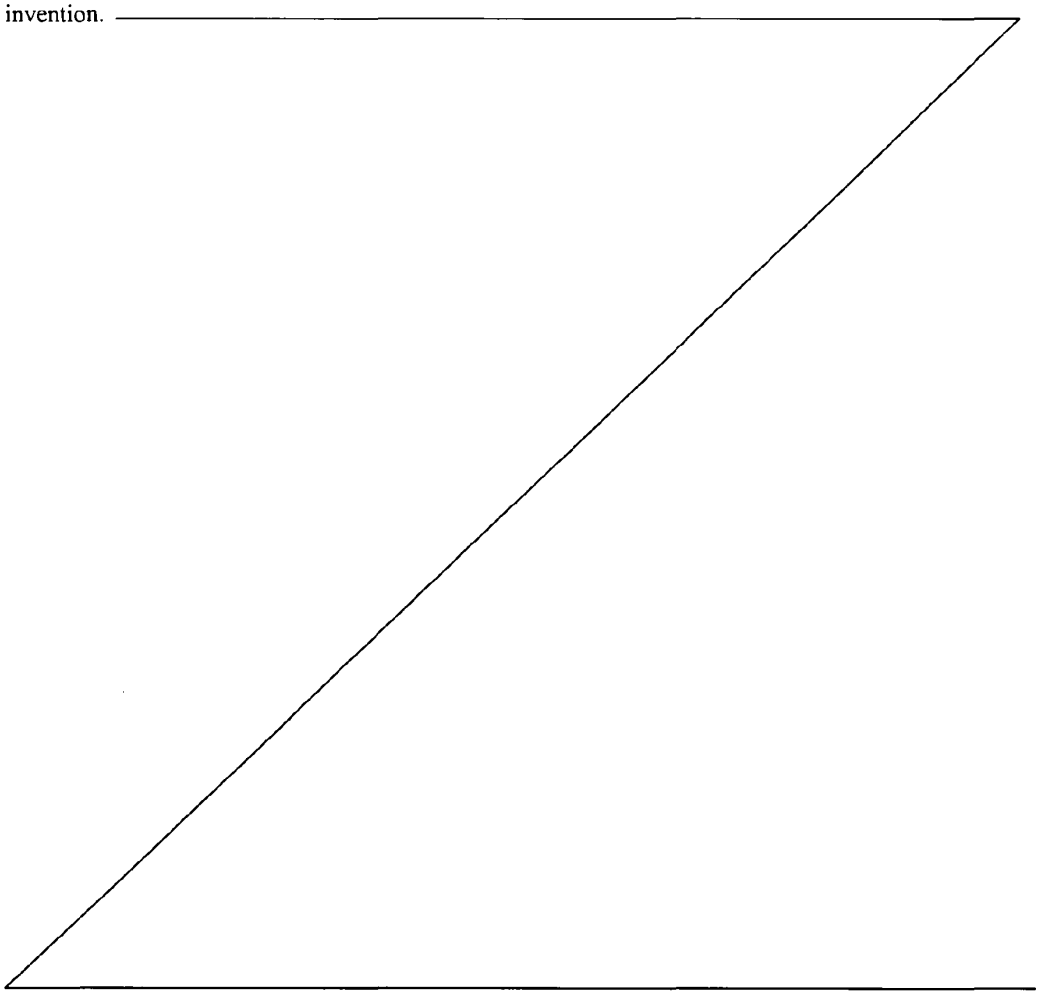
BRIEF DESCRIPTION OF THE DRAWINGS

[0014] Other systems, methods, features and advantages of the invention will be or will become apparent to one with skill in the art upon examination of the following figures and detailed description. It is intended that all such additional systems, methods, features and advantages be included within this description, be within the scope of the invention, and be protected by the accompanying claims. Component parts shown in the drawings are not necessarily to scale, and may be exaggerated to better illustrate the important features of the invention. In the drawings, like reference numerals may designate like parts throughout the different views, wherein:

[0015] FIG. 1 is a block diagram showing an audio transceiving computing device transmitting data to an audio receiving computing device in accordance with one embodiment of the present invention.

[0016] FIG. 2 is a block diagram showing functional components that make up an audio transceiving computing device according to an embodiment of the present invention.

[0017] FIG. 3 depicts a periodic enclosed content message according to an embodiment of the present invention.



20121100462 24 Apr 2012

[0018] FIG. 4 is a block diagram depicting message content in an enclosed content message according to an embodiment of the present invention.

[0019] FIG. 5 is a block diagram showing functional components of an audio receiving computing device according to an embodiment of the present invention.

[0020] FIG. 6 is a process flow diagram showing steps for an audio transceiving computing device to request authentication from an audio receiving computing device according to an embodiment of the present invention.

[0021] FIG. 7 depicts additional process steps for inputting content for an enclosed content message into an audio transceiving computing device in advance of requesting authentication according to an embodiment of the present invention.

[0022] FIG. 8 is a process flow diagram showing steps for receiving an audio transmission of enclosed content data using a microphone input of a receiving computing device according to an embodiment of the present invention.

[0023] FIG. 9 depicts additional process steps for authenticating an audio transceiving device according to an embodiment of the present invention.

DETAILED DESCRIPTION

[0024] The present invention relates to a method and system for near field authentication of users and computing devices using sound waves. Such users and computing devices may be referred to collectively herein as "sources". Authenticating a source according to the present invention may involve authenticating only a user, only a computing device, or both a user and a computing device.

[0025] As seen in FIG. 1, a system 100 for authenticating sources using sounds waves can include, for example, an audio transceiving computing device 102, and an audio receiving computing device 104. The audio transceiving computing device 102 can transmit data to the audio receiving computing device 104 as a modulated carrier wave 106. The modulated carrier wave 106 can be, for example, a sound wave. Sound waves can transmit information accurately over a very short distance (near field communications) using inexpensive equipment. In different embodiments, the sound wave can have a frequency that is substantially below, within, or above the audible frequencies, such as below 20 Hz, between 20 Hz and 20 kHz, or above 20 kHz. For example, the sound wave could be an ultrasonic wave.

[0026] The audio transceiver computing device 102 can be, for example, a mobile phone, a personal digital assistant, a tablet, a laptop, a music player, or any other device having a processor operatively coupled to memory and capable of transmitting the modulated carrier wave 106 responsive to operation of the processor. As seen in FIG. 2, the audio transceiver computing device 102 can include, for example

20121100462 24 Apr 2012

one or more microprocessors, which are collectively shown as CPU 202. The audio transceiver computing device 102 also includes, for example, a memory 204, an interconnect 206, an input 208, an output 210, and/or a network access circuitry 212. The CPU 202 can retrieve data and/or instructions from the memory 204 and execute the retrieved instructions. The memory 204 can include generally any computer-readable medium including, for example, persistent memory such as magnetic and/or optical disks, ROM, and PROM and volatile memory such as RAM.

[0027] The CPU 202 and the memory 204 are connected to one another through the interconnect 206, which is a bus in this illustrative embodiment. The interconnect 206 connects the CPU 202 and the memory 204 to the input devices 208, the output devices 210, and the network access circuitry 212. The input devices 208 can include, for example, a keyboard, a keypad, a touch-sensitive screen, a mouse, a microphone, and/or one or more cameras. The output devices 210 can include, for example, a display – such as a liquid crystal display (LCD) – and/or one or more speakers. The network access circuitry 212 sends and receives data through computer networks such an intranet or the Internet.

[0028] A number of components of the audio transceiver computing device 102 are stored in the memory 204. In particular, a near field authentication transceiver logic 214 is part of one or more computer processes executed within the CPU 202 from the memory 204 in this illustrative embodiment, but can also be implemented using digital logic circuitry. As used herein, "logic" refers to (i) logic implemented as computer instructions and/or data within one or more computer processes and/or (ii) logic implemented in electronic circuitry.

[0029] In an embodiment, the near field authentication transceiver logic 214 is executable software stored within the memory 204. For example, when the audio transmitting computing device 102 receives a request from the user to transmit the modulated carrier wave 106, the audio transceiver computing device 102 executes the near field authentication transceiver logic 214 to transmit the modulated carrier wave 106 to the audio receiving computing device 104. As previously noted the modulate carrier wave 106 can be an analog signal, such as a sound signal. Advantageously, an analog signal has an infinite amount of signal resolution. Furthermore, the use of sound signals increases the permissible transmission distance. That is, the theoretical and practical working distance for completing a transaction using the present invention is increased and can be measured, for example, in feet or meters instead of centimeters. This allows the user to utilize the audio transceiver computing device 102 for additional functions simultaneously while completing a transaction. It also reduces a likelihood that the user will be prone to dropping or otherwise damaging the audio transceiver computing device 102 by moving the audio transceiver computing device 102 into very close proximity with the audio receiving computing device 104.

[0030] When the near field authentication transceiver logic 214 is executed, the audio transceiver computing device 102 scans a plurality of predetermined frequencies for a free frequency. The predetermined frequencies can be, for example, frequencies for which the audio transceiver computing device 102 is authorized to transmit the modulated carrier wave or which are known to the audio receiving computing device 104. In an embodiment, the predetermined frequencies can be selected to be outside the audible frequencies. From the predetermined frequencies, the near field authentication transceiver logic 214 can select a free frequency. The free frequency can be, for example, a frequency which has a noise level below a predetermined noise level threshold or a frequency that has an interference level below a predetermined interference level threshold.

[0031] The near field authentication transceiver logic 214 can also generate a periodic enclosed content message 216 as shown in FIG. 2. To generate the periodic enclosed content message 216, the near field authentication transceiver logic 214 can utilize a device ID generation logic 218 or a biometric data input logic 220, or both. The device ID generation logic 218 can generate, for example, device identification data of the audio transceiver computing device 102. In an embodiment, the device ID generation logic 218 can utilize known techniques for generating a device fingerprint. The biometric data input logic 220 can display, for example, a user interface for requesting and receiving a voice or image input representing biometric data. The device identification data or the biometric data, or both, can be included in a content of the periodic enclosed content message 216, which will be described later.

[0032] The near field authentication transceiver logic 214 can also generate a modulated carrier wave 106 representing the periodic enclosed content message. The modulated carrier wave 106 can be transmitted at the free frequency to the audio receiving computing device 104. Preferably, the periodic enclosed content message is generated initially in digital format, and is then converted into an analog signal and used to modulate the carrier wave. In an embodiment, the digital form of the periodic enclosed content message 216 can be encrypted using standard RSA (PKI) keys. Key exchanges may occur out-of-band, such as during registration of the audio transceiver computing device 102, or may be built-in to the near field authentication transceiver logic 214.

[0033] As can be seen in FIG. 3, the periodic enclosed content message 216 includes, for example, multiple periods with each period including an enclosed content message 302. Thus, the periodic enclosed content message 216 includes a plurality of enclosed content messages 302 such as enclosed content messages 302a – 302n for a total of N enclosed content messages. Each of the enclosed content messages includes a begin indication 304, a content 306, and an end indication 308. The begin indication 304 can be any type of signal that uniquely indicates the beginning of the enclosed content message, for example, a specified sequence of binary bits. Similarly, the end indication 308 can be any type of signal that indicates the ending of the enclosed content message. In one embodiment, the begin indication 304

2012100462 24 Apr 2012

and the end indication 308 comprise different signals. In another embodiment, the begin indication 304 and the end indication 308 comprise identical signals, i.e. two of the same signals in sequence. In another embodiment, an end indication 308(n-1) and the next begin indication 304(n) may be one and the same signal.

[0034] Referring to FIG. 4, the content 306 can include, for example, biometric data 402 or a device identification data 404 or a combination of both. The biometric data 402 can include, for example, the data corresponding to a voice of a user, a fingerprint of the user, an image of the user, or any other physiological data of the user which can be used to verify an identity of the user. The device identification data 404 can include, for example, a MAC address of the audio transceiver computing device 102, a hard disk serial number of the audio transceiver computing device 102, a device ID number of the audio transceiver computing device 102, a device phone number of the audio transceiver computing device 102, a device fingerprint of the audio transceiver computing device 102, or any other information which could be used to identify and verify the authenticity of the audio transceiver computing device 102.

[0035] A device fingerprint comprises binary data that identifies the audio transceiver computing device 102 by deriving a unique data string from multiple portions of indicia stored in memory locations within the device, where such indicia can include, for example, data representing a manufacture name, a model name, or a device type. Device fingerprints and generation thereof are known and are described, e.g., in U.S. Patent 5,490,216 (sometimes referred to herein as the '216 Patent), and in related U.S. Patent Application Publications 2007/0143073, 2007/0126550, 2011/0093920, and 2011/0093701 (the "related applications"), the descriptions of which are fully incorporated herein by reference.

[0036] In general, the device fingerprint comprises a bit string or bit array that includes or is derived from user-configurable and non-user-configurable data specific to the audio transceiver computing device 102. Non-user-configurable data includes data such as hardware component model numbers, serial numbers, and version numbers, and hardware component parameters such as processor speed, voltage, current, signaling, and clock specifications. User-configurable data includes data such as registry entries, application usage data, file list information, and MAC address. In an embodiment, the audio transceiver computing device 102 can also include, for example, manufacture name, model name, and/or device type of the audio transceiver computing device 102.

[0037] Generation of the device fingerprint includes a combination of operations on the data specific to the audio transceiver computing device 102, which may include processing using a combination of sampling, concatenating, appending (for example, with a nonce value or a random number), obfuscating, hashing, encryption, and/or randomization algorithms to achieve a desired degree of uniqueness. For example, the desired degree of uniqueness may be set to a practical level such as 99.999999% or higher, to achieve a probability of less than 1 in 100,000,000 that any two of the audio transceiver computing

2012100462 24 Apr 2012

devices will generate identical fingerprints. In an embodiment, the desired degree of uniqueness may be such that the device fingerprint generated is unlike any other device fingerprint generatable responsive to a request to transmit the modulated carrier wave 106 to the audio receiving computing device 104.

[0038] In one embodiment, the device fingerprint may be stored in volatile memory and erased after transmission of the modulated carrier wave 106 to the audio receiving computing device 104. In another embodiment, the device fingerprint may be stored in persistent memory and written over each time a new fingerprint is generated by the device ID generation logic 218.

[0039] Referring back to FIG. 3, the amount of time it takes to transmit the modulated carrier wave 106 representing the periodic enclosed content message, T_{PECM}, can be a sum of the time it takes to transmit a modulated carrier wave representing each of the enclosed content messages 302 in the periodic enclosed content message 216. For example, the time it takes to transmit each of the modulated carrier waves representing an enclosed content message 302 can be T_{ECM}. Thus, the amount of time it takes to transmit the modulated carrier wave 106 T_{PECM} can be, for example, represented by the equation $T_{PECM} = N \times T_{ECM}$ where N represents the total number of enclosed content messages 302 in the periodic enclosed content message 216.

[0040] The total number N of enclosed content messages 302 in the periodic enclosed content messages 216 can be a function of the total number of frequencies in the plurality of predetermined frequencies. That is, the total number N of enclosed content messages 302 should be sufficient such that the audio receiving computing device 104 can scan through the predetermined frequencies to determine the free frequency on which the modulated carrier wave 106 is transmitted, and have time enough to receive at least one of the enclosed content messages 302. This will be discussed in more detail below. In an embodiment, the near field authentication transceiver logic 214 can transmit the modulated carrier wave 106 for a predetermined number of periods, or a predetermined period of time. In another embodiment, the near field authentication transceiver logic 214 can transmit the modulated carrier wave 106 until a stop indication is received from the user. Such indication can come, for example, from the input 208 in the form of a button depression, a tap on a screen, a vocal indication, or any other type of indication from the user to stop transmission of the modulated carrier wave 106.

[0041] In an embodiment, the near field authentication transceiver logic 214 using the biometric data input logic 220 can display a user interface on the output 210 when the output 210 is, for example, a display screen. The user interface can request the biometric data 402 from the user. For example, the user interface can prompt the user for voice input to be newly received by the biometric data input logic 220 and subsequently the near field authentication transceiver logic 214 through a microphone input on the audio transceiver computing device 102. A characteristic voice print in digital form may be derived from the voice input using technology known in the art. In another example, the user interface can

prompt the user for photographic input, such as the user's face or biometric fingerprint using a camera or scanning device on the audio transceiving computing device 102. A digital representation of the facial image or biometric fingerprint may be derived using technology known in the art. Responsive to receiving the biometric data 402, the near field authentication transceiver logic 214 can generate the periodic enclosed content message 216, wherein the content 306 in each period of the periodic enclosed content message 216 includes the biometric data (or a derivation thereof) 402.

[0042] Referring to FIGS. 1 and 5, the audio receiving computing device 104 can be, for example, a register, an ATM machine, a kiosk, a mobile phone, a personal digital assistant, a tablet, a laptop, a music player, or any other device capable of receiving the modulated carrier wave 106. As seen in FIG. 5, the audio receiving computing device 104 can include, for example one or more microprocessors, which are collectively shown as CPU 502. The audio receiving computing device 104 also includes, for example, a memory 504, an interconnect 506, an input 508, an output 510, and/or a network access circuitry 512. The CPU 502 can retrieve data or instructions from the memory 504 and execute the retrieved instructions. The memory 504 can include generally any computer-readable medium including, for example, persistent memory such as magnetic or optical disks, ROM, and PROM and volatile memory such as RAM.

[0043] The CPU 502 and the memory 504 are connected to one another through an interconnect 506, which is a bus in this illustrative embodiment. The interconnect 506 connects the CPU 502 and the memory 504 to the input devices 508, the output devices 510, and the network access circuitry 512. The input devices 508 can include, for example, a keyboard, a keypad, a touch-sensitive screen, a mouse, a microphone, and/or one or more cameras. The output devices 510 can include, for example, a display – such as a liquid crystal display (LCD) – or one or more loudspeakers. The network access circuitry 512 sends and receives data through computer networks such an intranet or the Internet.

[0044] A number of components of the audio receiving computing device 104 are stored in the memory 504. In particular, a near field authentication receiver logic 514 is part of one or more computer processes executed within CPU 502 from memory 504 in this illustrative embodiment, but can also be implemented using digital logic circuitry.

[0045] In an embodiment, the near field authentication receiver logic 514 is executable software stored within the memory 504. For example, the near field authentication receiver logic 514 can receive signals such as the modulated carrier wave 106 to verify the authenticity of the audio transceiver computing device 102.

[0046] When the near field authentication receiver logic 514 is executed, it scans a plurality of predetermined frequencies to detect a signal using the microphone disclosed as the input 508. In an embodiment, the signal is a sound wave. In another embodiment, the microphone may be a specialized

2012100462 24 Apr 2012

band-pass microphone that is mechanically configured or otherwise designed to receive frequencies within the range of the predetermined frequencies. Such a microphone may be tuned, for example, to receive only ultrasonic frequencies of interest, and attenuate all frequencies outside the desired range. Such a microphone may be designed to plug in to the audio receiving computing device 104 through a standard audio input such as TRS or USB.

[0047] In an embodiment, the near field authentication receiver logic 514 scans each of the frequencies in the predetermined frequencies for a predetermined scanning period of time. The predetermined scanning period of time at each frequency, T_{SCAN}, is equal to at least twice the time T_{ECM}, which is the time it takes to transmit each period of the modulated carrier wave representing the enclosed content message 302. This ensures that the near field authentication receiver logic 514 has the opportunity to receive the complete enclosed content message instead of a partial enclosed content message.

[0048] That is, the enclosed content message 302 should include the begin indication 304, the content 306, and the end indication 308. In some embodiments, however, only the begin indication 304 and the end indication 308 need be detected by the near field authentication receiver logic 514 in order for the near field authentication receiver logic 514 to consider the enclosed content message 302 to be a complete enclosed content message. Otherwise, if the enclosed content message 302 is missing, for example, the begin indication 304 or the end indication 308, it is not considered a complete enclosed content message, and instead is considered a partial enclosed content message.

[0049] However, the predetermined scanning period of time T_{SCAN} may also include an additional period of time K_{ECM} to compensate for any delays or lag. Thus, the predetermined scanning period of time at each frequency may be represented as $T_{SCAN} = 2 \times T_{ECM} + K_{ECM}$. If there are F predetermined frequencies, then the minimum amount of time spent scanning the predetermined frequencies, $T_{MIN\ TOTAL\ SCAN}$, will be represented by the equation $T_{MIN\ TOTAL\ SCAN} = F \times (T_{SCAN})$.

[0050] Since the near field authentication receiver logic 514 will spend at least a $T_{MIN\ TOTAL\ SCAN}$ time period scanning the predetermined frequencies, the near field authentication transceiver logic 214 should transmit the modulated carrier wave for at least a $T_{MIN\ TOTAL\ SCAN}$ time period. Thus, the amount of time it takes to transmit the modulated carrier wave 106 representing the periodic enclosed content message, T_{PECM}, should be equal to or greater than the $T_{MIN\ TOTAL\ SCAN}$ time period. However, $T_{PECM} = N \times T_{ECM}$. Therefore, $T_{MIN\ TOTAL\ SCAN} = N \times T_{ECM}$. Thus, the total number of enclosed content messages 302 in the periodic enclosed content message 216 (N) is represented by the equation $N = T_{MIN\ TOTAL\ SCAN} / T_{ECM}$. Substituting for $T_{MIN\ TOTAL\ SCAN}$ yields $N = F \times (T_{SCAN}) / T_{ECM}$. We can also replace T_{SCAN} such that we get $N = [F \times (2 \times T_{ECM} + K_{ECM})] / T_{ECM}$ or more succinctly, $N = 2 \times F + (F \times K_{ECM}) / T_{ECM}$.

[0051] Thus, at a minimum the number of enclosed content messages (N) should be equal to twice the number of frequencies in the frequency period (F) plus some additional number of enclosed content

messages with a minimum number of (F x K_{ECM} / T_{ECM}). For convenience, K_{ECM} may be expressed in integral multiples of T_{ECM}, so that N results in an integer value. The additional number of enclosed content messages (F x K_{ECM} / T_{ECM}) can be selected to be sufficiently large to allow for any latency in execution of the near field authentication receiver logic 514, or switching between frequencies by the near field authentication receiver logic 514.

[0052] Referring back to FIG. 5, responsive to detecting the signal, the near field authentication receiver logic 514 can verify that the signal includes at least one enclosed content message. The enclosed content message should be a complete enclosed content message, instead of a partial enclosed content message. Partial enclosed content messages are discarded. In one embodiment, the near field authentication receiver logic 514 can stop scanning the predetermined frequencies once a signal is detected, or when the signal is verified to include at least one enclosed content message.

[0053] In an embodiment, the near field authentication receiver logic 514 can extract a content from the enclosed content message. Such extraction can occur through demodulation, A/D conversion, decryption, decoding, deciphering, descrambling, or any other methods needed to recover the original content so that it is recognizable and useable by the near field authentication receiver logic 514. Furthermore, when keys are used for decryption of the content, standard RSA (PKI) keys can be used. Key exchanges may occur out-of-band, such as during registration of the audio receiving computing device 104, or built-in to the near field authentication receiver logic 514.

[0054] In an embodiment, the near field authentication receiver logic 514 can also compare the extracted content to an authorized content 516. The authorized content 516 can include, for example, authenticated biometric data or authenticated device identification data, or both. The authenticated biometric data and authenticated device identification data can be, respectively, biometric data and device identification data that the user of the transceiver computing device 102 has registered beforehand as being authentic.

[0055] The near field authentication receiver logic 514 can determine if there is a match between the extracted content and the authorized content 516 to authenticate the audio transceiver computing device 102. In FIG. 5, the authorized content 516 is stored in the memory 504. However, the authorized content 516 could also be kept in other storage devices which have a database or memory accessible by the audio receiving computing device 104. In one embodiment, the near field authentication receiver logic 514 can stop scanning the predetermined frequencies when the audio transceiver computing device 102 has been authenticated.

[0056] In an embodiment, when the audio transceiver computing device 102 is authenticated, the near field authentication receiver logic 514 can, for example, perform a financial transaction based on the content. In such a case, the content can include, for example, financial data such as a credit card number,

2012100462 24 Apr 2012

a bank account number, or other data needed to complete a financial transaction. Of course additional functions could also be performed by the near field authentication receiver logic 514 once the audio transceiver computing device 102 is authenticated, such as ticket verification, entry into a restricted area, or any other type of function which would require authentication of the audio transceiver computing device 102, its user, or both.

[0057] Once the near field authentication receiver logic 514 authenticates the audio transceiver computing device 102, the near field authentication receiver logic 514 can display or provide a an acknowledgement indication that the authentication has occurred. The acknowledgement indication may be provided locally by the device 104, for example, in the form of a visual indication or an audible tone. Alternatively or in combination, the acknowledgement indication may also be provided to the user of the device 102 by means of a locally generated audible tone, locally generated visual indication (such as an LED illuminating or changing color), or by sending a remote indication to the device 102 via a network link or by means of a sound wave using a free frequency according to the same methods disclosed herein for generating and transmitting the enclosed content message. The user of device 102, responsive to receiving the indication, may then stop transmission of the modulated carrier wave 106 by manual or automatic action. However, if the near field authentication receiver logic 514 fails to authenticate the audio transceiver computing device 102, such as if the content does not match the authorized content 516, or if no content was discovered, then the near field authentication receiver logic 514 can display or provide some sort of indication to indicate that an authentication failure has occurred. Furthermore, a log could be stored indicating the time, location, and/or the content if available. This can help with any troubleshooting requests, and/or any investigations of fraud.

[0058] In one implementation of an acknowledgment indication, the device 104 may scan for a free frequency from among the plurality of predetermined frequencies until one is found, or it may transmit acknowledgements on a special predetermined frequency that is reserved only for transmitting such acknowledgements. In an acknowledgement message so transmitted, device 104 may include acknowledgement content in the form of a special binary code that is recognized by transceiver logic 214 within device 102 as an acknowledgement signal, and it may also include a device identifier of either or both of devices 102 and 104. In such case, device 104 may also include its own device identifier (not shown) stored in local memory 504 and recognizable by transceiver logic 214.

[0059] In an embodiment, a transaction flow diagram 600 as shown in FIG. 6 illustrates a near field authentication of sources to an audio receiving computing device 104 using an audio transceiver computing device 102. To facilitate appreciation and understanding of the invention, transaction flow diagram 600 is described in the context of an illustrative example of a user seeking to purchase a product

2012100462 24 Apr 2012

at a register using his mobile phone. Of course the near field authentication of sources could occur for other transactions.

[0060] In step 602, the audio transceiver computing device 102 scans a plurality of predetermined frequencies for a free frequency. For example, the mobile phone through its microphone can scan a plurality of predetermined frequencies for a free frequency.

[0061] In step 604, the audio transceiver computing device 102 selects the free frequency from the plurality of predetermined frequencies. For example, the mobile phone can identify the first free frequency it scans that has no discernable signal, or that has no signal strength that satisfies a minimum amplitude threshold, or that otherwise meets a pre-established criteria for being a free frequency.

[0062] In step 606, the audio transceiver computing device 102 generates a periodic enclosed content message. For example, the mobile phone can generate the periodic enclosed content message by representing one or more of user biometric data, device identification data, and the user's credit card information in binary form.

[0063] In step 608, the audio transceiver computing device 102 generates a modulated carrier wave representing the periodic enclosed content message. For example, the mobile phone can generate a carrier wave and modulate the carrier wave using the periodic enclosed content message. Amplitude, frequency, or phase modulation may be used.

[0064] In step 610, the audio transceiver computing device 102 transmits the modulated carrier wave at the free frequency. For example, the mobile phone can transmit the modulated carrier wave at the free frequency through its output speaker in a directional or omnidirectional broadcast.

[0065] Thus, the user need not use a credit card to purchase the product. Instead, the user can use a device such as a mobile phone that can store credit card information. Furthermore, the mobile phone need not have its physical components modified with expensive equipment, but can use the speaker already included in the mobile phone. Thus, the user can complete the transaction using sound waves. In addition, the mobile phone need not be adjacent the register. Therefore, the user does not need to extend his arm to place the mobile phone adjacent the register, but instead can safely hold the mobile phone in a more comfortable and secure position. Furthermore, the user can also simultaneously perform other actions on the phone while the transaction is occurring, which would not be possible if the user had to extend his arm to place the phone adjacent the register. Should any issues arise in the transaction, the user can more easily troubleshoot the issue because the user is able to manipulate the mobile phone.

[0066] In an embodiment, a transaction flow diagram 700 as shown in FIG. 7 illustrates additional steps to the transactional flow diagram 600 (FIG. 6), in which there is a near field authentication of sources associated with an audio transceiver computing device 102 by an audio receiving computing device 104.

2012100462 24 Apr 2012

[0067] In step 702, a user interface is displayed on the audio transceiver computing device 102 requesting biometric data from the user. For example, a user interface can be displayed on a screen of the mobile phone. The user interface can request the biometric data such as a voice recording of the user, to be received by means of biometric data input logic operating within the mobile phone when the user speaks a requested word or phrase into a microphone on the mobile phone.

[0068] In step 704, responsive to receiving the biometric data, the audio transceiver computing device 102 generates the periodic enclosed content message, wherein the content in each period of the periodic enclosed content message includes the biometric data. For example, responsive to receiving voice data corresponding to a voice of the user, near field authentication transceiver logic operating within the mobile phone generates the periodic enclosed content message, wherein the content in each period of the periodic enclosed content message includes a digital representation of the voice data corresponding to the voice of the user.

[0069] In an embodiment, a transaction flow diagram 800 as shown in FIG. 8 illustrates a near field authentication of sources using a microphone input of an audio receiving computing device 104. To facilitate appreciation and understanding of the invention, transaction flow diagram 800 is described in the context of an illustrative example of a seller seeking to sell a product at a register to a user transmitting financial data using his mobile phone. Of course the near field authentication of sources could occur for other transactions.

[0070] In step 802, the audio receiving computing device 104 scans a plurality of predetermined frequencies using a microphone input to detect a signal. For example, the register scans a plurality of predetermined frequencies to detect a signal using a microphone input of the register. The predetermined frequencies can be, for example, a set of known frequencies in which the mobile phone will be transmitting the periodic enclosed content message. Also, step 802 may commence automatically responsive to the audio receiving computing device 104 being powered on. Scanning may occur continuously, that is, the audio receiving computing device may scan all predetermined frequencies in some sequence, such that each frequency is scanned for a period T_{SCAN}, and that each pass across all scanned frequencies F requires a scanning period of F x (T_{SCAN}). When all frequencies are scanned, the scanning may be repeated, and scanning in this manner may repeat indefinitely, to allow audio receiving computing device 104 to listen continuously for enclosed content messages.

[0071] In step 804, responsive to detecting the signal, the audio receiving computing device 104 verifies that the signal includes at least one enclosed content message. For example, responsive to detecting the signal, a near field authentication receiver logic in the register checks to ensure that there is a beginning indication and an ending indication in the signal to verify that the signal includes at least one

20121100462 24 Apr 2012

enclosed content message. Any signal which does not include both the begin indication and the end indication will be discarded.

[0072] In step 806, the audio receiving computing device 104 extracts a content from the enclosed content message. For example, the near field authentication receiver logic in the register extracts the content from the enclosed content message. The content can include, for example, biometric data of the user, device identification data of the mobile phone, and the user's financial account information. Thus, the content can include the user's voice data, the device fingerprint of the mobile phone, and the user's credit card number.

[0073] In an embodiment, a transaction flow diagram 900 as shown in FIG. 9 illustrates additional steps to the transactional flow diagram 800 (FIG. 8), to enhance near field authentication of sources using a microphone input of an audio receiving computing device 104.

[0074] In step 902, the audio receiving computing device 104 compares the extracted content to authorized content to authenticate a transceiver computing device 102 that transmitted the enclosed content message. For example, the near field authentication receiver logic in the register compares the extracted content to authorized content to authenticate the mobile phone that transmitted the enclosed content message. For example, the register can compare the user's voice data and the device fingerprint of the mobile phone to authenticated versions of the user's voice data and the device fingerprint of the mobile phone to authenticate the user or the mobile phone, or both.

[0075] In step 904, the audio receiving computing device 104 performs a financial transaction based on the enclosed content message when the transceiver computing device 102 is authenticated. For example, the register debits the user's financial account based on the enclosed content message when the user or the mobile phone, or both, are authenticated. Thus, the register can debit the user's financial account using the credit card number when the user or the mobile phone, or both, are authenticated.

[0076] Thus, to perform a transaction, the register need not be modified with expensive equipment. Instead, a relatively inexpensive microphone can be added to allow the register to perform the transaction using sound waves.

[0077] In an embodiment, the near field authentication of sources using audio waves can be used in conjunction with a more conventional online transaction to provide enhanced security for transactions, such as payments and electronic or personal access to confidential files or secure locations. In other words, near field authentication according to the invention may provide an additional layer of security during a more complex authentication procedure. For example, a transaction may be initiated by a user of a mobile device using an on-line log-in procedure in a first phase of authentication. If the first phase of authentication procedure is successful, the authenticating authority may require a second phase of authentication using a near-field authentication technique described herein to complete the procedure.

2012100462 03 Jul 2012

[0078] In another example, where secure information is large or requires additional security, it may be stored at a remote location from the audio transceiver computing device. Once multiples layers of authentication have occurred for the user or the audio transceiver computing device, or both, the audio receiver computing device can directly access, indirectly access, or receive the secure information from the remote location. Of course, such examples are only exemplary and are non-limiting as the quantity, manner, and amount of information stored remotely from the audio transceiver computing device can be varied as desired. This can also vary how the near field authentication of sources using audio waves can be used in conjunction with the conventional online transaction.

[0079] Exemplary embodiments of the invention have been disclosed in an illustrative style. Accordingly, the terminology employed throughout should be read in an exemplary rather than a limiting manner. Although minor modifications to the teachings herein will occur to those well versed in the art, it shall be understood that what is intended to be circumscribed within the scope of the patent warranted hereon are all such embodiments that reasonably fall within the scope of the advancement to the art hereby contributed, and that that scope shall not be restricted, except in light of the appended claims and their equivalents.

[0080] The reference to any prior art in this specification is not, and should not be taken as, an acknowledgement of any form of suggestion that such prior art forms part of the common general knowledge.

[0081] It will be understood that the term "comprise" and any of its derivatives (eg. comprises, comprising) as used in this specification is to be taken to be inclusive of features to which it refers, and is not meant to exclude the presence of any additional features unless otherwise stated or implied.

2012100462 18 Sep 2012

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

1. A method for near field authentication of a source, the source using an audio transceiver computing device comprising:

scanning a plurality of predetermined frequencies for a free frequency;

selecting the free frequency from the plurality of predetermined frequencies;

generating a periodic enclosed content message;

generating a modulated carrier wave representing the periodic enclosed content message; and

transmitting the modulated carrier wave at the free frequency;

wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication; and

wherein the content includes at least one of biometric data, or device identification data.

2. The method of claim 1 further comprising:

displaying a user interface on the audio transceiver computing device requesting the biometric data from a user; and

responsive to receiving the biometric data, generating the periodic enclosed content message, wherein the content in each period of the periodic enclosed content message includes the biometric data.

3. The method of claim 1 or 2, wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

4. The method of claim 1 or 2, wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.

5. The method of any one of claims 1 to 4 wherein the modulated carrier wave comprises a sound wave.

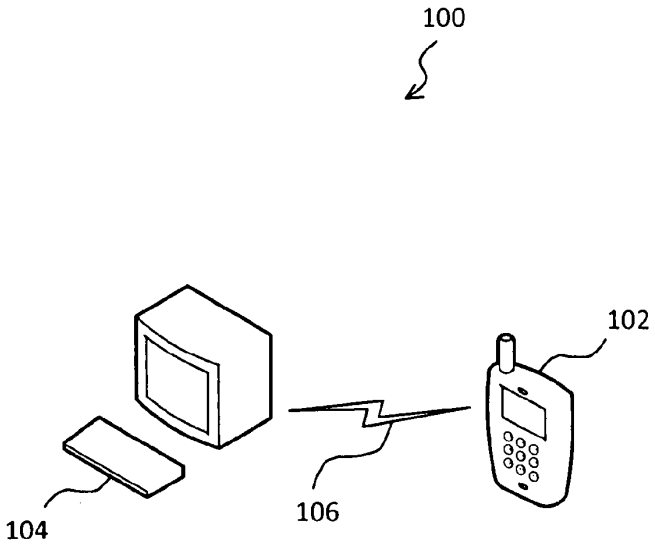


FIG. 1

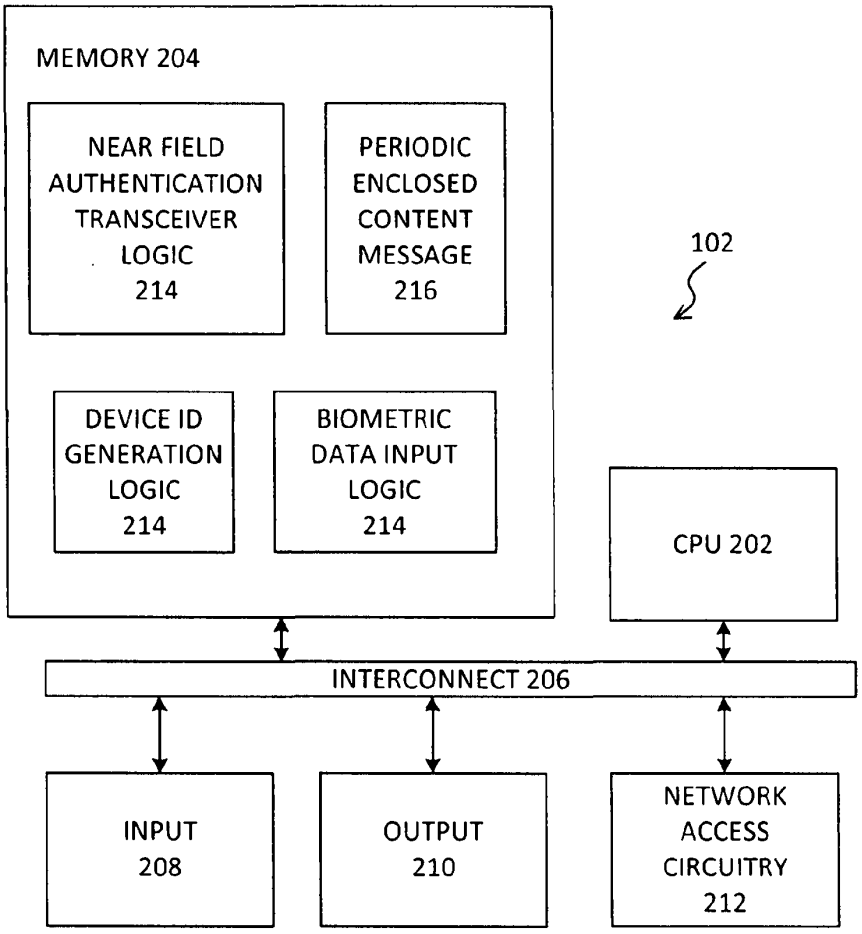

MEMORY 204
NEAR FIELD AUTHENTICATION TRANSCEIVER LOGIC 214
PERIODIC ENCLOSED CONTENT MESSAGE 216
DEVICE ID GENERATION LOGIC 214
BIOMETRIC DATA INPUT LOGIC 214
102
CPU 202
INTERCONNECT 206
INPUT 208
OUTPUT 210
NETWORK ACCESS CIRCUITRY 212

FIG. 2

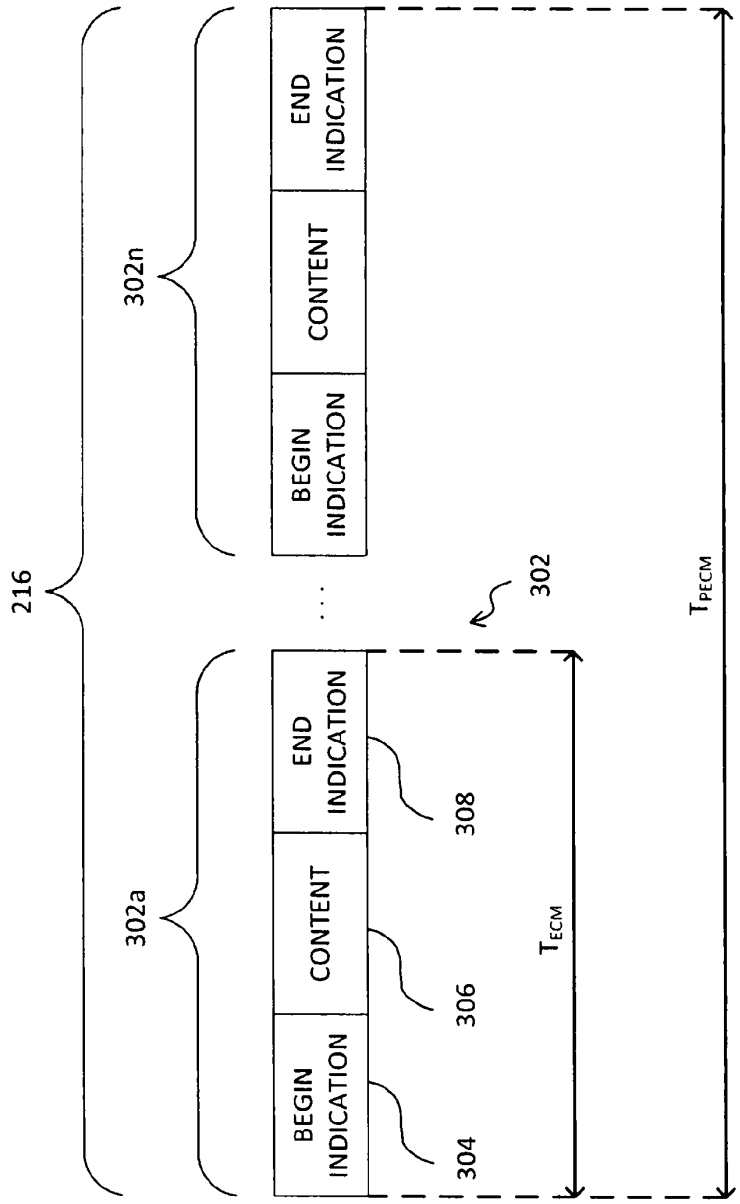

216
302a
302n
BEGIN INDICATION
CONTENT
END INDICATION
BEGIN INDICATION
CONTENT
END INDICATION
304
306
308
302
T_{ECM}
T_{PECM}

FIG. 3

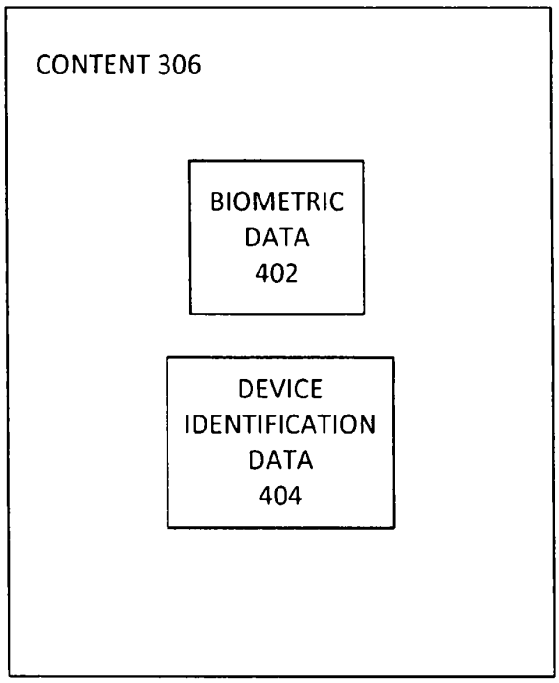

CONTENT 306
BIOMETRIC DATA 402
DEVICE IDENTIFICATION DATA 404

FIG. 4

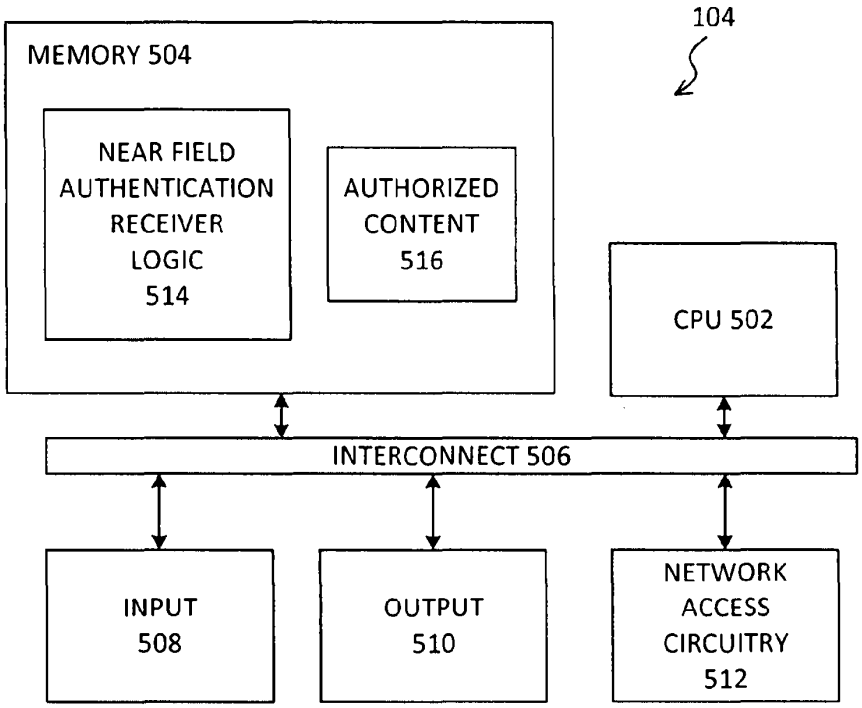

104
MEMORY 504
NEAR FIELD AUTHENTICATION RECEIVER LOGIC 514
AUTHORIZED CONTENT 516
CPU 502
INTERCONNECT 506
INPUT 508
OUTPUT 510
NETWORK ACCESS CIRCUITRY 512

FIG. 5

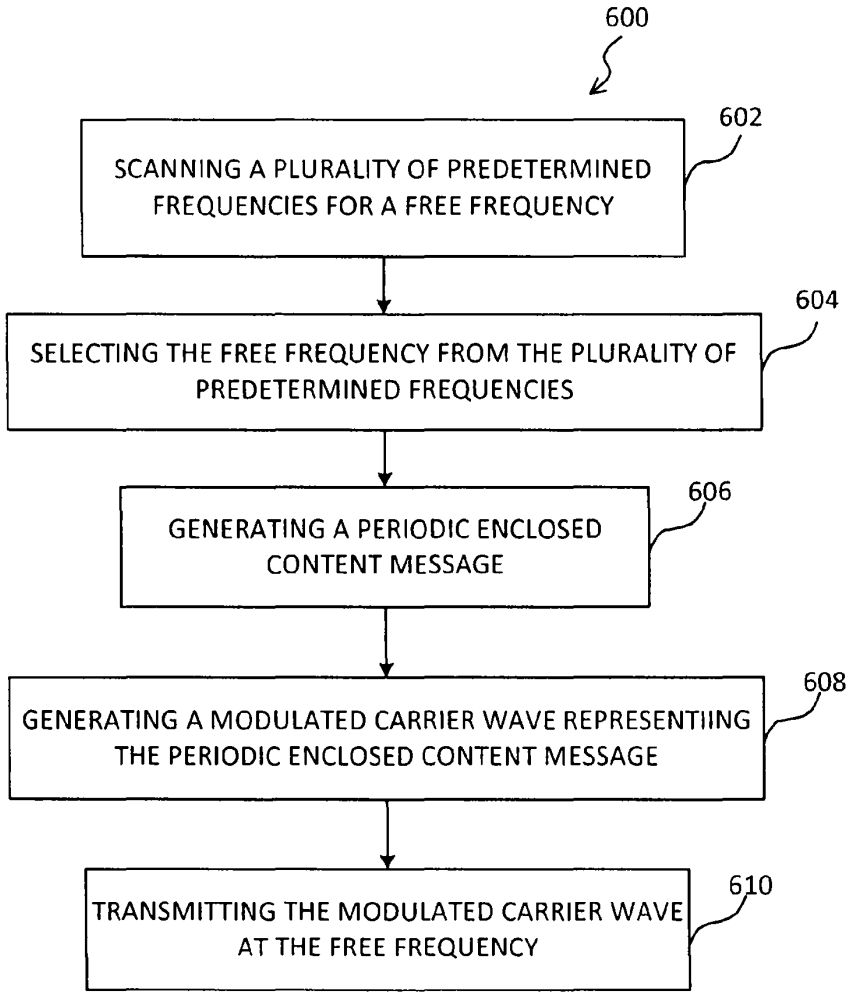

600
602
SCANNING A PLURALITY OF PREDETERMINED FREQUENCIES FOR A FREE FREQUENCY
604
SELECTING THE FREE FREQUENCY FROM THE PLURALITY OF PREDETERMINED FREQUENCIES
606
GENERATING A PERIODIC ENCLOSED CONTENT MESSAGE
608
GENERATING A MODULATED CARRIER WAVE REPRESENTIING THE PERIODIC ENCLOSED CONTENT MESSAGE
610
TRANSMITTING THE MODULATED CARRIER WAVE AT THE FREE FREQUENCY

FIG. 6

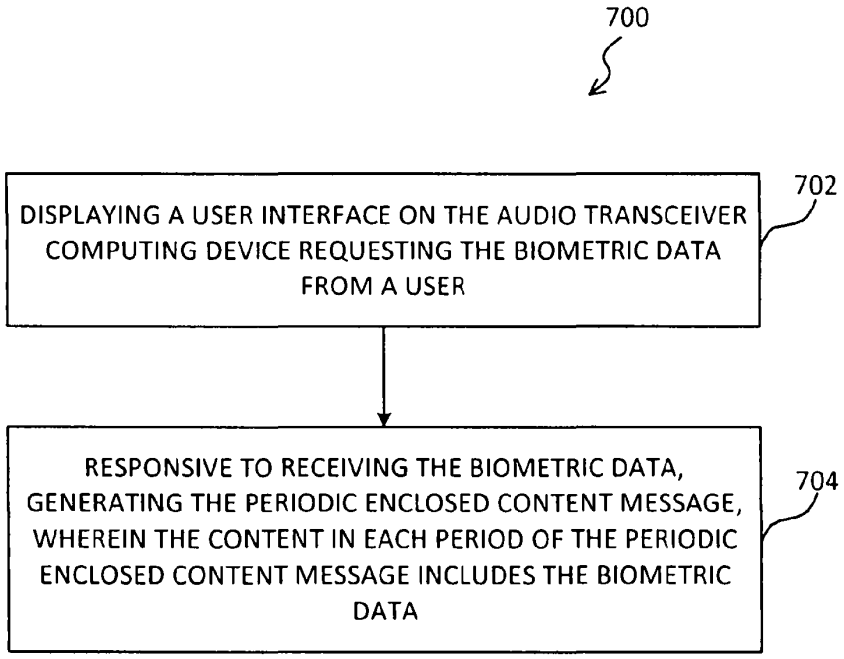

700
DISPLAYING A USER INTERFACE ON THE AUDIO TRANSCEIVER COMPUTING DEVICE REQUESTING THE BIOMETRIC DATA FROM A USER
702
RESPONSIVE TO RECEIVING THE BIOMETRIC DATA, GENERATING THE PERIODIC ENCLOSED CONTENT MESSAGE, WHEREIN THE CONTENT IN EACH PERIOD OF THE PERIODIC ENCLOSED CONTENT MESSAGE INCLUDES THE BIOMETRIC DATA
704

FIG. 7

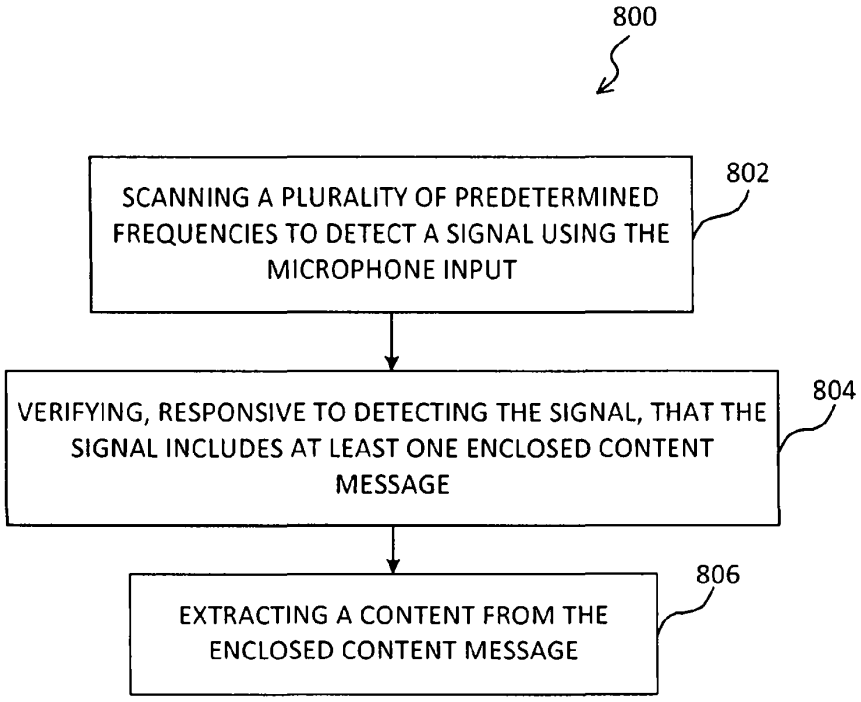

800
SCANNING A PLURALITY OF PREDETERMINED FREQUENCIES TO DETECT A SIGNAL USING THE MICROPHONE INPUT
802
VERIFYING, RESPONSIVE TO DETECTING THE SIGNAL, THAT THE SIGNAL INCLUDES AT LEAST ONE ENCLOSED CONTENT MESSAGE
804
EXTRACTING A CONTENT FROM THE ENCLOSED CONTENT MESSAGE
806

FIG. 8

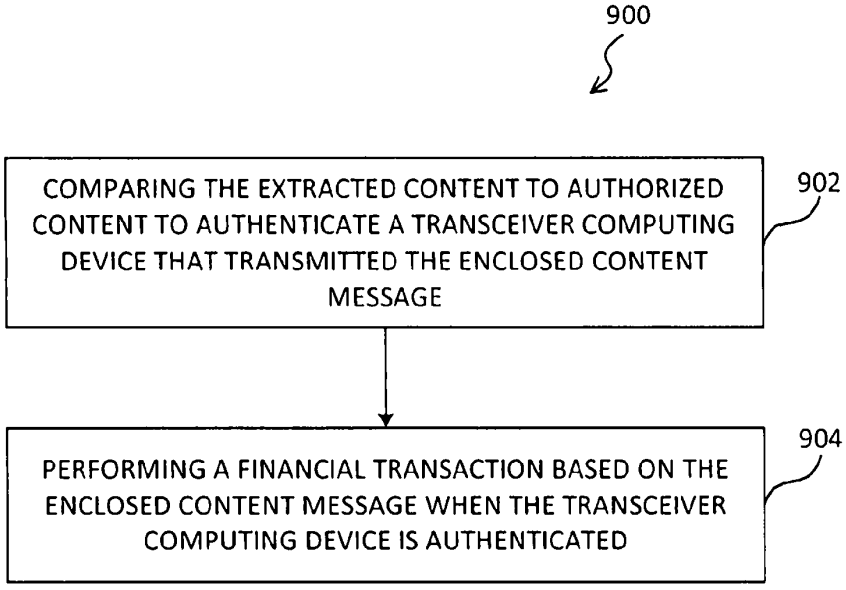

900
COMPARING THE EXTRACTED CONTENT TO AUTHORIZED CONTENT TO AUTHENTICATE A TRANSCEIVER COMPUTING DEVICE THAT TRANSMITTED THE ENCLOSED CONTENT MESSAGE
902
PERFORMING A FINANCIAL TRANSACTION BASED ON THE ENCLOSED CONTENT MESSAGE WHEN THE TRANSCEIVER COMPUTING DEVICE IS AUTHENTICATED
904

FIG. 9

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. no.:	13/734,178	Conf. no.	3155
Applicant:	Craig S. Etchegoyen	Art Unit:	2649
Filed:	January 4, 2013	Examiner:	Ajibola A. Akinyemi

Title: NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES

RESPONSE TO OFFICE ACTION

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir,

In response to the Office Action mailed September 6, 2013, please amend the present application as follows:

Amendments to the Specification are provided on page 2.
Amendments to the Claims begin on page 3.
Remarks begin on page 5.

IN THE SPECIFICATION:

Please amend the paragraph beginning on p. 19 at line 8 with the following amended paragraph:

[0058] Once the near field authentication receiver logic 514 authenticates the audio transceiver computing device 102, the near field authentication receiver logic 514 can display or provide [[a]] an acknowledgement indication that the authentication has occurred. The acknowledgement indication may be provided locally by the device 104, for example, in the form of a visual indication or an audible tone. Alternatively or in combination, the acknowledgement indication may also be provided to the user of the device 102 by means of a locally generated audible tone, locally generated visual indication (such as an LED illuminating or changing color), or by sending a remote indication to the device 102 via a network link or by means of a sound wave using a free frequency according to the same methods disclosed herein for generating and transmitting the enclosed content message. The user of device 102, responsive to receiving the indication, may then stop transmission of the modulated carrier wave 106 by manual or automatic action. However, if the near field authentication receiver logic 514 fails to authenticate the audio transceiver computing device 102, such as if the content does not match the authorized content 516, or if no content was discovered, then the near field authentication receiver logic 514 can display or provide some sort of indication to indicate that an authentication failure has occurred. Furthermore, a log could be stored indicating the time, location, and/or the content if available. This can help with any troubleshooting requests, and/or any investigations of fraud.

IN THE CLAIMS:

1. (currently amended) A method for near field authentication of a source, the source using an audio transceiver computing device, the method comprising:

scanning a plurality of predetermined frequencies for a free frequency;

selecting the free frequency from the plurality of predetermined frequencies;

generating a periodic enclosed content message;

generating a modulated carrier wave representing the periodic enclosed content message; and

transmitting the modulated carrier wave at the free frequency;

wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication; and

wherein the content includes at least one of biometric data, or device identification data.

2. (original) The method of claim 1 further comprising:

displaying a user interface on the audio transceiver computing device requesting the biometric data from a user; and

responsive to receiving the biometric data, generating the periodic enclosed content message, wherein the content in each period of the periodic enclosed content message includes the biometric data.

3. (previously presented) The method of claim 1, wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

4. (previously presented) The method of claim 1, wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.

5. (previously presented) The method of claim 1 wherein the modulated carrier wave comprises a sound wave.

6. (previously presented) The method of claim 2, wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

7. (previously presented) The method of claim 2, wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.

8. (previously presented) The method of claim 4 wherein the modulated carrier wave comprises a sound wave.

9. (new) The method of claim 1 wherein the carrier wave is modulated by the periodic enclosed content message.

REMARKS

Applicant thanks Examiner Akinyemi for his thorough review of the application papers and for his opinion on patentability.

Claims 1-8 are pending in the application. Claim 1 is amended herein. Claim 9 is new. Applicant respectfully requests reconsideration of all pending claims in view of the amendments and remarks herein.

Response to Rejections Under 35 USC §102

Claim 1 was rejected under 35 USC §102(b) as being anticipated by U.S. Application Pub. 2004/0038716 (*"Gass"*). Applicant respectfully traverses this rejection and requests reconsideration and withdrawal of this rejection in view of the following.

1. The Invention Being Claimed

The invention teaches a method for fraud protection by providing an extra layer of security for near-field transactions between two computing devices. For example, the invention can be used to authenticate a transaction in a store between (i) a point-of-sale computer (i.e. a computerized cash register) operated by a merchant and (ii) a mobile phone operated by a customer who is doing business inside the store. The invention is particularly useful for virtual credit card transactions in which credit card information is exchanged between the point-of-sale computer and the mobile phone.

In lieu of or in addition to a WAN or Internet-based authentication procedure in which the merchant's computer verifies a credit card number provided by the mobile phone, the invention provides a way to verify that the transaction is in fact being authorized by a customer who is physically present inside the store and who is a registered owner of the mobile phone. It does this by using near-field signals transmitted between the mobile phone and the merchant's computer. Near-field signals are low power signals limited to transmission over very short distances, e.g. centimeters or feet. See Specification at par. 0004.

For example, to authenticate the transaction, the merchant computer may send a text message to the mobile phone asking the customer to transmit a device identifier or biometric identifier (or both) to the merchant's computer using a sound wave. Sound waves generated

through the acoustic speaker of a mobile phone are very low power signals, therefore when such a wave is picked up by the microphone of the merchant computer, it provides a very high level of confidence that the customer is physically present inside the store, and probably within a few feet of the merchant computer. The invention allows the customer's mobile phone to modulate the sound wave with an encoded message (i.e., a "periodic enclosed content message") that contains the device identifier data and/or the biometric identifier. The merchant computer can then decode the message, extract the identifier, and compare it against a list of pre-authorized identifiers to complete the authentication.

To discern the identifier, the merchant computer is constantly "listening" on a plurality of frequencies, whether acoustic or electromagnetic. There may be multiple mobile devices simultaneously attempting local transactions with the merchant computer. Therefore, according to the invention, each mobile device must scan the frequencies to identify a free frequency, then transmit a signal on that frequency in the form of a periodic enclosed content message encoded with the device and/or biometric identifier. To extract the encoded identifier, the merchant computer hears the periodic signal, and must then detect beginning and end points within the signal that enclose the encoded bit pattern that comprises the identifier. The invention therefore provides a periodic enclosed content message that includes a "begin indication", a "content", and an "end indication".

In this manner, the identifier(s) may be extracted from the content portion of the signal to authenticate the transacting mobile device. This will help to prevent fraudulent transactions that involve stolen account numbers. For example, a thief who has copied a stolen credit card number to his own mobile device is prevented from completing a virtual credit card transaction from a remote location when prompted for near-field authentication. And locally, the thief is prevented from completing the transaction through inability to generate the correct device or biometric identifier using near-field waves.

2. The *Gass* Reference

Gass teaches a system for converting GSM (cell phone) signals into FM radio signals to enable "hands free" cell phone communications while driving a car. *Gass* is not concerned with fraud prevention and is not dedicated to providing methods for securing network transactions between clients and servers.

Gass does provide some teachings that are relevant to scanning frequencies for free frequencies that enable a cell phone to effect near-field communications between the cell phone and the FM receiver of a car stereo system. However, there are no teachings in *Gass* that anticipate elements of the invention that enable mobile device authentication. These differences are discussed below.

3. Claim Amendments

Claim 1 has been amended to make the claims identical to those that were allowed in the Australian case (AU2012100462) to which the present application claims priority, and to ensure that applicant is in compliance with its petition for examination under the Patent Prosecution Highway procedure. Through a clerical error, the claims presented for examination as amended on March 22, 2013 omitted the most recent amendments made in the Australian case prior to grant. With the exception of new claim 9, the claims as amended herein now correspond identically with those in AU2012100462.

New claim 9 has been added to further narrow claim 1 in a manner that applicant believes will shed light on a novel aspect of the invention. Claim 9 recites "wherein the carrier wave is modulated by the periodic enclosed content message". In other words, in this embodiment the encoded identifiers that are needed to authenticate the mobile device comprise signals that are used to modulate the near-field carrier wave.

4. Claim 1 is Novel Over *Gass*

Regarding claim 1, the Office Action dated September 6, 2013 ("Office Action") stated that *Gass* at paragraphs 0015-0016 teaches a method for near field authentication of a source. Office Action, pp. 2-3. Applicant respectfully disagrees.

Gass at pars. 0015-0016 fails to teach any methods of *source* authentication of human users and fails to teach any methods of *source* authentication of computing devices, both of which types of source authentication are recited in claim 1. To wit, claim 1 now recites:

> *wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication; and*
>
> *wherein the content includes at least one of biometric data, or device identification data.*

As noted above, *Gass's* objective is to allow a driver to talk on his cell phone "hands free", and is not concerned with authenticating the phone or its user as a condition for allowing the cell phone to communicate with the FM radio. *Gass* clearly falls short of teaching generating an enclosed content message having content that includes biometric or device identification data.

By contrast, claim 1 of applicant's invention performs a method which authenticates the identity of the user of the mobile phone, and the identity of the mobile phone itself, or both, based on a periodic enclosed content message generated by a close-proximity ("near field") source. The message is generated for the express purpose of authenticating the source device and/or the user operating the source device. Specification (Abstract; pars. 0002, 0007-0008, 0011, 0025, 0032-0035, 0058, 0073, and 0075-0076). Particularly instructive is par. 0032:

> To generate the periodic enclosed content message 216, the near field authentication transceiver logic 214 can utilize a device ID generation logic or a biometric data input logic 220, or both. The device ID generation logic 218 can generate, for example, device identification data of the audio transceiver computing device 102. The device identification data or the biometric data, or both, can be included in a content of the periodic enclosed content message 216.

And Paragraph 0058:

> Once the near field authentication receiver logic 514 authenticates the audio transceiver computing device 102, the near field authentication receiver logic can display or provide an acknowledgment indication that an authentication has occurred.

Gass thus fails to teach methods of source authentication of human users and fails to teach methods of source authentication of computing devices, both of which types of source authentication are recited in claim 1 as amended.

Applicant acknowledges the Office Action's citation to *Gass* at par. 0016 for teachings related to encoding the RDS signal that is transmitted from the cell phone to the FM radio. However, unlike the present invention, *Gass* is not modulating the carrier wave with an enclosed content message; instead *Gass* is encoding only the RDS portion of the signal modulated at the subcarrier frequency 57 kHz (see FIG. 3), which is reserved, *e.g.*, for digital display data.

Moreover, the only data that *Gass* encodes for modulation on the RDS subcarrier is data representing the "free frequency 4". *Gass* at par. 0016:

> If a free channel is detected, the detected free channel … is reported as a free frequency or free channel information 4 to the RDS encoder RE. The RDS encoder encodes said frequency or channel information generating a corresponding RDS signal 5 modulated on the RDS subcarrier at 57 kHz.

Thus, to the extent that *Gass* teaches encoding, those teachings don't anticipate encoding for purposes of source authentication and certainly fail to anticipate encoding a carrier frequency with an enclosed content message that includes source identification data as recited in claim 1.

For all of the foregoing reasons, applicant requests that the §102 rejection of claim 1 be withdrawn.

Response to Rejections Under 35 USC §103

Claim 2 was rejected under 35 USC §103(a) as being unpatentable over *Gass* in view of U.S. Application Pub. 2007/0038716 ("*Martin*"). Claims 3-5 were rejected under 35 USC §103(a) as being unpatentable over *Gass* in view of U.S. Patent 5,019,813 ("*Kip*"). Claims 6-8 were rejected under 35 USC §103(a) as being unpatentable over *Gass* in view of *Martin* and *Kip*. Applicant respectfully traverses.

1. Generally, Claims 2-8 are Allowable Over the Prior Art Based on Dependency.

Claims 2-8 each depend from claim 1. Applicant requests withdrawal of all obviousness rejections of claims depending from claim 1, on grounds of dependency, and for the same reasons presented above that distinguish claim 1 over the teachings of *Gass*.

2. Claim 2

Specifically with regard to claim 2, the Office Action incorporated the rejection of claim 1 and stated further that *Gass* does not disclose the limitation of claim 2, but that *Martin* at pars. 0062-0063, however, discloses a user interface on the audio transceiver computing device requesting the biometric data from a user, and that it would have been obvious to combine the teaching of *Martin* with the teaching of *Gass* to provide a security system wherein the user is provided with a dual layered verification system in addition to a unique identifier given to the user. Office Action, page 4. Applicant respectfully disagrees.

It is respectfully submitted that there is no teaching, suggestion, or motivation to combine the teachings of *Gass* and *Martin* because *Gass* does not provide for encoding signals with *any*

type of identifier for source authentication purposes. As explained above, the only identifier contemplated by *Gass* is the free frequency. *Gass* is simply too far afield from *Martin* to reasonably expect a skilled artisan to combine their teachings. Moreover, under *KSR v. Teleflex*, it is the Office's burden to articulate the rationale for combining references. Applicant respectfully submits that this burden has not been met.

For the foregoing reasons, applicant requests that the rejection of claim 2 be withdrawn.

3. Claim 3

With regard to claim 3, the Office Action incorporated the rejection of claim 1 and stated further that *Gass* does not disclose the limitation of claim 3 "*wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time*". Office Action, pp. 4-5.

The Office Action further states that *Kip*, however, discloses the above limitations at col. 5, lines 39-44 and that it would have been obvious to combine this teaching of *Kip* with the teaching of *Gass* "to provide a universally applicable data exchange system operating in a contactless manner". Office Action, p. 5. Applicant respectfully disagrees that *Kip* teaches the limitation of claim 3.

Kip at 5:39-44 discloses the following:

> For the sake of clarity, the modulated carrier wave signal is shown in FIG. 5 during the first eight periods P1 and during the next period P2, with the reply signal from the data carrier above it in case the status of the data line SDA is "low" ("0")(FIG. 5a) or "high" ("1")(FIG. 5b).

This is not an express teaching that reads on the limitation of claim 3. *Kip* teaches a method for data exchange between an active transceiver and a passive data carrier. The transceiver amplitude-modulates an AC field that is picked up by the passive data carrier to provide clock pulses and supply power needed for the passive data carrier to operate. *Kip*, Abstract. There is no disclosure anywhere in *Kip* that teaches or suggests that a modulated carrier wave be transmitted only for a predetermined number of periods or for a predetermined period of time. FIG. 5 of *Kip* shows *continuous* transmission of a modulated carrier wave. *Kip* expressly states that "the modulated carrier wave signal is shown in FIG. 5 during the first eight periods P1 and during the next period P2 …"

The reason that P1 has a different waveform than P2 is because the modulating signal happened to transmit 8 consecutive bits of "logical 1" that each modulated a single period of the carrier signal, *i.e.* "one bit of information is transmitted in each period". *Kip* at 3:1-3. But just because the carrier signal waveform is unaltered in a particular period in which the modulating signal is a "logical 0", that doesn't mean that the carrier wave, as a whole, is not being transmitted. It is in fact being transmitted continuously, with some periods such as P1 modulated with a logical 1 and other periods such as P2 modulated with a logical 0.

In any event, the Office Action has taken *Kip's* teaching out of context and attempted to combine it with the teachings of *Gass*. The motivational explanation for such a combination is lacking. In *Gass*, both the cell phone and the FM radio are active devices that have their own power sources. No one would be motivated to use a *Kip*-type transceiver to transmit an amplitude-modulated AC field to provide wireless power for *Gass's* active devices that are already powered.

For the foregoing reasons, applicant requests that the rejection of claim 3 be withdrawn.

4. Claim 4

With regard to claim 4, the Office Action stated that *Kip* discloses the method wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user, and for support cites to *Kip* at FIG. 5b and 5:39-44. Office Action, p. 5. Applicant respectfully disagrees.

The referenced aspect of *Kip* (col. 5, lines 39-44) fails to teach transmitting a modulated RF carrier wave until a stop indication is received from a user. Instead, *Kip* (col. 5, lines 39-44) in this context merely references FIG. 5 of *Kip*, and by implication FIG. 5b thereof which figure 5b portrays the word "stop" beneath the horizontal axis of the drawing, but which is clearly not a stop indicator received from a user as recited in claim 4.

Moreover, applicant further disagrees that it would be obvious to combine the referenced teaching of *Kip* into that of *Gass* because of the reasons presented above with respect to claim 3, and because such combination has no reasonable expectation of success in producing the benefits of claim 1 upon which claim 4 depends. Such combination is effectively impossible in that *Gass* fails to teach the authenticating of source devices or operators of source devices, let alone teach

authentication of both at the option of a user. Authentication of source devices and users thereof is not possible with any such proposed combination of *Gass* and *Kip*.

For the foregoing reasons, applicant requests that the rejection of claim 4 be withdrawn.

5. Claim 5

The Office Action rejects claim 5 on the basis that *Gass* discloses the method wherein the modulated carrier wave comprises a sound wave. Office Action, p. 5. However, the Office Action references par. 0016 of *Gass*, which does not actually mention any sound waves.

Gass's teachings apply exclusively to GSM and FM signals. Such signals comprise electromagnetic waves transmitted at RF frequencies such as 87 MHz to 107 MHz. *Gass* at 0016. While these radio waves may contain *audio* signals, they are not *sound waves*. It is well known that sound waves are waves that are propagated by collisions of molecules in media such as air and water.

For the foregoing reasons, applicant requests that the rejection of claim 5 be withdrawn.

6. Claim 6

With regard to claim 6, the Office Action incorporated the rejection of claim 2 and stated further that *Gass* and *Martin* do not disclose wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time. Office Action, p. 5. The Office Action further states that *Kip* discloses this above limitation (col. 5, lines 39-44) and that it would have been obvious to utilize the teaching of *Kip* into the teaching of *Gass* in view of *Martin* in order to provide a universally applicable data exchange system operating in a contactless manner. Office Action, pp. 5-6. Applicant respectfully disagrees.

Applicant reasserts here the foregoing arguments in favor of claims 2 and 3 and requests that the rejection of claim 6 be withdrawn for the same reasons presented above with respect to claims 2 and 3.

7. Claim 7

With regard to claim 7, the Office Action stated that *Kip* discloses the method wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop

indication is received from a user (Fig. 5b, col. 5, lines 39-44). Office Action, p. 6. Applicant respectfully disagrees.

Applicant reasserts here the foregoing arguments in favor of claims 2 and 4 and requests that the rejection of claim 7 be withdrawn for the same reasons presented above with respect to claims 2 and 4.

8. Claim 8

The Office Action rejects claim 8 on the basis that *Gass* discloses the method wherein the modulated carrier wave comprises a sound wave. Office Action, p. 5. However, the Office Action references par. 0016 of *Gass*, which does not actually mention any sound waves.

Applicant reasserts here the foregoing arguments in favor of claim 5 and requests that the rejection of claim 8 be withdrawn for the same reasons presented above with respect to claim 5.

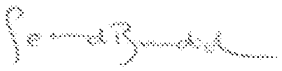
9. Claim 9

Claim 9 is a new claim dependent upon and further narrowing claim 1. No new subject matter, however, has been added to the application thereby and this new claim has been introduced for purposes of overall claim construction and is fully supported by applicant's original specification. *See, e.g.* Specification at par. 0033.

Conclusion

In view of all of the above, applicant believes that all pending claims are in condition for allowance and earnestly requests that these claims be passed to issuance. If the Examiner believes that a telephone conversation would help to expedite prosecution, please call the undersigned attorney at the number below.

Respectfully Submitted,



Sean D. Burdick
Reg. No. 51,513

Uniloc USA, Inc.
7160 N. Dallas Parkway, Suite 380
Plano, Texas 75024
(972) 905-9580 x227

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. no.: 13/734,178	Conf. no. 3155
Applicant: Craig S. Etchegoyen	Art Unit: 2649
Filed: January 4, 2013	Examiner: Ajibola A. Akinyemi

Title: NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicant hereby submits, without admission of prior art effect thereof, form(s) PTO/SB/08 pursuant to the duty of disclosure requirements of 37 CFR §§ 1.56, 1.97 and 1.98.

Applicant has listed publication dates on the attached form(s) PTO/SB/08 based on information presently available to the undersigned. However, the listed publication dates should not be construed as an admission that the information was actually published on the date indicated.

It is respectfully requested that the Examiner initial and return a copy of the enclosed forms PTO/SB/08, and to indicate in the official file wrapper of this patent application that the documents have been considered.

Applicant submits concurrently herewith the fee set forth in § 1.17(p).

Respectfully Submitted,

Sean D. Burdick
Reg. No. 51,513

Uniloc USA, Inc.
7160 N. Dallas Parkway
Suite 380
Plano, TX 75024
(972) 905-9580 x227

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO
(modified by Applicant)

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	13/734,178
Filing Date	January 4, 2013
First Named Inventor	Craig S. Etchegoyen
Art Unit	2649
Examiner Name	Ajibola A. Akinyemi
Attorney Docket Number	UN-NP-SC-085

U. S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-2008/0097924	04/24/2008	Carper et al.	
		US-2009/0099830	04/16/2009	Gross et al.	
		US-7,818,573	10/19/2010	Martin et al.	
		US-7,965,843	06/21/2011	Maino et al.	
		US-2003/0070067	04/10/2003	Saito, Shin	
		US-2003/0131001	07/10/2003	Matsuo, Masanobu	
		US-2003/0182435	09/25/2003	Redlich et al.	
		US-2003/0237004	12/25/2003	Okamura, Mine	
		US-2006/0075134	04/6/2006	Aalto et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code – Number – Kind Code	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T
		EP 1 903 518	09/10/2007	NCR Corp.		
		JP 5181734	07/23/1993	Hitachi Ltd		
		GB 2391965	02/18/2004	MessageLabs Ltd.		
		WO 2006/102399	09/28/2006	Absolute Software Corporation		

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date page(s), volume-issue number(s), publisher, city and/or country where published.	T

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

REQUEST FOR PARTICIPATION IN THE PPH PILOT PROGRAM BETWEEN IPAU AND THE USPTO
(continued)

Application No.:	13/734,178	First Named Inventor:	Craig S. Etchegoyen

II. Claims Correspondence Table:

Claims in US Application	Patentable Claims in AU Application	Explanation regarding the correspondence
1	1	US claim 1 sufficiently corresponds to the scope of AU claim 1
2	2	US claim 2 sufficiently corresponds to the scope of AU claim 2
3	3	US claim 3 is embodied by multiply dependent AU claim 3
4	4	US claim 4 is embodied by multiply dependent AU claim 4
5	5	US claim 5 is embodied by and narrower in scope to AU claim 5
6	3	US claim 6 is embodied by multiply dependent AU claim 3
7	4	US claim 7 is embodied by multiply dependent AU claim 4
8	5	US claim 8 sufficiently corresponds to the scope of AU claim 5
9	1	US claim 9 sufficiently corresponds to the scope of AU claim 1

III. All the claims in the US application sufficiently correspond to the patentable/allowable claims in the AU application.

Signature /Sean D. Burdick/	Date November 14, 2013
Name (Print/Typed) Sean D. Burdick	Registration Number 51513

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 903 518 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
26.03.2008 Bulletin 2008/13

(51) Int Cl.:
G07F 7/10 (2006.01) *G07F 19/00* (2006.01)

(21) Application number: **07253584.2**

(22) Date of filing: **10.09.2007**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC MT NL PL PT RO SE SI SK TR
Designated Extension States:
AL BA HR MK YU

(30) Priority: **15.09.2006 US 521712**

(71) Applicant: **NCR Corporation**
Dayton, Ohio 45479 (US)

(72) Inventors:
- **Whytock, Alexander W.**
  Blairgowrie
  Perthshire PH10 6TL (GB)
- **Neilan, Michael J.**
  Liff
  Dundee DD2 5RU (GB)
- **Henderson, James**
  St. Andrews
  Fife KY16 9NQ (GB)

(74) Representative: **Williamson, Brian et al**
NCR International, Inc.,
206 Marylebone Road
London NW1 6LY (GB)

(54) Security validation of machine components

(57) A method of validating machine components in a self-service terminal is disclosed which comprises providing at least one machine component with a machine readable identifier and reading identity data from the machine readable identifier using a processing unit. The identity data is compared with identity data stored in the memory of the processing unit to determine if the identity of a component has changed. If the identity has changed, the processing unit compares the identity data with source data to determine if the component is from a trusted source. In one embodiment, the self service terminal is an ATM and the components are an encrypting Personal Identification Number (PIN) pad, a cash dispenser unit and a card reader.

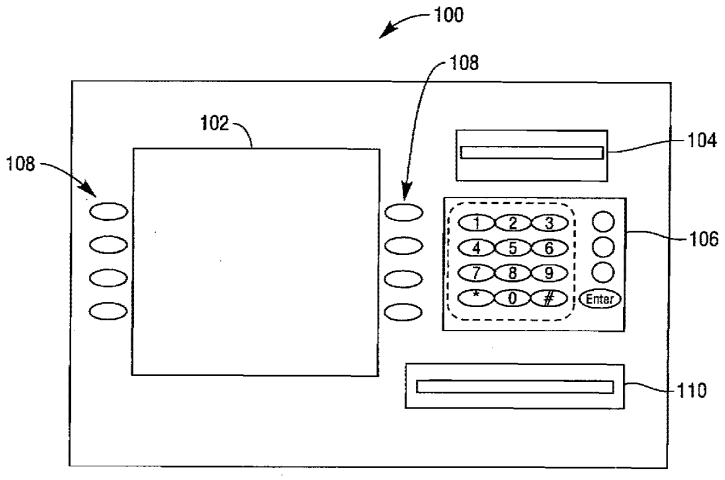


FIG. 1

Printed by Jouve, 75001 PARIS (FR)

EP 1 903 518 A1

Description

[0001] The present invention relates to security validation for component parts of Self-Service Terminals (SST) and, in particular, but not exclusively to components for Automated teller Machines (ATMs).

[0002] SSTs comprise machines which dispense goods to or perform services for a user. A common example of an SST is an ATM. When these machines develop a fault or are due for a service after they have been installed at a site, an engineer or maintenance operator is usually sent to diagnose the problem and/or correct the fault. Where correction of the fault requires installing a replacement component, there is a risk that that replacement component may be of a lower standard than the component initially installed by the manufacturer of the SST.

[0003] Taking the example of an ATM, there is a particular concern that the replacement component is of a high standard as an ATM is used as an interface for financial transactions. Moreover, ATMs are often the target of thieves, who could deliberately install a replacement component with a malicious purpose, for example, to gain access to security information entered by a subsequent user of the ATM.

[0004] In one prior art method, the problem is addressed by requiring an engineer to certify that replacement components are in good working order immediately following their installation. The process proceeds substantially as follows:

[0005] When an engineer is called to a faulty SST, he or she uses a device within the ATM known as an Operator Panel. An Operator Panel is a processing unit arranged to provide a user interface to the engineer and to guide the engineer through servicing and diagnostic procedures. In order to run the procedures, the engineer must pass a security clearance test. This is normally achieved by requiring the engineer to use a USB security dongle known in this context as a Service Security Key.

[0006] Whilst servicing the SST, the engineer may be required to replace a faulty component. The SST is arranged such that certification that the component is fully functional is required before the SST returns to normal operation. The certification is executed by the engineer through the Operator Panel and using the Service Security Key. A problem with this method is that should the engineer not have his or her Security Service Key, or should the Key itself be faulty, then the SST will not return to normal operation. Further, while the method ensures that the replacement component is functional, it does not ensure that the replacement component comes from a trusted source.

[0007] According to a first aspect of the invention, there is provided a method of validating machine components in a self-service terminal comprising: providing at least one machine component with identity information in the form of a machine readable identifier reading identity data from the machine readable identifier; comparing the identity data with stored identity data to determine if the identity of a component has changed; and if the identity has changed, comparing the identity data with source data to determine if the component is from a trusted source.

[0008] This provides a convenient method of checking the quality and integrity of components. It will be appreciated that self-service terminals often accept cash and some, for example Automated Teller Machines (ATMs), are used for financial transactions. This means that high standards must be maintained for the components of terminals. Where a component is from a trusted source, it can be assumed that the high standard will have been met. In addition, terminals are often targets by malicious persons and as such it is important to be able to verify that components are genuine and not capable of being used to defraud users of a terminal.

[0009] Preferably, the method is carried out on start-up of the terminal. This is convenient as a terminal will generally be shut down in order to replace a component thereof. Checking the source of any replaced components on start-up means that any components which are not from a trusted source will be detected before use can be made of the terminal.

[0010] In such embodiment, the method may comprise disabling the terminal if a component is not from a trusted source. This is advantageous as it prevents the terminal from being operational with untrustworthy components.

[0011] The method may further comprise replacing the stored identity data with the changed identity data if the identity has changed. This is advantageous as the source of a component will not be determined in future unless the component is replaced.

[0012] In a preferred embodiment, the method comprises verifying security data before the stored identity data is replaced with changed identity data. This is advantageous as it helps to ensure that any replacement of a component has been carried out by an authorized operator or engineer.

[0013] According to a second aspect of the invention, there is provided a Self-service terminal processing unit comprising a memory for storing identity data, a requesting means arranged to request identity data from components of the terminal and a comparing means arranged to compare identity data received by the requesting means with identity data stored in the memory to detect any changes in identity data.

[0014] In one embodiment, the memory of the processing unit comprises component source data and the comparing means is arranged to compare changed identity data with the source data to determine if the component derives from a trusted source.

[0015] Preferably, the processing unit further comprises a security means arranged to receive security data from a maintenance operator and use the security data to determine whether a maintenance operator is an authorized operator.

[0016] Preferably, the processing unit is arranged to allow a terminal with which it is associated to operate

only if the or each component is from a trusted source.

[0017] According to a third aspect of the invention, there is provided a self-service terminal comprising a processing unit according to the second aspect of the invention and further comprising at least one of the following components: an encrypting PIN pad, a cash dispenser unit and a card reader, the terminal being arranged such that identity data associated with the or each component can be read by the processing unit.

[0018] In a preferred embodiment, the terminal comprises one of each of the components mentioned above and the processing unit is arranged to determine whether each of the components is from a trusted source and to allow the terminal to operate only if all the components are from a trusted source.

[0019] Preferably, the identity data associated with the or each component is provided on a chip.

[0020] In one embodiment, the self-service terminal is an Automated Teller Machine.

[0021] According to a fourth aspect of the invention, there is provided computer software arranged to perform the method of the first aspect of the invention.

[0022] According to a fifth aspect of the invention, there is provided computer software, which, which loaded onto a processing unit causes the processing unit to act as the processing unit of the second aspect of the invention.

[0023] Embodiments of the present invention will now be described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 shows the fascia of a Self-service terminal;

Figure 2 schematically shows the internal components of a Self-service terminal according to one embodiment of the present invention;

Figure 3 shows a flowchart of the steps in 'first ever' start-up of an ATM; and

Figure 4 shows a flowchart of the steps in subsequent start-ups of an ATM.

[0024] The Self Service Terminal shown in Figures 1 and 2 is an Automated Teller Machine (ATM) 100. The ATM 100 comprises a screen 102, a card slot 104, data entry devices in the form of a 16-button key pad 106 and menu selection buttons 108, and a dispensing slot 110.

[0025] Figure 2 shows the components of the ATM 100. The components comprise an encrypting Personal Identification Number (PIN) pad 202, a cash dispenser unit 204 and a card reader 206. The ATM 100 further comprises a processing unit in the form of a PC core 208. Each of the components contain embedded therein an identity chip 212 comprising data providing a manufacturers identity. The encrypting PIN Pad 202, cash dispenser unit 204, card reader 206 and the chip 212 associated with each component 202, 204, 206 are capable of communicating with the PC core 208 via a system bus 210.

[0026] The PC core 208 comprises a memory 214 arranged to store data. The memory 214 is capable of storing persistent data, i.e. storing data in a non-volatile manner. The PC Core 208 further comprises a requesting means 216 which is arranged to request and receive data from the chips 212 and a comparing means 218 arranged to compare identity data received by the requesting means with identity data stored in the memory 214. The PC Core 208 further comprises a security means 220, arranged to carry out a security routine to verify the identity of a maintenance operator or engineer and to ensure that that person is authorized to install a replacement component 202, 204, 206.

[0027] In normal use of the ATM 100, a user inserts a card bearing a magnetic strip and/or an encrypted data chip, usually a bank card, into the card slot 104. The card reader 206 reads the magnetic strip or encrypted data chip to obtain details associated with the card, including encrypted Personal Identification Number (PIN) data. The screen 102 is then used to display a message asking the user to enter a PIN, which the user then enters using the key pad 106. The input made is supplied to the encrypting PIN pad 202, which encrypts the entered number. The result of this encryption is compared with the encrypted PIN data read from the card and, assuming that there is a match, the user can access services though the ATM 100 by using the menu selection buttons 103 to select services shown on the screen 102. If the user asks for cash, the cash dispenser unit 204 will pick the required notes from a series of stacks of currency providing different denominations and transfer the cash to the dispensing slot 110, where it can be collected by the user.

[0028] Two further examples of start-up of the ATM 100 are now described. The process on 'first ever' start-up of the ATM 100 is described with reference to the flow chart of Figure 3. The validation process for components on each subsequent start-up is then described with reference to the flowchart of Figure 4.

[0029] Prior to 'first ever' start up, the ATM 100 is built using known source components to provide the encrypting PIN pad 202, the cash dispenser unit 204, the card reader 206 and the PC core 208 (step 302). In this context, by a 'known source' it is meant that that the manufacturer of the component 202, 204, 206 may be known and has been identified as a trusted source of high-quality, reliable components 202, 204, 206. The requesting means 216 of the PC core 208 requests manufacturer identity data from the components 202, 204, 206 via the system bus 120 (step 304). Each of the components 202, 204, 206 supply the requested data, which in this example comprises a serial number in step 306. This is then stored as persistent data in the memory 214 of the PC core 208 in step 306.

[0030] In each subsequent start-up (step 402), the requesting means 216 of the PC core 208 again requests manufacturer identity data from the components 202,

204, 206 via the system bus 120 (step 404). Each of the components 202, 204, 206 supply the requested data to the requesting means 216 in step 406. The comparing means 218 of the PC core 208 checks each of the supplied identities against those stored in the memory in step 408. If there is no change in any of the identity data, then the ATM start-up completes in step 409. If however the identity of one or more of the components has changed, the comparing means 218 of the PC core 208 checks to see whether the new components come from a trusted source in step 410.

[0031] In this embodiment, the identity of a component from a known source is in the form of a serial number which conforms to a predetermined format which can be processed to verify its authenticity. However, in other embodiments, the PC core 208 may be arranged to verify the identity against identities stored in a database, which may be remote from the ATM 100.

[0032] If the new components 202, 204, 206 do not come from a trusted source then the ATM 100 is disabled in step 412. If however the new components do come from a trusted source then the PC core 208 requests that the engineer enters security data to ensure that the installation of the new component(s) has been made by an authorized individual (step 414). In this example, the security data is provided in the form USB security dongle known in this context as a Service Security Key.

[0033] In step 416, the security means 220 of the PC core 208 checks whether the Service Security Key belongs to an authorized engineer. If this is not the case then the ATM 100 is disabled in step 418. If the engineer is authorized, then the PC core updates its memory 214 with the new identification data in step 420. The start up of the ATM 100 then completes in step 422.

[0034] It will be understood that the above description of a preferred embodiment is given by way of example only and that various modifications may be made by those skilled in the art. For example, the chips 212 could be replaced with Radio Frequency IDentification (RFID) tags or other remotely accessible data stores such as those readable using Bluetooth® or Infrared technologies. As these devices can be read remotely, this removes the need for a system bus 214.

Claims

1. A method of validating machine components in a self-service terminal comprising:

   providing at least one machine component with identity information in the form of a machine readable identifier;
   reading identity data from the machine readable identifier;
   comparing the identity data with stored identity data to determine if the identity of a component has changed; and
   if the identity has changed, comparing the identity data with source data to determine if the component is from a trusted source.

2. A method according to claim 1 which is carried out on start-up of the terminal.

3. A method according to claim 1, which comprises replacing the stored identity data with the identity data from a new component if the identity has changed and the component has proven to be from a trusted source.

4. A method according to claim 1, which comprises the step of verifying security data before the stored identity data is replaced with changed identity data.

5. A Self-service terminal processing unit comprising a memory for storing identity data, a requesting means arranged to request identity data from components of the terminal and a comparing means arranged to compare identity data received by the requesting means with identity data stored in the memory to detect any changes in identity data.

6. A processing unit according to claim 5 wherein the memory of comprises component source data and the comparing means is arranged to compare changed identity data with the source data to determine if the component derives from a trusted source.

7. A processing unit according to claim 5, which further comprises a security means arranged to receive security data from a maintenance operator and use the security data to determine whether a maintenance operator is an authorized operator.

8. A processing unit according to claim 5, which is arranged to allow a terminal with which it is associated to operate only if the or each component is from a trusted source.

9. A Self-service terminal comprising a self-service terminal processing unit comprising a memory for storing identity data, a requesting means arranged to request identity data from components of the terminal and a comparing means arranged to compare identity data received by the requesting means with identity data stored in the memory to detect any changes in identity data, further comprising at least one of the following components with associated identity data: an encrypting pin pad, a cash dispenser unit and a card reader, the terminal being arranged such that the identity data associated with the or each component can be read by the processing unit.

10. A self-service terminal according to claim 9 which comprises one of each of the components and the

processing unit is arranged to determine whether each of the components is from a trusted source and to allow the terminal to operate only if all the components are from a trusted source.

11. A self-service terminal according to claim 9, in which the identity data associated with the or each component is provided on a chip.

12. A self-service terminal according to claim 9, which is an Automated Teller Machine.

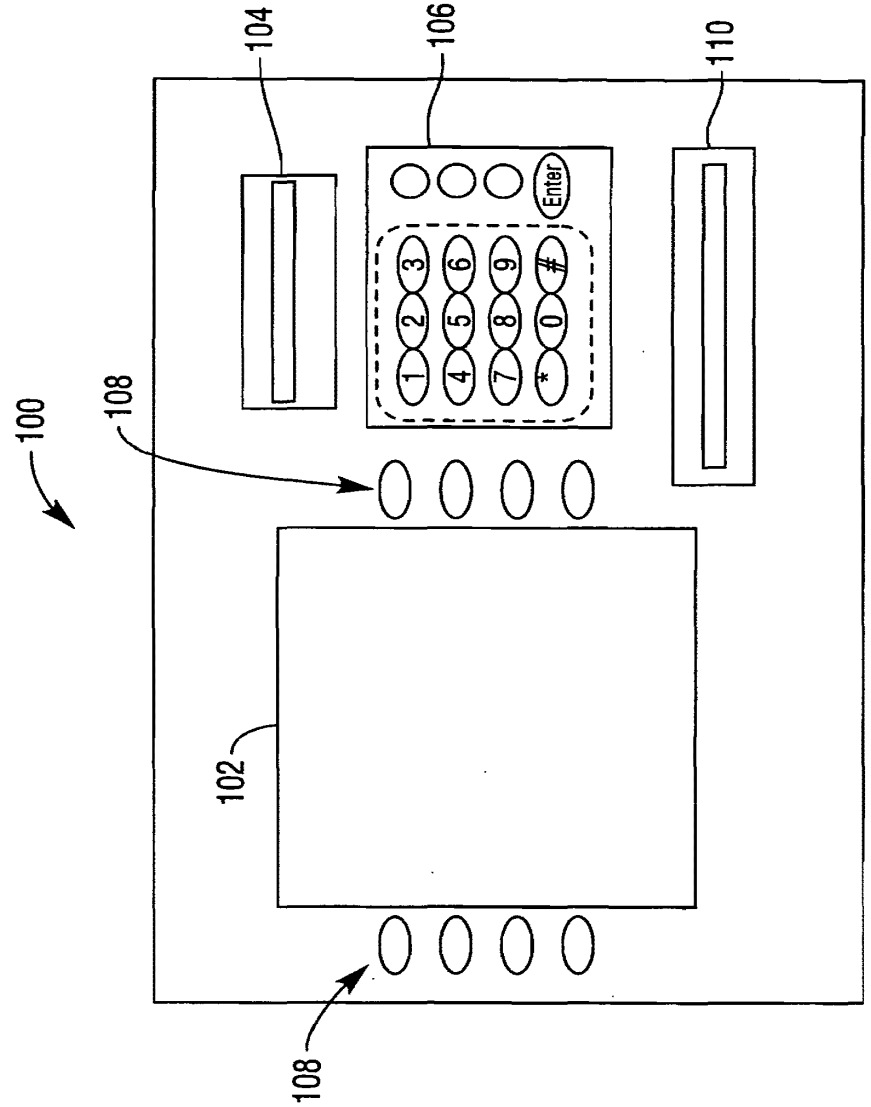


FIG. 1

FIG. 2

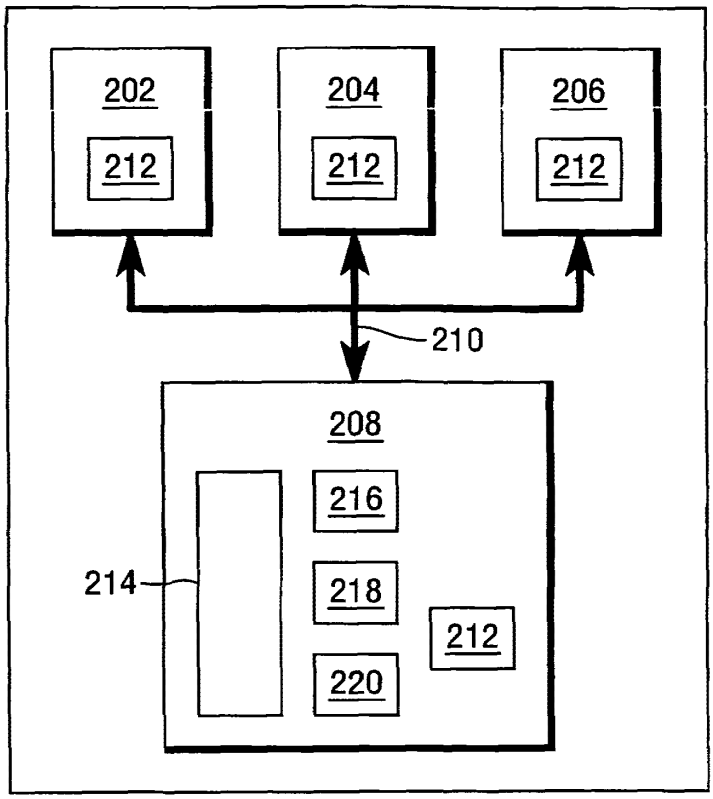
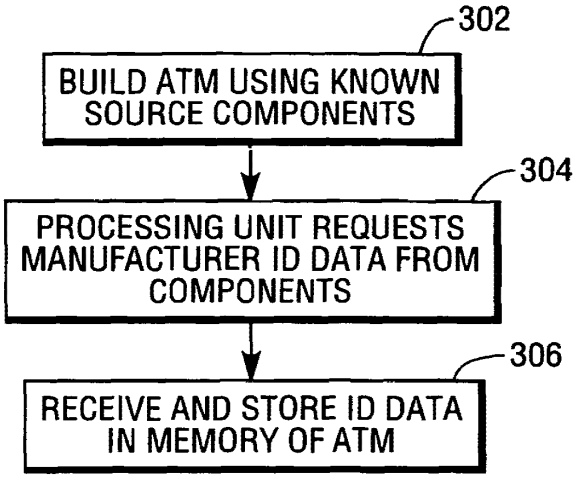


FIG. 3


302
BUILD ATM USING KNOWN SOURCE COMPONENTS
304
PROCESSING UNIT REQUESTS MANUFACTURER ID DATA FROM COMPONENTS
306
RECEIVE AND STORE ID DATA IN MEMORY OF ATM

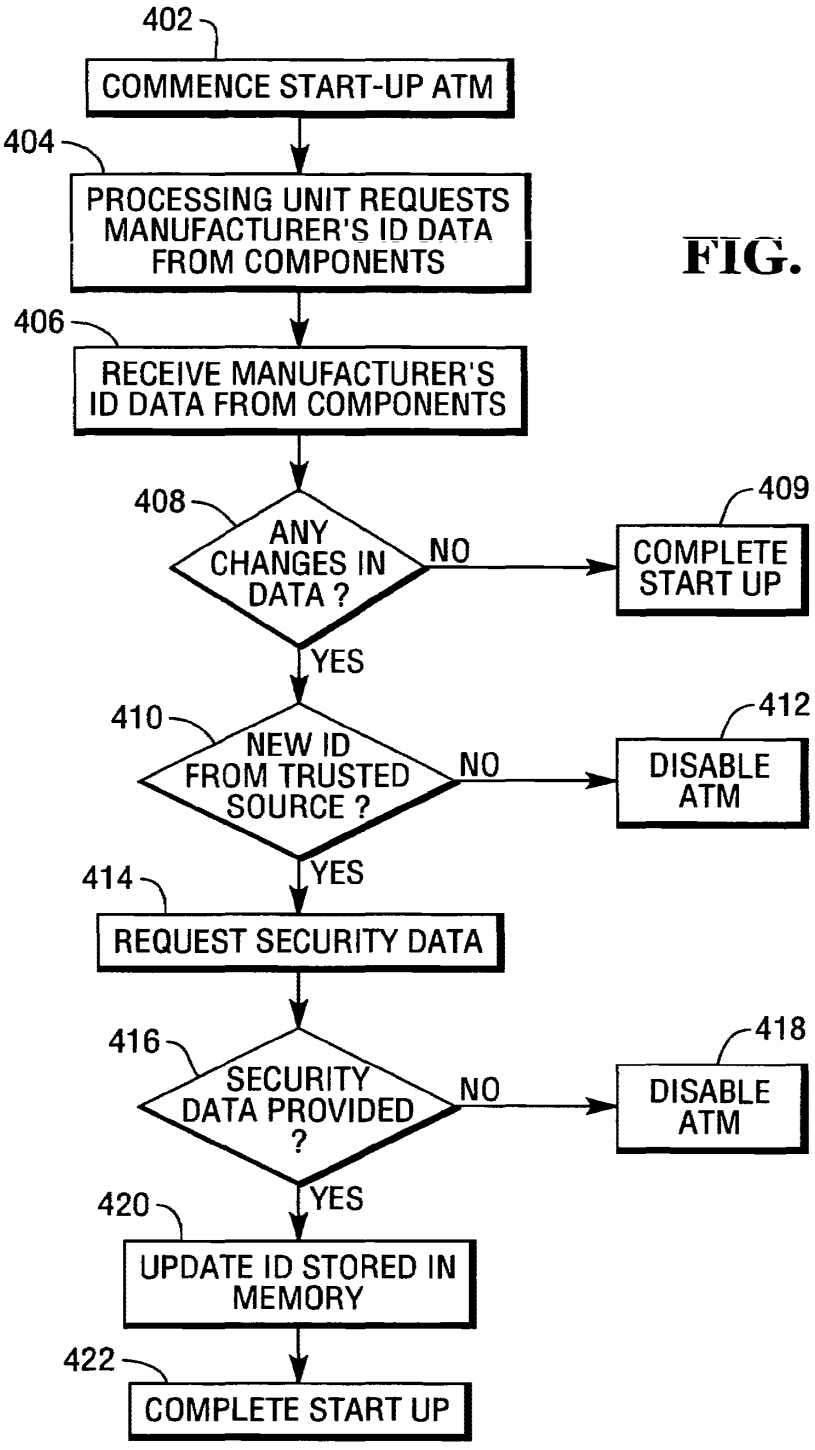

402
COMMENCE START-UP ATM
404
PROCESSING UNIT REQUESTS MANUFACTURER'S ID DATA FROM COMPONENTS
406
RECEIVE MANUFACTURER'S ID DATA FROM COMPONENTS
408
ANY CHANGES IN DATA ?
NO
409
COMPLETE START UP
YES
410
NEW ID FROM TRUSTED SOURCE ?
NO
412
DISABLE ATM
YES
414
REQUEST SECURITY DATA
416
SECURITY DATA PROVIDED ?
NO
418
DISABLE ATM
YES
420
UPDATE ID STORED IN MEMORY
422
COMPLETE START UP

FIG. 4

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 07 25 3584

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	WO 01/82035 A (SUN MICROSYSTEMS INC [US]) 1 November 2001 (2001-11-01) * abstract * * page 1, line 14 - line 20 * * page 2, line 7 - line 15 * * page 3, line 6 - line 15 * * page 7, line 21 - line 25 * * page 11, line 4 - line 11 * * page 14, line 24 - line 31 * * page 17, line 30 - page 18, line 2 *	1-12	INV. G07F7/10 G07F19/00
P,X	US 7 121 460 B1 (PARSONS DONALD [US] ET AL) 17 October 2006 (2006-10-17) * column 3, line 53 - line 58 * * column 9, line 29 - line 39 * * sentence 56 *	1-12	
A	US 2004/149818 A1 (SHEPLEY STEVEN [US] ET AL) 5 August 2004 (2004-08-05) * paragraph [0007] * * paragraph [0010] * * paragraph [0035] * * paragraph [0040] * * paragraph [0114] * * paragraph [0198] *	1-12	TECHNICAL FIELDS SEARCHED (IPC) G07F G07C

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	17 December 2007	Wolles, Bart

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 07 25 3584

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

17-12-2007

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0182035 A	01-11-2001	AU 5555301 A	07-11-2001
US 7121460 B1	17-10-2006	US 7229009 B1	12-06-2007
US 2004149818 A1	05-08-2004	US 2005269397 A1	08-12-2005

EPO FORM P0459

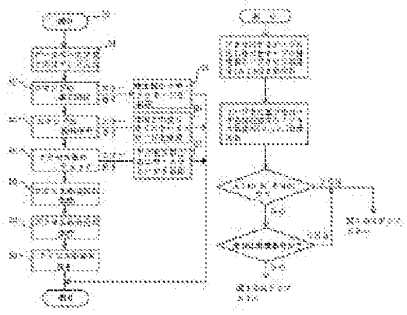
For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

ACCESS RIGHT MANAGEMENT CONTROL SYSTEMS FOR DATA BASE AND FILE SYSTEM

Publication number: JP5181734 (A)
Publication date: 1993-07-23
Inventor(s): KATO MASAMICHI; TASAKA MITSUNOBU +
Applicant(s): HITACHI LTD +
Classification:
- international: ***G06F12/00;*** **G06F12/00**; (IPC1-7): G06F12/00
- European:
Application number: JP19910358775 19911228
Priority number(s): JP19910358775 19911228

Abstract of **JP 5181734 (A)**

PURPOSE:To easily execute the access right management control of each data base and each file in a different distributed processing system by judging the permission or inhibition of an access in accordance with the size relation of access right numbers. CONSTITUTION:Judging processing compares an access right number Atno obtained from a table name management list with an access right number Auno applied from a user individual management list and judges whether the relation of Atno>=Auno is formed or not. When the access right number of the table is smaller than the user access right number, whether the sort of an access instruction is a reference instruction or not is checked. Since no access right is applied when the access instruction is not a reference instruction, processing is shifted to step 57 and an error message indicating access inhibition is returned to an access source. When the table access right number is larger or equal than/to the user access right number, the processing is shifted to step 58 and an access instruction string is formed. When the sort of the instruction is a reference instruction, the processing is shifted to the step 58 because of the existence of instruction execution right and an access instruction string is formed.



(12) UK Patent Application (19) GB (11) 2 391 965 (13) A

(43) Date of A Publication 18.02.2004

(21) Application No: 0218993.4

(22) Date of Filing: 14.08.2002

(71) Applicant(s):
MessageLabs Limited
(Incorporated in the United Kingdom)
1270 Landsdowne Court,
Gloucester Business Park, GLOUCESTER,
GL3 4AB, United Kingdom

(72) Inventor(s):
Alex Shipp

(74) Agent and/or Address for Service:
J A Kemp & Co.
14 South Square, Gray's Inn, LONDON,
WC1R 5JJ, United Kingdom

(51) INT CL[7]:
G06F 1/00 // G06F 1/00

(52) UK CL (Edition W):
G4A AAP

(56) Documents Cited:
WO 2002/033525 A2
IBM Technical Disclosure Bulletin, April 1990, "System for detecting undesired alteration of software"
Elsevier, Computers and Security, Vol 15 No 7, 1996, Vesselin Bontchev, "Possible macro virus attacks and how to prevent them", pages 595 to 626
"Proceedings of the second international virus bulletin conference", 2-3 September 1992, pages 1 to 14, Hruska J, "Virus Structure"

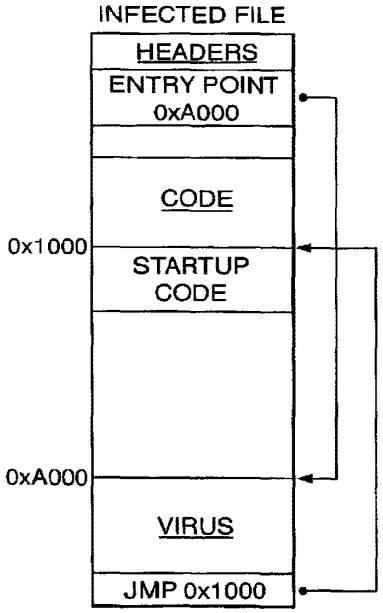
(58) Field of Search:
UK CL (Edition V) **G4A**
INT CL[7] **G06F**
Other: **WPI, EPODOC, PAJ, INSPEC, IBM TDB, IEEE, INTERNET**

(54) Abstract Title: **Heuristically detecting viruses in executable code**

(57) A method of, and system for, virus detection has a database of known patterns of start-up code for executable images created using a collection of known compilers and uses examination of the start-up code of the image by reference to this database to determine whether or not the executable image is likely to have been subject to infection by viral code. In particular, the system seeks to determine whether the expected flow and execution of the image during start up has had viral code interjected into it. Various heuristics to assist in assessing the likely presence of viral code are disclosed.

Fig.1b.

EXAMPLE OF VIRUS CHANGING PROGRAM ENTRY POINT



At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

GB 2 391 965 A

Fig.1a.

EXAMPLE OF VIRUS CHANGING PROGRAM ENTRY POINT

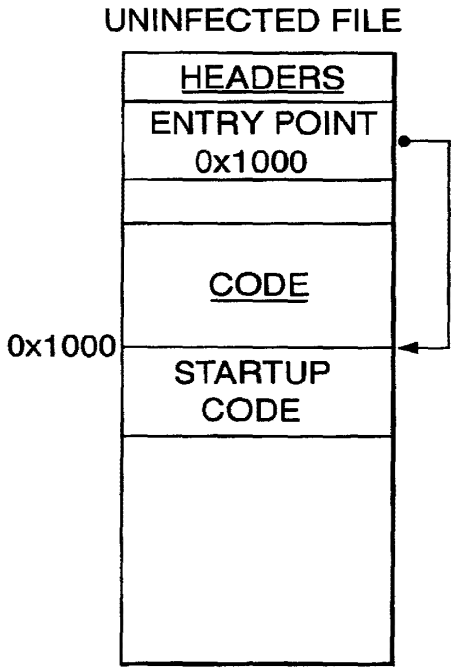


Fig.1b.

EXAMPLE OF VIRUS CHANGING PROGRAM ENTRY POINT

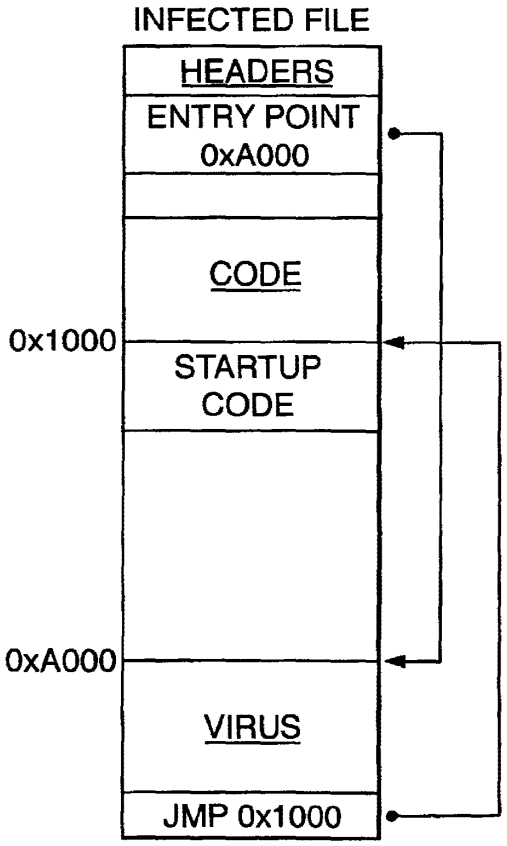


Fig.2a.

EXAMPLE OF VIRUS OVERWRITING CODE AT PROGRAM ENTRY POINT

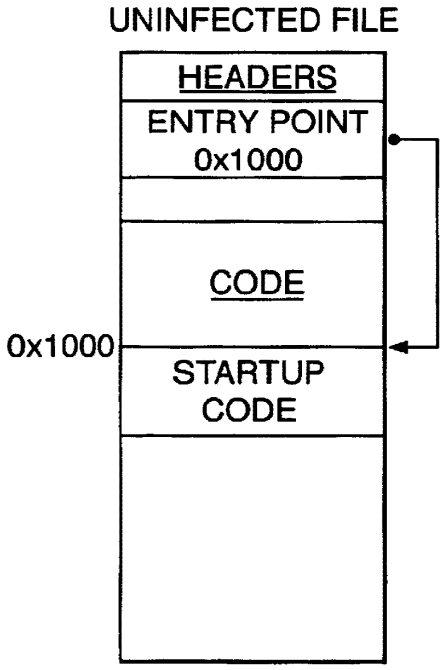


Fig.2b.

EXAMPLE OF VIRUS OVERWRITING CODE AT PROGRAM ENTRY POINT

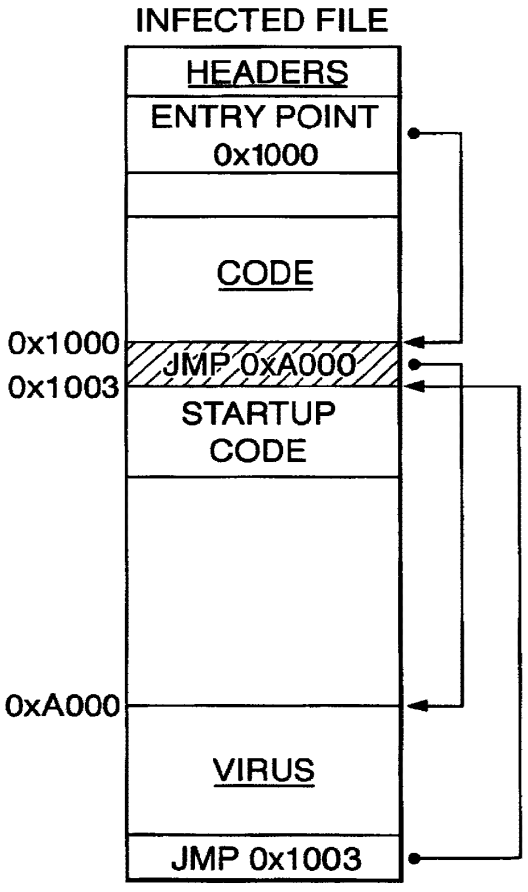
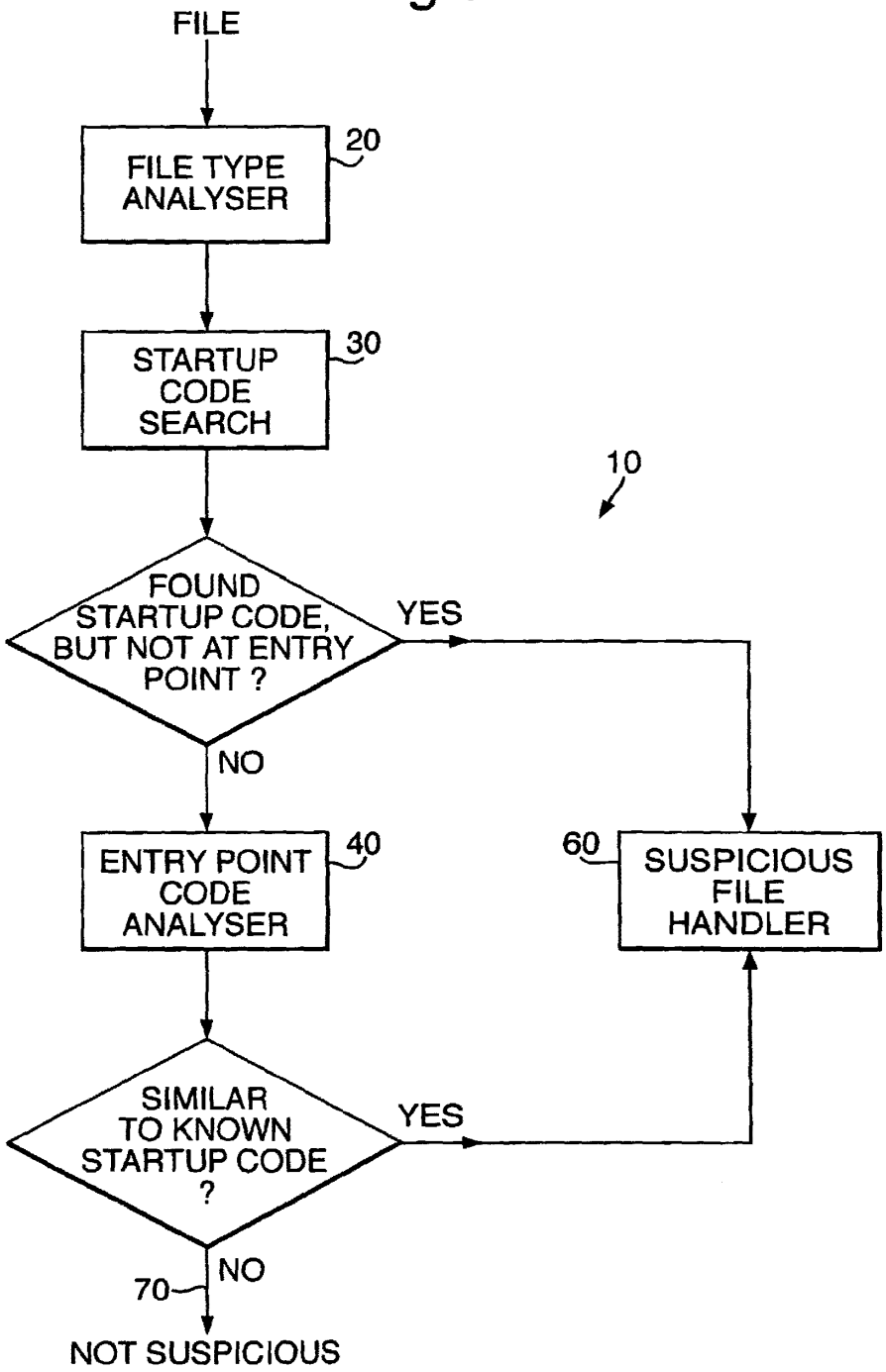


Fig.3.


FILE
FILE TYPE ANALYSER
20
STARTUP CODE SEARCH
30
10
FOUND STARTUP CODE, BUT NOT AT ENTRY POINT ?
YES
NO
ENTRY POINT CODE ANALYSER
40
60
SUSPICIOUS FILE HANDLER
SIMILAR TO KNOWN STARTUP CODE ?
YES
NO
70
NOT SUSPICIOUS

METHOD OF, AND SYSTEM FOR, HEURISTICALLY DETECTING VIRUSES IN EXECUTABLE CODE

The present invention relates to a method of, and system for, heuristically detecting viruses in executable code by searching the code for known startup sequences.

A common form of computer virus infection is where the virus's executable code is attached to, or embedded in, a program or other computer file containing executable code which appears, on the face of it, to be benign. One well-established method of virus propagation is where the virus, once activated on a host machine such as a user's PC, will attach itself to one or more programs found on the host in such a way that that program, once run, will execute the virus's code giving it the opportunity to propagate again and/or to undertake whatever other malignant behaviours (such as destruction of files, etc.) have been programmed into it. This method of propagation does, of course, provide an opportunity to detect the virus, for example by associating checksums with program files and detecting when this checksum changes. That is of course only one of the many strategies which have been devised to detect viruses.

Another well-known method of detecting viruses, implemented in many of the anti-virus software packages which are available, involves scanning program and other files for certain characteristic sequences of bytes (known as signatures) which indicate the likely presence of a virus. One of the practical problems with signature-based detection is that it requires some skill and a significant amount of time, when a new virus is first detected, to establish a suitable characteristic signature of it. This signature needs to be one which does not produce too many false positives and which does not misidentify the virus, for example as an existing one with a more benign payload. This signature information then needs to be disseminated to sites which use the anti-virus package in question before it can be used there to detect the newly-identificd virus. In recent years, many of the notable virus outbreaks have

involved viruses which propagate over the internet and it takes time for publishers of anti-virus software to react when a virus outbreak occurs.

Some internet service providers offer anti-virus scanning of internet traffic passing through their internet nodes as a value-added service.

The present invention relates to a method of virus detection which is intended to be useful for ISPs performing anti-virus scanning, e.g. of executables such as program files attached to emails, though it is by no means limited to that application and may be used in any anti-virus package.

According to the present invention there is provided a method of detecting virus infection of an executable image comprising:

identifying by reference to a database of known executable image layouts, the layouts to which the executable image conforms;

identifying start-up code within the executable image by reference to the identified image layout; and

examining the start-up code with reference to a database of start-up code characteristics to determine whether the image is likely to have been subject to viral modification.

The invention also provides a system for detecting virus infection of an executable image comprising:

means for identifying, by reference to a database of known executable image layouts, to which one of those layouts the executable image conforms;

means for identifying start-up code within the executable image by reference to the identified image layout; and

means for examining the start-up code with reference to a database of start-up code characteristics to determine whether the image is likely to have been subject to viral modification.

The invention will be further described by way of non-limiting example with reference to the accompanying drawings, in which:-

Figures 1a and 1b show an example of a virus changing the program entry point;

Figures 2a and 2b show an example of a virus overwriting code at the program entry point; and

Figure 3 shows a system according to the present invention.

Before proceeding with the description of the illustrated embodiment of the invention, some terms will be explained.

MD5 (message digest 5) checksum. MD5 is a one-way hashing algorithm – it generates a large number (the MD5 checksum) after analysing a byte stream – such as a file. The chances of two files generating the same large number are very small. It is also very difficult to create a file which will generate any particular MD5 checksum.

False positive: A false positive occurs when an anti-virus product identifies a particular file as being malware, whereas in fact it is not.

Regular expression: Regular expressions are strings which can be used to express patterns for pattern matching purposes. For instance, the perl regular expression

```
/^hello [0-9]+/
```

matches any string starting with the letters 'hello', then a space, then one or more digits. Some languages such as perl have native support for regular expressions; for others, libraries are available which implement regular expression matching.

Compiler: According to strict usage, a compiler generates one or more object modules from program source code. These object modules are typically not executable programs per se but require an additional step of linking by a linker. The action of a linker is typically to generate an image of an executable by linking together the object module(s), and external binary libraries which the module(s) reference; the production of the image may involve the pre-pending of a header region according to an executable file layout of a target operating system as well as the addition of resources such as bitmaps and the like. The term "compiler" as used herein is intended to include a linker, if required from a technical standpoint. What the compiler produces is not necessarily a stand-alone program, of course: compilers also produce executables such as dynamic link libraries and device drivers.

Program image: A program image is a sequence of bytes of executable code, which may exist on disk, in memory or in a network socket stream. In its on-disk form the image may be part of a program file which also includes a program header containing the information normally found in such programs.

To gain control, a virus must insert itself into the execution path of program code. Although, theoretically, the virus can insert itself anywhere in a program, if it inserts itself into the middle then this lessens the chance of it gaining control, since the place it inserts itself into may be executed rarely or never. Therefore, many viruses replace the startup code of programs with their own startup code. This guarantees they will be executed, giving them a better chance of survival. The on-disk image of an executable program must conform to a layout appropriate to the operating system and any given operating system may support a number of said layouts. At the time of writing the majority of Microsoft Windows ™ programs conform to the "Windows PE" layout. These layouts, as exemplified in Figure 1, usually begin with a header containing e.g. checksum and relocation tables for segment fix-ups which are carried out by the operating system's (OS) loader as it loads the program. At

some point the OS will hand over control to the program by a call to the program's entry point, which is indicated in the program header.

What happens after that depends on the nature of the program and on the compiler and linker which have been used to create it. Fully compiled, user-runnable, programs generally have a runtime library link which handles a number of common tasks. In particular, the runtime library usually contains routines which are involved at start-up and perform tasks such as setting up in-memory structures such as the program stack and heap. The program code written by the program's author generally assumes that these actions will have been performed by start-up code in the runtime library before the author's code begins to execute. All this is not to say that for a given compiler and linker and runtime library, the start-up code of a program created using them will be completely invariant, but rather that different programs compiled with the same compiler and linker and runtime library exhibit sufficient similarity, at least in terms of code found via the program entry point, to provide the basis for determining whether viral code has been patched into the program after it was compiled and linked.

To gain control at startup, a virus can change the program start point to point to the virus start code, or it can change part of the actual startup code, replacing it with a jump or call to its own code. Figure 1 shows an example of a virus changing the program start point to point to its own code. Figure 2 shows an example of a virus changing the startup code, replacing it with a jump to its own code.

As mentioned above, often a particular compiler and set of libraries will generate the same startup code for all, or a large proportion of programs it generates. Sometimes, this is because it starts with a standard library sequence that performs common tasks necessary during startup. Sometimes this is because the compiler generates applications in a particular way (eg Visual BASIC).

If it can be identified that a particular program contains the common startup code, but that the program does not actually start with this code, then this is very suspicious, and the program can be flagged as potentially containing a virus. This would be the case with the example in Figure 1.

If it can be identified that a particular program starts with code similar to the common startup code, but that the beginning of this code has been changed, then this is very suspicious, and the program can be flagged as potentially containing a virus. This would be the case with the example in Figure 2.

The operation of the present embodiment proceeds by examination of an image of a program, be it on disk, in memory, or part of a network packet stream, with reference to a database of characteristics of programs created using known compilers and a pattern matcher to determine whether the program image, in particular the start-up code deviates from what would be expected from that compiler in a way which makes the program suspicious.

Figure 3 shows one embodiment of the invention. For the purposes of illustration, it may be assumed that files to be scanned are delivered from an input queue and each one is processed by the system 10 shown in Figure 3.

1) By analysing the suspicious image using a file-type analyser 20, the type can be determined. For instance, it may be non-program, or program. Non-programs are not analysed further. Programs are further classified depending on their type – for instance, DOS, Windows PE, Windows NE, Linux ELF, Macintosh, etc. This analysis is done by file-type analyser 20. Note that in the case of a file image, the file type (e.g. .EXE, .DLL, etc.) should be disregarded.

2) Depending on the type of program, this can then be searched by start up code search 30 for appropriate start-up code against a database of start-up code sequences. For instance, Windows PE files may be searched for startup code created by the Microsoft Visual

Studio C compiler, Borland C compilers, the Microsoft Visual BASIC compiler and the Delphi compiler.

3) If the startup code search 30 determines that start-up code is found, but the program does not actually start with this code, then it hands to the suspicious file handler (step 6).

4) If entry point code analyser 40 determines that the program starts with code similar to known startup code, then go to the exception list step (6) which is handled by the suspicious file handler 60.

5) If execution arrives at the exit point 70 the program is flagged 'not suspicious' and no further action is taken.

6) The suspicious file handler 60 may make use of an exception list to prevent false positives. For instance, there may be genuine program files which appear to contain startup code, but do not, programs which contain recognised startup code but not at the entry point and programs which for some reason contain the startup code but start with some other code. These genuine files can be included in the exception list. The exception list can work in various ways, including but not limited to comparing the MD5 checksum of a file with a list of known checksums, or by searching the files for regular expressions, or by comparing the actual startup code with a list of known exception startup codes. If any exception list match occurs, no further action is taken.

A further consideration for which the suspicious file handler may be programmed to take account is that utility programs exist which "repackage" program files in certain ways. One such type of utility is the compression utility exemplified by Blinker (www.blink.com) which compresses an executable and adds a stub loader so that when the program is run, the stub loader is invoked and decompresses the executable's image. In most cases, the compression utility will compress the original executable's startup code which will

not therefore be found by pattern matching for startup code. However, supposing for some reason a particular startup code sequence was uncompressible, and therefore remained unaltered. This could then generate a false positive. To avoid this, an exception list entry could be created which would, in effect, say "Ignore all programs packed by Blinker". There are various ways to do this for the different utilities which exist, including detecting the startup code of their own which they insert in the executable image and also checking the section characteristics (such as name, sequence, flags) in layouts such as a PE file.

7) Otherwise, the program is flagged as possibly containing a virus. This may be used as an absolute decision, or combined with other heuristics to make an overall decision as to whether the program is viral or not.

Programs which are stopped as viral, but which do not turn out to be viral, can be analysed, and an exception list entry generated, so that similar false positives do not occur in future.

As well as using this as a stand-alone virus detection algorithm, this can be combined with other techniques as part of a larger system. For instance, programs flagged as viral by this method may be allocated a certain score, or variety of scores depending on the exact circumstances. Scores may also be assigned using other heuristic techniques, and only if the total score passes some limit is the program flagged as viral.

Once flagged as viral, any suitable remedial action may be taken, either by the system acting autonomously e.g. by moving the program file to a quarantine directory, or by signalling a human operator that intervention is required.

Example of examining a suspicious file

Following is a simplistic example of an algorithm for determining if a file is likely to be a Windows PE file, which may be implemented by the file type analyser 20.

Read in first 2 bytes. If these are not 'MZ' then stop
Read in another 58 bytes.
Read in 4 bytes into variable x (treating using intel byte-ordering)
Seek to offset x in file
Read in 4 bytes
If bytes are P E \0 \0, then file is likely to be a Windows PE file

Example of searching file for known startup code

The following is a common startup sequence for programs generated for the Microsoft Development Studio C compiler for the windows environment.

```
Hex bytes in file                  Human-readable disassembly

55                                 push    ebp
8B EC                              mov     ebp, esp
6A FF                              push    0FFFFFFFFh
68 10 11 00 01                     push    offset var1
68 80 22 00 01                     push    offset loc_1002280
64 A1 00 00 00 00                  mov     eax, large fs:0
50                                 push    eax
64 89 25 00 00 00 00               mov     large fs:0, esp
83 C4 E0                           add     esp, 0FFFFFFE0h
53                                 push    ebx
56                                 push    esi
57                                 push    edi
89 65 E8                           mov     [ebp+var_18], esp
C7 45 FC 00 00 00 00               mov     [ebp+var_4], 0
6A 01                              push    1
FF 15 40 10 00 01                  call    ds:__set_app_type
83 C4 04                           add     esp, 4
C7 05 B0 32 00 01 FF FF FF FF      mov     dword_10032B0, 0FFFFFFFFh
C7 05 B4 32 00 01 FF FF FF FF      mov     dword_10032B4, 0FFFFFFFFh
FF 15 4C 10 00 01                  call    ds:__p__fmode
8B 0D D0 30 00 01                  mov     ecx, dword_10030D0
89 08                              mov     [eax], ecx
FF 15 68 10 00 01                  call    ds:__p__commode
8B 15 CC 30 00 01                  mov     edx, dword_10030CC
89 10                              mov     [eax], edx
A1 64 10 00 01                     mov     eax, ds:_adjust_fdiv
8B 08                              mov     ecx, [eax]
89 0D B8 32 00 01                  mov     dword_10032B8, ecx
E8 16 01 00 00                     call    unknown_libname_2
A1 AC 30 00 01                     mov     eax, dword_10030AC
85 C0                              test    eax, eax
75 0E                              jnz     short loc_1002171
68 60 22 00 01                     push    offset unknown_libname_1
FF 15 60 10 00 01                  call    ds:__setusermatherr
83 C4 04                           add     esp, 4
E8 CA 00 00 00                     call    __setdefaultprecision
68 0C 30 00 01                     push    offset unk_100300C
68 08 30 00 01                     push    offset unk_1003008
E8 B1 00 00 00                     call    _initterm
83 C4 08                           add     esp, 8
8B 15 C8 30 00 01                  mov     edx, dword_10030C8
89 55 D8                           mov     [ebp+var_28], edx
```

```
8D 45 D8                lea     eax, [ebp+var_28]
50                      push    eax
8B 0D C4 30 00 01       mov     ecx, dword_10030C4
51                      push    ecx
8D 55 E0                lea     edx, [ebp+envp]
52                      push    edx
8D 45 D4                lea     eax, [ebp+argv]
50                      push    eax
8D 4D E4                lea     ecx, [ebp+argc]
51                      push    ecx
FF 15 58 10 00 01       call    ds:__getmainargs
83 C4 14                add     esp, 14h
68 04 30 00 01          push    offset unk_1003004
68 00 30 00 01          push    offset unk_1003000
E8 76 00 00 00          call    _initterm
83 C4 08                add     esp, 8
FF 15 30 10 00 01       call    ds:__p___initenv
8B 55 E0                mov     edx, [ebp+envp]
89 10                   mov     [eax], edx
8B 45 E0                mov     eax, [ebp+envp]
50                      push    eax
8B 4D D4                mov     ecx, [ebp+argv]
51                      push    ecx
8B 55 E4                mov     edx, [ebp+argc]
52                      push    edx
E8 40 F5 FF FF          call    _main
83 C4 0C                add     esp, 0Ch
89 45 DC                mov     [ebp+var_24], eax
50                      push    eax
FF 15 48 10 00 01       call    ds:exit
EB 22                   jmp     short loc_1002210
8B 45 EC                mov     eax, [ebp-14h]
8B 08                   mov     ecx, [eax]
8B 09                   mov     ecx, [ecx]
89 4D D0                mov     [ebp-30h], ecx
50                      push    eax
51                      push    ecx
E8 31 00 00 00          call    _XcptFilter
83 C4 08                add     esp, 8
```

```
    C3                                  retn
    8B 65 E8                            mov     esp, [ebp-18h]
    8B 55 D0                            mov     edx, [ebp-30h]
    52                                  push    edx
    FF 15 50 10 00 01                   call    ds:_exit
    83 C4 04                            add     esp, 4
    C7 45 FC FF FF FF FF                mov     [ebp+var_4], 0FFFFFFFFh
    8B 4D F0                            mov     ecx, [ebp+var_10]
    64 89 0D 00 00 00 00                mov     large fs:0, ecx
    5F                                  pop     edi
    5E                                  pop     esi
    5B                                  pop     ebx
    8B E5                               mov     esp, ebp
    5D                                  pop     ebp
    C3                                  retn
```

However, we cannot simply search for this particular byte pattern (55, 8B, EC, 6A, FF, 68, 10, 11, 00, 01, etc); many of the values are offsets to other routines or data structures, which will vary from program to program because they will be located in different places, and therefore have different offsets. For instance, the fourth instruction, push offset var1, has the byte sequence 68 10 11 00 01 in the example, because the variable var1 is located at offset 0x01001110 in this program. In another program, var1 may be located at a different offset (say 0x10011EF), and the fourth instruction will then have the byte sequence 60 EF 11 00 01.

A simplistic search could therefore match those bytes that are constant, and skip over the bytes that vary. For every byte in the program file, we attempt to see if the search pattern fits, and if it does we have found the code. If it does not, we carry on with the next byte in the file and so on until the end of the file is reached.

Match 1 byte: 55
Match 2 bytes: 8B, EC
Match 2 bytes: 6A, FF
Match 1 byte: 68
Skip the next 4 bytes
Match one byte: 68
Skip the next 4 bytes

...and so on until
Match 2 bytes 8B, E5
Match 1 byte 5D
Match 1 byte C3

A more detailed search could perform other checks on the bytes that vary. For instance, if the bytes are known from knowledge of the start-up code which the compiler generates to be an offset to a data structure containing a value such as 'Press any key to continue', the search could check that this offset actually contains this data. If they are an offset to a known routine, the search could recursively check that the known routine matches a correct pattern.

For instance, suppose that in the original pattern, that var1 contains the string 'hello'. The search algorithm might now be:

Match 1 byte: 55
Match 2 bytes: 8B, EC
Match 2 bytes: 6A, FF
Match 1 byte: 68
Read the next 4 bytes into variable offsetcheck1
Match one byte: 68
Skip the next 4 bytes

...and so on until
Match 2 bytes 8B, E5
Match 1 byte 5D
Match 1 byte C3

Then:
Move to the location held in offsetcheck1 (in our example, this would be 0x01001110).
Match the next 5 bytes: 'hello'
If we find this startup code pattern, we then check if it is located at the entry point of the program. If it is, then all is OK. If not, then this is flagged as suspect (startup code found, but program does not start with this code).

Example of searching file for changed startup code

Using the same example startup code as before, we could use the following algorithm to determine if the file contained changed startup code:

Go to offset of program start.
Skip 15 bytes
Match 6 bytes: 64, A1, 00, 00, 00, 00
Match 1 byte: 50
Match 7 bytes: 64 89 25 00 00 00 00

...and so on until
Match 2 bytes 8B, E5
Match 1 byte 5D
Match 1 byte C3

If code did not match, stop search.

If code does match, then the bytes from offset 15 onwards are part of a known startup sequence. If the first 15 bytes also match this startup sequence, all is OK. Otherwise this is potentially interesting. The checks therefore continue as follows.

Go to offset program start
Match 1 byte: 55
Match 2 bytes: 8B, EC
Match 2 bytes: 6A, FF
Match 1 byte: 68
Skip the next 4 bytes
Match one byte: 68
Skip the next 4 bytes

If all matches succeeded, then this is part of a known startup sequence.

Otherwise,this is flagged as 'changed startup code'.

CLAIMS

1. A method of detecting virus infection of an executable image comprising:

identifying by reference to a database of known executable image layouts, the layouts to which the executable image conforms;

identifying start-up code within the executable image by reference to the identified image layout; and

examining the start-up code with reference to a database of start-up code characteristics to determine whether the image is likely to have been subject to viral modification.

2. A method according to claim 1, wherein the database of start-up code characteristics includes patterns characteristic of start-up code generated by a set of known compilers.

3. A method according to claim 2 for scanning the executable image for patterns of start-up code expected to be present as a consequence of that compiler having been used to create the executable image and determining, in regard to patterns so found, whether there is evidence of viral code interposed in the execution path from the entry point of the executable image.

4. A method according to claim 3 wherein, if it is determined that the executable image contains known start-up code but that execution of the image will not actually start with that code, flagging the image as suspicious from the point of view of possibly containing viral code.

5. A method according to claim 3 or 4 wherein, if it is determined that the executable image starts with code similar to the known start-up code but the beginning of this code has been changed, flagging the image as suspicious from the point of view of possibly containing viral code.

6. A method according to any one of the preceding claims wherein the start up code database includes records of data values associated with routines which form part of the start up code and including the step of identifying the data in the executable image corresponding to at least one such data value and comparing it with that value.

7. A system for detecting virus infection of an executable image comprising:

means for identifying, by reference to a database of known executable image layouts, to which one of those layouts the executable image conforms;

means for identifying start-up code within the executable image by reference to the identified image layout; and

means for examining the start-up code with reference to a database of start-up code characteristics to determine whether the image is likely to have been subject to viral modification.

8. A system according to claim 7, wherein the database of start-up code characteristics includes patterns characteristic of start-up code generated by a set of known compilers.

9. A system according to claim 8 for scanning the executable image for patterns of known startup code and determining, in regard to patterns so found, whether there is

evidence of viral code interposed in the execution path from the entry point of the executable image.

10. A system according to claim 9 wherein, if it is determined that the executable image contains known start-up code but that execution of the image will not actually start with that code, flagging the image as suspicious from the point of view of possibly containing viral code.

11. A system according to claim 9 or 10 wherein, if it is determined that the executable image starts with code similar to the expected start-up code but the beginning of this code has been changed, flagging the image as suspicious from the point of view of possibly containing viral code.

12. A system according to any one of claims 7-11 wherein the start up code database includes records of data values associated with routines which form part of the start up code and including means for identifying the data in the executable image corresponding to at least one such data value and comparing it with that value.

13. A method of detecting virus infection of an executable image substantially as hereinbefore described and with reference to the accompanying drawings.

14. A system for of detecting virus infection of an executable image substantially as hereinbefore described and with reference to the accompanying drawings.

Application No:	GB 0218993.4	**Examiner:**	Michael Powell Waters
Claims searched:	1 to 14	**Date of search:**	10 April 2003

Patents Act 1977 : Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
Y	1 and 7	WO 2002/033525 A2 (CHUANG) see whole document
Y	1 and 7	IBM Technical Disclosure Bulletin, April 1990, "System for detecting undesired alteration of software"
Y	1 and 7	Elsevier, Computers and Security, Vol 15 No 7, 1996, Vesselin Bontchev, "Possible macro virus attacks and how to prevent them", pages 595 to 626, see section 2.2.1.
Y	1 and 7	"Proceedings of the second international virus bulletin conference", 2-3 September 1992, pages 1 to 14, Hruska J, "Virus Structure", see section 1.1 and figure 5

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC[V]:

G4A

Worldwide search of patent documents classified in the following areas of the IPC[7]:

G06F

The following online and other databases have been used in the preparation of this search report:

WPI, EPODOC, PAJ, INSPEC, IBM TDB, IEEE, INTERNET

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 September 2006 (28.09.2006)

PCT

(10) International Publication Number
WO 2006/102399 A1

(51) International Patent Classification:
G06F 21/00 (2006.01)

(21) International Application Number:
PCT/US2006/010381

(22) International Filing Date: 20 March 2006 (20.03.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/663,496	18 March 2005 (18.03.2005)	US
60/663,615	18 March 2005 (18.03.2005)	US
60/756,796	7 January 2006 (07.01.2006)	US

(71) Applicant *(for all designated States except US)*: **ABSOLUTE SOFTWARE CORPORATION** [CA/CA]; 111 Dunsmuir Street, Suite 800, Vancouver, BC V6B 6A3 (CA).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **GARDNER, Philip, B.** [US/US]; 1765 Spinaker Drive, Woodbury, Minnesota 55125 (US).

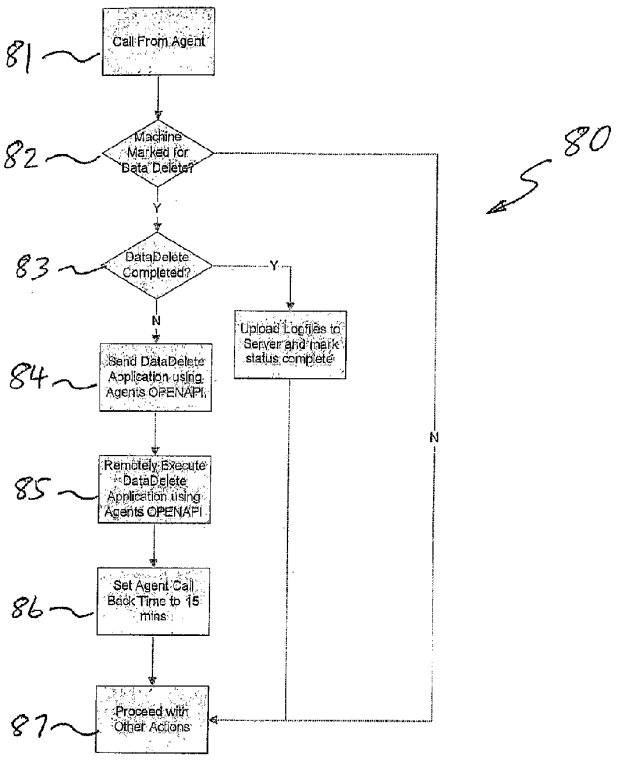
(74) Agent: **LIU, Wen**; LIU & LIU, 444 S. Flower Street, Suite 1750, Los Angeles, California 90071 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: PERSISTENT SERVICING AGENT



(57) Abstract: A tamper resistant servicing Agent for providing various services (e.g., data delete, firewall protection, data encryption, location tracking, message notification, and updating software) comprises multiple functional modules, including a loader module (CLM) that loads and gains control during POST, independent of the OS, an Adaptive Installer Module (AIM), and a Communications Driver Agent (CDA). Once control is handed to the CLM, it loads the AM, which in turn locates, validates, decompresses and adapts the CDA for the detected OS environment. The CDA exists in two forms, a mini CDA that determines whether a full or current CDA is located somewhere on the device, and if not, to load the full- function CDA from a network; and a full-function CDA that is responsible for all communications between the device and the monitoring server. The servicing functions can be controlled by a remote server.

WO 2006/102399 A1

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

PERSISTENT SERVICING AGENT

This application claims the priority of U.S. Provisional Application No. 60/663,496, filed March 18, 2005, U.S. Provisional Application no. 60/663,615, filed March 18, 2005, and U.S. Provisional Application no. 60/756,796, filed January 7, 2006. This application is a continuation-in-part application of U.S. Patent Application No. 11/093,180, filed March 28, 2005. These documents are fully incorporated by reference as if fully set forth herein.

All publications referenced herein are fully incorporated by reference, as if fully set forth herein.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a persistent or tamper resistant servicing agent in a computer and network environment.

2. Description of Related Art

In today's competitive business environment, information technology (IT) is playing an increasingly important role in the exchange of knowledge in day-to-day business functions. Individuals, systems, organizations, and other business assets are interconnected in this emerging economic web, and as this IT landscape grows increasingly complex, so does the need to efficiently manage computer assets. As a result, organizations now, more than ever, are recognizing the need to take control of, manage and secure their computer asset base, in order to maximize their investment and attempt to control costs.

The amount of time and fiscal resources required to manage computers in a network can be significant. These assets support key business processes such as e-commerce and business intelligence. If these assets are not protected, and there is no ability to proactively manage them, the potential for short and long-term loss is enormous.

One of the main challenges organizations are encountering is the ability to manage a specific software image and required updates on the device storage drive, and to track the location and ongoing migration of their computers. Knowing what assets one has and how they are changing in time is fundamental to ongoing IT asset and policy management. This knowledge also enables better planning and budgeting, such as hardware or software upgrades, or computer retirement. This problem is further compounded as companies expand geographically, and as the adoption of mobile and remote systems becomes increasingly popular. Keeping track of these assets and the software images on them is not only important for the value of the computer itself, but often more importantly, for the protection of the valuable data residing on the machine. A missing or misconfigured asset may have readable confidential

or proprietary information on it, or not have anti-virus updated, or it may still have rights to access a corporate network. Companies must be able to account for their assets and their configuration; and know not only what is on them in terms of hardware and software, but also where they are, and who is using them. Only with this additional information can organizations begin to address issues of security and regulatory compliance with remote and mobile users.

With the increase in processing power for mobile computing devices, more and more individuals have opted for mobile computing devices, either as replacements to their desktop units, or as additional devices for home or small business networks. While individuals are not primarily concerned with computer asset inventory and configuration management, they nonetheless share similar concerns as large organizations, in regards to keeping track of personal computer assets and protection of personal data.

Most IT departments will support the statement that conventional asset management solutions can't accurately account for the ever-increasing population of remote and mobile users. In fact, a typical organization will lose up to 15% of its PC assets over a 2 year period to PC drift1 – where assets are not necessarily lost or stolen, but they simply cannot be accounted for due to the many times they've changed owners or departments since first being provisioned. On average, most organizations can only accurately identify 65% of their actual PC asset base when asked to do an inventory. Best practices demands that IT know where at least 90% of PC assets are located at all times.

Remote and mobile computer assets that travel outside a LAN are problematic in a number of ways. Initially, most asset tracking software cannot track these machines when they are not connected to the local network. Also, these remote machines pose a large security threat to the entire IT network. More often than not the remote user is responsible for the administration and configuration updating of the machine rather than the IT administrator. Most users are normally not as security conscious as they should be. Users may lower security settings, install malicious software unknowingly, let anti-virus software fall out of date and fail to install the latest security patches. What may seem like minor security faults to a remote user can have drastic effects on the entire network. When the remote user connects the LAN they may infect the entire network due to these relaxed security concerns. Without effective asset management tools for these remote machines IT administrators cannot ensure the integrity of the entire network. A network is only as secure as its weakest link. The annual CSI/FBI survey on computer security shows that 57% of stolen PC assets are used to perpetrate additional crimes against corporations.

In a response to recent corporate accounting scandals, identity theft and malicious hacking, governments are establishing regulations that force businesses to protect and be accountable for all sensitive digital information. The Sarbanes-Oxley Act of 2002 is an excellent example of such a regulation. With Sarbanes-Oxley there is increased exposure when not accurately reporting assets.

Executives are asked to legally verify if the proper controls and regulations are in place to ensure accurate asset reporting. It is now the fiduciary responsibility of the CFO and CEO to ensure that accurate asset reporting is performed. The legal, regulatory and financial exposure to an organization that inaccurately reports its asset base could be significant. Computers often make up a material percentage of an organizations asset base and thus require accurate reporting. The Gramm-Leach-Bliley (GLB) Act is another regulation to ensure customer records are protected in the financial sector. Likewise, the Health Insurance Portability and accountability Act (HIPAA) established federal privacy standards to protect the confidentiality of medical records and health information. If organizations do not effectively track all of their computing assets there could be severe regulatory concerns.

For an asset tracking and/or configuration management application to undertake its tracking function, it should be able to resist certain level of tampering by a user. In the context of asset tracking, typically, an authorized user is a person responsible for some aspect of the life-cycle management of the computer. In this context, the tracking agent should be able to protect the authorized user from the accidental removal of the tracking agent, while allowing the legitimate need to disable the agent (for example at end of life of the computer asset). An unauthorized user is a person who wishes to remove the agent software, but who is typically not responsible for the life-cycle management of the computer. A reason for a deliberate, unauthorized attempt to remove the agent would include actions of a thief or potential thief who wishes to ensure that any tracking software is permanently removed. An attempt of un-authorized yet accidental removal would include someone's successful or unsuccessful attempt to install a new operating system, or re-image the hard drive, for example.

Attempts to track, manage and update PC assets and their configurations are further challenged in view of the fact that during a PC's lifecycle it will undergo many hardware, software and image changes including: break/fix repairs, configuration changes, operating system reinstalls, hard-drive reformats/replacements, system crashes and user-driven configuration changes. Many of these changes will require a reinstallation of the operating system whereby the original footprint, identification or tracking agent of the PC asset can be disabled or removed. This change, if not diligently recorded and tracked, is the beginning of a PC asset drifting from a known state into an unknown state. These routine PC life cycle operating requirements can increase the complexity and challenge of tracking PC assets, especially those that are remote and mobile.

Heretofore, existing asset tracking applications are deficient in the Windows NT/2000/XP environment to the extent that they do not display the features necessary to achieve the required persistence against tampering by unauthorized users. These tracking applications are generally easily

defeated by the unauthorized or accidental user actions referred above, or other simple acts such as deletion of registry settings or deletion of application files.

Absolute Software Corporation, the assignee of the present invention, has developed and is marketing Computrace, a product and service that securely tracks assets and recovers lost and stolen assets, and AbsoluteTrack, a secure asset tracking, and inventory management, solution powered by the Computrace technology platform. Computrace deploys a stealth agent, which is a software client that resides on the hard drive of host computers. Once installed, the agent automatically contacts a monitoring center on a regular basis transmitting location information and all auto-discovered asset data points. Ongoing communication between the agent and the monitoring center requires no user intervention and is maintained via an Internet or phone connection. As long as the computer is turned on and has either a connection to a telephone line or access to the Internet (through an ISP or through a company network), the Computrace agent will be able to report asset data to the monitoring center. The user intervention-free communication between the agent and a monitoring center ensures the authorized user of the agent to have secure access to up-to-date location information and comprehensive asset data about their entire computer inventory. Whether used stand-alone, or as a complement to an existing asset management tool, AbsoluteTrack has been a cost-effective application service for helping businesses of all sizes monitor remote, mobile and desktop computers and perform daily hardware and software inventory tracking functions. Computrace has been an effective tool to track theft of mobile computers, and to recovery of stolen mobile computers.

The technology underlying various Computrace products and services have been disclosed and patented in the U.S. and other countries, which patents had been commonly assigned to Absolute Software Corporations. See, for example, U.S. patent nos. 5,715,174; 5,764,892; 5,802,280; 6,244,758; 6,269,392; 6,300,863; and 6,507,914; and related foreign patents. Further information concerning AbsoluteTrack has been published by Absolute Software Corporation (e.g., AbsoluteTrack – Secure Computer Asset Tracking Solution, a white paper, published April 25, 2003).

The agent that is deployed on each protected device is stealthy, making it resistant to detection by the user of the computer. The level of tamper-resistance directly impacts the difficulty of detection and level of skill required to defeat the Computrace service. While the Computrace agent is as tamper-resistant as a disk-based utility can be, it would be desirable to develop an improved agent that provide additional level of tamper-resistance, and further enable, support and/or provides services beyond asset tracking and recovery.

SUMMARY OF THE INVENTION

The present invention is directed to a servicing Agent for enabling, supporting and/or providing services relating to management and protection of assets (including without limitation hardware, firmware, software, data, etc.) and their software configurations, with improved tamper resistance. The services may include asset tracking, asset recovery, data delete, software deployment, etc.

The servicing Agent comprises multiple modules. Each module is designed to function in a specific operating environment. The modular design provides flexibility in configuring the agent for deployment in the particular operating environment, for example, in the BIOS or on the hard drive, without having to rebuild the entire application. The Agent may be implemented wholly or partly by software (including hardware microcode), and may reside in software, firmware and/or hardware components within a system.

In accordance with one aspect of the invention, a loader module is loaded and gains control during power-on self-test (POST). The Agent can be relied upon to enable, support and/or provide services (e.g., tracking, data delete and software updates) with respect to the device in which it is installed, as well as assets associated with the device in which the Agent is installed. Once control is handed to the loader, it acts to load other functions and modules of the Agent, including as necessary and at the appropriate time, the reloading across the network (e.g., Internet) of portions of the Agent that may have been removed or missing from the machine. The servicing Agent has the ability to be persistent in spite of actions that might ordinarily be expected to remove it.

In one embodiment of the present invention, at least one module and/or data for the agent code of the persistent Agent is implemented in the firmware of a device, such as a ROM, and in particular the basic input output system (BIOS) or its functional equivalent, resident in the device. The servicing Agent can load itself to be ready to perform its designed servicing function (e.g., tracking, data delete and software updates), independent of the operating system of the device, and can adapt itself to the environment (e.g., the operating system of the device) that controls certain basic operations (e.g., input/output) of the device by detecting the operating environment, so that the Agent can make use of such basic operations of the system to perform its designed servicing functions.

In another embodiment, the persistent agent comprises three main modules, including the "Computrace" Loader Module (CLM), the Adaptive Installer Module (AIM), and the Communications Driver Agent (CDA). The CLM loads the AIM, which in turn locates, validates, decompresses and adapts the CDA for the detected OS environment. In one embodiment, the CDA exists in two forms, a partial or mini CDA and a full-function CDA. The function of the mini CDA is to determine whether a full or current CDA is located somewhere on the device, and if not, to load the full-function CDA across the network (e.g., Internet) from a monitoring server. The full-function CDA is then responsible for all

communications between the device and the monitoring server. In another embodiment, the different modules, and in particular the CLM, may be programmable, which may require custom functionality to adapt to their specific environment. By providing Agent in several modules, the level of customization could be kept to a minimum. In one embodiment, at least the CLM is stored in firmware, such as the BIOS, with one or more of the other modules stored in hard drive partition gap, or the hard drive Host Protection Area (HPA). In another embodiment, the CLM is stored in a substitute Master Boot Record (MBR), or a combination of the foregoing.

In another aspect, the servicing functions that the Agent performs can be controlled by a remote server, by combining generic sub-function calls available in the Agent. This programmable capability of the Agent allow its functionality to be extended based on server-driven commands. The extensibility is critical to the successful deployment of the Agent in firmware, such as the BIOS, where space is at a premium and frequent updates to add or change functionality is not economical. The extensibility feature is a primary component of the activation process and the reactivation process of the Agent.

In another aspect of the present invention, the extensibility of the Agent enables a data delete application, for erasing data stored at the client device.

In yet another aspect of the present invention , the extensibility of the Agent enables software updates to be delivered and programmed onto the client device.

The invention improves upon the ability for a pre-deployed servicing Agent to remain "active" regardless of the actions of a "user" of the device. In the context of the invention, "active" refers to the specific ability of a component of the Agent software to load itself and then reconstruct its full capabilities over a wide range of "user" actions, including, for example in one embodiment, low-level commands to format the hard drive, re-installation of an operating system, re-imaging of the hard drive using an imaging utility, and replacement of the hard drive. "User" refers to an individual who is performing these actions and may be acting in an authorized or unauthorized capacity. Their actions to remove the Agent may be intentional or accidental.

The invention protects the authorized user from the accidental removal of the servicing Agent, while allowing the legitimate need to disable the Agent (for example at end of life of the computer asset). The invention prevents an unauthorized user from removing the Agent software. The persistent attributes of the present invention have value in asset protection, data and network security, IT asset management, software deployment, and other types of applications. In the context of a secure, stealthy device-tracking software application, the invention is of significant value as it makes theft of a valuable asset much more difficult to conceal, as regardless of actions taken by a thief, the software will persist and make itself available for contacting a remote monitoring center. In addition, the persistent nature of the servicing

Agent provides peace of mind to security personnel, as it provides confidence that the Agent cannot be accidentally removed. In the context of a secure asset management application, this is of further value as it ensures continuity of tracking an asset over its whole lifecycle. A key challenge for IT administrators today is the ability to track assets over the whole lifecycle. During the lifecycle devices are frequently transferred from one user to another, during which they may be re-imaged, or have the operating system reinstalled or otherwise be subjected to maintenance procedures that render tracking of the asset difficult, but which is made easier by the present invention. In addition to asset tracking services, other services can be enabled, supported and/or provided by the persistent and extensible Agent.

BRIEF DESCRIPTION OF THE DRAWINGS

For a fuller understanding of the nature and advantages of the present invention, as well as the preferred mode of use, reference should be made to the following detailed description read in conjunction with the accompanying drawings. In the following drawings, like reference numerals designate like or similar parts throughout the drawings.

FIG. 1 is a schematic diagram depicting representative communication links including networks by which asset tracking may be implemented in accordance with one embodiment of the present invention.

FIG. 2 is a schematic diagram depicting attachment of a PCI Option ROM to the BIOS, which includes the Persistent Agent, in accordance with one embodiment of the present invention.

FIG. 3 is a schematic diagram depicting the module components of the Persistent Agent present in the PCI Option ROM, in accordance with one embodiment of the present invention.

FIG. 4 is a schematic flow diagram depicting the Option ROM loading routine, in accordance with one embodiment of the present invention.

FIG. 5 is a schematic flow diagram depicting the routine performed by the CLM of the Persistent Agent, in accordance with one embodiment of the present invention.

FIG. 6a and 6b are schematic flow diagrams depicting the routine performed by the Interrupt Handler of the CLM, in accordance with one embodiment of the present invention.

FIG. 7 is a schematic flow diagram depicting the routine performed by the AIM of the Persistent Agent, in accordance with one embodiment of the present invention.

FIG. 8 is a schematic flow diagram depicting the Installer Mode routine of the CDA of the Persistent Agent, in accordance with one embodiment of the present invention.

FIG. 9 is a schematic flow diagram depicting the Service Mode routine of the CDA, in accordance with one embodiment of the present invention.

FIG. 10 is a schematic depiction of the CDA in Application Mode, in accordance with one embodiment of the present invention.

FIG. 11 is a schematic depiction of Flash Image Management, in accordance with one embodiment of the present invention.

FIG. 12 is a schematic depiction of Host Protected Area Image Management, in accordance with one embodiment of the present invention.

FIG. 13 is a schematic depiction of Partition Gap Image Management, in accordance with one embodiment of the present invention.

FIG. 14 is a schematic depiction of a communication session between the CDA of the Persistent Agent and the remote server, in accordance with one embodiment of the present invention.

FIG. 15 is a schematic flow diagram depicting the client side Date Delete routine of the CDA in accordance with one embodiment of the present invention.

FIG. 16 is a schematic flow diagram depicting the server side Data Delete routine in accordance with one embodiment of the present invention.

FIG. 17 is a schematic flow diagram depicting the Data Delete executable routine in accordance with one embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The present description is of the best presently contemplated mode of carrying out the invention. This description is made for the purpose of illustrating the general principles of the invention and should not be taken in a limiting sense. The scope of the invention is best determined by reference to the appended claims. The present invention can find utility in a variety of implementations without departing from the scope and spirit of the invention, as will be apparent from an understanding of the principles that underlie the invention. For purpose of illustrating the features of the persistent Agent of the present invention, reference is made to asset tracking as one example of the services provided by the Agent, and a tracking Agent, and data delete as another example of the services provided by the Agent. It is understood that the Agent may be used for other services, such as distribution of software and updates, without departing from the scope and spirit of the present invention.

The detailed descriptions that follow are presented largely in terms of methods or processes, symbolic representations of operations, functionalities and features of the invention. These method descriptions and representations are the means used by those skilled in the art to most effectively convey the substance of their work to others skilled in the art. A software implemented method or process is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. These steps require physical manipulations of physical quantities. Often, but not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It will be further appreciated that the line between hardware and software is not

always sharp, it being understood by those skilled in the art that software implemented processes may be embodied in hardware, firmware, or software, in the form of coded instructions such as in microcode and/or in stored programming instructions.

Tracking System Overview

Asset tracking function is an example of the services that can be enabled, supported and/or provided by the persistent Agent of the present invention. Referring to Fig. 1, the asset tracking system in accordance with one embodiment of the present invention involves a client/server architecture, which may comprise the following main components: (a) client device A consisting of any one of the electronic devices shown which have been implanted with the Agent. The Agent software runs on the client devices for the purpose of reporting asset, location and other information, and receiving instructions from a remote server to program the Agent to support and execute a desired function. The invention provides the ability of the agent software to be more persistent to accidental or deliberate removal and the programmability of the client from the monitoring server; (b) a communication link B, such as an information exchange network, which may include switched communications networks, the Internet, private and public intranet, radio networks, satellite networks, and cable networks; and (c) a host monitoring system C, which include a host monitoring server 3 that monitors the communications between the client device A and the host monitoring system C, which is contacted on a regular basis by the client devices records information from the client devices. The monitoring server also provides instructions to the client on what actions to perform, including what actions the client is to perform, what data to collect and the clients next scheduled call time. The client devices contact the monitoring server via the communication link B (e.g., an IP connection or via a dial-up telephone connection). The monitoring server can perform its functions either as a service offered over the Internet, or as a customer-owned server over a corporate intranet. The host monitoring system C may include a reporting and administration portal, which provides customers, administrators and asset tracking service providers the ability to view data and manage the functions of the monitoring server and the client devices. The host monitoring server can notify customers, designated representative and law enforcement agencies concerning status of asset monitoring via a number of communication means. Each of these components will be further elaborated below.

Referring to FIG. 1, useful client devices A in which the persistent servicing Agent in accordance with the present invention can be implemented include, but are not limited to, general or specific purpose digital processing, information processing and/or computing devices, which devices may be standalone devices or a component part of a larger system (e.g., a mass storage device), portable, handheld or fixed in location. Different types of client devices may be implemented with the servicing Agent application of the present invention. For example, the servicing Agent application of the present invention may be applied to

desktop client computing devices, portable computing devices (e.g., laptop and notebook computers), or hand-held devices (e.g., cell phones, PDAs (personal digital assistants), personal electronics, etc.), which have the ability to communicate to an external server, as further explained below. The client devices may be selectively operated, activated or configured by a program, routine and/or a sequence of instructions and/or logic stored in the devices, in addition to the operating systems resident in the devices. In short, use of the methods described and suggested herein is not limited to a particular processing configuration.

To facilitate an understanding of the principles, features and functions of the present invention, they are explained with reference to its deployments and implementations in illustrative embodiments. By way of example and not limitation, the present invention is described in reference to examples of deployments and implementations relating to the context of the Internet and in reference to a laptop or notebook computer as the client device A (computer A1 is schematically represented as a desktop device, but may instead comprise a portable computing device). It will be understood by one of ordinary skill in the art that the application of this invention to any currently existing of future global network is contemplated herein. Further, although the Internet aspect of this invention is described and illustrated with respect to client computer A1 it should be understood that the Internet application is readily applicable to other client devices without departing from the scope and spirit of the present invention.

Fig. 1 is a schematic representation of the communication links B in the form of information exchange networks in which the present invention may be deployed for asset tracking. The information exchange network accessed by the asset tracking Agent application in accordance with the present invention may involve, without limitation, distributed information exchange networks, such as public and private computer networks (e.g., Internet, Intranet, WAN, LAN, etc.), value-added networks, communications networks (e.g., wired or wireless networks), broadcast networks, cable networks, radio networks, and a homogeneous or heterogeneous combination of such networks. As will be appreciated by those skilled in the art, the networks include both hardware and software and can be viewed as either, or both, according to which description is most helpful for a particular purpose. For example, the network can be described as a set of hardware nodes that can be interconnected by a communications facility, or alternatively, as the communications facility, or alternatively, as the communications facility itself with or without the nodes. It will be further appreciated that the line between hardware, firmware and software is not always sharp, it being understood by those skilled in the art that such networks and communications facility, and the components of the persistent agent technology platform, involve software, firmware and hardware aspects.

The Internet is an example of an information exchange network including a computer network in which the present invention may be implemented. Details of various hardware and software components

comprising the Internet network (such as servers, routers, gateways, etc.) are not shown, as they are well known in the art. Further, it is understood that access to the Internet by the user/client devices and servers may be via any suitable transmission medium L, such as coaxial cable, telephone wire, wireless RF links, or the like, and tools such as browser implemented therein. Communication between the servers and the clients takes place by means of an established protocol. As will be noted below, the persistent asset tracking Agent application of the present invention may be configured in or as one of the clients, which can communicate with one of the servers over the information exchange network. This invention works in conjunction with other existing technologies, which are not detailed here, as it is well known in the art and to avoid obscuring the present invention. Specifically, for example, methods currently exist involving the Internet, web based tools and communication, and related methods and protocols.

Referring to Fig. 1, the host monitoring system C may simply be a computer (e.g., a server 3) that is configured to exchange data with client devices A that have an Agent installed thereon, via one or more (concurrently or in parallel) of the communication links B. The host monitoring system C includes routines for identifying and filtering external user access (C1). The host monitoring system C also communicates (C3) directly or indirectly with the owners and/or representatives of the tracked client devices A concerning information related to the tracked devices A (e.g., network location information), via the reporting and administration portal. For example, the host monitoring system C may communicate by email, fax, paging, phone, etc. to the owner of a tracked device, his designated representative, a company designated department or representative, a staffed monitoring service station, law enforcement agency, etc. Alternatively, the host monitoring system C may itself be a staffed monitoring service station, or part of a law enforcement agency. The host monitoring system C and/or downstream target locations (e.g., staffed monitoring service station) may maintain an inventory list of the tracked assets, or the lost/stolen status of the tracked assets. Though only one host monitoring system C is shown in Fig. 1, a plurality of host monitoring systems C may be distributed across the communication networks, for example in different geographic regions.

One of the important functions of the Agent is to contact the host monitoring system C to report the identity, location, and/or other information relating to its associated client device A. According to one embodiment of the invention, each client device A is associated with a unique identification, which may be part of the information delivered by the client device A to the host monitoring station C. The unique identification can be in the form of an Electronic Serial Number (ESN), Media Access Control (MAC) number, Internet host name/IP address, an owner/user specified identification, or other numeric, alpha or alphanumeric information that represents, identifies and/or allows identification of the client device, and further information such as date and time, which might present further basis for determination or

validation of the actual or virtual geographical location of the Agent and its identification.

The general concept of using a stealth Agent to track assets and/or recover stolen or lost devices A had been disclosed in the patents assigned to Absolute Software Corporation, the assignee of the present invention. The Agent has to determine the appropriate time for it to call the host monitoring system C. If is suffice to mention briefly here that once the Agent is installed and running it will either periodically (e.g. every N hours), or after specified periods have elapsed (e.g. from system or user logon), or after device system boot, or upon the occurrence of certain pre-determined conditions, or triggered by some internal or external events such as hardware reconfiguration, report its identity and/or location via the communication link B to the host monitoring system C, without user intervention to initiate the communication process. The Agent may also concurrently report its identity and location via two or more available communication links B to the host monitoring system C. The location of the Agent, hence the tracked device, may be determine, for example, by a traceroute routine to obtain a listing of all IP routers used to enable communication between the client device A and host monitoring system C via the Internet.

All location and asset related data transmitted to the monitoring system C may be kept in a central repository and can be accessed 24x7 by authorized administrators via secure web-based or network based console. In one embodiment, when the agent transfers location and asset data, the monitoring system C sends and programs the instructions for the next set of tasks, and the next scheduled call time and date to the Agent. The monitoring system C archives all Agent transmissions, providing a current and accurate audit trail on each computer (C2). A comprehensive computer asset tracking and inventory solution will capture this information on systems connected locally to the corporate network, as well as on remote and mobile systems connecting remotely via IP or dial-up. In addition, information needs to be captured on a regular basis to ensure the most up-to-date view of the assets is being provided.

As will be further explained below, the tracking Agent is persistent with high resistance to tampering, and the Agent may be configured to remain transparent to an unauthorized user. The Agent, in order to remain hidden to the user, will not interfere with any running applications unless designed to interfere. The novel features, functions and operations of the Agent in accordance with the present invention will be discussed more fully below.

Overview of Architecture of Persistent Agent Platform

IT administrators need the ability to consistently track all computer assets throughout their entire life cycle. This includes remote and mobile computers that operate outside the LAN. Asset tracking agents need to be installed once at the beginning of a computers life cycle and communicate regularly until the computer is retired. During its life cycle a computer will undergo many user, hardware and software changes and it is critical that the tracking agent be persistent and able to report changes in these three

areas. The persistent Agent in accordance with the present invention can report the original identification of the PC asset and its status throughout the PCs lifecycle, regardless of, for example, IMAC and break/fix operations, even if the hard drive has been reformatted or the operating system reinstalled or tampered with. The persistent Agent is designed to protect itself and will survive any unauthorized removal attempts. This persistence feature is critical in order to remain connected to PC assets in case of theft and to ensure accurate and secure asset tracking.

The persistent Agent is a low-level undetectable software client that resides on the host computer. The Agent is persistent software and extremely difficult to remove. The Agent incorporates self-healing technology that functions to rebuild the agent software installation even if the agent service is deleted by conventional means. The agent will survive an operating system installation, hard drive format, and even a hard drive replacement. This survivability is critical to the success of asset tracking and theft recovery (and other services that the Agent may also enable, support and/or provide). The self-healing function is not resident within the file system and is more difficult to detect and remove than traditional software. The persistent and self-healing portion of the software is difficult to remove because it is stealthy. The software is normally removed only by an authorized IT administrator with the correct password. The self-healing feature will function to repair an Agent installation in newly formatted and installed operating systems as well as newly imaged systems.

In another aspect of the present invention, the Agent is programmable to extend its functions beyond what was initially programmed. The Agent communicates with a remote server, wherein the remoter server sends and programs the Agent by providing the Agent with instructions for next set of tasks.

The Agent may be implemented in the hardware, firmware or software of any electronic device. Alternatively, the Agent may be implemented in any component of a device, as with an electronic component such as the DSP in a modem or the CPU in a computer. Furthermore, the functionality of the Agent may be implemented in the circuitry of any hardware device capable of establishing a communication link through sending and/or receiving packets of data. For example, the Agent may be embodied in non-volatile memory (such as ROM BIOS, ROM, Flash ROM, EPROM, EEPROM, or the like) of the electronic device, a software program, a micro-code program, a digital signal processor ("DSP") program or a built-in function of the operating system.

In accordance with one embodiment of the present invention, the persistent tracking Agent (hereinafter also referred to as a "Persistent Agent") is embodied in BIOS (or its functionally equivalent system). As is known in the art, BIOS is the startup code that always executes on system power up or reset. This can be microcode embedded into the processing unit or software (instructions) starting from a

fixed location in memory space. These instructions handles startup operations such as the Power-On Self-Test (POST) and low-level control for hardware, such as disk drives, keyboard, and monitor, independent of and typically before the booting of the operating system resident on the device. In one embodiment, the Persistent Agent is embodied in firmware, such as a read-only memory (ROM), in the client device A, such as personal computers. When BIOS is embodied in a chip, it includes a set of instructions encoded in ROM. It is understood that all references to BIOS hereunder is not limited to ROM bases BIOS.

Popular brands of BIOS chips on motherboards sold today include Phoenix Technologies, Intel, IBM and American Megatrends, Inc. Some system components have their own BIOS chip, whose instructions are also read into the device's memory at startup. The BIOS on a hard disk controller, for example, stores a table of tracks and sectors on the drive. Unlike the BIOS based Agent disclosed in Absolute Software Corporation's earlier patents, the present invention presents an improvement, that includes the use of a BIOS-based loader for the Agent. The BIOS-based loader makes the Agent components more persistent, and hence it is more difficult to defeat the asset tracking or other servicing function. The BIOS-based loader also eliminates the need to reverse the boot order on the machine and thus removes a step in the manufacturing process. A BIOS-based loader also reduces potential compatibility issues with products such as anti-virus scanners, full-disk encryption and other utilities that read or modify the operating system loader in the Master Boot Record (MBR).

In accordance with one embodiment of the present invention, the Persistent Agent 10 is initially stored in an Option ROM, such as a an Option ROM based on peripheral component interface bus - PCI Option ROM 12 attached to the Core BIOS Flash Image 13, as depicted in Fig. 2. There may be additional Option ROMs attached (not shown), which supports other functions not related to the Persistent Agent. The Persistent Agent 10 comprises multiple modules. The three main modules are the "Computrace" Loader Module (CLM) 14, the Adaptive Installer Module (AIM) 16, and the Communications Driver Agent (CDA) 18, as depicted in Fig. 3.

The small (can be approximately 22 Kb – compressed) PCI Option ROM 12 containing the three modules of Persistence Agent 10 are bound to the standard core flash image and loaded into protected memory along with the BIOS and other Option ROMs during BIOS POST. The small PCI Option ROM is recognized by POST and loaded into read/write shadow memory along with the BIOS and other Option ROMs during BIOS POST. This configuration provides a modular architecture that will enable the security enhancing features while minimizing the development effort and number of interface points in the core BIOS which must be re-qualified.

The CLM incorporates the PCI (in the case of a PC device), Image Management and Execution Environment functions. It is responsible for the interface to the BIOS, locating and unpacking the AIM,

resizing the PCI Option ROM to its final size, and executing the AIM within the proper context on the system. The AIM accesses the hard drive, detects active operating systems, and adapts the mini CDA to the discovered installations. The mini CDA is the communications driver. It includes support for the HTTP protocol, an application layer for communicating with the monitoring server, a service layer for interfacing to an OS and an adaptive layer for interfacing with the AIM.

The mini CDA is responsible for checking whether the full-function CDA is available in the computer's file system to run as a service when the operating system is loaded. If the full-function CDA is not available, the mini CDA will initiate download of the full-function CDA from the monitoring server. Once the full function CDA is present, it will frequently check for newer versions of itself on the monitoring server, and if available, will replace itself with a new version.

These and other embodiments of the various modules will be discussed more fully below.

BIOS POST sequence and Option ROM load process

The Option ROM load process 20 is depicted in the flow diagram of Fig. 4. At boot up of the client device A in which the Persistent Agent 10 has been deployed, the BIOS POST process performs a self-test and chipset configuration routine 21, and reaches a point where the bus is scanned at 22 for Option ROMs that support functions on the motherboard or on extension cards. At this point, the PCI Option ROM 12 containing the Persistence Agent 10 is loaded into low memory (e.g., a RAM) at 22 and its initialization vector (CLM 14, as discussed below) is called at 23. The initialization routine determines the status of the function to be supported and its final image size. Subsequently at 25 and 26, the BIOS POST process then completes the Option ROM scan and calculates the final locations of each Option ROM whose function is present. Each PCI Option ROM is then relocated and its completion vector is called, including the Persistent Agent enabled PCI Option ROM 12. (In certain Phoenix BIOS, for example, the PCI Option ROMs are not relocated, but simply shrink to fit the final size declared in the header before returning from the initialization vector.) After all Option ROMs have been relocated, the BIOS memory is write-protected at 27. The boot-devices are called in turn until an operating system is successfully started at 28. At this point, both the device operating system and the Agent would be running simultaneously.

PCI Option ROM

- **A. Loader Module CLM**

The CLM 14 is responsible for setting up a temporary Execution Environment for the AIM 16, loading and decompressing the AIM 16 and calling it in an appropriate context. The last "act" of the CLM

14 is to shrink to a minimum size (2K) and return execution to POST. The CLM only "fails" if the AIM 16 is not found or invalid.

The CLM 14 is the interface to POST, or the "front-end" of the PCI Option ROM 12. The PCI Option ROM header is in the CLM 14 and its entry points are advertised according to the standard in this header. The CLM 14 provides two function points for integration with the BIOS POST.

1. ROM header and PCI Option ROM header pair
2. Interrupt Handler

These and other functions of various components of the PCI Option ROM will be described below in reference to an IBM BIOS, for example installed in the IBM Model T43 notebook computer.

1. **ROM Entry point**

The initial interface is presented during PCI Option ROM enumeration by the BIOS. This interface is a standard legacy ROM header and PCI Option ROM header pair. For example, in reference to a Phoenix BIOS, a PCI Vendor ID of 1917h and the device ID 1234h may be set. As noted above, when the BIOS POST process scans the bus for Option ROMs that support functions on the motherboard or on extension cards, the whole PCI Option ROM 12 is loaded and the initialization vector of the CLM 14 is called. The Option ROM loads and executes a compressed .COM application. The ROM entry point is defined by the START_SEG label. The START_SEG Segment contains the ROM header and its link to the PCI Option ROM header. The Option ROM is initialized by a FAR CALL to offset 3 in the Option ROM. The jump instruction chain here passes control to the OptRomProc.

Referring to Fig. 5, the routine 30 undertaken by the PCI Option ROM CLM 14 may be summarized as follows:

a. Find the BIOS POST Memory Manager at 31.

b. Allocate a control STUB_BLOCK at 32(e.g., 2K for interrupt handling and application execution).

c. Allocate extended memory for the COMPRESSED application and a backup of application memory (e.g., 64K) at 33.

d. Allocate a block of application memory (e.g., 64K) in conventional memory for the DECOMPRESSED execution of the application at 34.

e. If disk services are available at 35 (as determined by count at 40:75h; number of hard disks), then execute application immediately at 36, then proceeds to free memory at 39 and shrink Option ROM to Zero at 40.

f. Else if Video vector (int 10h) is below the XBDA (40:0Eh) at 37, then hook Int 15h.to STUB_BLOCK, at 38, and Shink Option ROM to Zero at 40.

g. Else nothing to hook and nothing to do - Failed! Free memory at 39, and shrink Option ROM to Zero at 40.

2. **Interrupt handler**

The second interface is an Interrupt Handler. This executes after the initial load and execution of the initialization procedure of the PCI Option ROM from memory allocated from the BIOS POST memory manager. This interface executes first on int 15h and then on an alternate trigger. Int 19h is the preferred alternate trigger and the default. The interrupt handler is only activated if BIOS Disk Services (int 13h) is not yet available during initialization of the PCI Option ROM. Int 19h is the preferred trigger method because in some cases there is no Int 13h issued by the BIOS after the last int 15h/func 9100h. Another issue is that physical drive 80h by not be consistent with physical drive 80h at Int 19h until shortly before Int 19h. ComFileStub contains the main interrupt hook entry point.

Referring to Figs. 6a and 6b, the process 41 undertaken by the Interrupt handler may be summarized as follows:

a. On each int 15h trigger at 42, function 9100h (hard disk IRQ complete, this indicates that INT 13h is in use.)

b. Check hard disk services available at 43(count 40:75h).

c. And Video vector above or equal to the XBDA (40:0Eh; this indicates that SETUP phase of POST is complete).

d. Chain if not yet ready at 44.

e. Restore Int 15h hook and hook a trigger Int xxh at 45 (_TRIGGER_INTNUM setting = Int 13h or Int 19h) to wait for the next Int xxh.

f. On the next trigger Int xxh (Int 13h or Int 19h) at 46, restore trigger Int xxh at (Int 13h or Int 19h).

g. Switch stacks at 48.

h. Backup copy of DECOMPRESSED appmem to extended memory BACKUP_BLOCK at 49.

i. Copy COMPRESSED application to DECOMPRESSED appmem block at 50.

j. Call application and restore contents of DECOMPRESSED appmem from extended memory BACKUP_BLOCK at 51.

k. Switch stacks back at 52.

l. Chain to complete the intercepted trigger Int xxh call at 53.

B. Agent Installer Module (AIM)

The AIM 16 is designed to be loaded under the execution context set up by the CLM 14. Referring to Fig. 7, the routine 54 undertaken by AIM 16 includes the following steps. When executed, the AIM 16 scans the partition table to find the active partition at 55. On the active partition it looks for the operating

system (OS) system directories or the configuration files at 56, which point to them and then creates and installs the installer mode instance of the Communication Driver Agent CDA at 57. The installation mechanism is specific and unique to each OS, and AIM 16 uses standard OS installation mechanisms.

C. **Communications Driver Agent (CDA)**

The CDA 18 exists in two forms, a mini CDA and a full-function CDA. In one embodiment, the mini-CDA resides in the PCI Option ROM 12. The function of the mini CDA is to determine whether a full-function and/or current version CDA is installed and functioning on the device, and if not, to load the full-function CDA across the Internet from the host monitoring server C (Fig. 1). The full-function CDA is then responsible for all communications between the device and the host monitoring server C.

Referring to Fig. 8, the mini CDA first runs (via AIM 16) an installer mode 58, in which the primary function of the mini CDA is to register as an OS service. The installer mode instance of the agent creates another instance of itself at 59 and registers the copy with the Service Manager at under 2000/XP, for example, at 60. The executable then cleans up the installer copy of itself and exits. It runs in Installer mode only once, as the full-function CDA takes over the normal operations of the CDA from that point.

Referring to Fig. 9, on subsequent start of the OS, the service mode instance of the mini CDA is executed as a Service under 2000/XP, for example. The Service sets up a service manager environment at 62 and at an appropriate time (after waiting at 63), launches an instance of itself as an application at 64. The application mode is the normal mode of operation of the mini-CDA. The Agent is now in "active" mode.

If the current full-function CDA is not found in the device, the mini CDA application initiates communications with the host monitoring server C using, for example, the HTTP protocol by default, as depicted in Fig. 10. Other protocols are supported by additional modules are uploaded from the host monitoring server C to the Agent. The host monitoring server C performs functions such as identifying the Agent, storing monitoring history, configuration and software updates. The host monitoring server C conducts a session with the mini CDA to activate and install a full version of the CDA, disable the mini-CDA (e.g., at end of life of the device, or for disabling self healing function so that it can be upgraded to a newer version), update the Agent, or configure the Agent, as required for that platform. The communications between the client device A and the server C via communication link B are depicted in Fig. 10 in accordance with one embodiment of the present invention. For example, if the mini CDA provides identification or type of BIOS or device platform to the server C, a copy of BIOS or platform specific full-function CDA or its updates can be downloaded to the device A.

As noted before in reference to Fig. 1, the general concept of using a stealth Agent to track devices and/or recovery stolen or lost devices A had been disclosed in the patents assigned to Absolute Software Corporation, the assignee of the present invention. The application level functionality of the device

tracking and communication functions of the full-function CDA can be similar to the functions of the stealth agent earlier described and patented by the assignee of the present invention (which patents have been incorporated by reference herein) and/or the AbsoluteTrack asset tracking product developed by the assignee of the present invention.

Generally, in one embodiment of the Internet application, which can run alone or concurrently with or applications based on other communication links B (e.g., PSTN), the Agent initiates a call to the host at predetermined, random, event based or deferred intervals. According to one embodiment, in its "active" mode the Agent calls the host every predetermined number of hours. The Agent uses the current time and the unique Agent identification to encode an Internet host name. In one embodiment, the Agent then forms a DNS request using an encoded Internet host name. The Agent sends this DNS request to the host through the Internet. If the agent's attempt to send the DNS request to the Internet times out after a predetermined time period has elapsed, the Agent will sleep for a predetermined period of time, e.g., one minute, and then repeat the call. If the call fails due to another error (such as the absence of Winsock facilities which enable communication with the Internet, and/or the failure of the computer to be configured for TCP/IP communication) then the Agent will repeat the cycle several hours later. In this way, the Agent inherently checks for the existence of an Internet connection.

After sending its DNS request, the Agent waits for a response. Upon receiving a valid response from the host, the IP address is extracted from the response and compared against a reference IP address. For example, the reference IP address may be set as "204.174.10.1". If the extracted IP address equals "204.174.10.1" then the Agent's mode is changed from "active" to "alert" on the Internet side. The host will send this IP address, for example, when it, or the operator at the host, has determined that the Agent identification matches one of the entries on a list of reported lost or stolen computers stored at the host. If the IP address extracted from the host response does not equal "204.174.10.1" then the Agent remains in active mode and does not call the host for another four hours. However, when the Agent goes into "alert" mode in the Internet application, the Agent initiates a traceroute routine which provides the host with the Internet communication links that were used to connect the client computer to the host. These Internet communication links will assist the host system in tracking the client computer. The IP address of the source of the DNS query is sent to the host within the DNS query. However, if the source of the query is transmitted through a "proxy" server, then the IP address of the client computer (which may not be unique since it may not have been assigned by the InterNIC) will likely be insufficient to track the location of the client computer. In such a scenario, it is necessary to determine the addresses of other IP routers that were accessed to enable communication between the client and the host. These addresses and the times that they were accessed are compared with internal logs of the proxy server that record its clients' Internet access

history. In this way, the client can be uniquely identified and located. Additionally, the transfer of the Internet application into "alert" mode is a condition that triggers the transfer of the other available communication applications to "alert" mode.

CDA – Server Communication

A. Extensible Protocol

Deploying the Persistence Agent successfully in BIOS, for example, makes heavy use of an extensibility designed into the communications protocol. Without this extensibility the Agent would be larger and require frequent updates to add or change functionality. Such updates are neither practical nor economical, since the BIOS is programmed into the flash EEPROM of the platform and special tools (most often requiring user interaction) must be used to update the BIOS. Also, intensive testing is performed by the OEM on the BIOS since its integrity is critical to the operation of the computer.

The key elements of the extensible protocol are:

1) A method to read and write Agent's memory space
2) A method to allocate memory
3) A method to free memory
4) A method to load an external module
5) A method to determine a procedure address
6) A method to call a procedure

The Agent's protocol is designed to provide these mechanisms.

The format of a read packet is: | ADDRESS | NUMBER_OF_BYTES

The format of a write packet is: | ADDRESS | NUMBER_OF_BYTES | DATA...

The communications protocol distinguishes a read packet by determining that no DATA is contained in the packet. If there is DATA, then it is a write. This address based protocol is the basis of the extensibility design.

The general sequence of steps in a communication session, based on the extensible protocol, between the client device A and the server C via communication link B is schematically depicted in Fig. 14 in accordance with one embodiment of the present invention. Examples of specific transactions handled by a communication session is further disclosed below.

A typical session begins with a connection sequence such that:

1) The client connects
2) The server responds with a special read from address 0xffffffff | 0xffffffff | 4
3) The client replies with the address of its session handle

The handle structure contains important information like the version of the client, the version of the supporting OS and the Command Packet. The client interprets "writes" to the Command Packet as "special" and will call the CommandPacketProcessor() function when the Command Packet is written. The CommandPacketProcessor() function takes the arguments: function code, parameter address, number of parameters, and the result address. The minimum set of function codes which must be implemented are:

- CMD_FUNC_CCALL (Call 'C' function)
- CMD_FUNC_STDCALL (Call a STDCALL function)
- CMD_GETMH (Get Module Handle)
- CMD_GETPA (Get Procedure Address)
- CMD_ALLOC (Allocate Memory)
- CMD_FREE (Free Memory)

Other function codes which may be implemented are for chaining Command Packets together to improve efficiency:

- CMD_ENDC (End Chain)
- CMD_IF (Conditional Branch)
- CMD_GOTO (Unconditional Branch)

This small library of commands can be strung together in packets to accomplish any management task. The critical management tasks are:

1) CreateFile
2) Load as Library of functions, or as executable
3) Call procedure in the operating system or from created file
4) Allocate and Free Memory in the context of the Agent

B. Transactions

The following section describes the communication between the Agent and the remote (e.g., monitoring) server (also known as CTSRV). Note that each item described represents one transaction (message pair between the client and server). Some transactions occur on every agent call, others depend on the service implemented and others are done on one call only as a result of a flag set by maintenance or recovery personnel. Below are tables of typical communications sessions between the server and the Agent.

Basic communication (Every Agent Call)

Action	Packets
Initialize communication, get client handle	1
Read client flags	2,3

Read client settings	4,5
Lock agent	6,7
Get address of TAPI info structure on the client	8,9
Get address of local IP from TAPI info structure	10,11
Receive client local IP info	12,13
Request for serial #, version, client time, next call date, next call date IP, last call date, last call date IP and OEM CTID	14-17
Unlock agent	18,19
Lock agent	20, 21
Send next call date	22,23
Send last call date	24,25
Set flag call successful on the client.	26,27

Call With Basic Asset Tracking (Every Call - If client has subscribed to such tracking services with the monitoring service provider) Using AT1 DLL On Client

AT1 data (for subscribers to asset tracking/monitoring services) is retrieved. Note that this is a sub-set of the data collected by the AT2 DLL. Either the AT1 or AT2 DLL will be executed on the client, never both.

Action	Packets
Basic Agent Call as Described Above	1-27
Unlock agent	28,29
Allocate one big chunk of memory on the client	30,31
Write new receive buffer size to client CTHANDLE	32,33
Set new receive address to client	34,35
Write new transmit buffer size to client	36,37
Read current transmit buffer address from client	37,39
Write offset to the new transmit buffer	40-43
Set new transmit buffer address to client CTHANDLE	44,45
Read client's tinfo structure	47,48
Set client window size	49
Get Kernel32 procedure addresses	50-59

Call Kernel32 GetSystemDirectory function on client	60-63
Get client's system folder path	64,65
Checking encryption DLL timestamp, call Kernel32 FindFirstFile function on client	66-71
Call Kernel32 FindClose function on client	72-75
Load WCEPRV.DLL on client	76-79
Set encryption communication, read old transmit address	80,81
Read old receive address	82,83
Call WceSet on client	84-91
Setup encryption key on client, call WceStartup	92-99
Get WceSend procedure address	100-103
Get WceRecv procedure address	104-107
Set new transmit address	108,109
Set new receive address	110,111
Enable encryption on client, call WceEnable	112-119
Check transmit (WceSend) procedure address	120-123
Check AT-I on client, call Kernel32 FindFirstFile on client	124-129
Call Kernel32 FindClose on client	130-133
Load AT DLL on client, call Kernel32 LoadLibrary function	134-137
Call GetHWInfo on client	138-147
Call GetEmailAddress on client	148-155
Read AT-I data	156,157
Unload AT DLL on client, call Kernel32 FreeLibrary function	158-161
Reset encryption, call Free WceEnable on client	162-165
Write old transmit address	166,167
Write old receive address	168,169
Free WCEPRV.DLL on client	170-173
Set flag call successful	174-185
Send close to agent	186,187

Call With Advanced Asset Tracking (Every Call - If client has purchased AbsoluteTrack or ComputraceComplete products) Using AT2 DLL On Client

AT-II data (e.g., for AbsoluteTrack & ComputraceComplete customers) is retrieved. Note that this is a super-set of the data collected by the AT1 DLL. Either the AT1 or AT2 DLL will be executed on the client, never both.

Action	Packets
Basic Agent Call as Described Above	1-27
Unlock agent	28,29
Allocate one big chunk of memory on the client	30,31
Write new receive buffer size to client CTHANDLE	32,33
Set new receive address to client	34,35
Write new transmit buffer size to client	36,37
Read current transmit buffer address from client	37,39
Write offset to the new transmit buffer	40-43
Set new transmit buffer address to client CTHANDLE	44,45
Read client's tinfo structure	47,48
Set client window size	49
Get Kernel32 procedure addresses	50-59
Call Kernel32 GetSystemDirectory function on client	60-63
Get client's system folder path	64,65
Checking encryption DLL timestamp, call Kernel32 FindFirstFile function on client	66-71
Call Kernel32 FindClose function on client	72-75
Load WCEPRV.DLL on client	76-79
Set encryption communication, read old transmit address	80,81
Read old receive address	82,83
Call WceSet on client	84-91
Setup encryption key on client, call WceStartup	92-99
Get WceSend procedure address	100-103
Get WceRecv procedure address	104-107
Set new transmit address	108,109

Set new receive address	110,111
Enable encryption on client, call WceEnable	112-119
Check transmit (WceSend) procedure address	120-123
GetHWInfoII, check diag2.dll time stamp. Call Kernel32 FindFirstFile on client	124-129
Call Kernel32 FindClose on client	130-133
Load diag2.dll on client	134-137
Call GetHWInfo on client	138-147
Call GetHWInfoII on client	148-155
Read AT-II result	156,157
Call EnumSWInstallations on client	158-166
Allocate necessary memory on client	167,168
Send SW CRC to client	169,170
Call GetSWInfo on client	171-178
Read result	179-189
Call EnumAllPrinters on client	190-197
Allocate necessary memory on client	198,199
Call GetPrinterInfo on client	200-207
Read result	208,209
Call GetEmailAddress on client	210-217
Read AT-I result	218,219
Call EnumAllAccounts on client	220-227
Allocate necessary memory on client	228,229
Call GetAllEmailAddresses on client	230-237
Read result	238,239
Free AT-II DLL on client	240-243
Check AT-II on client, call Kernel32 FindFirstFile on client	244-249
Call Kernel32 FindClose on client	250-253
GetregSW, load diag2.dll on client	254-257
Call EnumRegSWInstallations on client	258-265
Allocate necessary memory on client	266,267
Write CRC to client	268,269

Call GetRegSWInfo on client	270-277
Read result	278,279
Free AT-II DLL on client	280-283
Check AT-II on client, call Kernel32 FindFirstFile on client	284-290
Call Kernel32 FindClose on client	290-293
Load diag2.dll on client	294-297
Copy search pattern to client	298,299
Allocate necessary memory on client	300,301
Copy SW license info header to client	302,303
Call GetSWLicenseInfoPattern on client	304-313
Read result	314-317
Free AT-II DLL on client	318-321
Reset encryption, call Free WceEnable on client	322-325
Write old transmit address	326,327
Write old receive address	328,329
Free WCEPRV.DLL on client	330-333
Set agent flag call successful	334-345
Send close to agent	346,347

Basic Call AND Upgrade Agent Version Remotely (One-Off Based On Tech Support Action)

Check client agent version and compare with version on the server. If client version is lower then perform remote upgrade.

Action	Packets
Basic Agent Call as Described Above	1-27
Unlock client	28,29
Init call environment, allocate one big chunk of memory on the client	30,31
Write new receive buffer size to client CTHANDLE	32,33
Set new receive address to client	34,35
Write new transmit buffer size to client	36,37
Read current transmit buffer address from client	37,39
Write offset to the new transmit buffer	40-43

Set new transmit buffer address to client CTHANDLE	44,45
Read client's tinfo structure	47,48
Set client window size	49
Get Kernel32 procedure addresses	50-59
Call Kernel32 GetSystemDirectory function on client	60-63
Get client's system folder path	64,65
Copy NTAgent to client. Call Kernel32 CreateDirectory function on client	66-69
Call Kernel32 CreateFile on client	70-73
Copy NtAgent to client	74-917
Call Kernel32 CloseHandle on client	918-921
Copy upgrd.exe to client	921-951
Execute Upgrd.exe on client, get address of client tapi info structure which contains service token	952,955
Call Advapi32 CreateProcessAsUser function on client, it restart agent and session is finished	956-969

Basic Call AND Retrieve Make, Model & Serial Number (One-Off Based On Tech Support Action)

Function retrieves make, model and serial number from client and change boot order.

Action	Packets
Basic Agent Call as Described Above	1-27
Unlock client	28,29
Init call environment, allocate one big chunk of memory on the client	30,31
Write new receive buffer size to client CTHANDLE	32,33
Set new receive address to client	34,35
Write new transmit buffer size to client	36,37
Read current transmit buffer address from client	37,39
Write offset to the new transmit buffer	40-43
Set new transmit buffer address to client CTHANDLE	44,45
Read client's tinfo structure	47,48
Set client window size	49

Get Kernel32 procedure addresses	50-59
Delete file C:\\DMI.TXT on the client, call Kernel32 DeleteFile function	60-63
Call Kernel32 GetLastError function on client	64-67
Call Kernel32 GetSystemDirectory on client	68-71
Read result from client	72,73
Copy ctsetup.ini to client	74-125
Run ESN specific App, Call Kernel32 GetSystemDirectory function on client	126-129
Read result from client	130,131
Check time stamp of dmiinfo.exe on client. Call Kernel32 FindFirstFile function	132-137
Copy dmiinfo.exe to client	138-421
Execute dmiinfo.exe on client	422-439
Close process handle on client. Call Kernel32 CloseHandle function	440-443
Close thread handle on client. Call Kernel32 CloseHandle function	444-447
Call Kernel32 GetLastError on client	448-451
Delete dmiinfo.exe on client, call Kernel32 DeleteFile function	452-455
Copy C:\\DMI.TXT from client, open file, call Kernel32 CreateFile function	456-459
Call Kernel32 GetFileSize on client	460-463
Calling Kernel32 ReadFile on client in the loop	464-471
Call Kernel32 CloseHandle on client	472-475
Delete C:\\DMI.TXT on client	476-479
Delete CTSETUP.INI on client	480-483
Set flag call successful	484-495
Send close to agent	496,497

C. The Application Module's Activation Process

The activation process links the Application agent identity to a customer account and installs the Persistent Agent module. This process is described as follows:

- The Application Agent connects

- The Server uses the extensibility features in the protocol to send down and inventory DLL to identify the computer – this DLL gathers attributes such as the BIOS, chassis and hard-drive serial numbers.
- An inventory record is stored on the server and linked to the customer account read from the Application agent.
- A unique identifying number (the Electronic Serial Number) is assigned to the device associated with this inventory record.

A typical inventory record is shown below:

<?xml version="1.0" encoding="UTF-8" ?>
- <CT:data version="**1.00**" xmlns:CT="http://www.absolute.com/atinfo/persistence">
- <CT:section name="**MachineInfo**">
<CT:setting name="**ComputerMakeWMI**" value="**VIA TECHNOLOGIES, INC.~~**" />
<CT:setting name="**ComputerModelWMI**" value="**MS-6321~MS-6321~**" />
<CT:setting name="**ComputerSerialWMI**" value="**~~**" />
<CT:setting name="**ComputerMake**" value="**VIA TECHNOLOGIES, INC.~~**" />
<CT:setting name="**ComputerModel**" value="**MS-6321~MS-6321~MS-6321~**" />
<CT:setting name="**ComputerSerial**" value="**~~**" />
<CT:setting name="**ComputerAsset0**" value="" />
<CT:setting name="**ComputerAsset1**" value="" />
<CT:setting name="**SystemSMBIOSVersion**" value="" />
<CT:setting name="**SystemBiosVersion**" value="**VIA694 - 42302e31 Award Modular BIOS v6.00PG**" />
<CT:setting name="**SystemBiosDate**" value="**08/22/01**" />
<CT:setting name="**BaseBoardVersion**" value="" />
<CT:setting name="**HDDSerialNumber0**" value="**Y3NYPZDE**' />
<CT:setting name="**HDDSerialNumber1**" value="**YMDYMLJ0046**" />
<CT:setting name="**HDDSerialNumber2**" value="" />
<CT:setting name="**HDDSerialNumber3**" value="" />
<CT:setting name="**ComputerName**" value="**PBGR7**" />
<CT:setting name="**MACAddress0**" value="**0050ba432204**" />
<CT:setting name="**MACAddress1**" value="**0050ba4434da**" />
<CT:setting name="**OSProductKey**" value="**VF4BY-WXV47-RR9JQ-H297B-6QQVW**" />
<CT:setting name="**IBMComputraceStatus**" value="**FFFFFFFF**' />
</CT:section>
</CT:data>

D. The Persistent Module's Reactivation Process

Once the Persistent Agent module is launched, the following steps happen to reinstall the Application agent and restore the configuration:

- The Persistence Module Agent calls the Monitoring Server (CTSRV)
- The Monitoring Server uses the extensibility features in the protocol to send down an inventory DLL to identify the computer – this DLL gathers attributes such as the BIOS, chassis and hard-drive serial numbers and compares with those previously stored.
- The inventory record stored at first activation is found and previous ESN associated with this device's inventory is reassigned. The Application agent is downloaded and installed and the Application agent then calls normally.

The above process applies to both BIOS and software persistence (see further discuss below) – i.e. regardless of where the persistence module is located.

Data Delete

Data delete is another example of a service enabled, supported and/or provided by the Agent. As discussed above, the enhanced survivability of the CDA improves tracking physical location of the asset. It is recognized that even when location of asset is established, physical recovery of tracked device is not always feasible due to applicable local laws, police enforcement and burden of proof of ownership. In such instances, programmable capabilities based on the extensible protocol of the CDA offers alternate means of safeguarding confidential or sensitive user data on the device. User defined data files, user profiles or other user defined information, e.g., stored on a hard drive at the client device A, can be deleted under control from the monitoring server. Data deletion can be done on selected data items, or complete device storage medium, including the operating system can be erased, in accordance with the features and options specified by the monitoring server.

Specific examples of Data Delete features and options include:

1. Selective Data Delete - ability to delete all or specific files or directories (and leave the rest of the device intact) based on user preference.

2. Data Delete restart on reboot - Data Delete client to restart itself if the device is rebooted while Data Delete is in progress.

3. 2-stage Data Delete process for full operating system delete - To ensure that the Agent (e.g., the CDA) uploads the log files when a "full O/S Data Delete" option is specified by the monitoring server, Agent undertakes a 2-stage delete process. Log files are obtained by the monitoring server from the Agent

after a first stage delete before deleting the operating system in a second stage. The full O/D Data Delete option includes the following steps:

a) Delete all files except the O/S

b) Force an agent call and upload the logfiles

c) Delete the O/S files

4. Data Delete override – Data Delete executable is turned off by the monitoring server to stop the Data Delete running again if the computer is subsequently recovered.

5. Data Delete Pre-launch check - Additional pre-launch Data Delete checks for an affected client device is provided by the monitoring server to ensure: (a) theft report exists for the affected client device, (b) client device is positively identified and no duplicates exist, (c) there is authorization by the client device owner (e.g., a pre-authorization agreement in place between the owner representative and the entity maintaining the monitoring server such as the host monitoring station).

6. Notification - when launching Data Delete, notifications (e.g., via email, SMS - short messaging service) are send to the interested parties (e.g., authorizing owner representative, and/or requestor).

Fig. 15 is a schematic flow diagram depicting the client side Date Delete routine 70 of the CDA in accordance with one embodiment of the present invention. Fig. 16 is a schematic flow diagram depicting the server side Data Delete routine 80 in accordance with one embodiment of the present invention. Fig. 17 is a schematic flow diagram depicting the Data Delete executable routine 90 in accordance with one embodiment of the present invention. Referring to these figures, in a typical Data Delete operation on the server side, when the full function CDA contacts the monitoring server at 72 and 81, the identity of the device is verified. If the device is verified to have been marked for data delete actions at 82, then the extensible communication protocol described above is used to trigger the data delete executable or sub-functions of the CDA at 74. Data delete executable or sub-functions are called at 84 and 85 with parameters defining the data to be deleted (at 91), with wildcard variables to delete complete data structures. The server instructs the Agent at 86 to contact back the server within a set period of time (e.g., 15 minutes). CDA sub-functions may use US Department of Defense recommended algorithms to delete the data so as to make it non-recoverable (e.g., US Department of Defense Standard 5220.22-M Clearing and Sanitization Matrix). CDA sub functions also use available built in operating system support to delete data. These data deletion algorithms and mechanisms are publicly well known by persons skilled in the art, and actual delete mechanism does not alter the system capabilities being described herein.

The data delete application will delete applications and data on the hard drive at 93, for example, then will make a call back in to the monitoring server at 95, where it will upload at 76 and 88 a report (e.g., logfiles) to the server detailing the success of the data delete application (e.g., at 94, create/append to

logfile a log of each action, and/or log full path of deleted file). If the data delete application has been instructed to exclude deletion of the operating system, the data delete application will delete all data and application files, except those required for the operating system and the Agent function. At the end of the delete process at 83, the Agent will attempt to return at 94 a status report (e.g., logfiles) to the monitoring server at 76 and 88. The client device will remain operational after the delete process. The Data Delete routine for the server and the Agent would proceed with other actions at 78 and 87. For example, if the data delete application has also been instructed by the server to delete the operating system, it will then continue to delete the operating system files.

The routine for data delete of the operating system is as follows. In the first pass, the data delete application will delete all data and application files, except those required for the operating system and the Agent to function. At the end of the first pass in the delete process, the Agent returns a status report to the monitoring server. The data delete application will then continue to delete the remainder of the files on the device. This may cause the device to become non-operational. The Agent may not be able to call the monitoring server once the full data delete process has been completed. If the user reinstalls an operating system, the Agent will regain its original function.

In either configuration, the data delete service has the following features:

- Writes a pattern of 0 and 1 three times to the file
- Writes random data to the file
- Changes the file attributes to "directory"
- Changes file date/time stamp to a fixed value
- Sets the file size to "0"
- Changes the file name to a randomly-generated file name
- Removes the new file name from the directory

In keeping with the objective to operate as stealthily as possible, the data delete application is disguised. The service that runs during the delete process is titled "WCTSYS.EXE", in an attempt to conceal the delete process running in the background. If the user stops the process before the deletion is completed, the application is able to resume the deletion process where it left off, once the Agent makes it's next call to the monitoring server. For example, at 92, the Agent determines if data delete is perpetual. If perpetual, then proceeds to rest of date delete functions (i.e., 93, etc.) If not perpetual, and if data delete has not been completed before (at 97), the process proceeds to data delete functions. If data delete has been completed (at 97), the data delete process terminates. For all client devices enabled with data delete, the Agent call back period may be set to a predetermined value for both modem and IP calls (e.g., at 86).

The time required for the data delete process to complete is dependant on a number of variables, including the speed of the processor, the size of the hard drive, the amount of data to be deleted and the amount of activity already taking place on the client device. It has been determined that the data delete process can be expected to take between several minutes to half an hour or more to complete.

The report that is returned on a successful deletion contains the following information:

- Confirmation that the Data Delete application was downloaded and executed
- List of files deleted
- Change in hard drive space (This information will only be available if the asset tracking service has been enabled, so data can be collected from the PC.

This information may be provided to the user on the success of the Data Delete process.

The functionality of the data delete can be controlled by a policy file downloaded from the server, at 84 or 85. The policy file will dictate to Data Delete application what files, folders, or file types to delete. The policy can also dictate other data selection criteria.

Sample Policy File Format as implemented.

|items||item name=|*.extensionToBeDeleted| type=|U| instruction=|P$C:\ *.extensionToBeDeleted | seq=|0|/|

|item name=|C:\FolderNameToBeDeleted\| type=|U| instruction=|P$C:\ FolderNameToBeDeleted \| seq=|1|/|

|item name=|C:\LJ\FilenameWithExtensionToBeDeleted | type=|U| instruction=|P$C:\LJ\ FilenameWithExtensionToBeDeleted | seq=|2|/|

|/items|

Further Application of Extensible Protocol

As noted above and further below, full function CDA and mini-CDA (e.g., in the non-BIOS or software persistence embodiments) use the extensible protocols to keep itself current with the most up to date version available on the monitoring server. It also uses this capability to keep other asset tracking extensions updated to the current version. Generic sub-functions included in the extensible protocol are generic and flexible so they can be leveraged to have a multitude of functionalities, in addition to asset tracking and data delete described above. An example of another application of the extensible protocol is to provide downloading and launching applications from the monitoring server. An executable file can be downloaded into memory and then launched. Alternatively, an installer can be downloaded from the monitoring server and launched to install an application, or upgrade an existing application.

Examples applications that leverage the agent's extensible protocol to provide functionality include:

- Persistent Firewall: The Agent can download and enforce network communication firewall. The Agent can also monitor and correct any changes to firewall configurations or removal or disabling

of the firewall. Since the Agent is persistence (cannot be detected or removed) it can provide and enforce security features such as firewall in a much more persistence way.

- Data Encrypt: Persistence Agent, upon instruction from the server, can encrypt the data on the machine. This will enable data protection in a theft or loss scenario, in a much more persistent mechanism. Agent can also change the encryption keys or passwords post theft to protect user's data. Changing encryption passwords or keys can also protect machines in internal theft scenarios where the user knows the passwords.
- Location Tracking: One of the primary functions of the Agent is to contact the host monitoring system to report the identity and physical location of the device. The physical location can be implied by the machine's IP address or other related network parameters. The agent could use data from built in GPS receivers or cellular network receivers and transmitters for identifying the physical location of the device. In these configurations, the agent can log GPS or Assisted GPS location information (current, or a series of logged information). The CDA can periodically read the GPS location and create a log file, that can be uploaded to the server during a call.

Alternate Embodiments of Modules

This invention can be implemented in a variety of embodiments of Persistent Agent to adapt to their specific environment based upon factors including, but not limited to: (a) different BIOS implementations from different device (e.g., PC) manufacturers; (b) different interface requirements with the BIOS; (c) variation of flash memory space available from different device manufacturers or on different device models; and (d) ability to work without a BIOS PCI Option ROM enumeration hook. To adapt to these factors, the CLM is formatted as a PCI Option ROM and the AIM and CDA may be stored separately, or being bound to the CLM. The CLM shrinks down to a small stub at the end of the POST cycle. If the device has a BIOS that does not enumerate the PCI Option ROM, then the CLM may reside in a partition gap and use a substitute Master Boot Record (MBR). The different embodiments of the Persistent Agent module configurations are described more fully below.

A. Flash-Resident

In the flash-resident embodiment of the invention, the CLM, AIM and mini CDA are all loaded in the BIOS flash image. This approach leverages existing processes used in BIOS where PCI Option ROMs are loaded from the BIOS flash image. The additional modules (the AIM and the mini CDA) may be stored separately in flash or bound to the CLM in PCI Option ROM, as is in the case of Fig. 3.

If the AIM and mini CDA are bound to the CLM, an 18 – 20 KB PCI Option ROM is loaded by POST into upper shadow memory and the AIM is unpacked by the CLM. The AIM in turn adapts and configures the mini CDA for the system and returns control to the CLM. The CLM shrinks the size of PCI

Option ROM image to a minimum and remains in the upper memory region as a 2 KB ROM block. If the AIM (~6 KB) and CDA (~10 KB) are simply stored in the flash image, and not bound to the CLM, the CLM incorporates additional image access functions to locate and unpack the AIM and mini CDA. The operation of the CLM, AIM, and mini CDA are similar to the bound method above. The size of the CLM is slightly larger and specially tailored to the platform for which the flash image is targeted. This approach assumes the pre-establishment of a vendor ID to allow recognition of the flash-resident PCI Option ROM. The management of the flash image is depicted in Fig. 11.

B. Hard Drive Partition Gap

Depending on BIOS-specific space limitations, there may not be sufficient space in the BIOS flash memory for all the modules of the complete Persistent Agent. In this case, depending on the device vendor support, the AIM, or the AIM and the mini CDA may be resident in a user inaccessible area in a mass storage device, such as the hard drive partition gap. This is and example of a form of "software persistence" In this embodiment, the CLM still resides in flash and gets called during the PCI Option ROM enumeration process as in the earlier embodiment, but CLM loads AIM, which in turn executes the CDA from another location.

Fig. 13 depicts the partition gap image management involved in the situation in which the additional modules of the Persistent Agent will reside within the partition gap. This gap exists between the MBR and the first partition. The gap is 62 sectors, for example, on most new hard drives, but some of the sectors are reserved by the installation utility to maintain compatibility with other software and the useable size is about 27 Kb. This size is sufficient to include the base modules of the Agent (AIM, CDA) necessary to communicate with the server and bootstrap the rest of the modules into the OS.

C. Host Protected Area (HPA)

Referring to Fig. 12, alternatively, in a situation in which there may not be sufficient space in the BIOS flash memory for all the modules, instead of storing the additional modules of the Persistent Agent (i.e., AIM, and/or mini CDA) in the hard drive partition as in the previous embodiment, the additional modules of the Persistent Agent will reside in another user inaccessible area on the mass storage device, such as within the HPA, or its functional equivalent. This is another example of software persistence. Additional support is required to Lock and Unlock HPA. This HPA access mechanism will be PC OEM specific. The images within the HPA may need to be managed at runtime. The driver and applications will support the existing methods to authenticate with the BIOS interfaces and obtain the necessary runtime access to manage our portion of the HPA space. In this embodiment, the CLM still resides in flash and gets called during the PCI Option ROM enumeration process as in the earlier embodiment, but CLM loads AIM, which in turn executes the CDA from another location.

D. Non Flash CLM

While the most secure embodiments will involve the CLM being resident in the BIOS flash memory, there may be environments where this is not supported. This may be the case where OEM has not configured the BIOS to enumerate the CLM header in flash during PCI Option ROM scan. On these systems, an alternative location for the CLM will still provide a superior solution relative to existing products. The use of a substitute Master Boot Record offers a solution to this. In this embodiment, the CLM loads from the substitute Master Boot Record. CLM then loads and passes control to the AIM and mini CDR, which would be located in the partition gap, as described in the earlier embodiments. The substituted MBR approach for an agent subloader has been patented by the assignee, and incorporated by reference herein. The CLM herein may take advantage of similar subloading approach, although in the present invention, the CLM has additional and different functions in relation to the AIM and CDA not found in the earlier patents.

E. Integrated into Flash-Resident Operating System Image

In this embodiment, the mini-CDA is integrated into an operating system image entirely stored in flash memory. Persistence is achieved by being included in the persistent operating system image and is protected by the same security mechanisms used to protect accidental and deliberate modifications to the operating system. In this case, the mini-CDA or is directly loaded and run by an operating system utility. The full-function CDA is subsequently downloaded and installed into volatile memory. In another very similar embodiment, a CLM is loaded by the operating system utility and it subsequently loads and runs the mini-CDA. In this latter case, both the CLM and the mini-CDA are included in the persistent operating system image.

F. Server Initiated Communications

In this embodiment, the server initiates communications with the CDA instead of waiting for the CDA to initiate communication with the server. Server initiated communications permits the execution of server instructions that are time critical and cannot wait until the next scheduled call by the client. In this case, the server may use the same or a different communications network and protocol from the principal network or protocol used by the CDA to call the server. An example of a time sensitive scenario is the execution of a data delete operation on a misplaced or stolen mobile device before communications are interrupted by the network operator as a result of the device being reported stolen. Any time-sensitive service may be invoked in this manner.

G. Integrated into the Operating System Distribution

In this embodiment, the mini-CDA is integrated into an operating system distribution (e.g., software, firmware of hardware). Persistence is achieved by being included as a fundamental, inseparable component of the operating system. In this case, it is protected by the same security mechanisms used to protect accidental and deliberate modifications to the operating system. In the case of operating system reinstallation, the mini-CDA is reinstalled from the operating installation medium and, as a result, the services provided by the mini-CDA are enabled in the second installation. In this embodiment, the mini-CDA is directly loaded and run by an operating system function. The full-function CDA is subsequently downloaded and installed as in other embodiments.

H. Extensible Firmware Interface (EFI)

The BIOS embodiment of the persistence modules (i.e. AIM and CLM) can be modified to install the mini-CDA or the agent in an EFI environment, either as an EFI driver or EFI application prior to OS loader. Persistence is achieved when the EFI loads CLM, which then uses AIM to install or restore mini-CDA similar to the BIOS embodiment. The mini-CDA, after OS boot can then download and install the full featured agent, as in BIOS embodiment.

Optimization

The CLM PCI Option ROM is not difficult to integrate into the system BIOS. For example, the IBM Model T43 notebook computer is installed with an IBM BIOS having an option ROM structure. Its form and function parallels video option ROMs or motherboard controller option ROMs already existing in the BIOS. In the simple case, the BIOS must simply be reconfigured to recognize the vendor ID of the CLM. If the form and function of the CLM is more tightly integrated to the host BIOS, some size-optimization can occur. There is an opportunity to save a little space in the ~20 KB required to store the CLM, AIM, and CDA modules within the Flash Image. Below is a table listing various functions within the three main modules and the approximate size of each major functional group. The "optimization" column lists an estimate of the optimization opportunity of the functional group within each module.

Function	*Size*	*Module*	*Optimization*
OS Detection	2 KB	AIM	n/a
File System Support	6 KB	AIM	n/a
IP/HTTP support	4 KB	CDA	n/a
Application Layer	4 KB	CDA	n/a
Service Layer	1 KB	CDA	n/a
Adaptive Layer	1 KB	CDA	n/a
PCI Function	.5 KB	CLM	0 KB
Image Management	.5 KB	CLM	.3 KB
Execution Environment	1 KB	CLM	.8 KB

Of the various functions in the modules, only the CLM functions (PCI, Image Management, and the Execution Environment) may be optimized with specific support from the host BIOS. The size of the Image Management functions can be reduced by about .3 KB by using the compression algorithm of the BIOS and by using the "bound" method to store the AIM and CDA modules. The size of the Execution Environment setup and control function can reduced by .8 KB by ensuring that the PCI Option ROM is loaded late in POST so that all disk resources are available and that POST Memory Manager support is not needed. The lower range of the ~20 KB size is about ~18.9 KB. On the upper side, if platform specific support is needed within the CLM, it may grow by 2 KB.

If the BIOS interface exposes an application program interface (API) for detecting and configuring the CLM through SMBIOS, then the 2 KB visible ROM "stub requirement" is relaxed.

Persistent Servicing Agent Deployment in Portable Digital Devices

The persistent servicing Agent may be extended to track additional devices, such as portable digital devices. The intelligent Agent may reside in BIOS Option ROM, partition gap on hard drive, hard drives Host protected area (HPA), embedded firmware (e.g., OS ROM) of a consumer electronic device (e.g. Apple IPOD™ digitial media player, MP3 player, cell phone or gaming device such as Microsoft XBOX™ or Sony PlayStation™). Once the CDA executes, it will communicate with the monitoring server (either CDA initiated or server initiated communication), as described in examples discussed above. CDA functions can be generic functions such as copy to memory, copy from memory and execute from memory. These functions will be executed based on the sequences provided by the monitoring server during the communications with the CDA. These sequences can be executed to copy an application into memory, execute it, and read the results back to the monitoring server. The persistent agent may be programmable, as disclosed above.

The persistent servicing Agent may be deployed in various portable and/or personal digital devices, for example:

- Personal digital assistant (PDA)
- Digital media devices, such as an MP3 player, digital recorder, portable TV, radio, etc.
- Wireless devices, such as a cellular phone, two-way radio, etc.
- Handheld devices, such as global positioning system (GPS), etc.
- Gaming devices, such as portable versions of computer gaming (Nintendo, Sony PlayStation), etc.
- Digital cameras

Specific examples of deployment of Agent includes:

1. IPOD™ digital media player

The Agent would be programmed to contact, or be contacted by, a monitoring server proactively. Agent will be in a standby state until the device is connected to the Internet, or connected to another base device (e.g., a personal computer) that is connected to the Internet. Once the device connects to a third party website (such as ITunes), the Agent would use the website's embedded controls to connect to the monitoring server. Alternatively, the Agent could install a copy of itself, or another Agent onto the connected base device to connect to the monitoring server. Once connected, the Agent validates the device's status from the monitoring server. The validation may include checking a unique identification information of the device (e.g., an electronic serial number (ESN), manufacturer's serial number, or a serial number embedded into the Agent). This unique identification information would be matched against a database at the monitoring server. If the portable device is flagged missing (e.g., by the device's original owner or representative), the Agent will trigger the portable device to render itself non-functional (e.g., Data Delete discussed above, or shut off or disable or other similar actions rendering at least certain functions of the portable device inoperable at least to some extent to discourage continue use of the portable device). Alternatively or in addition, the Agent will trigger the device to display informational messages to the person in possession of the portable device. The message could instruct that person to contact the owner, device vendor or an asset tracking company for further information, such as return of device to its owner, associated rewards for return or re-enabling of the device.

2. Cell Phone:

The Agent would be programmed to contact a monitoring server proactively (e.g., server initiated or Agent initiated). Once the device is connected to the wireless network, the Agent could use standard communication protocols to communicate with the monitoring server, or alternatively or in addition send SMS messages (or another choice of protocol) to the monitoring server or the owner representative. Once connected, the Agent would validate the device's unique identification information against the database at the monitoring server. The validation may include checking the identification number, such as ESN or serial number of the device (manufacturer's serial number or a serial number embedded into the Agent, or SIM card ID etc. This unique identification information would be matched against a database at the monitoring server. If the device is flagged missing by the device's original owner, the agent will trigger the device to render itself non-functional (e.g., Data Delete discussed above, or shut off or disable or other similar actions rendering at least certain functions of the portable device inoperable at least to some extent to discourage continue use of the portable device). Alternatively or in addition, the Agent will trigger the device to display informational messages to the person in possession of the portable device. The message could instruct that person to contact the owner, device vendor or an asset tracking company for further

information, such as return of device to its owner, associated rewards for return or re-enabling of the device.

3. Gaming Console:

The Agent would be programmed to contact a monitoring server proactively (e.g., server initiated or Agent initiated). Once the gaming device connects to an online gaming server, the agent could use standard communication protocols (e.g., IP) embedded into the gaming site to communicate with the monitoring server. Alternatively it could send TCP/IP or standard Internet protocols to another third party monitoring server. Once connected, the Agent would validate the device's unique identification information, and take appropriate actions in much the same manner as the earlier embodiments described above.

* * *

The servicing Agent as disclosed above has the ability to be persistent in spite of actions that might ordinarily be expected to remove it. The programmable capabilities of the Agent allows its functionality to be extended based on server-driven commands. The invention improves upon the ability for a pre-deployed servicing Agent to remain "active" regardless of the actions of a "user" of the device. The users' actions with respect to the Agent may be intentional or accidental. The invention protects the authorized user from the accidental removal of the servicing Agent, while allowing the legitimate need to disable the Agent (for example at end of life of the computer asset). The invention prevents an unauthorized user from removing the Agent software. The persistent attributes of the present invention have value in both security and asset management applications. In the context of a secure, stealthy device-tracking software application, the invention is of significant value as it makes theft of a valuable asset much more difficult to disguise, as regardless of actions taken by a thief, the software will persist and make itself available for contacting a remote monitoring center. In addition, the persistent nature of the servicing Agent provides peace of mind to security personnel, as it provides confidence that the tracking Agent cannot be accidentally removed. In the context of a secure asset management application, this is of further value as it ensures continuity of tracking an asset over its whole lifecycle. A key challenge for IT administrators today is the ability to track assets over the whole lifecycle. During the lifecycle devices are frequently transferred from one user to another, during which they may be re-imaged, or have the operating reinstalled or otherwise be subjected to maintenance procedures that render tracking of the asset difficult.

The process and system of the present invention has been described above in terms of functional modules in block diagram format. It is understood that unless otherwise stated to the contrary herein, one or more functions may be integrated in a single physical device or a software module in a software product, or one or more functions may be implemented in separate physical devices or software modules at

a single location or distributed over a network, without departing from the scope and spirit of the present invention.

It is appreciated that detailed discussion of the actual implementation of each module is not necessary for an enabling understanding of the invention. The actual implementation is well within the routine skill of a programmer and system engineer, given the disclosure herein of the system attributes, functionality and inter-relationship of the various functional modules in the system. A person skilled in the art, applying ordinary skill can practice the present invention without undue experimentation.

While the invention has been described with respect to the described embodiments in accordance therewith, it will be apparent to those skilled in the art that various modifications and improvements may be made without departing from the scope and spirit of the invention. For example, the information extraction application can be easily modified to accommodate different or additional processes to provide the user additional flexibility for web browsing. Accordingly, it is to be understood that the invention is not to be limited by the specific illustrated embodiments, but only by the scope of the appended claims.

CLAIMS

1, A persistent servicing agent disposed in an electronic device connected to a network to a remote server, to enable, support and/or provide at least one service with respect to the electronic device, comprising:

a driver agent concealed in the electronic device, wherein the driver agent is configured to be persistent against external tampering, including self-healing in the event of tampering, and wherein the driver agent comprises at least one of a partial driver agent or a full function driver agent, wherein the full function driver agent is configured to communicate with the network in providing the service, and the partial driver agent is configured with a reduced set of functions compared to the full function driver agent, and to determine whether a full function driver agent is available in the electronic device; and

a run module configured to automatically initiate operation of the driver agent without user initiation or user intervention.

2. The persistent servicing agent as in claim 1, wherein driver agent is configured to enable, support and/or provide service comprising at least one of asset tracking, asset recovery, software deployment, data deletion, firewall protection, data encryption, location tracking, message notification, and software upgrade.

3. The persistent servicing agent as in claim 1, wherein the driver agent is configured to enable, support and/or provide data deletion service to delete selected data files at the electronic device, and wherein the driver agent provides a report of the data deleted to the remote external server.

4. The persistent servicing agent as in claim 3, wherein the driver agent is configured to enable, support and/or provide deletion of operating system of the electronic device.

5. The persistent servicing agent as in claim 4, wherein the driver agent is configured to first delete data files other than the operating system, provide the report to the remote server, and then delete the operating system.

6. The persistent servicing agent as in claim 3, wherein the driver agent is configured to reinitiate data deletion service in the event a prior data deletion service was interrupted before completion.

7. The persistent servicing agent as in claim 2, wherein the partial driver agent is located in the electronic device in at least one of a firmware, software and hardware.

8. The persistent servicing agent as in claim 7, wherein the firmware comprises a non-volatile memory.

9. The persistent servicing agent as in claim 8, wherein the non-volatile memory comprises at least one of a BIOS chip and flash memory.

10. The persistent servicing agent as in claim 7, wherein the software comprises an operating system of the electronic device.

11. The persistent servicing agent as in claim 3, wherein the driver agent is configured to communicate with the remote server, to receive instructions from the remote server in connection with data deletion of selected data files in the electronic device.

12. The persistent servicing agent as in claim 2, wherein the driver agent is configured to communicate with the remote server, to receive instructions from the remote server to perform the service in accordance with such instructions, wherein such communication may be initiated by the driver agent or the server.

13. The persistent servicing agent as in claim 12, wherein the driver agent is configured to communicate with the remote server, to receive instructions from the remote server in connection with establishing firewall protection in the electronic device.

14. The persistent servicing agent as in claim 12, wherein the driver agent is configured to communicate with the remote server, to receive instructions from the remote server in connection with undertaking data encryption in the electronic device.

15. The persistent servicing agent as in claim 12, wherein the driver agent is configured to communicate with the remote server, to receive instructions from the remote server in connection with location tracking of electronic device.

16. The persistent servicing agent as in claim 12, wherein the driver agent is configured to communicate with the remote server, to receive message notification and/or instructions to disable certain functionality of the electronic device.

17. An electronic device, comprising a persistent servicing agent as in claim 1.

18. A method of enabling, supporting and/or providing a service in an electronic device, comprising:

concealing a driver agent in the electronic device wherein the driver agent is configured to be persistent against external tampering, including self-healing in the event of tampering;

providing a run module configured to automatically initiate operation of the driver agent without user initiation or user intervention; and

operatively connecting the driver agent to a network to communicate with a remote server, to receive instructions relating to the service.

19. The method as in claim 17, wherein the service comprises at least one of asset tracking, asset recovery, software deployment, data deletion, firewall protection, data encryption, location tracking, message notification, and software upgrade.

20. The method as in claim 18, wherein the driver agent is configured to enable, support and/or provide data deletion service to delete selected data files at the electronic device, and wherein the driver agent is configured to enable, support and/or provide deletion of operating system of the electronic device.

21. The method as in claim 19, wherein the driver agent is configured to first delete data files other than the operating system, provide the report to the remote server, and then delete the operating system.

22. A system for providing at least one service at an electronic device connected to a network, comprising:

a remote server connected to the network;

a persistent servicing agent disposed in the electronic device, comprising a driver agent concealed in the electronic device, wherein the driver agent is configured to be persistent against external tampering, including self-healing in the event of tampering, wherein the driver agent comprises at least one of a partial driver agent or a full function driver agent, and wherein the full function driver agent is configured to communicate with the network in providing the service, and the partial driver agent is configured with a reduced set of functions compared to the full function driver agent, and to determine whether a full function driver agent is available in the electronic device; the persistent servicing agent further comprising a run module configured to automatically initiate operation of the driver agent without user initiation or user intervention;

wherein the persistent agent communicates with the remote server to receive instructions from the remote server to perform the service in accordance with such instructions.

23. The system as in claim 22, wherein such communication may be initiated by the driver agent or the server.

24. The system as in claim 22, wherein the persistent servicing agent is configured to communicate with the remote server, to receive instructions from the remote server in connection with at least one of:

(a) establishing firewall protection in the electronic device;

(b) undertaking data encryption in the electronic device;

(c) location tracking of electronic device;

(d) receiving message notification; and

(e) disabling certain functionality of the electronic device.

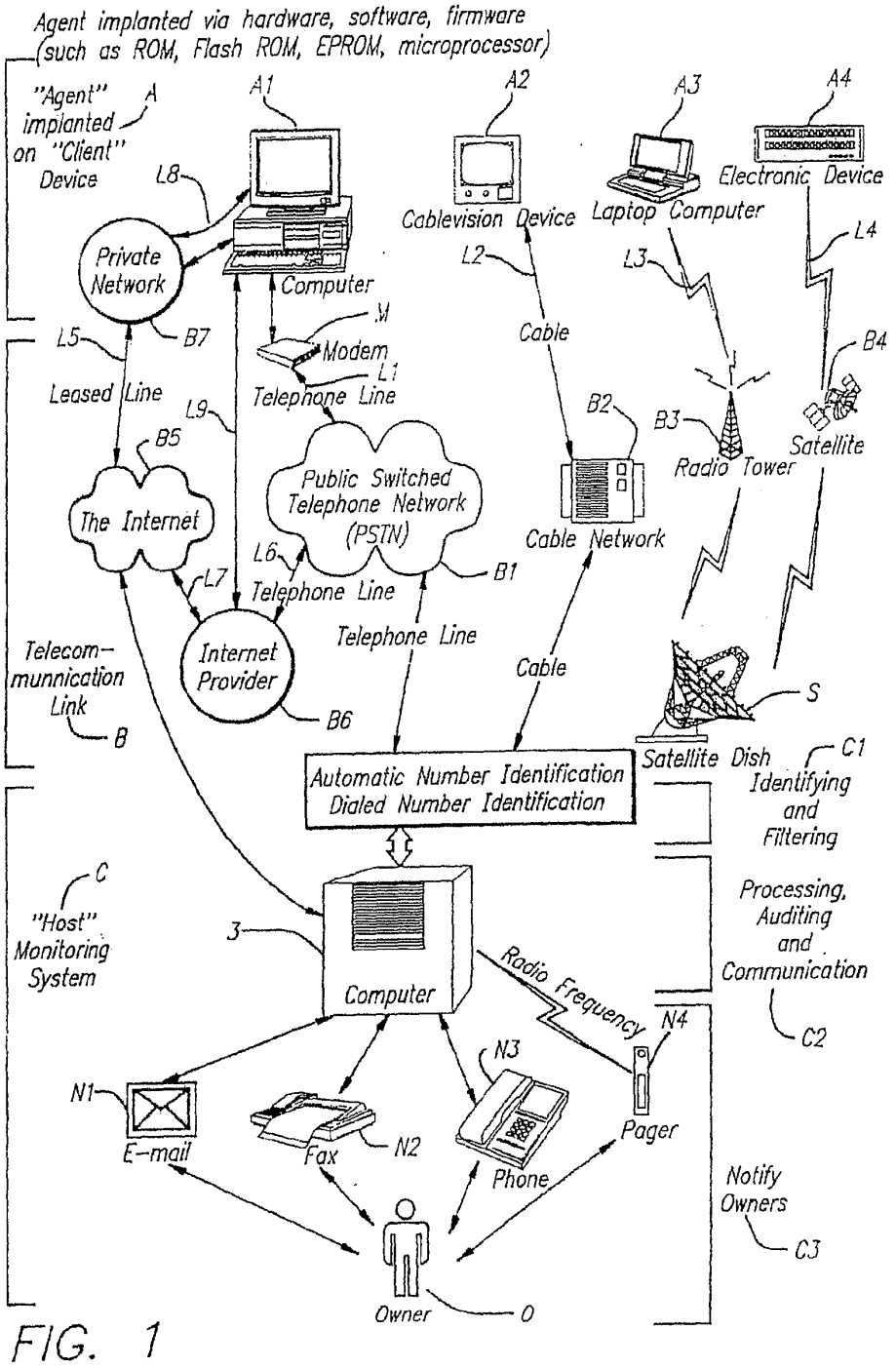

Agent implanted via hardware, software, firmware (such as ROM, Flash ROM, EPROM, microprocessor)
"Agent" implanted on "Client" Device
A
A1
A2
A3
A4
Electronic Device
Cablevision Device
Laptop Computer
L8
Private Network
Computer
L4
L2
L3
Cable
M
Modem
L1
Telephone Line
L5
B7
Leased Line
L9
B4
B2
B3
Satellite
Radio Tower
B5
Public Switched Telephone Network (PSTN)
Cable Network
The Internet
L6
B1
L7
Telephone Line
Telephone Line
Cable
Telecom-munnication Link
B
Internet Provider
B6
S
Satellite Dish
C1
Identifying and Filtering
Automatic Number Identification Dialed Number Identification
C
"Host" Monitoring System
3
Computer
Radio Frequency
N4
Processing, Auditing and Communication
C2
N3
N1
E-mail
Fax
N2
Phone
Pager
Notify Owners
C3
Owner
O

FIG. 1

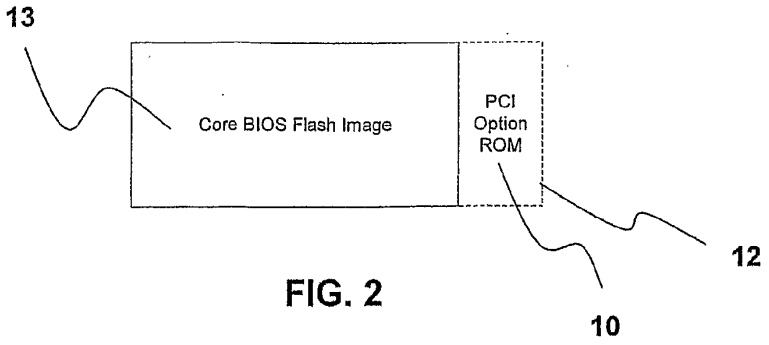

13
Core BIOS Flash Image
PCI
Option
ROM
12
10

FIG. 2

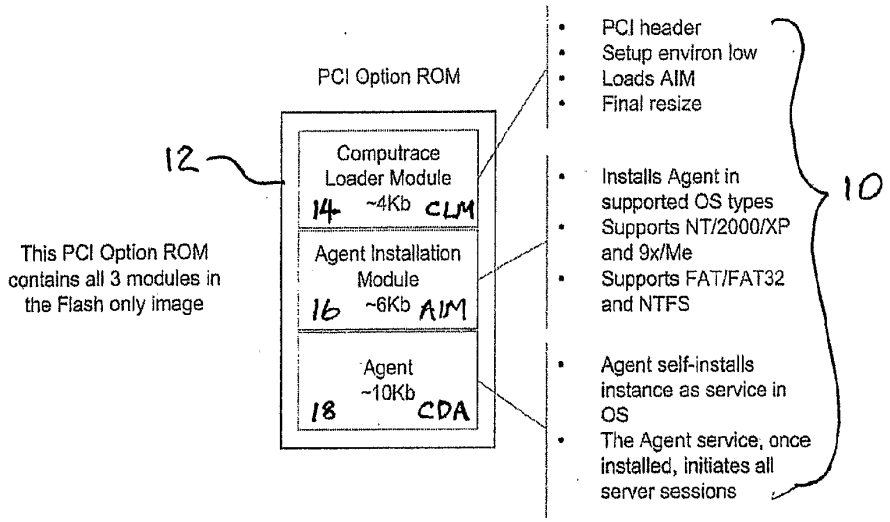

PCI Option ROM
12
Computrace
Loader Module
14 ~4Kb CLM
Agent Installation
Module
16 ~6Kb AIM
Agent
~10Kb
18 CDA
This PCI Option ROM
contains all 3 modules in
the Flash only image
• PCI header
• Setup environ low
• Loads AIM
• Final resize
• Installs Agent in
supported OS types
• Supports NT/2000/XP
and 9x/Me
• Supports FAT/FAT32
and NTFS
• Agent self-installs
instance as service in
OS
• The Agent service, once
installed, initiates all
server sessions
10

FIG. 3

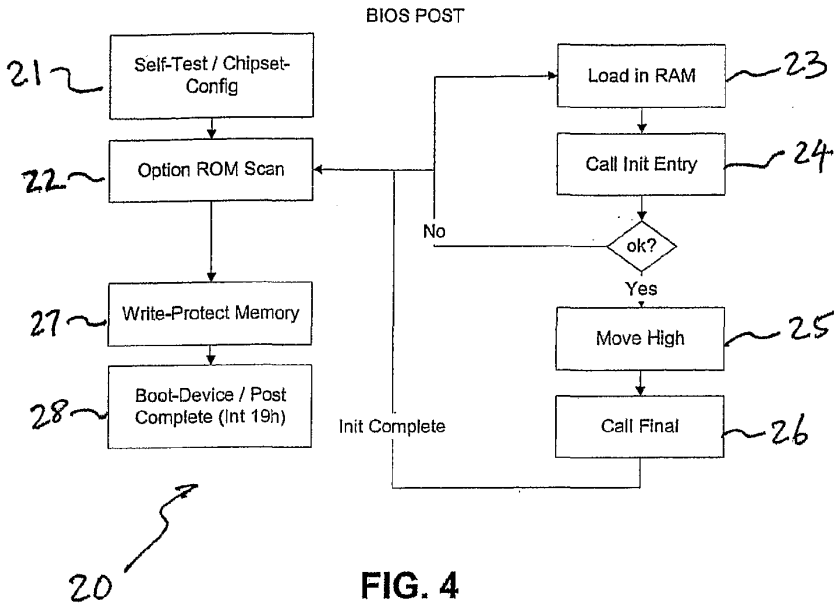

BIOS POST
21
Self-Test / Chipset-Config
22
Option ROM Scan
27
Write-Protect Memory
28
Boot-Device / Post Complete (Int 19h)
20
Load in RAM
23
Call Init Entry
24
No
ok?
Yes
Move High
25
Call Final
26
Init Complete

FIG. 4

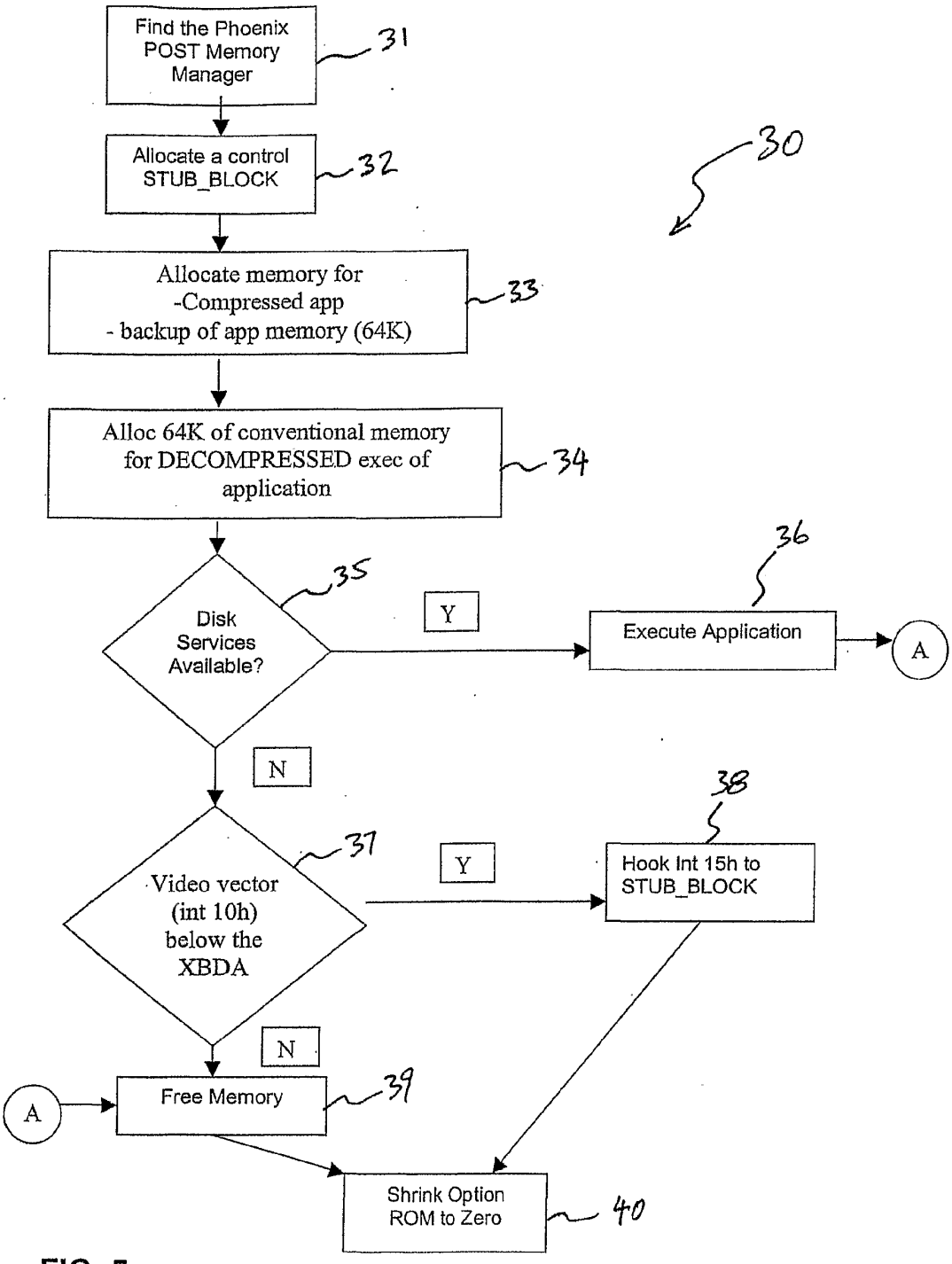

Find the Phoenix POST Memory Manager
31
Allocate a control STUB_BLOCK
32
30
Allocate memory for -Compressed app - backup of app memory (64K)
33
Alloc 64K of conventional memory for DECOMPRESSED exec of application
34
Disk Services Available?
35
Y
36
Execute Application
A
N
Video vector (int 10h) below the XBDA
37
Y
38
Hook Int 15h to STUB_BLOCK
N
A
Free Memory
39
Shrink Option ROM to Zero
40

FIG. 5

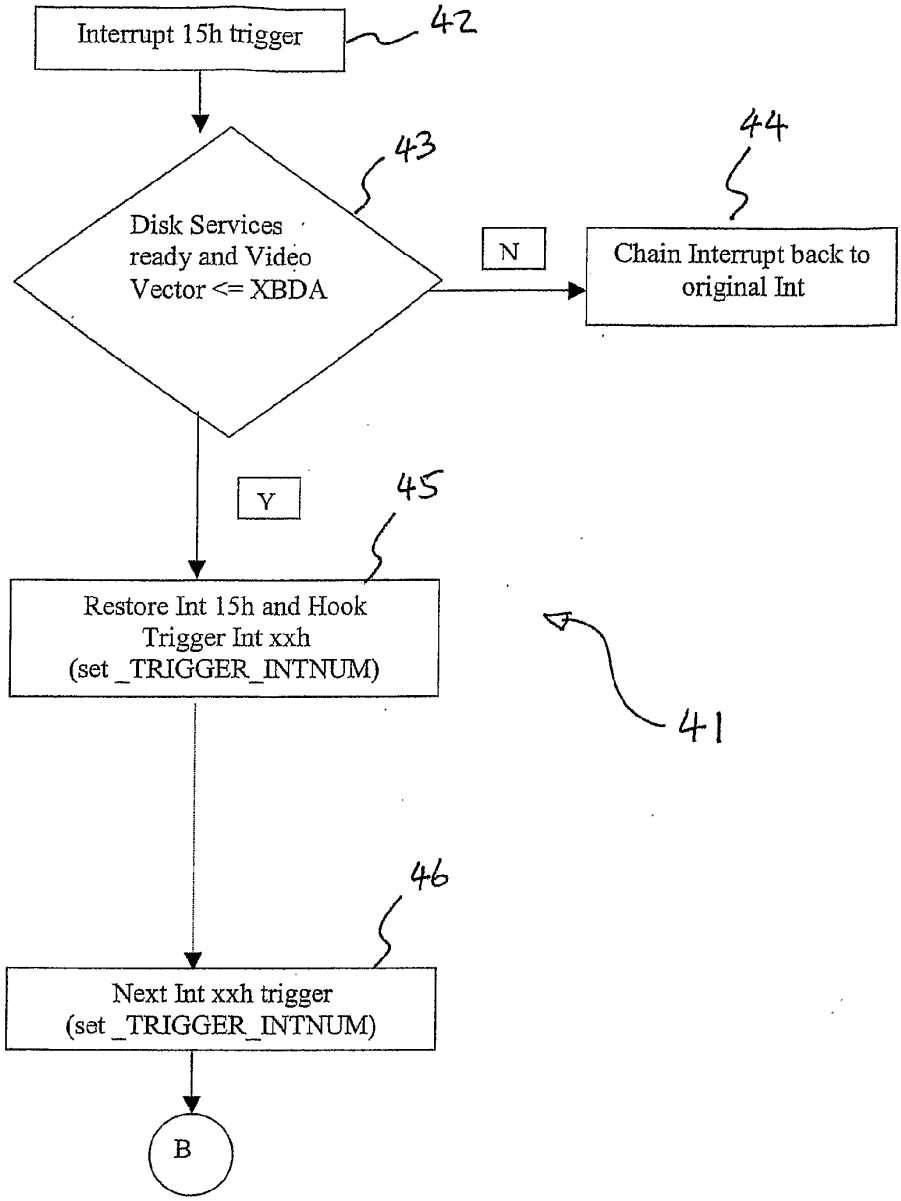

Interrupt 15h trigger
42
43
Disk Services ready and Video Vector <= XBDA
44
N
Chain Interrupt back to original Int
Y
45
Restore Int 15h and Hook Trigger Int xxh (set _TRIGGER_INTNUM)
41
46
Next Int xxh trigger (set _TRIGGER_INTNUM)
B

FIG. 6a

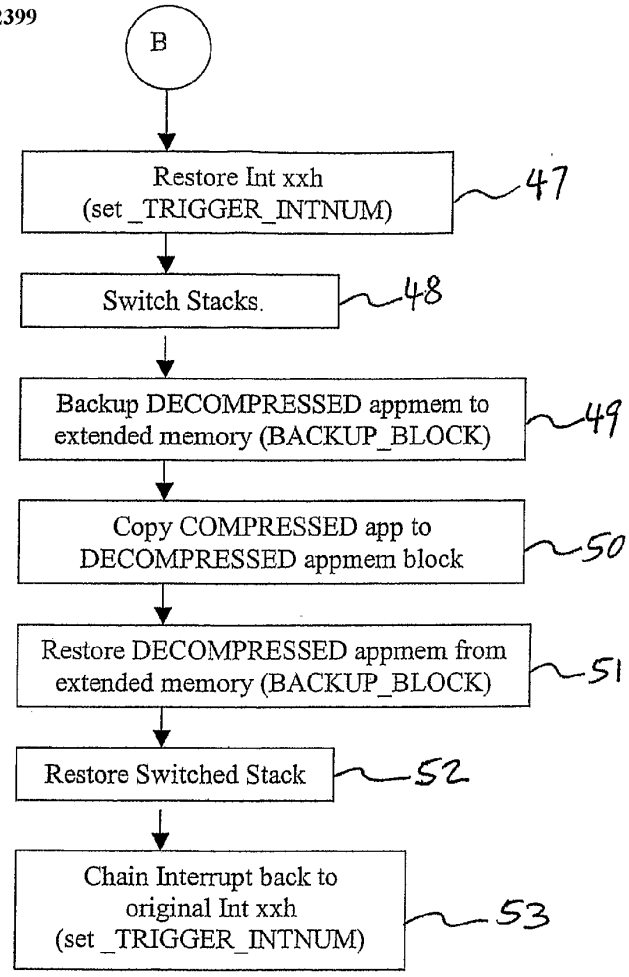

B
Restore Int xxh
(set _TRIGGER_INTNUM)
47
Switch Stacks.
48
Backup DECOMPRESSED appmem to
extended memory (BACKUP_BLOCK)
49
Copy COMPRESSED app to
DECOMPRESSED appmem block
50
Restore DECOMPRESSED appmem from
extended memory (BACKUP_BLOCK)
51
Restore Switched Stack
52
Chain Interrupt back to
original Int xxh
(set _TRIGGER_INTNUM)
53

FIG. 6b

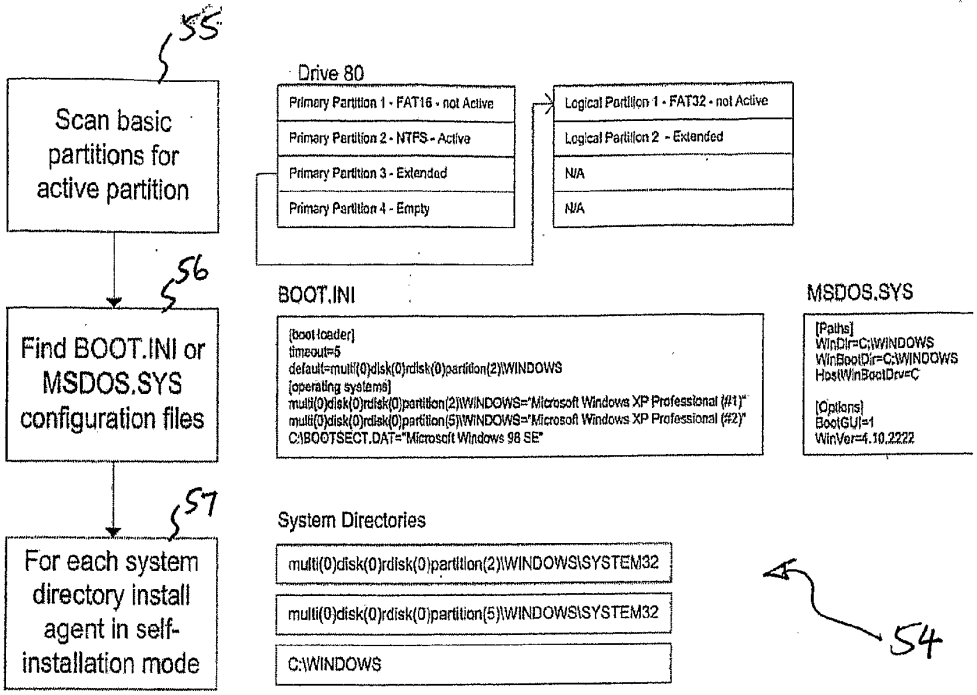

55
Scan basic partitions for active partition
56
Find BOOT.INI or MSDOS.SYS configuration files
57
For each system directory install agent in self-installation mode
Drive 80
Primary Partition 1 - FAT16 - not Active
Primary Partition 2 - NTFS - Active
Primary Partition 3 - Extended
Primary Partition 4 - Empty
Logical Partition 1 - FAT32 - not Active
Logical Partition 2 - Extended
N/A
N/A
BOOT.INI
[boot loader]
timeout=5
default=multi(0)disk(0)rdisk(0)partition(2)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(2)\WINDOWS="Microsoft Windows XP Professional (#1)"
multi(0)disk(0)rdisk(0)partition(5)\WINDOWS="Microsoft Windows XP Professional (#2)"
C:\BOOTSECT.DAT="Microsoft Windows 98 SE"
MSDOS.SYS
[Paths]
WinDir=C:\WINDOWS
WinBootDir=C:\WINDOWS
HostWinBootDrv=C
[Options]
BootGUI=1
WinVer=4.10.2222
System Directories
multi(0)disk(0)rdisk(0)partition(2)\WINDOWS\SYSTEM32
multi(0)disk(0)rdisk(0)partition(5)\WINDOWS\SYSTEM32
C:\WINDOWS
54

FIG. 7

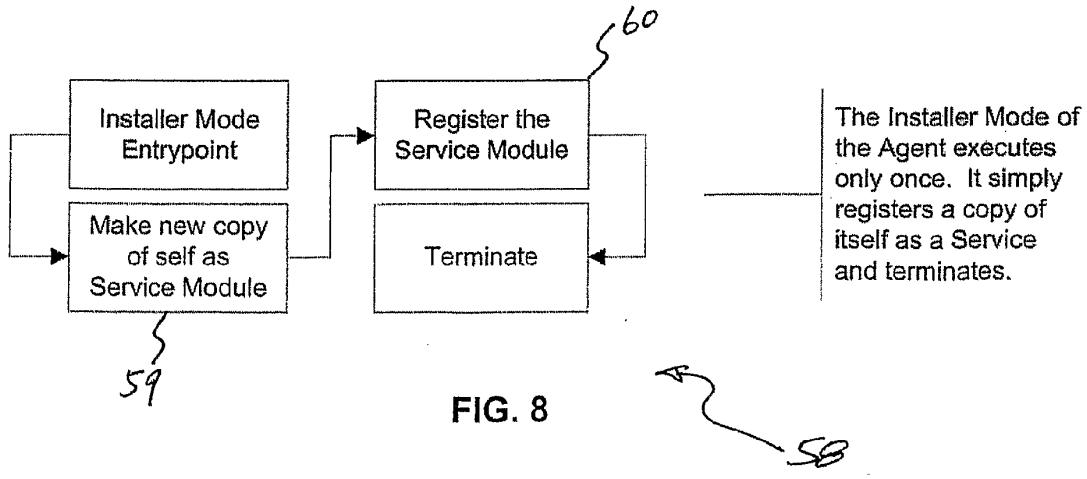

60
Installer Mode Entrypoint
Make new copy of self as Service Module
59
Register the Service Module
Terminate
The Installer Mode of the Agent executes only once. It simply registers a copy of itself as a Service and terminates.
58

FIG. 8

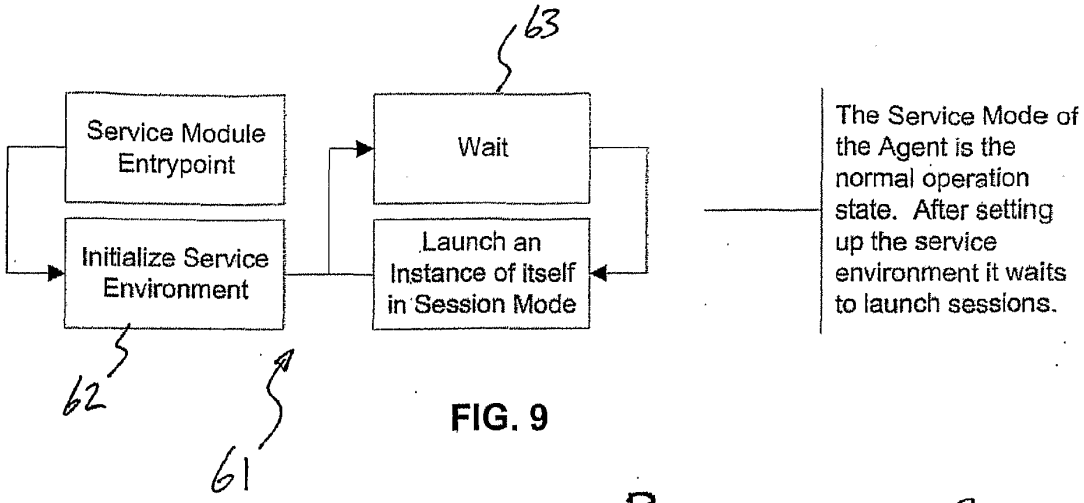

63
Service Module Entrypoint
Wait
Initialize Service Environment
Launch an Instance of itself in Session Mode
The Service Mode of the Agent is the normal operation state. After setting up the service environment it waits to launch sessions.
62
61

FIG. 9

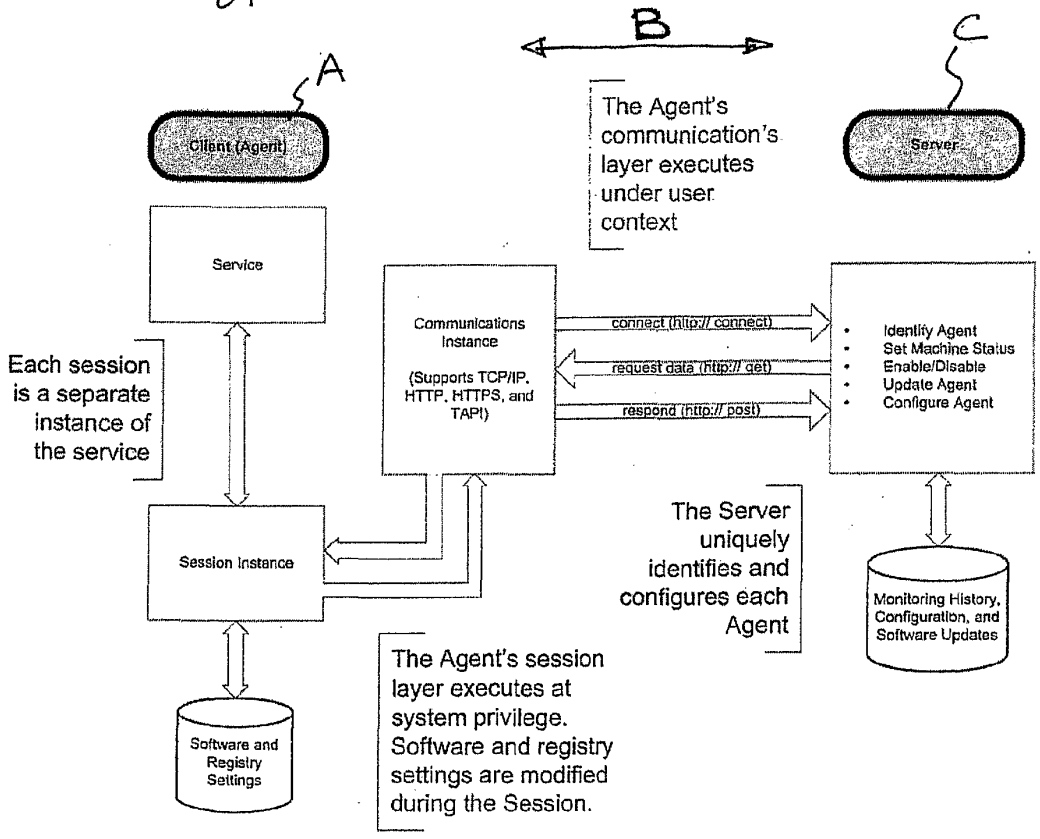

A
B
C
Client (Agent)
Server
The Agent's communication's layer executes under user context
Service
Each session is a separate instance of the service
Communications Instance
(Supports TCP/IP, HTTP, HTTPS, and TAPI)
connect (http:// connect)
request data (http:// get)
respond (http:// post)
Identify Agent
Set Machine Status
Enable/Disable
Update Agent
Configure Agent
Session Instance
The Server uniquely identifies and configures each Agent
Monitoring History, Configuration, and Software Updates
Software and Registry Settings
The Agent's session layer executes at system privilege. Software and registry settings are modified during the Session.

FIG. 10

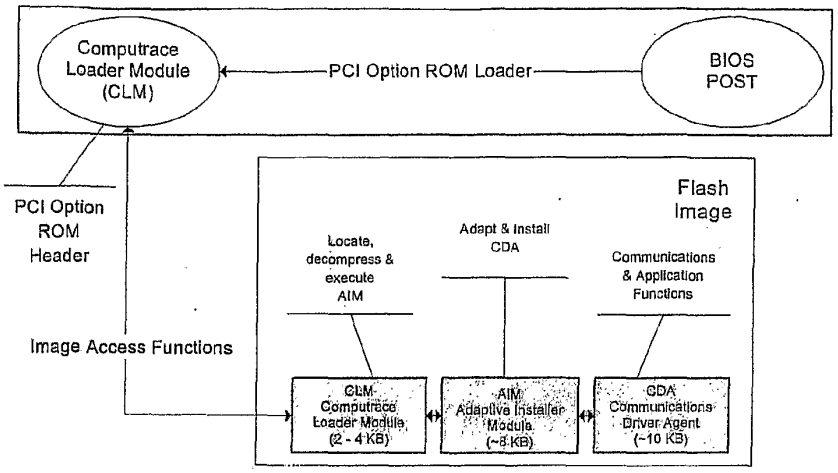

Computrace Loader Module (CLM)
PCI Option ROM Loader
BIOS POST
PCI Option ROM Header
Image Access Functions
Flash Image
Locate, decompress & execute AIM
Adapt & Install CDA
Communications & Application Functions
CLM Computrace Loader Module (2 - 4 KB)
AIM Adaptive Installer Module (~8 KB)
CDA Communications Driver Agent (~10 KB)

FIG. 11

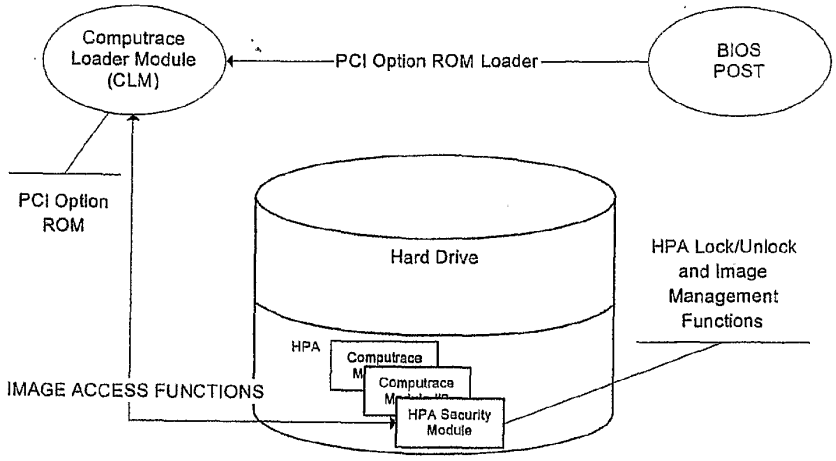

Computrace Loader Module (CLM)
PCI Option ROM Loader
BIOS POST
PCI Option ROM
IMAGE ACCESS FUNCTIONS
Hard Drive
HPA
Computrace
Computrace
HPA Security Module
HPA Lock/Unlock and Image Management Functions

FIG. 12

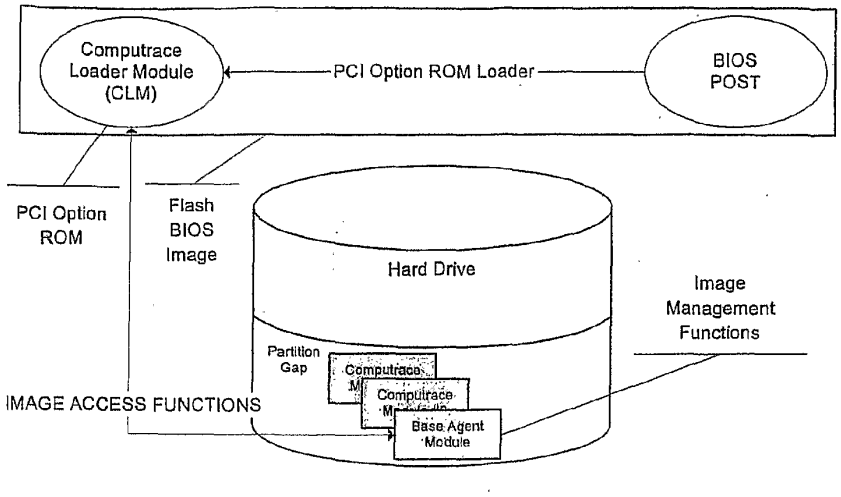

Computrace
Loader Module
(CLM)
PCI Option ROM Loader
BIOS
POST
PCI Option
ROM
Flash
BIOS
Image
Hard Drive
Image
Management
Functions
Partition
Gap
Computrace
M
Computrace
M
Base Agent
Module
IMAGE ACCESS FUNCTIONS

FIG. 13

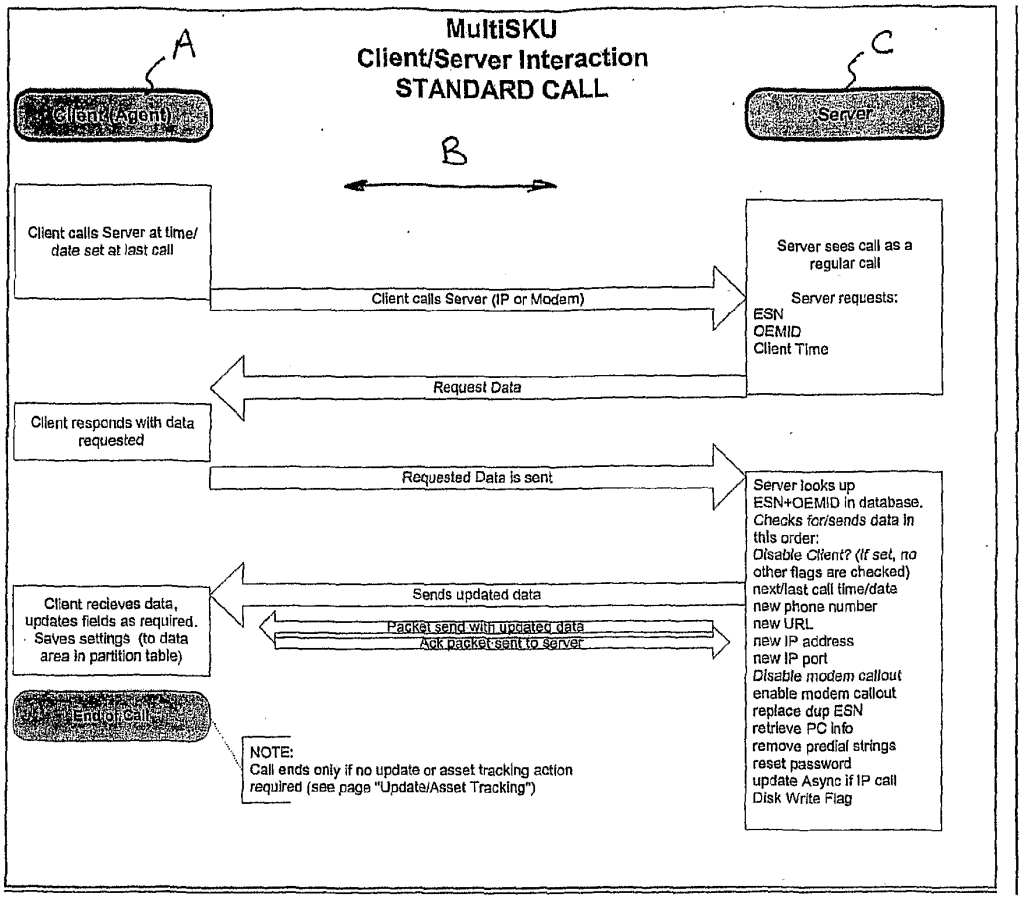

MultiSKU
Client/Server Interaction
STANDARD CALL
A
B
C
Client (Agent)
Server
Client calls Server at time/ date set at last call
Client calls Server (IP or Modem)
Server sees call as a regular call
Server requests:
ESN
OEMID
Client Time
Request Data
Client responds with data requested
Requested Data is sent
Server looks up ESN+OEMID in database.
Checks for/sends data in this order:
Disable Client? (If set, no other flags are checked)
next/last call time/data
new phone number
new URL
new IP address
new IP port
Disable modem callout
enable modem callout
replace dup ESN
retrieve PC info
remove predial strings
reset password
update Async if IP call
Disk Write Flag
Sends updated data
Client recieves data, updates fields as required. Saves settings (to data area in partition table)
Packet send with updated data
Ack packet sent to server
End of call
NOTE:
Call ends only if no update or asset tracking action required (see page "Update/Asset Tracking")

FIG. 14

Client Logic Flow

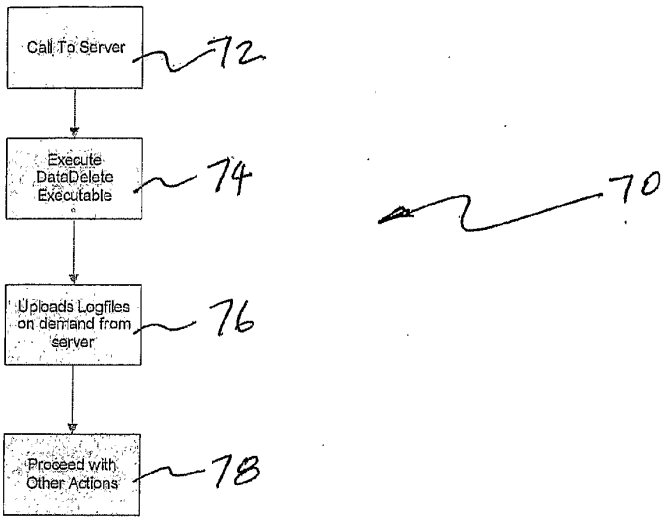


FIG. 15

Server Logic Flow

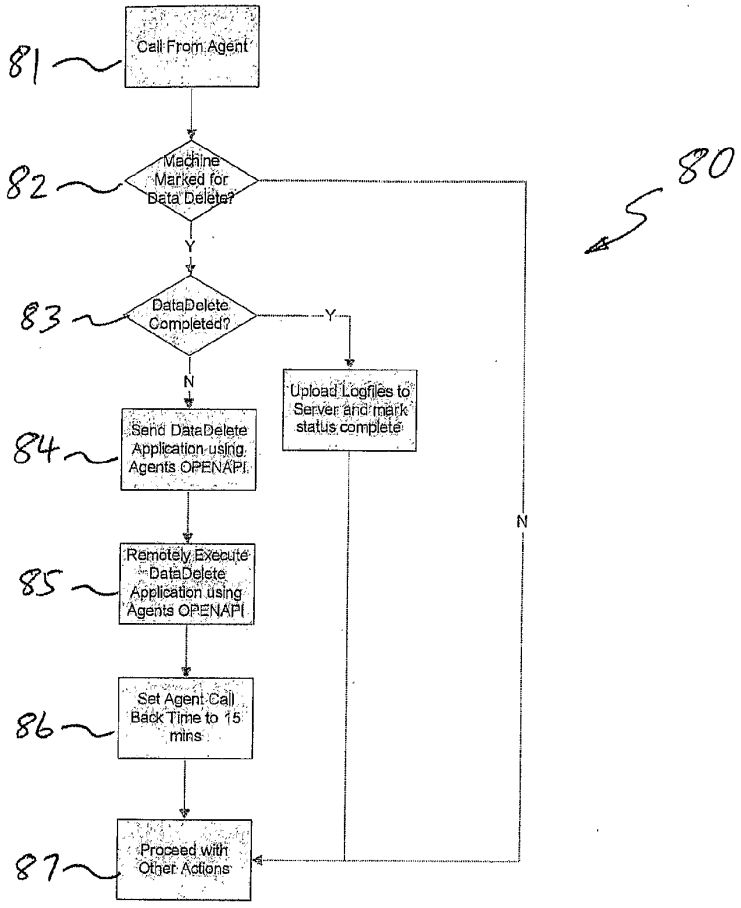


FIG. 16

Data Delete (WCTSYS.EXE) Logic Flow

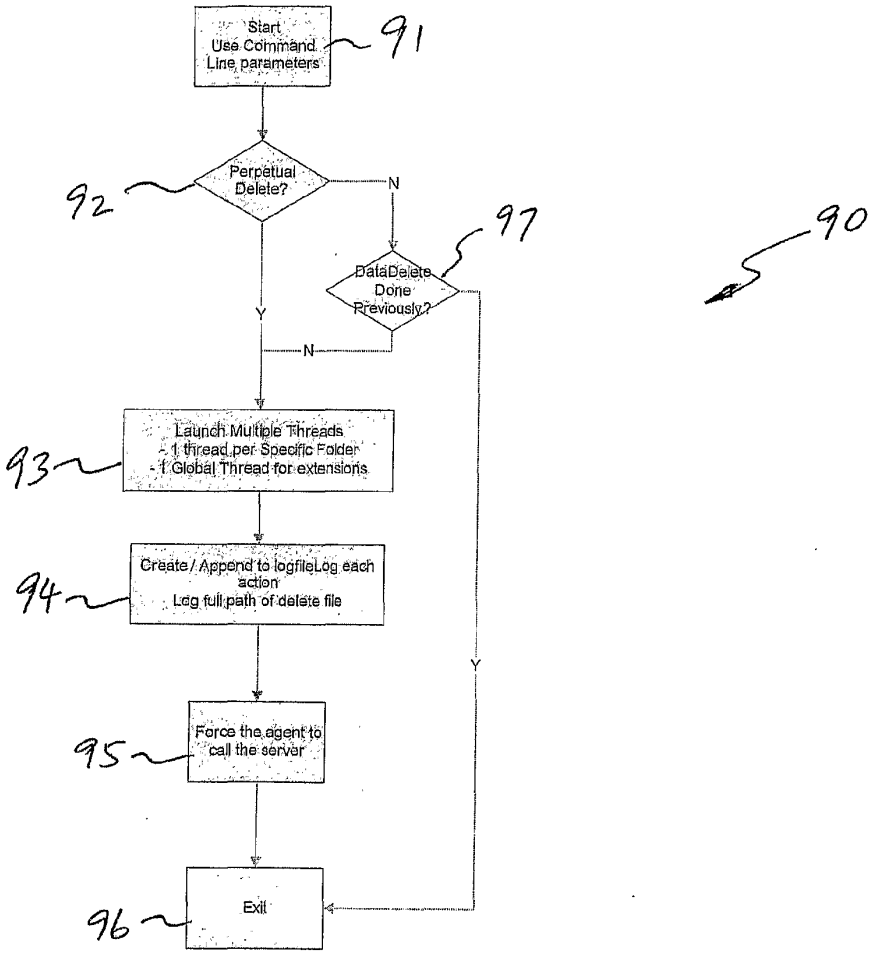


FIG. 17

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2006/010381

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	WO 2005/096122 A (ABSOLUTE SOFTWARE CORPORATION; GARDNER, PHILIP, B) 13 October 2005 (2005-10-13) claims 1-20; figures 1-14	1-22
X	US 5 680 547 A (CHANG ET AL) 21 October 1997 (1997-10-21) column 2, lines 10-42 column 4, lines 44-46	1-22
X	US 2003/051090 A1 (BONNETT WILLIAM B ET AL) 13 March 2003 (2003-03-13) paragraphs [0006] - [0009], [0022]	1-22
X	WO 01/84455 A (SOLAGENT, INC) 8 November 2001 (2001-11-08) page 3, lines 14-16	1-22

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 August 2006	24/08/2006

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Kerschbaumer, J

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2006/010381

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 748 084 A (ISIKOFF ET AL) 5 May 1998 (1998-05-05) claim 1	1-22

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2006/010381

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2005096122 A	13-10-2005	NONE	
US 5680547 A	21-10-1997	AU 1042895 A	15-05-1996
		JP 10511783 T	10-11-1998
		US 5444850 A	22-08-1995
US 2003051090 A1	13-03-2003	NONE	
WO 0184455 A	08-11-2001	AU 5391001 A	12-11-2001
		EP 1257958 A1	20-11-2002
		US 7047426 B1	16-05-2006
US 5748084 A	05-05-1998	NONE	

Form PCT/ISA/210 (patent family annex) (April 2005)

Electronic Patent Application Fee Transmittal	
Application Number:	13734178
Filing Date:	04-Jan-2013
Title of Invention:	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES
First Named Inventor/Applicant Name:	Craig S. ETCHEGOYEN
Filer:	Sean Dylan Burdick
Attorney Docket Number:	UN-NP-SC-085
Filed as Small Entity	

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	2806	1	90	90
		Total in USD ($)		**90**

Electronic Acknowledgement Receipt	
EFS ID:	17406962
Application Number:	13734178
International Application Number:	
Confirmation Number:	3155
Title of Invention:	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES
First Named Inventor/Applicant Name:	Craig S. ETCHEGOYEN
Customer Number:	96051
Filer:	Sean Dylan Burdick
Filer Authorized By:	
Attorney Docket Number:	UN-NP-SC-085
Receipt Date:	14-NOV-2013
Filing Date:	04-JAN-2013
Time Stamp:	17:39:26
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$90
RAM confirmation Number	4993
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Amendment/Req. Reconsideration-After Non-Final Reject	SC-085_Response_to_OA_of_09-06-2013_FINAL.pdf	91959 e9f6db0b4ee3a76c16b07b35df15e9b6fd235eec	no	13
Warnings:					
Information:					
2	Transmittal Letter	SC-085_IDS_transmittal.pdf	29760 3e14dd5877d209935da54ec3fb7e9ea002acf0ac	no	2
Warnings:					
Information:					
3	Information Disclosure Statement (IDS) Form (SB08)	SC-085_IDS_List.pdf	35915 f3d87d008380c8719633e8c81fe2c7845c9a6032	no	1
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
4	Examination support document	SC-085_new_claim_correspondence_table_FINAL.pdf	21464 f9e94b46ed2100517af4db0a84b45ff26ad8dd48	no	1
Warnings:					
Information:					
5	Foreign Reference	EP1903518_NCR_Corp.pdf	151977 884ca942198330681ad38eb19ab52f55256cf1cd	no	11
Warnings:					
Information:					
6	Foreign Reference	JP_5181734A_Hitachi_English_Abstract.pdf	37287 cff071346301af3cbc8206c064fd2a5cec502bdd	no	1
Warnings:					
Information:					
7	Foreign Reference	GB2391965_MessageLabs.PDF	697789 337ff22dafff2fad3ff3469097bafe1c95dd3b0a	no	21
Warnings:					
Information:					
8	Foreign Reference	WO_2006102399_Absolute_Software_Corp.pdf	9548421 cc311ce8131f62c71915f3af7942d71e031a7420	no	63
Warnings:					
Information:					
9	Fee Worksheet (SB06)	fee-info.pdf	30630 f65210b7a030cf01b98c8c49af111d21899aca5c	no	2

Warnings:	
Information:	
Total Files Size (in bytes):	10645202

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/734,178	Filing Date 01/04/2013	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 11/14/2013	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 9	Minus	** 20	= 0	X $40 =	0
Independent (37 CFR 1.16(h))	* 1	Minus	***3	= 0	X $210 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/NINA RATANAVONG/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/734,178	01/04/2013	Craig S. ETCHEGOYEN	UN-NP-SC-085	3155

96051 7590 01/21/2014

Uniloc USA Inc.
Legacy Town Center
7160 Dallas Parkway
Suite 380
Plano, TX 75024

EXAMINER	
AKINYEMI, AJIBOLA A	
ART UNIT	PAPER NUMBER
2649	

NOTIFICATION DATE	DELIVERY MODE
01/21/2014	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

sean.burdick@unilocusa.com
sbaker@unilocusa.com
tkiatkulpiboone@unilocusa.com

Office Action Summary	Application No. 13/734,178	Applicant(s) ETCHEGOYEN ET AL.	
	Examiner AJIBOLA AKINYEMI	Art Unit 2649	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11/14/2013*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-9* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-9* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *01/04/2013* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some * c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

1) The present application is being examined under the pre-AIA first to invent provisions.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained through the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under pre-AIA 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.

2. Ascertaining the differences between the prior art and the claims at issue.

3. Resolving the level of ordinary skill in the pertinent art.

4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

3. Claim 1 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Gass (Pub. No.: US 2004/0038716A1) and further in view of Philips (Pub. No.: US 2013/0159701A1).

With respect to claim 1:

Gass discloses a method for near field authentication of a source the source using an audio transceiver computing device comprising scanning a plurality of predetermined frequencies for a free frequency **(parag,0016 discloses scanning plurality of predetermined frequency for a free frequencies);** selecting the free frequency from the plurality of predetermined frequencies **(parag.0016 also discloses selecting free frequency from plurality of frequencies);** generating a periodic enclosed content message; generating a modulated carrier wave representing the periodic enclosed content message and transmitting the modulated carrier wave at the free frequency **(Parag. 0015 also discloses the RDS encoder encodes said frequency or channel information generating a corresponding RDS signal 5 modulated on the RDS sub carrier at 57 KHz).**

Gass does not explicitly disclose wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication; and wherein the content includes at least one of biometric data, or device identification data.

Philip discloses an enclosed content message includes a begin indication, a content, and an end indication; and wherein the content includes at least one of biometric data **(parag. 0084, 0090).** It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the teaching of Philips into the teaching of Gass in order to provide a digital container and encrypting the contents of the digital container with a symmetric encryption technique.

4. Claim 2 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Gass (Pub. No.: US 2004/0038716A1), Philips (Pub. No.: US 2013/0159701A1) as applied to claim 1 above and further in view of Martin (Pub. No.: US 2007/0198850A1).

With respect to claim 2:

The rejection of claim 1 is incorporated; Gass, Philips do not explicitly disclose the method further comprising displaying a user interface on the audio transceiver computing device requesting the biometric data from a user; and responsive to receiving the biometric data, generating the periodic enclosed content message, wherein the content in each period of the periodic enclosed content message includes the biometric data.

Martin discloses this limitation (parag. 0062-0063 discloses a user interface on the audio transceiver computing device requesting the biometric data from a user). It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the teaching of Martin into the teaching of Gass in view of Philips in order to provide a security system wherein the user is provided with dual layered verification system in addition to a unique identifier given to the user.

5. Claims 3-5 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Gass (Pub. No.: US 2004/0038716A1), Philips (Pub. No.: US 2013/0159701A1) as applied to claim 1 above and further in view of Kip (Patent No.: US 5019813).

With respect to claim 3:

The rejection of claim 1 is incorporated; Gass and Philip do not explicitly disclose wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

Kip discloses this above limitations (col.5, line 39-44). It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the teaching of Kip into the teaching of Gass view of Philip in order to provide a universally applicable data exchange system operating in a contactless manner.

With respect to claim 4:

Kip discloses the method wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user (fig.5b, col.5, line 39-44).

With respect to claim 5:

Gass discloses the method wherein the modulated carrier wave comprises a sound wave (parag. 0016).

6. Claims 6-8 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Gass (Pub. No.: US 2004/0038716A1), Philips (Pub. No.: US 2013/0159701A1), Martin (Pub. No.: US 2007/0198850A1) as applied to claim 2 above and further in view of Kip (Patent No.: US 5019813).

With respect to claim 6:

The rejection of claim 2 is incorporated; Gass, Philips and Martin do not disclose wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

Kip discloses this above limitations (col.5, line 39-44). It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the teaching of Kip into the teaching of Gass in view of Philips and Martin in order to provide a universally applicable data exchange system operating in a contactless manner.

With respect to claim 7:

Kip discloses the method wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user (fig.5b, col.5, line 39-44).

With respect to claim 8:

Gass discloses the method wherein the modulated carrier wave comprises a sound wave (parag. 0016).

7. Claim 9 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Gass (Pub. No.: US 2004/0038716A1) and further in view of Kasargod (Pub. No.: US 2010/0208899A1).

With respect to claim 9:

The rejection of claim 1 is incorporated; Gass does not explicitly disclose the method wherein the carrier wave is modulated by the periodic enclosed content message. Kasargod discloses this limitation (parag.0006). It would have been obvious to one of

ordinary skill in the art at the time the invention was made to utilize the teaching of Kasargod into the teaching of Gass in order to enhance bass effect in audio signals using low complexity non-linear saturating functions.

Response to Arguments

Applicant's arguments with respect to claim 1 have been considered but are moot because the arguments do not apply to any of the references being used in the current rejection.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to AJIBOLA AKINYEMI whose telephone number is (571)270-1846. The examiner can normally be reached on monday- friday (8.30-5pm) Est.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, YUWEN PAN can be reached on (571) 272-7855. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/AJIBOLA AKINYEMI/
Primary Examiner, Art Unit 2649

Notice of References Cited	Application/Control No. 13/734,178	Applicant(s)/Patent Under Reexamination ETCHEGOYEN ET AL.	
	Examiner AJIBOLA AKINYEMI	Art Unit 2649	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-5,019,813 A	05-1991	Kip et al.	340/10.51
*	B	US-2004/0038716 A1	02-2004	Gass, Vincent	455/569.1
*	C	US-2007/0198850 A1	08-2007	Martin et al.	713/186
*	D	US-2010/0208899 A1	08-2010	Kasargod et al.	381/1
*	E	US-2013/0159701 A1	06-2013	PHILLIPS et al.	713/155
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	3	scan$4 with message with header with begin$4 with end$3	US-PGPUB; USPAT	OR	OFF	2014/01/14 11:51
L2	3151	header with begin$4 with end$3	US-PGPUB; USPAT	OR	OFF	2014/01/14 11:53
L3	1652	header with begin$4 with end$3 same (message information content)	US-PGPUB; USPAT	OR	OFF	2014/01/14 11:53
L4	31	3 and biometric	US-PGPUB; USPAT	OR	OFF	2014/01/14 11:54

1/ 14/ 2014 1:41:48 PM
C:\ Users\ aakinyemi\ Documents\ EAST\ Workspaces\ 13288931.wsp

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO
(modified by Applicant)

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	13/734,178
Filing Date	January 4, 2013
First Named Inventor	Craig S. Etchegoyen
Art Unit	2649
Examiner Name	Ajibola A. Akinyemi
Attorney Docket Number	UN-NP-SC-085

U. S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-2008/0097924	04/24/2008	Carper et al.	
		US-2009/0099830	04/16/2009	Gross et al.	
		US-7,818,573	10/19/2010	Martin et al.	
		US-7,965,843	06/21/2011	Maino et al.	
		US-2003/0070067	04/10/2003	Saito, Shin	
		US-2003/0131001	07/10/2003	Matsuo, Masanobu	
		US-2003/0182435	09/25/2003	Redlich et al.	
		US-2003/0237004	12/25/2003	Okamura, Mine	
		US-2006/0075134	04/6/2006	Aalto et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code – Number – Kind Code	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T
		EP 1 903 518	09/10/2007	NCR Corp.		
		JP 5181734	07/23/1993	Hitachi Ltd		
		GB 2391965	02/18/2004	MessageLabs Ltd.		
		WO 2006/102399	09/28/2006	Absolute Software Corporation		

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date page(s), volume-issue number(s), publisher, city and/or country where published.	T

Examiner Signature	/Ajibola Akinyemi/	Date Considered	01/14/2014

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A./

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13734178	ETCHEGOYEN ET AL.
	Examiner	Art Unit
	AJIBOLA AKINYEMI	2649

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
455	41.1	1/14/2014	AA

SEARCH NOTES		
Search Notes	Date	Examiner
455/11.1,569.1	1/14/2014	AA

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13734178	ETCHEGOYEN ET AL.
	Examiner	**Art Unit**
	AJIBOLA AKINYEMI	2649

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	08/30/2013	01/14/2014							
	1	✓	✓							
	2	✓	✓							
	3	✓	✓							
	4	✓	✓							
	5	✓	✓							
	6	✓	✓							
	7	✓	✓							
	8	✓	✓							
	9		✓							

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. no.:	13/734,178	Conf. no.	3155
Applicant:	Craig S. Etchegoyen	Art Unit:	2649
Filed:	January 4, 2013	Examiner:	Ajibola A. Akinyemi

Title: NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES

RESPONSE TO OFFICE ACTION

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir,

In response to the Final Office Action mailed January 21, 2014 ("Final Action"), please reconsider the present application in light of the following remarks.

REMARKS

Applicant thanks Examiner Akinyemi for his thorough review of the application papers and for his opinion on patentability.

Claims 1-9 are pending in the application. Applicant respectfully requests reconsideration of all pending claims in view of the amendments and remarks herein.

Response to Rejections Under 35 USC §103

In the Final Action, claim 1 was rejected under 35 USC §103(a) as being unpatentable over U.S. Application Pub. 2004/0038716 (*"Gass"*) in further view of U.S. Application Pub. 2013/0159701 (*"Phillips"*). Claim 2 was rejected under 35 USC §103(a) as being unpatentable over *Gass*, *Phillips* and in further view of U.S. Application Pub. 2007/0198850 (*"Martin"*). Claims 3-5 were rejected over *Gass* in further view of U.S. Patent 5,019,813 (*"Kip"*). Claims 6-8 were rejected over *Gass*, *Phillips*, *Martin* and in further view of *Kip*. Claim 9 was rejected over *Gass* in further view of U.S. Application Pub. 2010/0208899 (*"Kasargod"*). Applicant respectfully traverses.

As detailed in Applicant's response filed November 14, 2013, the claimed invention is directed to method and apparatus for near field authentication of a financial transaction. See ¶ 9.[1] Specifically, the disclosure relates to a method to authenticate a transaction source (*e.g.*, a buyer) using a specifically-modulated audio signal. The invention may be used, for example, to add another level of security to an electronic transaction, by exploiting the audio transceiving capabilities of modern computing devices. That is, point-of-sale merchant computers already equipped with a microphone input can authenticate an electronic transaction with the buyer's mobile phone by receiving *near-field* audio transmissions from the audio speaker of the mobile phone when the buyer wants to complete the transaction. This ensures that the buyer must be physically present within the merchant's store, to prevent a remote identity thief from completing a phony transaction.

In one embodiment, the method requires the source device to scan several predetermined frequencies for an available or free frequency. See ¶ 63 and Fig. 6, step 602. Once the available

[1] References are made to the Specification as published in U.S. Application Pub. 2013/0203350.

frequency is identified, the source device generates a periodic enclosed content message by generating a modulated carrier wave. See ¶ 65. The modulated carrier wave represents the periodic enclosed content message. See ¶ 34. The content message may contain a device identifier and/or a biometric identifier. See ¶ 34 and 37. The merchant computer decodes the message, extracts the identifier and compares it to a list of authorized identifiers. The transaction is allowed to proceed only if the device is authenticated.

Consistent with this background, pertinent portions of claim 1 recite a method for near field source authentication "wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication; and wherein the content includes at least one of biometric data, or device identification data."

The references to *Gass* and *Phillips*, even if combined, fail to disclose or suggest at least this element. *Gass* is directed to a hands-free mobile phone communication system having a mobile terminal for receiving information over a telephone connection. The system includes a radio sender sending information over a selected frequency channel to an audio system. The audio system is equipped with a broadcast radio receiver and with an audio amplifier to provide an audio output of the received information. See Abstract. At ¶ 7 of the specification, *Gass* discloses that "[t]he basic principle of the invention is, that unused frequency channels are continuously determined, i.e. by carrying out periodically frequency scanning runs, in a hands-free communication system comprising a mobile terminal and an audio system, equipped with a radio sender and a radio receiver respectively."

The reference to *Phillips* is cited for allegedly teaching "each period of the periodic enclosed content message includes a begin indication, a content, and an end indication" and "the content includes at least one of biometric data, or device identification data." *Phillips*, however, fails to support the Office's contention.

Phillips is directed to securing digital content through encryption. See ¶ 3. *Phillips* secures the digital content from copying. In the Abstract section, the reference discloses: "[t]he secured digital container when locked to a user or user's device may not open or permit access to the contents if the digital container is transferred to another user's device." In one embodiment, the reference discloses a system that uses a token-based authentication and authorization procedure and involves the use of an authentication/authorization server. At ¶ 70, *Phillips*

discloses securing digital content using an atomic proxy encryption method. At ¶ 84, which was cited by the Office, *Phillips* discloses:

> The executable instructions of the container code module may read the atomic proxy re-key value 615 from the token 600. An atomic proxy algorithm 705 uses this re-key value 615, along with the unique container ID 210 read from the container, to securely re-encrypt the encrypted header of data block 1, as denoted by reference numeral 715. This one-time operation locks the encrypted content data to the user and/or the user's device 125 and takes place without ever exposing the content data in unencrypted form.

Paragraph 84 teaches using the atomic proxy algorithm and the container ID to *re-encrypt a data block header.* It does not disclose that a "periodic enclosed content message includes a begin indication, a content and an end indication"; nor does it disclose "the content includes at least one of biometric data, or device identification data." Paragraph ¶ 90 (which was also cited by the Office) discloses:

> Depending on what elements of the user's device or user input that were used to create the original machine footprint 335, the user may be prompted to recreate certain conditions that were in effect when the original machine foot print was created. For example, the user may be prompted to re-enter certain security codes or biometric measurements. If the Smart Card scenario was being used, the user may be prompted to re-insert this card in order to successfully reopen the container.

The cited portions of *Phillips* merely require the user to enter certain security codes and biometric information in order to access the files (*i.e.*, reopen the container). The cited portions do not disclose nor suggest "periodic enclosed content message includes a begin indication, a content and an end indication" and "the content includes at least one of biometric data, or device identification data." Clearly, a combination of *Gass* and *Phillips* fails to disclose each and every claimed element.

Moreover, the references may not be combined as suggested by the Office because such combination would render the device of *Gass* inoperable. *Gass* is directed to hands-free mobile communication. It requires a mobile device for receiving information over a telephone connection and a radio sender for sending information to an audio system. Modifying *Gass* in

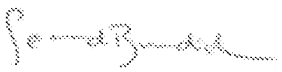
view of *Phillips* requires encrypting information transmissions at the mobile device and applying user input at the radio to decrypt the information received by the audio system. Such modification renders *Gass'* device inoperable because it is contrary to providing a hands-free communication system.

For at least these reasons, Applicant respectfully submits that claim 1 is patentable over *Gass* in view of *Phillips*. Claims 2-9 depend, either directly or indirectly, from an otherwise patentable independent claim. Claims 2-9 are deemed patentable at least by the virtue of their dependence on claim 1. Accordingly, additional reasons for patentability of dependent claims 2-9 will not be proffered. Reconsideration and withdrawal of the obviousness rejections are respectfully requested.

CONCLUSION

In view of all of the above, applicant believes that all pending claims are in condition for allowance and earnestly requests that these claims be passed to issuance. If the Examiner believes that a telephone conversation would help to expedite prosecution, please call the undersigned attorney at the number below.

Respectfully Submitted,



Sean D. Burdick
Reg. No. 51,513

Uniloc USA, Inc.
7160 N. Dallas Parkway, Suite 380
Plano, Texas 75024
(972) 905-9580 x227

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. no.:	13/734,178	Conf. no.	3155
Applicant:	Craig S. Etchegoyen	Art Unit:	2649
Filed:	January 4, 2013	Examiner:	Ajibola A. Akinyemi

Title: NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicant hereby submits, without admission of prior art effect thereof, form(s) PTO/SB/08 pursuant to the duty of disclosure requirements of 37 CFR §§ 1.56, 1.97 and 1.98.

Applicant has listed publication dates on the attached form(s) PTO/SB/08 based on information presently available to the undersigned. However, the listed publication dates should not be construed as an admission that the information was actually published on the date indicated.

It is respectfully requested that the Examiner initial and return a copy of the enclosed forms PTO/SB/08, and to indicate in the official file wrapper of this patent application that the documents have been considered.

Applicant submits concurrently herewith the fee set forth in § 1.17(p).

Respectfully Submitted,

Sean D. Burdick
Reg. No. 51,513

Uniloc USA, Inc.
7160 N. Dallas Parkway, Suite 380
Plano, TX 75024
(972) 905-9580 x227

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO
(modified by Applicant)

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	13/734,178
Filing Date	January 4, 2013
First Named Inventor	Craig S. Etchegoyen
Art Unit	2649
Examiner Name	Ajibola A. Akinyemi
Attorney Docket Number	UN-NP-SC-085

U. S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-5,019,813	05/28/1991	Kip et al.	
		US-5,249,178	09/28/1993	Kurano et al.	
		US-6,791,982	09/14/2004	Westberg, Lars	
		US-6,999,461	02/14/2006	Li et al.	
		US-7,600,039	10/06/2009	Tang et al.	
		US-8,018,937	09/13/2011	Epps et al.	
		US-2002/0163889	11/07/2002	Yemini et al.	
		US-2002/0178122	11/28/2002	Maes, Stephane	
		US-2007/0153764	07/05/2007	Thubert et al.	
		US-2010/0034207	02/11/2010	McGrew et al.	
		US-2010/0146589	06/10/2010	Safa, John Aram	
		US-2012/0275354	11/01/2012	Villain, Frederic	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code – Number – Kind Code	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date page(s), volume-issue number(s), publisher, city and/or country where published.	T

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

PTO/AIA/31 (03-14)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

NOTICE OF APPEAL FROM THE EXAMINER TO THE PATENT TRIAL AND APPEAL BOARD

Docket Number (Optional): UN-NP-SC-085

I hereby certify that this correspondence is being facsimile transmitted to the USPTO, EFS-Web transmitted to the USPTO, or deposited with the United States Postal Service with sufficient postage in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, on Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on _____.

Signature _____

Typed or printed name _____

In re Application of: Craig S. Etchegoyen

Application Number	Filed
13/734,178	January 4, 2013

For: NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION...

Art Unit	Examiner
2649	Ajibola A. Akinyemi

Applicant hereby **appeals** to the Patent Trial and Appeal Board from the last decision of the examiner.

The fee for this Notice of Appeal is (37 CFR 41.20(b)(1)) $ 800.00

☑ Applicant asserts small entity status. See 37 CFR 1.27. Therefore, the fee shown above is reduced by 50%, and the resulting fee is: $ 400.00

☐ Applicant certifies micro entity status. See 37 CFR 1.29. Therefore, the fee shown above is reduced by 75%, and the resulting fee is: $ _____
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 506053.

☑ Payment made via EFS-Web.

☐ A petition for an extension of time under 37 CFR 1.136(a) (PTO/AIA/22 or equivalent) is enclosed.
For extensions of time in reexamination proceedings, see 37 CFR 1.550.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant

☑ attorney or agent of record
Registration number 51513

☐ attorney or agent acting under 37 CFR 1.34
Registration number _____

Signature /Sean D. Burdick/

Typed or printed name Sean D. Burdick

Telephone Number 972-905-9580

Date June 23, 2014

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☑ * Total of 1 forms are submitted.

This collection of information is required by 37 CFR 41.20(b)(1) and 41.31. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	13734178
Filing Date:	04-Jan-2013
Title of Invention:	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES
First Named Inventor/Applicant Name:	Craig S. ETCHEGOYEN
Filer:	Sean Dylan Burdick
Attorney Docket Number:	UN-NP-SC-085

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Notice of Appeal	2401	1	400	400
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 2 months with $0 paid	2252	1	300	300
Miscellaneous:				
		Total in USD ($)		**700**

Electronic Acknowledgement Receipt	
EFS ID:	19384772
Application Number:	13734178
International Application Number:	
Confirmation Number:	3155
Title of Invention:	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES
First Named Inventor/Applicant Name:	Craig S. ETCHEGOYEN
Customer Number:	96051
Filer:	Sean Dylan Burdick
Filer Authorized By:	
Attorney Docket Number:	UN-NP-SC-085
Receipt Date:	23-JUN-2014
Filing Date:	04-JAN-2013
Time Stamp:	18:08:52
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$700
RAM confirmation Number	5268
Deposit Account	506053
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Response After Final Action	SC-085_Response_to_FOA_01-21-2014_FINAL.pdf	47905 d00b0bec8a11aa4e7a445e68ede6128140c20ae8	no	5
Warnings:					
Information:					
2	Transmittal Letter	SC-085_IDS_Transmittal.pdf	102176 6c0255fd89165605c21e6d96e8d9452e1c6e6d7b	no	2
Warnings:					
Information:					
3	Information Disclosure Statement (IDS) Form (SB08)	SC-085_IDS_List.pdf	94452 c16eaf080004d77456f18ed79d90c3bbebb8a96f	no	1
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
4	Notice of Appeal Filed	SC-085_aia0031_Notice_of_Appeal.pdf	157346 5b7760ab228aec73900ba23c3c709fe7a8a9f20c	no	2
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	32352 bc90b346b9a80d72b19649e679caf0e6b8665e09	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	434231		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Before the Patent Trial and Appeal Board

In re Application of: Etchegoyen, Craig S. Serial No.: 13/734,178 Filed: January 4, 2013 For: NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES	Patent Examiner: Ajibola A. Akinyemi Group Art Unit: 2649 Confirmation No.: 3155 *August 22, 2014*

Applicant respectfully requests that the Patent Trial and Appeal Board ("the Board") review the final rejection in the above-captioned application. The review is requested in view of clear errors identified below in the Final Office Action mailed January 21, 2014 ("Final Action"). These errors are summarized on the following pages.

Applicant filed a Notice of Appeal (Form PTO/SB/31) on June 23, 2014.

Table of Contents

I. REAL PARTY IN INTEREST

The real parties in interest are the assignee Uniloc Luxembourg S.A., and its exclusive licensee Uniloc USA, Inc.

II. RELATED APPEALS, INTERFERENCES, AND TRIALS

The instant application has not been appealed to the Board before. No related application has been appealed to the Board or other tribunal.

III. SUMMARY OF CLAIMED SUBJECT MATTER

The present invention provides a method for near field authentication of a computing device, such as a cell phone, using sound waves. The invention may be used with any computing device that has audio transceiving capability, e.g. a speaker and a microphone. Specification ("Spec.") at paragraph ("¶") 0007.[1] An inventive feature that is the focus of this appeal is a claim limitation wherein the computing device transmits an acoustic carrier wave modulated by a periodic enclosed content message, wherein the enclosed content includes a digital representation of biometric data of a user of the computing device, or device identification data for the computing the device itself, or both. Spec. at ¶ 0008; 0032. A receiving device, e.g., a server authenticating a secure transaction, is configured to scan for and receive the periodic enclosed content message, demodulate it,

[1] References are made to the Specification as filed.

and recover digital data representing the biometric or device identification data. Spec at ¶ 0011; 0033; 0043; 0054.

Claim 1 recites a method for near field authentication of a source, the source using an audio transceiver computing device, the method comprising (Spec. at ¶ 0007): scanning a plurality of predetermined frequencies for a free frequency (Spec. at ¶ 0007); selecting the free frequency from the plurality of predetermined frequencies (Spec. at ¶ 0007); generating a periodic enclosed content message (Spec. at ¶ 0007); generating a modulated carrier wave representing the periodic enclosed content message (Spec. at ¶ 0007); and transmitting the modulated carrier wave at the free frequency (Spec. at ¶ 0007); wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication (Spec. at ¶ 0008); and wherein the content includes at least one of biometric data, or device identification data (Spec. at ¶ 0008).

IV. ARGUMENT

Well-established patent law holds that an obviousness rejection cannot be sustained unless the cited reference(s) (a) provide a suggestion or motivation to combine reference teachings in the manner claimed; (b) provide a reasonable expectation of success; and (c) teach all of the claim limitations, except for those limitations already within the knowledge or common sense of a person of ordinary skill in the art. *In re Vaeck*, 947 F.2d 488 (Fed. Cir. 1991); *KSR Int'l Co.*

v. Teleflex, Inc., 550 U.S. 398 (2007). Moreover, the burden is on the examiner to articulate a reason to combine the references in the manner claimed, and to articulate rationale in support of obviousness rejections. *KSR*, 550 U.S. at 418.

A. The Obviousness Rejection of Claims 1-9 Over *Gass* in view of *Phillips* Should be Reversed Because the References Fail to Teach All Claimed Elements.

In the Final Action, claim 1 was rejected under 35 USC §103(a) as being unpatentable over U.S. Application Pub. 2004/0038716 ("*Gass*") in further view of U.S. Application Pub. 2013/0159701 ("*Phillips*"). Claim 2 was rejected under 35 USC §103(a) as being unpatentable over *Gass*, *Phillips* and in further view of U.S. Application Pub. 2007/0198850 ("*Martin*"). Claims 3-5 were rejected over *Gass* in view of *Phillips* and in further view of U.S. Patent 5,019,813 ("*Kip*"). Claims 6-8 were rejected over *Gass*, *Phillips*, and *Martin* in further view of *Kip*. Claim 9 was rejected over *Gass* in view of *Phillips* and in further view of U.S. Application Pub. 2010/0208899 ("*Kasargod*"). Thus, all claim rejections depend in part on the Examiner's proposed combination of *Gass* and *Phillips*.

As detailed in Applicant's response filed November 14, 2013, the claimed invention is directed to method and apparatus for near field authentication of a computing device. See Spec. at ¶¶ 0002; 0007. Specifically, the disclosure relates to a method to authenticate a transaction source using a specifically-modulated audio signal. The invention may be used,

for example, to add another level of security to an electronic transaction, by exploiting the audio transceiving capabilities of modern computing devices. For example, a point-of-sale merchant computer equipped with a microphone input can authenticate an electronic transaction with a buyer's mobile phone by receiving *near-field* audio transmissions from the audio speaker of the mobile phone when the buyer wants to complete the transaction. This ensures that the buyer must be physically present within the merchant's store, to prevent a remote identity thief from completing a phony transaction. The invention may be applied in fields other than financial transactions, for example, to allow a user to gain physical access to secure locations.

In one embodiment, the method requires the source device 102 to scan several predetermined frequencies for an available or free frequency. See Id. at ¶ 0061 and Fig. 6, step 602. Once the available frequency is identified, the source device transmits a periodic enclosed content message by modulating a carrier wave. See Id. at ¶ 0064. The signal modulating the carrier wave represents the periodic enclosed content message. Id. at ¶¶ 0033; 0064. The enclosed content of the message is binary in form and may contain a binary representation of a device identifier and/or a biometric identifier. Id. at ¶¶ 0034; 0035. The receiving device 104 demodulates and decodes the message, extracts the identifier and compares it to a list of authorized identifiers. Id. at ¶¶ 0043; 0054; 0055. The

transaction is allowed to proceed only if the device is authenticated. Id. at ¶ 0056.

Consistent with this background, pertinent portions of claim 1 recite the following inventive feature in the method for near field source authentication: "*wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication; and wherein the content includes at least one of biometric data, or device identification data.*"

The teachings of *Gass* and *Phillips* fail to disclose or suggest this inventive feature. *Gass* is directed to a hands-free mobile phone communication system having a mobile terminal for receiving information over a telephone connection. The system includes a radio sender sending information over a selected frequency channel to an audio system. The audio system is equipped with a broadcast radio receiver and with an audio amplifier to provide an audio output of the received information. See Abstract. At ¶ 7 of the specification, *Gass* discloses that "[t]he basic principle of the invention is, that unused frequency channels are continuously determined, i.e. by carrying out periodically frequency scanning runs, in a hands-free communication system comprising a mobile terminal and an audio system, equipped with a radio sender and a radio receiver respectively." The Final Action admits that *Gass* fails to teach the inventive feature of claim 1. Final Action at page 3.

The Final Action cites to *Phillips* at ¶¶ 0084; 0090 for

allegedly teaching "each period of the periodic enclosed content message includes a begin indication, a content, and an end indication" and "the content includes at least one of biometric data, or device identification data." *Phillips*, however, fails to support this allegation.

Generally, *Phillips* is directed to locking digital media to a particular user or computer using a symmetric encryption technique. See *Phillips* at ¶¶ 0003; 0012. *Phillips* secures the digital content to prevent unauthorized copying. In the Abstract, *Phillips* discloses: "[t]he secured digital container when locked to a user or user's device may not open or permit access to the contents if the digital container is transferred to another user's device." In one embodiment, *Phillips* discloses a system that uses a token-based authentication and authorization procedure and involves the use of an authentication/authorization server. At ¶ 0070, *Phillips* discloses securing digital content using an atomic proxy encryption method. At ¶ 0084, which was cited in the Final Action, *Phillips* discloses:

> The executable instructions of the container code module may read the atomic proxy re-key value 615 from the token 600. An atomic proxy algorithm 705 uses this re-key value 615, along with the unique container ID 210 read from the container, to securely re-encrypt the encrypted header of data block 1, as denoted by reference numeral 715. This one-time operation locks the encrypted content data to the user and/or the user's device 125 and takes place without ever exposing the content data in unencrypted form.

In other words, *Phillps* at ¶ 0084 teaches using the atomic proxy algorithm and the container ID to *re-encrypt a data block header*. It does not disclose that a "periodic enclosed content message includes a begin indication, a content and an end indication"; nor does it disclose "the content includes at least one of biometric data, or device identification data."

Phillips at ¶ 0090, which was also cited in the Final Action, discloses:

> Depending on what elements of the user's device or user input that were used to create the original machine footprint 335, the user may be prompted to recreate certain conditions that were in effect when the original machine foot print was created. For example, the user may be prompted to re-enter certain security codes or biometric measurements. If the Smart Card scenario was being used, the user may be prompted to re-insert this card in order to successfully reopen the container.

The cited portions of *Phillips* merely require the user to enter certain security codes and biometric information in order to access the files (*i.e.*, reopen the container). The cited portions neither disclose nor suggest enclosing machine footprints or biometric data within a modulated acoustic signal as a *periodic* enclosed content message. Nor do the cited portions teach or suggest that the "periodic enclosed content message includes a begin indication, a content and an end indication and wherein the content includes at least one of biometric data, or device identification data."

In sum, the proposed combination of *Gass* and *Phillips* fails

to teach the inventive feature, because neither reference suggests to one skilled in the art to encode *content* of a transmitted analog audio signal with a digital representation of biometric and/or device identification data. Applicant further submits that in modern cellular and Internet communications systems, it is decidedly *non*-obvious for skilled artisans to pursue solutions to network security problems through the use of analog acoustic waves, and in this respect the examiner has failed to articulate a convincing argument that such an artisan apprised of *Gass* and *Phillips* would reach this solution.

B. The Obviousness Rejection Based On A Combination of *Gass* and *Phillips* Is Unsound Because Such Combination Would Render *Gass* Unsuitable For Its Intended Purpose.

The *Gass* and *Phillips* references may not be combined as suggested in the Final Action because such combination would render the device of *Gass* unsuitable for its intended purpose. *Gass* is directed to hands-free mobile communication. It requires a mobile device for receiving information over a telephone connection and a radio sender for sending information to an audio system. Modifying *Gass* in view of *Phillips* requires encrypting information transmissions at the mobile device and applying user input at the radio to decrypt the information received by the audio system (*see Phillips* at ¶ 0090, above). Such modification renders *Gass's* device unsuitable for its intended purpose because the requirement for user input is contrary to *Gass's* objective of providing a hands-free

communication system.

For at least these reasons, Applicant respectfully submits that claim 1 is patentable over *Gass* in view of *Phillips*.

C. The Obviousness Rejections Of The Dependent Claims Should Be Reversed Based On Dependency From Claim 1.

Claims 2-9 all depend, either directly or indirectly, from an otherwise patentable independent claim. Therefore claims 2-9 are deemed patentable over *Gass* and *Phillips* in any combination with *Martin*, *Kip*¸ or *Kasargod* at least by the virtue of their dependence on claim 1. Accordingly, additional reasons for patentability of dependent claims 2-9 will not be proffered. Reversal of all obviousness rejections is respectfully requested.

Conclusion

Applicant respectfully submits that the rejections in this application are improper and should be overturned.

Very truly yours,

Sean Burdick
Registration No. 51,513
Attorney for Applicant

IV. CLAIMS APPENDIX

1. (previously presented) A method for near field authentication of a source, the source using an audio transceiver computing device, the method comprising:

scanning a plurality of predetermined frequencies for a free frequency;

selecting the free frequency from the plurality of predetermined frequencies;

generating a periodic enclosed content message;

generating a modulated carrier wave representing the periodic enclosed content message; and

transmitting the modulated carrier wave at the free frequency;

wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication; and

wherein the content includes at least one of biometric data, or device identification data.

2. (original) The method of claim 1 further comprising:

displaying a user interface on the audio transceiver computing device requesting the biometric data from a user; and

responsive to receiving the biometric data, generating the periodic enclosed content message, wherein the content in each period of the periodic enclosed content message includes the biometric data.

3. (previously presented) The method of claim 1, wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

4. (previously presented) The method of claim 1, wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.

5. (previously presented) The method of claim 1 wherein the modulated carrier wave comprises a sound wave.

6. (previously presented) The method of claim 2, wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

7. (previously presented) The method of claim 2, wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.

8. (previously presented) The method of claim 4 wherein the modulated carrier wave comprises a sound wave.

9. (previously presented) The method of claim 1 wherein the carrier wave is modulated by the periodic enclosed content message.

Electronic Acknowledgement Receipt

EFS ID:	19954445
Application Number:	13734178
International Application Number:	
Confirmation Number:	3155
Title of Invention:	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES
First Named Inventor/Applicant Name:	Craig S. ETCHEGOYEN
Customer Number:	96051
Filer:	Sean Dylan Burdick/Tanya Kiatkulpiboone
Filer Authorized By:	Sean Dylan Burdick
Attorney Docket Number:	UN-NP-SC-085
Receipt Date:	25-AUG-2014
Filing Date:	04-JAN-2013
Time Stamp:	14:54:15
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Appeal Brief Filed	SC-085_Appeal_Brief_FINAL.pdf	76475 85965ba833fd100877bd9958e2a0dba45cead0ed	no	13
Warnings:					
Information:					

Total Files Size (in bytes):	76475

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/734,178	01/04/2013	Craig S. ETCHEGOYEN	UN-NP-SC-085	3155

96051 7590 11/03/2014

Uniloc USA Inc.
Legacy Town Center
7160 Dallas Parkway
Suite 380
Plano, TX 75024

EXAMINER	
AKINYEMI, AJIBOLA A	
ART UNIT	PAPER NUMBER
2649	

NOTIFICATION DATE	DELIVERY MODE
11/03/2014	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

sean.burdick@unilocusa.com
tkiatkulpiboone@unilocusa.com
kris.pangan@unilocusa.com

Office Action Summary	Application No. 13/734,178	Applicant(s) ETCHEGOYEN ET AL.	
	Examiner AJIBOLA AKINYEMI	Art Unit 2649	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08/25/2014*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-9* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-9* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *01/04/2013* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some * c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

1) The present application is being examined under the pre-AIA first to invent provisions.

DETAILED ACTION

In view of the Appeal brief filed on 08/25/2014, PROSECUTION IS HEREBY REOPENED. New rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

/YUWEN PAN/

Supervisory Patent Examiner, Art Unit 2649

Claim Rejections - 35 USC § 103

1. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained through the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under pre-AIA 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.

2. Ascertaining the differences between the prior art and the claims at issue.

3. Resolving the level of ordinary skill in the pertinent art.

4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

3. Claims 1, 9 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Gass (Pub. No.: US 2004/0038716A1) and further in view of Kargl (Pub. No.: US 2011/0215158A1) and Bardsley (Pub. No.: US 2012/0216262A1).

With respect to claim 1:

Gass discloses a method for near field authentication of a source the source using an audio transceiver computing device comprising scanning a plurality of predetermined frequencies for a free frequency **(parag,0016 discloses scanning plurality of predetermined frequency for a free frequencies);** selecting the free frequency from the plurality of predetermined frequencies **(parag.0016 also discloses selecting free frequency from plurality of frequencies);** generating a periodic enclosed content message; generating a modulated carrier wave representing the periodic enclosed content message and transmitting the modulated carrier wave at the free frequency **(Parag. 0015 also discloses the RDS encoder encodes said frequency or channel information generating a corresponding RDS signal 5 modulated on the RDS sub carrier at 57 KHz).**

Gass does not explicitly disclose wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication; and wherein the content includes at least one of biometric data, or device identification data.

Kargl discloses an enclosed content message includes a begin indication, a content, and an end indication; **(fig.4B, item 402 represent begin indication, item 404 represents end indication and item 400 represent content as in parag. 0038).** It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the teaching of Kargl into the teaching of Gass in order to reduce the hardware complexity and increase data rate.

Gass and Kargl do not disclose content to include at least one of biometric data.

Bardsley disclose content with biometric data (**abstract, parag. 0007 with biometric data included in the header).** It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the teaching of Bardsley into teaching of Gass in view of Kargl for identification purpose.

With respect to claim 9:

Kargl discloses the method wherein the carrier wave is modulated by the periodic enclosed content message (abst. parag. 0005).

4. Claim 2 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Gass (Pub. No.: US 2004/0038716A1), Kargl (Pub. No. No. US 2011/0215158A1), Bardsley (Pub. No.: US 2012/0216262A1) as applied to claim 1 above and further in view of Martin (Pub. No.: US 2007/0198850A1).

With respect to claim 2:

The rejection of claim 1 is incorporated; Gass, Karl and Bardsley do not explicitly disclose the method further comprising displaying a user interface on the audio transceiver computing device requesting the biometric data from a user; and responsive to receiving the biometric data, generating the periodic enclosed content message, wherein the content in each period of the periodic enclosed content message includes the biometric data.

Martin discloses this limitation (parag. 0062-0063 discloses a user interface on the audio transceiver computing device requesting the biometric data from a user). It

would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the teaching of Martin into the teaching of Gass in view of Karlg and Bardsley in order to provide a security system wherein the user is provided with dual layered verification system in addition to a unique identifier given to the user.

5. Claims 3-5 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Gass (Pub. No.: US 2004/0038716A1), Kargl (Pub. No. No. US 2011/0215158A1), Bardsley (Pub. No.: US 2012/0216262A1) as applied to claim 1 above and further in view of Kip (Patent No.: US 5019813).

With respect to claim 3:

The rejection of claim 1 is incorporated; Gass, Kargl and Bardsley do not explicitly disclose wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

Kip discloses this above limitations (col.5, line 39-44). It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the teaching of Kip into the teaching of Gass view of Karlg and Bardsley in order to provide a universally applicable data exchange system operating in a contactless manner.

With respect to claim 4:

Kip discloses the method wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user (fig.5b, col.5, line 39-44).

With respect to claim 5:

Gass discloses the method wherein the modulated carrier wave comprises a sound wave (parag. 0016).

6. Claims 6-8 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Gass (Pub. No.: US 2004/0038716A1), Kargl (Pub. No. No. US 2011/0215158A1), Bardsley (Pub. No.: US 2012/0216262A1), Martin (Pub. No.: US 2007/0198850A1) as applied to claim 2 above and further in view of Kip (Patent No.: US 5019813).

With respect to claim 6:

The rejection of claim 2 is incorporated; Gass, Kargl, Bardsley and Martin do not disclose wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

Kip discloses this above limitations (col.5, line 39-44). It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the teaching of Kip into the teaching of Gass in view of Kargl, Bardsley and Martin in order to provide a universally applicable data exchange system operating in a contactless manner.

With respect to claim 7:

Kip discloses the method wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user (fig.5b, col.5, line 39-44).

With respect to claim 8:

Gass discloses the method wherein the modulated carrier wave comprises a sound wave (parag. 0016).

Response to Arguments

Applicant's arguments, see remark, filed 08/25/2014, with respect to the rejection(s) of claim(s) 1-9 under 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Kargl and Bardsley.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to AJIBOLA AKINYEMI whose telephone number is (571)270-1846. The examiner can normally be reached on monday- friday (8.30-5pm) Est.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, YUWEN PAN can be reached on (571) 272-7855. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/AJIBOLA AKINYEMI/
Primary Examiner, Art Unit 2649

Notice of References Cited	Application/Control No. 13/734,178	Applicant(s)/Patent Under Reexamination ETCHEGOYEN ET AL.	
	Examiner AJIBOLA AKINYEMI	Art Unit 2649	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-5,019,813 A	05-1991	Kip et al.	340/10.51
*	B	US-2004/0038716 A1	02-2004	Gass, Vincent	455/569.1
*	C	US-2007/0198850 A1	08-2007	Martin et al.	713/186
*	D	US-2010/0208899 A1	08-2010	Kasargod et al.	381/1
*	E	US-2011/0215158 A1	09-2011	Kargl et al.	235/492
*	F	US-2012/0216262 A1	08-2012	Bardsley et al.	726/5
*	G	US-2013/0159701 A1	06-2013	PHILLIPS et al.	713/155
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13734178	ETCHEGOYEN ET AL.
	Examiner	Art Unit
	AJIBOLA AKINYEMI	2649

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
455	41.1	10/28/2014	AA

SEARCH NOTES		
Search Notes	Date	Examiner
455/11.1,569.1	10/28/2014	AA

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO
(modified by Applicant)

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	13/734,178
Filing Date	January 4, 2013
First Named Inventor	Craig S. Etchegoyen
Art Unit	2649
Examiner Name	Ajibola A. Akinyemi
Attorney Docket Number	UN-NP-SC-085

U. S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-5,019,813	05/28/1991	Kip et al.	
		US-5,249,178	09/28/1993	Kurano et al.	
		US-6,791,982	09/14/2004	Westberg, Lars	
		US-6,999,461	02/14/2006	Li et al.	
		US-7,600,039	10/06/2009	Tang et al.	
		US-8,018,937	09/13/2011	Epps et al.	
		US-2002/0163889	11/07/2002	Yemini et al.	
		US-2002/0178122	11/28/2002	Maes, Stephane	
		US-2007/0153764	07/05/2007	Thubert et al.	
		US-2010/0034207	02/11/2010	McGrew et al.	
		US-2010/0146589	06/10/2010	Safa, John Aram	
		US-2012/0275354	11/01/2012	Villain, Frederic	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code – Number – Kind Code	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date page(s), volume-issue number(s), publisher, city and/or country where published.	T

Examiner Signature	/Ajibola Akinyemi/	Date Considered	10/28/2014

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A./

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13734178	ETCHEGOYEN ET AL.
	Examiner	**Art Unit**
	AJIBOLA AKINYEMI	2649

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	08/30/2013	01/14/2014	10/28/2014						
	1	✓	✓	✓						
	2	✓	✓	✓						
	3	✓	✓	✓						
	4	✓	✓	✓						
	5	✓	✓	✓						
	6	✓	✓	✓						
	7	✓	✓	✓						
	8	✓	✓	✓						
	9		✓	✓						

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	36	(begin$4 and end$3) near indication same data	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/10/28 09:58
L6	30	header with biometric adj information	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/10/28 10:09
L9	2	enclosed adj content adj message with biometric	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/10/28 10:19

EAST Search History (Interference)

< This search history is empty>

10/ 28/ 2014 11:35:54 AM
C:\ Users\ aakinyemi\ Documents\ EAST\ Workspaces\ 13621440.wsp

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. no.:	13/734,178	Conf. no.	3155
Applicant:	Craig S. Etchegoyen	Art Unit:	2649
Filed:	January 4, 2013	Examiner:	Ajibola A. Akinyemi

Title: NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES

RESPONSE TO OFFICE ACTION

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir,

In response to the Office Action mailed November 3, 2014 ("Office Action"), please reconsider the present application in light of the following remarks.

IN THE CLAIMS

1. (currently amended) A method for near field authentication of a source, the source using an audio transceiver computing device, the method comprising:

scanning a plurality of predetermined frequencies for a free frequency;

selecting the free frequency from the plurality of predetermined frequencies;

generating a periodic enclosed content message;

generating a modulated carrier wave representing the periodic enclosed content message; and

transmitting the modulated carrier wave at the free frequency;

wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication; and

wherein the content includes at least one of biometric data, or device identification data, wherein the device identification data includes a bit string or bit array derived from user-configurable and non-user-configurable data specific to the audio transceiver computing device.

2. (original) The method of claim 1 further comprising:

displaying a user interface on the audio transceiver computing device requesting the biometric data from a user; and

responsive to receiving the biometric data, generating the periodic enclosed content message, wherein the content in each period of the periodic enclosed content message includes the biometric data.

3. (previously presented) The method of claim 1, wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a

predetermined period of time.

4. (previously presented) The method of claim 1, wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.

5. (previously presented) The method of claim 1 wherein the modulated carrier wave comprises a sound wave.

6. (previously presented) The method of claim 2, wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

7. (previously presented) The method of claim 2, wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.

8. (previously presented) The method of claim 4 wherein the modulated carrier wave comprises a sound wave.

9. (previously presented) The method of claim 1 wherein the carrier wave is modulated by the periodic enclosed content message.

10. (new) The method of claim 1, wherein the non-user-configurable data comprises hardware component numbers, serial numbers, and version numbers.

REMARKS

Applicant thanks Examiner Akinyemi for his thorough review of the application papers and for his opinion on patentability.

Claims 1-10 are pending. New claim 10 was added to particularly point out and specifically claim an embodiment of the disclosure. No new matter has been added. Support for claim 10 is found throughout the specification, for example, at paragraph 0037 of the originally-filed specification. Applicant respectfully requests reconsideration of all pending claims in view of the amendments and remarks herein.

Response to Rejections Under 35 USC §103

Claims 1 and 9 stand rejected as allegedly unpatentable over U.S. Application Pub. 2004/0038716 (*"Gass"*) in further view of U.S. Application Pub. 2011/0215158 (*"Kargl"*) and U.S. Application Pub. 2012/0216262 (*"Bardsley"*). Applicant respectfully traverses.

Applicant's disclosure is directed to near field authentication of users and their computing devices through communication of enclosed content sound waves. Figure 1 shows system 100 for authenticating sources using sound waves, including audio transceiving computing device 102, and audio receiving computing device 104. The audio transceiving device 102 can transmit data to the audio receiving device 104 as a modulated carrier wave 106, for example, a sound wave. In the embodiment of Figure 6, the disclosure shows process flow diagram 600 having a near field authentication of sources to audio receiving computing device 104 using audio transceiver computing device 102. At step 602, audio transceiver computing device 102 scans a plurality of predetermined frequencies for a free frequency. At step 604, audio transceiver computing device 102 selects free frequency from the plurality of predetermined frequencies. At step 606, audio transceiver computing device 102 generates a periodic enclosed content message. At step 608, audio transceiver computing device 102 generates a modulated carrier wave representing the periodic enclosed content message. At step 610, audio transceiver computing device 102 transmits the modulated carrier wave at the free frequency.

As amended, claim 1 recites (at pertinent portions): *"wherein the device identification data comprises a bit string or bit array derived from user-configurable and non-user-*

configurable data specific to the audio transceiver computing device."

The references to *Gass*, *Kargl* and *Bardsley*, alone or in any combination, fail to disclose or suggest at least this feature. *Gass* is directed to a hands-free mobile phone communication system having a mobile terminal for receiving information over a telephone connection. The system includes a radio sender sending information over a selected frequency channel to an audio system. The audio system is equipped with a broadcast radio receiver and with an audio amplifier to provide an audio output of the received information. See Abstract. At ¶ 7 of the specification, *Gass* discloses:

> [t]he basic principle of the invention is, that unused frequency channels are continuously determined, i.e., by carrying out periodically frequency scanning runs, in a hands-free communication system comprising a mobile terminal and an audio system, equipped with a radio sender and a radio receiver respectively.

Gass does not disclose or suggest the amended portions of claim 1. Namely, the reference fails to teach "the device identification data comprises a bit string or bit array derived from user-configurable and non-user-configurable data specific to the audio transceiver computing device."

Kargl is directed to a RFID communication system, and in particular a passive RFID transponder and RFID reader. At Figure 1, *Kargl* shows passive RFID transponder 100 that includes coder 110 and modulator 120. Coder 110 generates a digital coded data stream 112 based on a digital data stream 102 to be transmitted. Modulator 120 modulates amplitude of carrier signal 104 with the digital coded data stream of 112 to amplitude-modulated coded signal 122. Figure 6 shows RFID reader 600 that includes receiver 610, demodulator 620 and a decoder 630. Receiver 610 receives amplitude-modulated coded reception signal 612 and demodulator 620 demodulates amplitude-modulated coded reception signal 612 on the basis of a carrier signal generated by the RFID reader 600 to digital coded data stream 622. Furthermore, decoder 630 determines a maximum data frequency of the digital coded data stream 622 and provides decoded digital data stream 632 based on maximum data frequency determined. *Kargl* clearly fails to disclose or suggest the amended portions of claim 1.

Bardsley is directed to methods, systems, and computer program products for determining an originator of a network packet using biometric information. In particular,

Bardsley discloses associating a network packet with biometric information for a user by identifying biometric identification information in at least one of a header and a trailer of a network packet without including biometric identification information in a payload of the network packet and sending the packet via a network, wherein the identifier identifies the network packet as having originated from the user. See Abstract. *Bardsley* also fails to disclose or suggest the amended recitations of claim 1.

None of *Gass*, *Kargl* or *Bardsley* disclose or suggest content including at least one of biometric data, or device identification data, wherein the device identification data comprises a bit string or bit array derived from user-configurable and non-user-configurable data specific to the audio transceiver computing device. Accordingly, *Gass*, *Kargl* and *Bardsley*, in any combination, fail to disclose each and every claimed element of claim 1. For at least these reasons, Applicant respectfully submits that claim 1 is patentable over *Gass* in view of *Kargl* and in further view of *Bardsley*.

Claim 2 is rejected under pre-AIA 35 USC §103(a) as being unpatentable over *Gass*, *Kargl* and *Bardsley* as applied to claim 1 above and further in view of U.S. Application Pub. 2007/0198850 ("*Martin*"). Claims 3-5 are rejected under pre-AIA 35 USC §103(a) as being unpatentable over *Gass*, *Kargl* and *Bardsley* as applied to claim 1 above and further in view of U.S. Patent 5,019,813 ("*Kip*"). Claims 6-8 are rejected under pre-AIA 35 USC §103(a) as being unpatentable over *Gass*, *Kargl*, *Bardsley* and *Martin* as applied to claim 2 above and further in view of *Kip*. Applicant respectfully traverses all of the foregoing rejections.

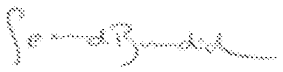
Claims 2-10 each depend, either directly or indirectly, from an otherwise patentable independent claim. Each of claims 2-9 is deemed patentable over *Gass*, *Kargl*, and *Bardsley* in any combination with *Martin* and *Kip* at least by virtue of their dependence on claim 1. Accordingly, additional reasons for patentability of dependent claims 2-10 will not be proffered.

Applicant respectfully requests reconsideration of all obviousness rejections and allowance of all claims.

CONCLUSION

In view of all of the above, applicant believes that all pending claims are in condition for allowance and earnestly requests that these claims be passed to issuance. If the Examiner believes that a telephone conversation would help to expedite prosecution, please call the undersigned attorney at the number below.

Respectfully Submitted,



Sean D. Burdick
Reg. No. 51,513

Uniloc USA, Inc.
7160 N. Dallas Parkway, Suite 380
Plano, Texas 75024
(972) 905-9580 x227

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO
(modified by Applicant)

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	13/734,178
Filing Date	January 4, 2013
First Named Inventor	Craig S. ETCHEGOYEN, et al.
Art Unit	2649
Examiner Name	Ajibola A. Akinyemi
Attorney Docket Number	UN-NP-SC-085

U. S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		8,020,190	09/13/2011	Plummer	
		8,375,221	02/12/2013	Thom, et al.	
		2004/0003288	01/01/2014	Wiseman, et al.	
		2006/0253584	11/09/2006	Dixon, et al.	
		2008/0114709	05/15/2008	Dixon, et al.	
		2008/0282338	11/13/2008	Beer	
		2010/0100962	04/22/2010	Boren	
		2010/0199188	08/05/2010	Abu-Hakima, et al.	
		2010/0269168	10/21/2010	Hegli, et al.	
		2011/0090896	04/21/2011	Bradley, Bob	
		2011/0295988	12/01/2011	Le Jouan	

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date page(s), volume-issue number(s), publisher, city and/or country where published.	T
		Harrington, D., et al., "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks," RFC 3411, IETF, Dec. 2002, pp. 1-64.	
		Moshchuk, Alexander, et al., "SpyProxy: Execution-based Detection of Malicious Web Content," 2007, pp. 27-42.	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. no.:	13/734,178	Conf. no.	3155
Applicant:	UNILOC LUXEMBOURG S.A.	Art Unit:	2649
Filed:	January 4, 2013	Examiner:	Ajibola A. Akinyemi

Title: NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENLCOSED CONTENT SOUND WAVES

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicant hereby submits, without admission of prior art effect thereof, form(s) PTO/SB/08 pursuant to the duty of disclosure requirements of 37 CFR §§ 1.56, 1.97 and 1.98.

Applicant has listed publication dates on the attached form(s) PTO/SB/08 based on information presently available to the undersigned. However, the listed publication dates should not be construed as an admission that the information was actually published on the date indicated.

It is respectfully requested that the Examiner initial and return a copy of the enclosed forms PTO/SB/08, and to indicate in the official file wrapper of this patent application that the documents have been considered.

Applicant submits concurrently herewith the fee set forth in § 1.17(p).

Respectfully Submitted,

Sean D. Burdick
Reg. No. 51,513

Uniloc USA, Inc.
7160 N. Dallas Parkway, Suite 380
Plano, TX 75024
972-905-9580 x227

Electronic Patent Application Fee Transmittal	
Application Number:	13734178
Filing Date:	04-Jan-2013
Title of Invention:	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES
First Named Inventor/Applicant Name:	Craig S. ETCHEGOYEN
Filer:	Sean Dylan Burdick
Attorney Docket Number:	UN-NP-SC-085
Filed as Small Entity	
Filing Fees for **Utility under 35 USC 111(a)**	

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	2806	1	90	90
		Total in USD ($)		**90**

Electronic Acknowledgement Receipt	
EFS ID:	21371629
Application Number:	13734178
International Application Number:	
Confirmation Number:	3155
Title of Invention:	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES
First Named Inventor/Applicant Name:	Craig S. ETCHEGOYEN
Customer Number:	96051
Filer:	Sean Dylan Burdick
Filer Authorized By:	
Attorney Docket Number:	UN-NP-SC-085
Receipt Date:	02-FEB-2015
Filing Date:	04-JAN-2013
Time Stamp:	14:45:30
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$90
RAM confirmation Number	991
Deposit Account	506053
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	UN-NP-SC-085_Response_to_20141103_OA_FINAL.pdf	56435 0b1cf816459204dcf9c5698d635f3af87daf2644	no	7
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	SC-085_IDS.pdf	29702 2d475718675cbf0cdc09f04434303f7905fc9059	no	1
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Non Patent Literature	Harrington_An_Architecture.pdf	1987395 11f2a5dc227f15d0ec8c962c63bbdcb95ea8ade7	no	64
Warnings:					
Information:					
4	Non Patent Literature	Moshchuk_etal_SpyProxy.pdf	1391792 f03ec1ce3f7029653b6a631d1ff73904512c67ca	no	16
Warnings:					
Information:					
5	Transmittal Letter	SC-085_IDS_Transmittal.pdf	62501 010228be01ae6ffd2f756dd50a120f1bfe27059f	no	2
Warnings:					
Information:					
6	Fee Worksheet (SB06)	fee-info.pdf	30881 a74db37ca29ca94156f921dc1f80a6dfddbb71a5	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	3558706		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/734,178	01/04/2013	Craig S. ETCHEGOYEN	UN-NP-SC-085	3155

96051 7590 03/04/2015

Uniloc USA Inc.
Legacy Town Center
7160 Dallas Parkway
Suite 380
Plano, TX 75024

EXAMINER
AKINYEMI, AJIBOLA A

ART UNIT	PAPER NUMBER
2649	

NOTIFICATION DATE	DELIVERY MODE
03/04/2015	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

sean.burdick@unilocusa.com
tkiatkulpiboone@unilocusa.com
kris.pangan@unilocusa.com

Office Action Summary	Application No. 13/734,178	Applicant(s) ETCHEGOYEN ET AL.	
	Examiner AJIBOLA AKINYEMI	Art Unit 2649	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02/02/2015*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-9* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-9* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *01/04/2013* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some * c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

1) The present application is being examined under the pre-AIA first to invent provisions.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained through the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under pre-AIA 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.

2. Ascertaining the differences between the prior art and the claims at issue.

3. Resolving the level of ordinary skill in the pertinent art.

4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

3. Claims 1, 9 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Gass (Pub. No.: US 2004/0038716A1) and further in view of Kargl (Pub. No.: US 2011/0215158A1) and Bardsley (Pub. No.: US 2012/0216262A1).

With respect to claim 1:

Gass discloses a method for near field authentication of a source the source using an audio transceiver computing device comprising scanning a plurality of predetermined frequencies for a free frequency **(parag,0016 discloses scanning plurality of predetermined frequency for a free frequencies);** selecting the free frequency from the plurality of predetermined frequencies **(parag.0016 also discloses selecting free frequency from plurality of frequencies);** generating a periodic enclosed content message; generating a modulated carrier wave representing the periodic enclosed content message and transmitting the modulated carrier wave at the free frequency **(Parag. 0015 also discloses the RDS encoder encodes said frequency or channel information generating a corresponding RDS signal 5 modulated on the RDS sub carrier at 57 KHz).**

Gass does not explicitly disclose wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication; and wherein the content includes at least one of biometric data, or device identification data.

Kargl discloses an enclosed content message includes a begin indication, a content, and an end indication; **(fig.4B, item 402 represent begin indication, item 404 represents end indication and item 400 represent content as in parag. 0038).** It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the teaching of Kargl into the teaching of Gass in order to reduce the hardware complexity and increase data rate.

Gass and Kargl do not disclose content to include at least one of biometric data.

Bardsley disclose content with biometric data (**abstract, parag. 0007 with biometric data included in the header).** It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the teaching of Bardsley into teaching of Gass in view of Kargl for identification purpose.

With respect to claim 9:

Kargl discloses the method wherein the carrier wave is modulated by the periodic enclosed content message (abst. parag. 0005).

4. Claim 2 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Gass (Pub. No.: US 2004/0038716A1), Kargl (Pub. No. No. US 2011/0215158A1), Bardsley (Pub. No.: US 2012/0216262A1) as applied to claim 1 above and further in view of Martin (Pub. No.: US 2007/0198850A1).

With respect to claim 2:

The rejection of claim 1 is incorporated; Gass, Karl and Bardsley do not explicitly disclose the method further comprising displaying a user interface on the audio transceiver computing device requesting the biometric data from a user; and responsive to receiving the biometric data, generating the periodic enclosed content message, wherein the content in each period of the periodic enclosed content message includes the biometric data.

Martin discloses this limitation (parag. 0062-0063 discloses a user interface on the audio transceiver computing device requesting the biometric data from a user). It

would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the teaching of Martin into the teaching of Gass in view of Karlg and Bardsley in order to provide a security system wherein the user is provided with dual layered verification system in addition to a unique identifier given to the user.

5. Claims 3-5 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Gass (Pub. No.: US 2004/0038716A1), Kargl (Pub. No. No. US 2011/0215158A1), Bardsley (Pub. No.: US 2012/0216262A1) as applied to claim 1 above and further in view of Kip (Patent No.: US 5019813).

With respect to claim 3:

The rejection of claim 1 is incorporated; Gass, Kargl and Bardsley do not explicitly disclose wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

Kip discloses this above limitations (col.5, line 39-44). It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the teaching of Kip into the teaching of Gass view of Karlg and Bardsley in order to provide a universally applicable data exchange system operating in a contactless manner.

With respect to claim 4:

Kip discloses the method wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user (fig.5b, col.5, line 39-44).

With respect to claim 5:

Gass discloses the method wherein the modulated carrier wave comprises a sound wave (parag. 0016).

6. Claims 6-8 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Gass (Pub. No.: US 2004/0038716A1), Kargl (Pub. No. No. US 2011/0215158A1), Bardsley (Pub. No.: US 2012/0216262A1), Martin (Pub. No.: US 2007/0198850A1) as applied to claim 2 above and further in view of Kip (Patent No.: US 5019813).

With respect to claim 6:

The rejection of claim 2 is incorporated; Gass, Kargl, Bardsley and Martin do not disclose wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

Kip discloses this above limitations (col.5, line 39-44). It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the teaching of Kip into the teaching of Gass in view of Kargl, Bardsley and Martin in order to provide a universally applicable data exchange system operating in a contactless manner.

With respect to claim 7:

Kip discloses the method wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user (fig.5b, col.5, line 39-44).

With respect to claim 8:

Gass discloses the method wherein the modulated carrier wave comprises a sound wave (parag. 0016).

Response to Arguments

Applicant's arguments filed 02/02/2015 have been fully considered but they are not persuasive. Regarding claim 1 and new claim, applicant argued that none of the cited references disclose "wherein the device identification data includes a bit string or bit array derived, from user- configurable and non-user-configurable data specific to the audio transceiver computing device" as in claim 1.

Examiner noticed that claim 1 in last office action was rejected based on **"at least one biometric data" and not "device identification**". Since there is OR in the two limitations, this gives examiner option to choose **Biometric data.**

Amending clam to further include "wherein the device identification data includes a bit string or bit array derived, from user- configurable and non-user-configurable data specific to the audio transceiver computing device" is improper. Applicant is advice to cancel or delete "**one of biometric data" in order to add the new limitation.**

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to AJIBOLA AKINYEMI whose telephone number is (571)270-1846. The examiner can normally be reached on monday- friday (8.30-5pm) Est.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, YUWEN PAN can be reached on (571) 272-7855. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/AJIBOLA AKINYEMI/
Primary Examiner, Art Unit 2649

Notice of References Cited	Application/Control No. 13/734,178	Applicant(s)/Patent Under Reexamination ETCHEGOYEN ET AL.	
	Examiner AJIBOLA AKINYEMI	Art Unit 2649	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-5,019,813 A	05-1991	Kip et al.	340/10.51
*	B	US-2004/0038716 A1	02-2004	Gass, Vincent	455/569.1
*	C	US-2007/0198850 A1	08-2007	Martin et al.	713/186
*	D	US-2010/0208899 A1	08-2010	Kasargod et al.	381/1
*	E	US-2011/0215158 A1	09-2011	Kargl et al.	235/492
*	F	US-2012/0216262 A1	08-2012	Bardsley et al.	726/5
*	G	US-2013/0159701 A1	06-2013	PHILLIPS et al.	713/155
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO
(modified by Applicant)

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	13/734,178
Filing Date	January 4, 2013
First Named Inventor	Craig S. ETCHEGOYEN, et al.
Art Unit	2649
Examiner Name	Ajibola A. Akinyemi
Attorney Docket Number	UN-NP-SC-085

U. S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number / Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		8,020,190	09/13/2011	Plummer	
		8,375,221	02/12/2013	Thom, et al.	
		2004/0003288	01/01/2014	Wiseman, et al.	
		2006/0253584	11/09/2006	Dixon, et al.	
		2008/0114709	05/15/2008	Dixon, et al.	
		2008/0282338	11/13/2008	Beer	
		2010/0100962	04/22/2010	Boren	
		2010/0199188	08/05/2010	Abu-Hakima, et al.	
		2010/0269168	10/21/2010	Hegli, et al.	
		2011/0090896	04/21/2011	Bradley, Bob	
		2011/0295988	12/01/2011	Le Jouan	

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date page(s), volume-issue number(s), publisher, city and/or country where published.	T
		Harrington, D., et al., "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks," RFC 3411, IETF, Dec. 2002, pp. 1-64.	
		Moshchuk, Alexander, et al., "SpyProxy: Execution-based Detection of Malicious Web Content," 2007, pp. 27-42.	

Examiner Signature	/Ajibola Akinyemi/	Date Considered	02/26/2015

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A./

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13734178	ETCHEGOYEN ET AL.
	Examiner	Art Unit
	AJIBOLA AKINYEMI	2649

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	08/30/2013	01/14/2014	10/28/2014	02/25/2015					
	1	✓	✓	✓	✓					
	2	✓	✓	✓	✓					
	3	✓	✓	✓	✓					
	4	✓	✓	✓	✓					
	5	✓	✓	✓	✓					
	6	✓	✓	✓	✓					
	7	✓	✓	✓	✓					
	8	✓	✓	✓	✓					
	9		✓	✓	✓					

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13734178	ETCHEGOYEN ET AL.
	Examiner	Art Unit
	AJIBOLA AKINYEMI	2649

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
455	41.1	2/26/2015	AA

SEARCH NOTES		
Search Notes	Date	Examiner
455/11.1,569.1	2/26/2015	AA

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

PTO/AIA/31 (03-14)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

NOTICE OF APPEAL FROM THE EXAMINER TO THE PATENT TRIAL AND APPEAL BOARD

Docket Number (Optional): UN-NP-SC-085

I hereby certify that this correspondence is being facsimile transmitted to the USPTO, EFS-Web transmitted to the USPTO, or deposited with the United States Postal Service with sufficient postage in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, on Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on _____.

Signature _____

Typed or printed name _____

In re Application of: Craig S. ETCHEGOYEN et al.

Application Number	Filed
13/734,178	January 4, 2013

For: NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED...

Art Unit	Examiner
2649	Ajibola A. Akinyemi

Applicant hereby **appeals** to the Patent Trial and Appeal Board from the last decision of the examiner.

The fee for this Notice of Appeal is (37 CFR 41.20(b)(1)) $ 800.00

☑ Applicant asserts small entity status. See 37 CFR 1.27. Therefore, the fee shown above is reduced by 50%, and the resulting fee is: $ 400.00

(Previously paid on June 23, 2014)

☐ Applicant certifies micro entity status. See 37 CFR 1.29. Therefore, the fee shown above is reduced by 75%, and the resulting fee is: $ _____

Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. _____.

☐ Payment made via EFS-Web.

☐ A petition for an extension of time under 37 CFR 1.136(a) (PTO/AIA/22 or equivalent) is enclosed.

For extensions of time in reexamination proceedings, see 37 CFR 1.550.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant

☑ attorney or agent of record. Registration number 51,513

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____

Signature /Sean D. Burdick/

Typed or printed name Sean D. Burdick

Telephone Number 972-905-9580 x227

Date May 19, 2015

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

* Total of 1 forms are submitted.

This collection of information is required by 37 CFR 41.20(b)(1) and 41.31. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. no.:	13/734,178	Conf. no.	3155
Applicant:	Uniloc Luxembourg S.A.	Art Unit:	2649
Filed:	January 4, 2013	Examiner:	Ajibola A. Akinyemi

Title: NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENLCOSED CONTENT SOUND WAVES

REINSTATEMENT OF APPEAL

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir,

Applicant hereby requests a Reinstatement of Appeal for a Notice of Appeal previously filed on June 23, 2014. Applicant also requests the $400 Notice of Appeal fee previously paid on June 23, 2014 to be applied to this reinstatement. No additional fee is due.

Respectfully Submitted,

Sean D. Burdick
Reg. No. 51,513

Uniloc USA, Inc.
7160 N. Dallas Parkway, Suite 380
Plano, Texas 75024
(972) 905-9580 x227

Electronic Acknowledgement Receipt

EFS ID:	22390921
Application Number:	13734178
International Application Number:	
Confirmation Number:	3155
Title of Invention:	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES
First Named Inventor/Applicant Name:	Craig S. ETCHEGOYEN
Customer Number:	96051
Filer:	Sean Dylan Burdick/Kristina Pangan
Filer Authorized By:	Sean Dylan Burdick
Attorney Docket Number:	UN-NP-SC-085
Receipt Date:	19-MAY-2015
Filing Date:	04-JAN-2013
Time Stamp:	16:19:20
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Notice of Appeal Filed	SC-085_Notice_of_Appeal.pdf	133369 88ab9deb0be4ada036037ed5d45b6a408e77f0c6	no	1

Warnings:	
Information:	

2	Notice of Appeal Filed	SC-085_Reinstatement_of_Appeal.pdf	58283 b836a9cd8c97c6932eb0e6a2a0561d15a292dc00	no	1

Warnings:	
Information:	
Total Files Size (in bytes):	191652

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. no.:	13/734,178	Conf. no.	3155
Applicant:	UNILOC LUXEMBOURG S.A.	Art Unit:	2649
Filed:	January 4, 2013	Examiner:	Ajibola A. Akinyemi

Title: NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENLCOSED CONTENT SOUND WAVES

REQUEST FOR REFUND

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicant requests a refund in the amount of $90 to our Deposit Account No. 50-6053. On June 23, 2014, when Applicant filed a Notice of Appeal with a two-month extension of time and Supplemental IDS, Applicant mistakenly paid only $700 in small entity fees--$400 for the Notice of Appeal and $300 for the two-month extension of time. On April 15, 2015, the USPTO charged $180 for the Supplemental IDS filed on June 23, 2014. Applicant is a small entity, so only $90 should have been deducted.

Respectfully submitted,

Sean D. Burdick
Reg. No. 51,513

Uniloc USA, Inc.
7160 N. Dallas Parkway, Suite 380
Plano, TX 75024
972-905-9580 x227

Electronic Acknowledgement Receipt	
EFS ID:	22391005
Application Number:	13734178
International Application Number:	
Confirmation Number:	3155
Title of Invention:	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES
First Named Inventor/Applicant Name:	Craig S. ETCHEGOYEN
Customer Number:	96051
Filer:	Sean Dylan Burdick
Filer Authorized By:	
Attorney Docket Number:	UN-NP-SC-085
Receipt Date:	19-MAY-2015
Filing Date:	04-JAN-2013
Time Stamp:	16:22:17
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Refund Request	SC-085_Request_for_Refund.pdf	52485 935c624d6f3b87bbfecc23531f7e3fff192bd969	no	1

Warnings:
Information:

Total Files Size (in bytes):	52485

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. no.:	13/734,178	Conf. no.	3155
Applicant:	UNILOC LUXEMBOURG S.A.	Art Unit:	2649
Filed:	January 4, 2013	Examiner:	Ajibola A. Akinyemi

Title: NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENLCOSED CONTENT SOUND WAVES

2015 MAY 19 PM 3:47

USPTO RECEIPTS ACCOUNTING DIVISION

REQUEST FOR REFUND

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicant requests a refund in the amount of $90 to our Deposit Account No. 50-6053. On June 23, 2014, when Applicant filed a Notice of Appeal with a two-month extension of time and Supplemental IDS, Applicant mistakenly paid only $700 in small entity fees--$400 for the Notice of Appeal and $300 for the two-month extension of time. On April 15, 2015, the USPTO charged $180 for the Supplemental IDS filed on June 23, 2014. Applicant is a small entity, so only $90 should have been deducted.

Respectfully submitted,

Sean D. Burdick
Reg. No. 51,513

Uniloc USA, Inc.
7160 N. Dallas Parkway, Suite 380
Plano, TX 75024
972-905-9580 x227

05/27/2015 EEKUBAY1 00000003 506053 13734178
01 FC:2806 90.00 DA

Adjustment date: 05/27/2015 EEKUBAY1 13734178
04/15/2015 NSCOTT 00000001 506053
01 FC:1806 180.00 CR

PTO/SB/30 (07-14)
Approved for use through 07/31/2016 OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Request for Continued Examination (RCE) Transmittal

Address to:
Mail Stop RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Application Number	13/734,178
Filing Date	January 4, 2013
First Named Inventor	Craig S. ETCHEGOYEN et al.
Art Unit	2649
Examiner Name	Ajibola A. Akinyemi
Attorney Docket Number	UN-NP-SC-085

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, to any international application that does not compy with the requirements of 35 U.S.C 371, or to any design application. See Instruction Sheet for RCEs (not to be submitted to the USPTO on page 2.)

1. Submission required under 37 CFR 1.114 Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

   a. ☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

      i. ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

      ii. ☐ Other _____

   b. ☑ Enclosed

      i. ☑ Amendment/Reply

      ii. ☐ Affidavit(s)/ Declaration(s)

      iii. ☐ Information Disclosure Statement (IDS)

      iv. ☐ Other _____

2. Miscellaneous

   a. ☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of _____ months. (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

   b. ☐ Other _____

3. Fees The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.

   a. ☑ The Director is hereby authorized to charge the following fees, any underpayment of fees, or credit any overpayments, to Deposit Account No. 50-6053 .

      i. ☑ RCE fee required under 37 CFR 1.17(e)

      ii. ☐ Extension of time fee (37 CFR 1.136 and 1.17)

      iii. ☐ Other _____

   b. ☐ Check in the amount of $ _____ enclosed

   c. ☐ Payment by credit card (Form PTO-2038 enclosed)

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Signature	/Sean D. Burdick/	Date	July 20, 2015
Name (Print/Type)	Sean D. Burdick	Registration No.	51,513

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop RCE, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450 or facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.

Signature			
Name (Print/Type)		Date	

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. no.:	13/734,178	Conf. no.	3155
Applicant:	Craig S. Etchegoyen	Art Unit:	2649
Filed:	January 4, 2013	Examiner:	Ajibola A. Akinyemi

Title: NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES

RESPONSE TO FINAL OFFICE ACTION

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir,

In response to the Final Office Action mailed March 4, 2015, Applicant respectfully requests continued examination in accordance with the following:

Amendments to the Claims begin on page 2; and

Remarks begin on page 5.

IN THE CLAIMS:

1. (currently amended) A method for near field authentication of a source, the source using an audio transceiver computing device, the method comprising:

scanning a plurality of predetermined frequencies for a free frequency;

selecting the free frequency from the plurality of predetermined frequencies;

generating a periodic enclosed content message;

generating a modulated carrier wave representing the periodic enclosed content message; and

transmitting the modulated carrier wave at the free frequency;

wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication; and

wherein the content includes ~~at least one of~~ biometric data~~, or device identification data, wherein the device identification data includes a bit string or bit array derived from user-configurable and non-user-configurable data specific to the audio transceiver computing device~~.

2. (original) The method of claim 1 further comprising:

displaying a user interface on the audio transceiver computing device requesting the biometric data from a user; and

responsive to receiving the biometric data, generating the periodic enclosed content message, wherein the content in each period of the periodic enclosed content message includes the biometric data.

3. (previously presented) The method of claim 1, wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

4. (previously presented) The method of claim 1, wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.

5. (previously presented) The method of claim 1 wherein the modulated carrier wave comprises a sound wave.

6. (previously presented) The method of claim 2, wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

7. (previously presented) The method of claim 2, wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.

8. (previously presented) The method of claim 4 wherein the modulated carrier wave comprises a sound wave.

9. (previously presented) The method of claim 1 wherein the carrier wave is modulated by the periodic enclosed content message.

10. (currently amended) The method of claim [[1]]11, wherein the non-user-configurable data comprises hardware component numbers, serial numbers, and version numbers.

11. (new) A method for near field authentication of a source, the source using an audio transceiver computing device, the method comprising:

scanning a plurality of predetermined frequencies for a free frequency;

selecting the free frequency from the plurality of predetermined frequencies;

generating a periodic enclosed content message;

generating a modulated carrier wave representing the periodic enclosed content message; and

transmitting the modulated carrier wave at the free frequency;

wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication; and

wherein the content includes device identification data including a bit string or bit array derived from user-configurable and non-user-configurable data specific to the audio transceiver computing device.

12. (new) The method of claim 11, wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

13. (new) The method of claim 11, wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.

14. (new) The method of claim 11 wherein the modulated carrier wave comprises a sound wave.

15. (new) The method of claim 11 wherein the carrier wave is modulated by the periodic enclosed content message.

REMARKS

Applicant thanks Examiner Akinyemi for his thorough examination and for his opinion on patentability. Claims 1-15 are pending in the application. Claims 1 and 10 are currently amended in response to the Examiner's prior suggestion. New claims 11-15 have been added to particularly point out and specifically claim an embodiment of the disclosure. No new matter has been added. Support for claims 11-15 is found throughout the specification, for example, at paragraphs 0035-0037 of the originally-filed specification.

Applicant has carefully studied the outstanding Office Action. The present Response is intended to be fully responsive to all points of rejection raised in the Office Action and is believed to place the application in condition for allowance. Favorable reconsideration and allowance of this application is respectfully requested. Applicant respectfully requests reconsideration and withdrawal of all rejections in view of the foregoing amendments and following remarks.

Response to Rejections Under 35 U.S.C. § 103

Claim 1

In the Final Action, Claim 1 was rejected under Pre-AIA 35 U.S.C. § 103(a) as being unpatentable over U.S. Application Pub. 2004/0038716 ("*Gass*") in view of U.S. Application Pub. 2011/0215158 ("*Kargl*"), and in further view of U.S. Application Pub. 2012/0216262 ("*Bardsley*"). Office Action, page 2. Applicant respectfully traverses.

If the Patent Office does not produce a *prima facie* case of unpatentability, then without more the applicant is entitled to grant of a patent. *In re Oetiker*, 977 F.2d 1443, 1445, 24 U.S.P.Q.2d 1443, 1444 (Fed. Cir. 1992); *In re Grabiak*, 769 F.2d 729, 733, 226 U.S.P.Q. 870, 873 (Fed. Cir. 1985). The initial burden of establishing a *prima facie* basis to deny patentability to a claimed invention is always upon the Patent Office. *In re Oetiker*, 977 F.2d 1443, 1445, 24 U.S.P.Q.2d 1443, 1444 (Fed. Cir. 1992); *In re Piasecki*, 745 F.2d 1468, 1472, 223 U.S.P.Q. 785, 788 (Fed. Cir. 1984). Applicant respectfully submits, for the reasons discussed herein below, that even if modified or combined as proposed by Examiner, the proposed combinations still fail to

yield or disclose all limitations of the claimed invention. Accordingly, Applicant submits that Examiner has not produced a *prima facie* case of obviousness.

Regarding the rejections under 35 U.S.C. § 103(a), the Supreme Court has held that rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. *KSR Int'l Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1741 (2007). A patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art. *Id.* An Examiner must "identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does." *Id.* And, the Examiner must make "explicit" this rationale of "the apparent reason to combine the known elements in the fashion claimed," including a detailed explanation of "the effects of demands known to the design community or present in the marketplace" and "the background knowledge possessed by a person having ordinary skill in the art." *Id.* Anything less than such an explicit analysis is insufficient to support a *prima facie* case of obviousness.

A. The Obviousness Rejection of Claim 1 Should be Reversed Because the References Fail to Teach All Claimed Elements.

1. *Gass* and the Other Cited References Fail to Teach a Source Using an Audio Transceiver to Perform the Near Field Authentication of Said Source.

Applicant respectfully submits that there are several limitations which the cited prior art fail to disclose or suggest. First, claim 1 recites a limitation (within the preamble) of a "[a] method for near field authentication of a source, the source using an audio transceiver computing device." (Claim 1) (emphasis added.) Section 2111.02(I) of the Manual of Patent Examining Procedure sets forth that any terminology in the preamble that limits the structure of the claimed invention must be treated as a claim limitation. Accordingly, the claimed method for near field authentication of a source computing device requires the source computing device to utilize an audio transceiver device to do so.

As detailed in Applicant's most recent response filed February 2, 2015, the claimed invention is directed to methods for near field authentication of a computing device. (Spec. at ¶¶ 0002, 0007.) Specifically, the disclosure relates to a method to authenticate a transaction source

using a specifically-modulated audio signal. The invention may be used, for example, to add another level of security to an electronic transaction, by exploiting the audio transceiving capabilities of modern computing devices. For example, a point-of-sale merchant computer equipped with a microphone input can authenticate an electronic transaction with a buyer's mobile phone by receiving *near-field* audio transmissions from the audio speaker of the mobile phone when the buyer wants to complete the transaction. (Spec. at ¶ 0066.) This ensures that the buyer must be physically present within the merchant's store, to prevent a remote identity thief from completing a phony transaction. The invention may be applied in fields other than financial transactions, for example, to allow a user to gain physical access to secure locations.

For example, to authenticate the transaction, the merchant computer may send a text message to the mobile phone asking the customer to transmit a device identifier or biometric identifier (or both) to the merchant's computer using a sound wave. Sound waves generated through the acoustic speaker of a mobile phone are very low power signals, therefore when such a wave is picked up by the microphone of the merchant computer, it provides a very high level of confidence that the customer is physically present inside the store, and probably within a few feet of the merchant computer. The invention allows the customer's mobile phone to modulate the sound wave with an encoded message (i.e., a "periodic enclosed content message") that contains the device identifier data and/or the biometric identifier. The merchant computer can then decode the message, extract the identifier, and compare it against a list of pre-authorized identifiers to complete the authentication.

The Final Action cites to *Gass* at ¶ 0016 for allegedly teaching "a method for near field authentication of a source, the source using an audio transceiver computing device comprising scanning a plurality of predetermined frequencies for a free frequency." *Gass*, however, fails to support this allegation. *Gass* teaches a system for converting GSM (cell phone) signals into FM radio signals to enable "hands free" cell phone communications while driving a car. In order to accomplish this task, *Gass* teaches the use of a mobile terminal (abbreviated "MT" in the specification) that includes a radio sender ("SD") transmitting through a "sending antenna" (see structure "A1" at Figure 1), allowing for the transmission of FM radio waves to an audio system such as a car radio connected to speakers. (*Gass* at ¶ 0016-0017.) While *Gass* teaches a separate antenna "B" (see Figure 1) that receives a GSM signal which is forwarded to a GSM receiver,

which plays no direct part in communications with the audio system (car radio), there is no teaching of a transceiver involved in communications with the audio system.

Thus, while Gass discloses a radio transmitter in a source device, as well as a radio receiver in a receiving audio system (car radio), *Gass* does not teach a source computing device using an audio transceiver (having both audio transmitting and receiving functionality) to perform a method of near field authentication of said source. At best, *Gass* teaches the use of a radio transmitter or "sender" to send radio waves to a car radio. In summary, neither *Gass*, nor any of the other cited references teach or suggest this inventive feature of a source computing device using an audio transceiver to perform the claimed method of near field authentication of said source.

2. *Gass* and the Other Cited References Fail to Teach the Generation of a Periodic Enclosed Content Message.

Claim 1 further recites a step of "generating a periodic enclosed content message." (Claim 1.) The Final Action cites to *Gass* at ¶ 0015-0016 for allegedly teaching the step of "generating a periodic enclosed content message." However, *Gass* includes no such teaching or even suggests that the mobile terminal ("MT") generates a periodic enclosed content message. While *Gass* teaches the transmission of a signal over FM radio waves, it does not teach or suggest that the signal includes an enclosed message at each period of the transmitted radio wave.

Likewise, *Kargl* also does not teach such generation of an enclosed content message at each period. *Kargl* rather teaches (at ¶¶ 0038-0039 pointed to by the Examiner) the use of "digital data streams" and "data packets," with no reference to any enclosed message content at any period. Figure 3 of *Kargl* illustrates the modulation of a digital data stream modulated by a carrier signal, showing no periodic enclosed content message. In summary, neither *Gass*, *Kargl*, nor any of the other cited references teach or suggest this inventive feature of generating a periodic enclosed content message.

B. The Obviousness Rejection of Claim 1, Based On a Combination of *Gass* and *Bardsley,* Is Improper Because Such Combination Would Render the Invention of *Gass* Unsuitable for Its Intended Purpose.

Claim 1 recites, with the context of a method for near field authentication of a source, the limitations of "generating a periodic enclosed content message . . . wherein the content includes at least one of biometric data." Examiner acknowledges that *Gass* and *Kargl* fail to disclose this feature of "wherein the content includes at least one of biometric data" and instead relies upon

Bardsley. Applicant respectfully submits that it would be improper to combine the teachings of *Bardsley* with the teachings of *Gass* because it would render the invention taught in Gass unsuitable for its intended purpose.

If a proposal for modifying the prior art in an effort to attain the claimed invention causes the art to become inoperable or destroys its intended function, then the requisite motivation to make the modification would not have existed. *See In re Fritch*, 972 F.2d 1260, 1265 n. 12 ("A proposed modification [is] inappropriate for an obviousness inquiry when the modification render[s] the prior art reference inoperable for its intended purpose"); *see also, In re Ratti*, 270 F.2d 810, 813 (CCPA 1959) (holding the suggested combination of references improper under § 103 because it "would require a substantial reconstruction and redesign of the elements shown in [a prior art reference] as well as change in the basic principles under which [that reference's] construction was designed to operate").

In the present case, *Gass* teaches the use of a radio transmitter on a mobile terminal to broadcast information to an audio system such as a car radio receiver including a radio data system (RDS) receiver. The thrust of the system taught by *Gass* is to provide for the broadcast of information from a mobile terminal to a car radio receiver (with RDS receiver) that can then amplify the volume of the communications over the car's speakers, thus allowing for hands-free communications while driving. (*Gass* at ¶¶ 0001-0007.)

In contrast, the use of biometric data and the authentication of such data taught by *Bardsley*, requires the storage of biometric identification information on a database, which must further be analyzed and associated with a user in order to authenticate the identity of the source user. (*Bardsley* at ¶ 0037.) *Bardsley* further teaches the transmission of such biometric information using "network packets" using "network protocols" such as "Ethernet, ATM, IP version 4(IPv4), IP Version 6 (IPv6), TCP, UDP, MPLS, etc." (*Bardsley* at ¶ 0098.)

Even to the extent that the mobile terminal taught by *Gass* could be modified to transmit such biometric information to the audio system (car radio receiver and speakers), which would itself require a major modification/redesign to the mobile terminal to store and transmit network packets using network protocols, the audio system (AU) taught by *Gass* would be rendered inoperable for its intended purpose – hands-free mobile communications.

In short, the audio system taught by *Gass* does not include a database or any other suitable

structure for storing biometric data so that it could associate any incoming biometric data with the user of the mobile terminal. Not only that, but the audio system taught by *Gass* has no means for analyzing any received biometric data even if such transmissions could be received. Further, the audio system taught by *Gass* has no means for receiving network packets using various network protocols – the entire thrust of *Gass* is to utilize radio transmissions in cars having radio receivers (including RDS receivers) such that no modification would be needed of preexisting car radios (*see Bardsley* at ¶ 0017). Just as noted in *In re Gatti*, the entire system taught by *Gass* would require a substantial reconstruction and redesign, as well as a change in the basic principles under which the system of *Gass* was designed to operate, in order to utilize biometric data for authentication purposes. Therefore, it is respectfully submitted that it is improper to combine *Gass*, *Kargl*, and *Bardsley* under § 103(a).

Claims 2-9

Claim 2 was rejected under 35 U.S.C. § 103(a) as being unpatentable over *Gass*, *Kargl*, and *Bardsley*, and in further view of U.S. Application Pub. 2007/0198850 ("*Martin*"). Claims 3-5 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Gass*, *Kargl*, and *Bardsley*, and in further view of U.S. Patent No. 5,019,813 ("*Kip*"). Claims 6-8 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Gass*, *Kargl*, *Bardsley*, *Martin*, and *Kip.* Claim 9 was rejected under 35 U.S.C. § 103(a) as being unpatentable over *Gass*, *Kargl*, and *Bardsley*.

Claims 2-9 all depend, either directly or indirectly, from an otherwise patentable independent claim 1. If an independent claim is nonobvious under 35 U.S.C. § 103, then any claim depending therefrom is nonobvious. *In Re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); MPEP § 2143.03. Therefore claims 2-9 are deemed patentable over *Gass, Kargl, and Bardsley,* in any combination with *Martin or Kip* at least by the virtue of their dependence on claim 1. Accordingly, additional reasons for patentability of dependent claims 2-9 will not be proffered. Reversal of all obviousness rejections is respectfully requested.

Claims 10-15

New claim 11 includes nearly identical limitations as claim 1 but instead of reciting that the content includes biometric data, claim 11 recites that the content includes device identification data and further recites the limitation of "wherein the device identification data includes a bit string

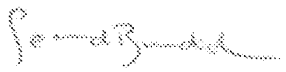
or bit array derived from user-configurable and non-user-configurable data specific to the audio transceiver computing device." None of the cited references teach the foregoing limitation, which was not disputed by the Examiner in the most recent Action. Claims 10 and 12-15 all depend, either directly or indirectly, from an otherwise patentable independent claim 11. Therefore claims 10 and 12-15 are deemed patentable over *Gass, Kargl, and Bardsley,* in any combination with *Martin or Kip* at least by the virtue of their dependence on claim 11. Accordingly, additional reasons for patentability of dependent claims 10 and 12-15 will not be proffered.

Applicant respectfully requests reconsideration of all obviousness rejections and allowance of all claims.

CONCLUSION

It is respectfully urged that the claims of the subject application are patentable over the references cited in the Office Action, and are now in condition for allowance. Applicant requests consideration of the application and allowance of the claims. If there are any outstanding issues that the Examiner feels may be resolved by way of a telephone conference, the Examiner is cordially invited to contact the undersigned attorney at the number below.

Respectfully Submitted,



Sean D. Burdick
Reg. No. 51,513

Uniloc USA, Inc.
7160 N. Dallas Parkway, Suite 380
Plano, TX 75024
(972) 905-9580 x 227

Electronic Patent Application Fee Transmittal					
Application Number:	13734178				
Filing Date:	04-Jan-2013				
Title of Invention:	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES				
First Named Inventor/Applicant Name:	Craig S. ETCHEGOYEN				
Filer:	Sean Dylan Burdick/Tanya Kiatkulpiboone				
Attorney Docket Number:	UN-NP-SC-085				
Filed as Small Entity					
Filing Fees for **Utility under 35 USC 111(a)**					
Description		**Fee Code**	**Quantity**	**Amount**	**Sub-Total in USD($)**
Basic Filing:					
Pages:					
Claims:					
Miscellaneous-Filing:					
Petition:					
Patent-Appeals-and-Interference:					
Post-Allowance-and-Post-Issuance:					
Extension-of-Time:					

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Request for Continued Examination	2801	1	600	600
		Total in USD ($)		**600**

Electronic Acknowledgement Receipt	
EFS ID:	22969593
Application Number:	13734178
International Application Number:	
Confirmation Number:	3155
Title of Invention:	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES
First Named Inventor/Applicant Name:	Craig S. ETCHEGOYEN
Customer Number:	96051
Filer:	Sean Dylan Burdick/Tanya Kiatkulpiboone
Filer Authorized By:	Sean Dylan Burdick
Attorney Docket Number:	UN-NP-SC-085
Receipt Date:	20-JUL-2015
Filing Date:	04-JAN-2013
Time Stamp:	19:21:39
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$600
RAM confirmation Number	6261
Deposit Account	506053
Authorized User	BURDICK, SEAN D
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	SC-085_RCE_Transmittal.pdf	100111 f00a366462fb9649a71a077d71de3138ee23afc4	no	1
Warnings:					
This is not a USPTO supplied RCE SB30 form.					
Information:					
2	Amendment/Argument after Notice of Appeal	SC-085_RCE_Resp_to_20150304_FOA_FINAL.pdf	92988 9b1da05b597b0d4437495a487da519f80c9fb7dd	no	11
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	31133 873c29cf0365e3ac05454c230be602d1f685a918	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	224232		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/734,178	Filing Date 01/04/2013	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	07/20/2015	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 15	Minus	** 20	= 0	X $40 =	0
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $210 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	0

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/ALLYSON PURNELL/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/734,178	01/04/2013	Craig S. ETCHEGOYEN	UN-NP-SC-085	3155

96051 7590 08/13/2015

Uniloc USA Inc.
Legacy Town Center
7160 Dallas Parkway
Suite 380
Plano, TX 75024

EXAMINER
AKINYEMI, AJIBOLA A

ART UNIT	PAPER NUMBER
2649	

NOTIFICATION DATE	DELIVERY MODE
08/13/2015	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

sean.burdick@unilocusa.com
tkiatkulpiboone@unilocusa.com
kris.pangan@unilocusa.com

Office Action Summary	Application No. 13/734,178	Applicant(s) ETCHEGOYEN ET AL.	
	Examiner AJIBOLA AKINYEMI	Art Unit 2649	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07/20/2015*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-15* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-15* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *01/04/2013* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some * c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

1) The present application is being examined under the pre-AIA first to invent provisions.

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 07/20/2015 has been entered.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained through the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under pre-AIA 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.

2. Ascertaining the differences between the prior art and the claims at issue.

3. Resolving the level of ordinary skill in the pertinent art.

4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

3. Claims 1, 9, 11, 15 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Gass (Pub. No.: US 2004/0038716A1) and further in view of Kargl (Pub. No.: US 2011/0215158A1) and Bee (Pub. No.: US 2008/0080750A1).

With respect to claim 1:

Gass discloses a method for near field authentication of a source the source using an audio transceiver computing device comprising scanning a plurality of predetermined frequencies for a free frequency **(parag,0016 discloses scanning plurality of predetermined frequency for a free frequencies);** selecting the free frequency from the plurality of predetermined frequencies **(parag.0016 also discloses selecting free frequency from plurality of frequencies);** generating a periodic enclosed content message; generating a modulated carrier wave representing the periodic enclosed content message and transmitting the modulated carrier wave at the free frequency **(Parag. 0015 also discloses the RDS encoder encodes said frequency or channel information generating a corresponding RDS signal 5 modulated on the RDS sub carrier at 57 KHz).**

Gass does not explicitly disclose wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication; and wherein the content includes at least one of biometric data;

Kargl discloses an enclosed content message includes a begin indication, a content, and an end indication; **(fig.4B, item 402 represent begin indication, item 404 represents end indication and item 400 represent content as in parag. 0038).** It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the teaching of Kargl into the teaching of Gass in order to reduce the hardware complexity and increase data rate.

Gass and Kargl do not disclose content to include at least one of biometric data.

Bee discloses transmitting content with biometric data via all kinds of transmission frequencies or wireless transmission/reception technologies such as a general car-use frequency channel or transmission/reception module of Bluetooth wireless communication, 802.11a/b/g **(parag. 0025).**

It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the teaching of Bee into teaching of Gass in view of Kargl so as to promote system's security and convenience of wireless remote control.

With respect to claims 9, 15:

Kargl discloses the method wherein the carrier wave is modulated by the periodic enclosed content message (abst. parag. 0005).

With respect to claim 11:

Gass discloses a method for near field authentication of a source, the source using an audio transceiver computing device, the method comprising scanning a plurality of predetermined frequencies for a free frequency **(parag,0016 discloses scanning plurality of predetermined frequency for a free frequencies);**; selecting the free frequency from the plurality of predetermined frequencies **(parag.0016 also discloses selecting free frequency from plurality of frequencies);** generating a periodic enclosed content message; generating a modulated carrier wave representing the periodic enclosed content message; and transmitting the modulated carrier wave at the free frequency **(Parag. 0015 also discloses the RDS encoder encodes said frequency or channel information generating a corresponding RDS signal 5 modulated on the RDS sub carrier at 57 KHz).**

Gass does not explicitly disclose wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication; and wherein the content includes device identification data including a bit string or bit array derived from user-configurable and non-user-configurable data specific to the audio transceiver computing device.

Kargl discloses an enclosed content message includes a begin indication, a content, and an end indication; **(fig.4B, item 402 represent begin indication, item 404 represents end indication and item 400 represent content as in parag. 0038).** It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the teaching of Kargl into the teaching of Gass in order to reduce the hardware complexity and increase data rate.

Bee discloses content includes device identification data including a bit string or bit array derived from user-configurable and non-user-configurable data specific to the audio transceiver computing device (**parag. 0024-0025 discloses a fingerprint image processing and control unit 12 for providing the functions of fingerprint image processing, fingerprint template extraction, and identification; transmitting content with biometric data via all kinds of transmission frequencies or wireless transmission/reception technologies such as a general car-use frequency channel or transmission/reception module of Bluetooth wireless communication, 802.11a/b/g).**

It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the teaching of Bee into teaching of Gass in view of Kargl so as to promote system's security and convenience of wireless remote control.

4. Claim 2 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Gass (Pub. No.: US 2004/0038716A1), Kargl (Pub. No. No. US 2011/0215158A1), Bee (Pub. No.: US 2008/0080750A1) as applied to claim 1 above and further in view of Martin (Pub. No.: US 2007/0198850A1).

With respect to claim 2:

The rejection of claim 1 is incorporated; Gass, Karl and Bee do not explicitly disclose the method further comprising displaying a user interface on the audio transceiver computing device requesting the biometric data from a user; and responsive to receiving the biometric data, generating the periodic enclosed content message,

wherein the content in each period of the periodic enclosed content message includes the biometric data.

Martin discloses this limitation (parag. 0062-0063 discloses a user interface on the audio transceiver computing device requesting the biometric data from a user). It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the teaching of Martin into the teaching of Gass in view of Karlg and Bee in order to provide a security system wherein the user is provided with dual layered verification system in addition to a unique identifier given to the user.

5. Claims 3-5, 12-14 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Gass (Pub. No.: US 2004/0038716A1), Kargl (Pub. No. No. US 2011/0215158A1), Bee (Pub. No.: US 2008/0080750A1) as applied to claim 1 above and further in view of Kip (Patent No.: US 5019813).

With respect to claims 3, 12:

The rejection of claim 1 is incorporated; Gass, Kargl and Bee do not explicitly disclose wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

Kip discloses this above limitations (col.5, line 39-44). It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the teaching of Kip into the teaching of Gass view of Karlg and Bee in order to provide a universally applicable data exchange system operating in a contactless manner.

With respect to claims 4, 13:

Kip discloses the method wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user (fig.5b, col.5, line 39-44).

With respect to claims 5, 14:

Gass discloses the method wherein the modulated carrier wave comprises a sound wave (parag. 0016).

6. Claims 6-8 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Gass (Pub. No.: US 2004/0038716A1), Kargl (Pub. No. No. US 2011/0215158A1), Bee (Pub. No.: US 2008/0080750A1), Martin (Pub. No.: US 2007/0198850A1) as applied to claim 2 above and further in view of Kip (Patent No.: US 5019813).

With respect to claim 6:

The rejection of claim 2 is incorporated; Gass, Kargl, Bee and Martin do not disclose wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

Kip discloses this above limitations (col.5, line 39-44). It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the teaching of Kip into the teaching of Gass in view of Kargl, Bee and Martin in order to provide a universally applicable data exchange system operating in a contactless manner.

With respect to claim 7:

Kip discloses the method wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user (fig.5b, col.5, line 39-44).

With respect to claim 8:

Gass discloses the method wherein the modulated carrier wave comprises a sound wave (parag. 0016).

Response to Arguments

Applicant's arguments with respect to claims 1, 11 have been considered but are moot because the arguments do not apply to any of the references being used in the current rejection.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to AJIBOLA AKINYEMI whose telephone number is (571)270-1846. The examiner can normally be reached on monday- friday (8.30-5pm) Est.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, YUWEN PAN can be reached on (571) 272-7855. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/AJIBOLA AKINYEMI/
Primary Examiner, Art Unit 2649

Notice of References Cited	Application/Control No. 13/734,178	Applicant(s)/Patent Under Reexamination ETCHEGOYEN ET AL.	
	Examiner AJIBOLA AKINYEMI	Art Unit 2649	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-5,019,813 A	05-1991	Kip et al.	340/10.51
*	B	US-2004/0038716 A1	02-2004	Gass, Vincent	455/569.1
*	C	US-2007/0198850 A1	08-2007	Martin et al.	713/186
*	D	US-2008/0080750 A1	04-2008	Bee et al.	382/124
*	E	US-2010/0208899 A1	08-2010	Kasargod et al.	381/1
*	F	US-2011/0215158 A1	09-2011	Kargl et al.	235/492
*	G	US-2012/0216262 A1	08-2012	Bardsley et al.	726/5
*	H	US-2013/0159701 A1	06-2013	PHILLIPS et al.	713/155
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13734178	ETCHEGOYEN ET AL.
	Examiner	**Art Unit**
	AJIBOLA AKINYEMI	2649

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	08/30/2013	01/14/2014	10/28/2014	02/25/2015	08/07/2015				
	1	✓	✓	✓	✓	✓				
	2	✓	✓	✓	✓	✓				
	3	✓	✓	✓	✓	✓				
	4	✓	✓	✓	✓	✓				
	5	✓	✓	✓	✓	✓				
	6	✓	✓	✓	✓	✓				
	7	✓	✓	✓	✓	✓				
	8	✓	✓	✓	✓	✓				
	9		✓	✓	✓	✓				
	10					✓				
	11					✓				
	12					✓				
	13					✓				
	14					✓				
	15					✓				

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	3	scan$4 same free near frequency same message	US-PGPUB; USPAT	OR	OFF	2015/08/07 13:05
L2	3	1 AND ((H04B1/034 OR H04B1/205 OR H04B5/0031 OR H04B5/02).CPC.)	US-PGPUB; USPAT	OR	OFF	2015/08/07 13:08

EAST Search History (Interference)

< This search history is empty>

8/ 7/ 2015 1:10:16 PM
C:\ Users\ aakinyemi\ Documents\ EAST\ Workspaces\ 14219992.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13734178	ETCHEGOYEN ET AL.
	Examiner	Art Unit
	AJIBOLA AKINYEMI	2649

CPC- SEARCHED		
Symbol	Date	Examiner
H04B1/034; H04B1/205; H04B5/0031; H04B5/02	8/7/2015	AA

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
455	41.1	8/7/2015	AA

SEARCH NOTES		
Search Notes	Date	Examiner
H04B1/034; H04B1/205; H04B5/0031; H04B5/02	8/7/2015	AA

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. no.:	13/734,178	Conf. no.	3155
Applicant:	Craig S. ETCHEGOYEN	Art Unit:	2649
Filed:	January 4, 2013	Examiner:	Ajibola A. Akinyemi

Title: NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES

RESPONSE TO OFFICE ACTION

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir,

In response to the Office Action mailed August 13, 2015, Applicant respectfully requests reconsideration of all pending claims in view of the amendments and remarks set forth herein:

IN THE CLAIMS:

1. (currently amended) A method for near field authentication of a source, the source using an audio transceiver computing device, the method comprising:

scanning a plurality of predetermined frequencies for a free frequency;

selecting the free frequency from the plurality of predetermined frequencies;

generating a periodic enclosed content message;

generating a modulated carrier wave representing the periodic enclosed content message; and

transmitting the modulated carrier wave at the free frequency;

wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication; ~~and~~

wherein the content includes biometric data[[.]]; and

wherein the modulated carrier wave comprises a sound wave.

2. (original) The method of claim 1 further comprising:

displaying a user interface on the audio transceiver computing device requesting the biometric data from a user; and

responsive to receiving the biometric data, generating the periodic enclosed content message, wherein the content in each period of the periodic enclosed content message includes the biometric data.

3. (previously presented) The method of claim 1, wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

4. (previously presented) The method of claim 1, wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.

5. (canceled)

6. (previously presented) The method of claim 2, wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

7. (previously presented) The method of claim 2, wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.

8. (canceled).

9. (previously presented) The method of claim 1 wherein the carrier wave is modulated by the periodic enclosed content message.

10. (previously presented) The method of claim 11, wherein the non-user-configurable data comprises hardware component numbers, serial numbers, and version numbers.

11. (currently amended) A method for near field authentication of a source, the source using an audio transceiver computing device, the method comprising:

scanning a plurality of predetermined frequencies for a free frequency;

selecting the free frequency from the plurality of predetermined frequencies;

generating a periodic enclosed content message;

generating a modulated carrier wave representing the periodic enclosed content message; and

transmitting the modulated carrier wave at the free frequency;

wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication; ~~and~~

wherein the content includes device identification data including a bit string or bit array derived from user-configurable and non-user-configurable data specific to the audio transceiver computing device[[.]]; and

wherein the modulated carrier wave comprises a sound wave.

12. (previously presented) The method of claim 11, wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

13. (previously presented) The method of claim 11, wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.

14. (canceled).

15. (previously presented) The method of claim 11 wherein the carrier wave is modulated by the periodic enclosed content message.

REMARKS

Applicant thanks Examiner Akinyemi for his thorough examination and for his opinion on patentability. Claims 1-4, 6-7, 9-13, and 15 are pending in the application. Claims 1 and 11 are currently amended. Claims 5, 8, and 14 have been cancelled. No new matter has been added.

Response to Rejections Under 35 U.S.C. §103

Claims 1 and 11

In the most recent Action, independent claims 1 and 11 were rejected under Pre-AIA 35 U.S.C. § 103(a) as being unpatentable over U.S. Application Pub. 2004/0038716 ("*Gass*") in view of U.S. Application Pub. 2011/0215158 ("*Kargl*"), and in further view of U.S. Application Pub. 2008/0080750 ("*Bee*"). Office Action, page 3. Applicant respectfully traverses.

If the Patent Office does not produce a *prima facie* case of unpatentability, then without more the applicant is entitled to grant of a patent. *In re Oetiker*, 977 F.2d 1443, 1445, 24 U.S.P.Q.2d 1443, 1444 (Fed. Cir. 1992); *In re Grabiak*, 769 F.2d 729, 733, 226 U.S.P.Q. 870, 873 (Fed. Cir. 1985). The initial burden of establishing a *prima facie* basis to deny patentability to a claimed invention is always upon the Patent Office. *In re Oetiker*, 977 F.2d 1443, 1445, 24 U.S.P.Q.2d 1443, 1444 (Fed. Cir. 1992); *In re Piasecki*, 745 F.2d 1468, 1472, 223 U.S.P.Q. 785, 788 (Fed. Cir. 1984). Applicant respectfully submits, for the reasons discussed herein below, that even if modified or combined as proposed by Examiner, the proposed combinations still fail to yield or disclose all limitations of the claimed invention. Accordingly, Applicant submits that Examiner has not produced a *prima facie* case of obviousness.

Regarding the rejections under 35 U.S.C. § 103(a), the Supreme Court has held that rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. *KSR Int'l Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1741 (2007). A patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art. *Id.* An Examiner must "identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does." *Id.* And, the Examiner must make "explicit" this rationale of "the apparent reason to combine the known elements in the fashion

claimed," including a detailed explanation of "the effects of demands known to the design community or present in the marketplace" and "the background knowledge possessed by a person having ordinary skill in the art." *Id.* Anything less than such an explicit analysis is insufficient to support a *prima facie* case of obviousness.

A. The Obviousness Rejection of Claims 1 and 11 Should be Reversed Because the References Fail to Teach All Claimed Elements.

1. *Gass* and the Other Cited References Fail to Teach an Audio Transceiver to Generate a Modulated Carrier Wave Comprising a Sound Wave.

Applicant respectfully submits that there are several limitations which the cited prior art fail to disclose or suggest. Claims 1 and 11 recite a limitation of "generating a modulated carrier wave representing the periodic enclosed content message" and now, as the claims have been amended herein, further recite a limitation of "wherein the modulated carrier wave comprises a sound wave." In short, Applicant has incorporated the limitations of previously presented claims 5, 8, and 14 into independent claims 1 and 11. As discussed in further detail below, neither *Gass* nor the other cited references teach the generation and transmission of sound waves.

The claimed invention is directed to methods for near field authentication of a computing device using sound waves. (Spec. at ¶ 0025.) Specifically, the disclosure relates to a method to authenticate a transaction source using a specifically-modulated carrier wave that can be a sound wave. (Spec. at ¶ 0026.) The invention may be used, for example, to add another level of security to an electronic transaction, by exploiting the audio transceiving capabilities of modern computing devices. For example, a point-of-sale merchant computer equipped with a microphone input can authenticate an electronic transaction with a buyer's mobile phone by receiving *near-field* audio transmissions from the audio speaker of the mobile phone when the buyer wants to complete the transaction. (Spec. at ¶ 0066.) This ensures that the buyer must be physically present within the merchant's store, to prevent a remote identity thief from completing a phony transaction. The invention may be applied in fields other than financial transactions, for example, to allow a user to gain physical access to secure locations.

For example, to authenticate the transaction, the merchant computer may send a text message to the mobile phone asking the customer to transmit a device identifier or biometric identifier (or both) to the merchant's computer using a sound wave. Sound waves generated

through the acoustic speaker of a mobile phone are very low power signals, therefore when such a wave is picked up by the microphone of the merchant computer, it provides a very high level of confidence that the customer is physically present inside the store, and probably within a few feet of the merchant computer. The invention allows the customer's mobile phone to modulate the sound wave with an encoded message (i.e., a "periodic enclosed content message") that contains the device identifier data and/or the biometric identifier. The merchant computer can then decode the message, extract the identifier, and compare it against a list of pre-authorized identifiers to complete the authentication.

In the most recent Action, the Examiner cites to *Gass* at ¶ 0016 for allegedly disclosing a modulated carrier wave comprising a sound wave. Action at 8-9. However, *Gass* neither discloses nor suggests the generation or transmission of a sound wave. In contrast, *Gass* teaches a system for converting GSM (cell phone) signals into FM radio signals to enable "hands free" cell phone communications while driving a car. To accomplish this task, *Gass* teaches the use of a mobile terminal (abbreviated "MT" in the specification) that includes an FM radio sender ("SD") transmitting through a "sending antenna" (see structure "A1" at Figure 1), allowing for the transmission of FM radio waves to an audio system such as a car radio connected to speakers. (*Gass* at ¶ 0016-0017.)

Thus, while *Gass* discloses the generation and transmission of radio waves, *Gass* does not teach the generation of sound waves. It is well-known that radio waves are electromagnetic in nature and thus have materially different properties and behaviors as compared to sound waves and thus, are not equivalent types of waves. In summary, neither *Gass*, nor any of the other cited references teach or suggest this inventive feature of generating a modulated carrier wave that comprises a sound wave.

B. The Obviousness Rejection of Claims 1 and 11, Based On a Combination of *Gass* and *Bee,* Is Improper Because Such Combination Would Render the Invention of *Gass* Unsuitable for Its Intended Purpose.

Claim 1 recites, with the context of a method for near field authentication of a source, the limitations of "generating a periodic enclosed content message . . . wherein the content includes at least one of biometric data." Claim 11 recites, with the context of a method for near field authentication of a source, the limitations of "generating a periodic enclosed content message . . . wherein the content includes device identification data including a bit string or bit array derived

from user-configurable and non-user-configurable data specific to the audio transceiver computing device." Examiner acknowledges that *Gass* and *Kargl* fail to disclose the foregoing limitations and instead relies upon *Bee* to supply the disclosure. Applicant respectfully submits that it would be improper to combine the teachings of *Bee* with the teachings of *Gass* because it would render the invention taught in *Gass* unsuitable for its intended purpose.

If a proposal for modifying the prior art in an effort to attain the claimed invention causes the art to become inoperable or destroys its intended function, then the requisite motivation to make the modification would not have existed. *See In re Fritch*, 972 F.2d 1260, 1265 n. 12 ("A proposed modification [is] inappropriate for an obviousness inquiry when the modification render[s] the prior art reference inoperable for its intended purpose"); *see also, In re Ratti*, 270 F.2d 810, 813 (CCPA 1959) (holding the suggested combination of references improper under § 103 because it "would require a substantial reconstruction and redesign of the elements shown in [a prior art reference] as well as change in the basic principles under which [that reference's] construction was designed to operate").

In the present case, *Gass* teaches the use of a radio transmitter on a mobile terminal to broadcast information to an audio system such as a car radio receiver including a radio data system (RDS) receiver. The thrust of the system taught by *Gass* is to provide for the broadcast of information from a mobile terminal to a car radio receiver (with RDS receiver) that can then amplify the volume of the communications over the car's speakers, thus allowing for hands free communications while driving. (*Gass* at ¶¶ 0001-0007.)

The use of biometric data and the authentication of such data taught by *Bee*, requires the storage of biometric identification information on a database, which must further be analyzed and associated with a user in order to authenticate the identity of the source user. Likewise, the utilization of a bit string or bit array derived from user-configurable and non-user-configurable data specific to the audio transceiver computing device for authentication purposes would also require the storage of corresponding data to authenticate the source device. Even to the extent that the mobile terminal taught by *Gass* could be modified to transmit such biometric information or user-configurable and non-user-configurable data to the audio system (car radio receiver and speakers), the audio system (AU) taught by *Gass* would be rendered inoperable for its intended purpose – hands free mobile communications.

In short, the audio system taught by *Gass* does not include a database or any other suitable structure for storing biometric data or user-configurable and non-user-configurable data so that it could associate any incoming data with the user of the mobile terminal. Not only that, but the audio system taught by *Gass* has no means for analyzing any received biometric data (or user-configurable and non-user-configurable data) even if such transmissions could be received.

Further, it should be noted that *Gass* teaches one-way communication from the mobile terminal to the audio terminal. (*Gass* at ¶ 0017; Figs. 1, 2.) *Gass* neither discloses nor suggests two-way communications between the mobile terminal and the audio terminal. In contrast, *Bee* teaches away from one-way communication, noting that such unilateral communications is a deficiency in prior art remote control systems. (*Bee* at ¶ 0003.) *Bee* goes on to teach the benefits of the use of "interactive two-way communication to ensure the accuracy of the execution result of the wireless remote control device and to obtain the real-time status feedback of the device." (*Bee* at ¶ 0008) (Emphasis added.) Just as noted in *In re Gatti*, the entire system taught by *Gass* would require a substantial reconstruction and redesign, as well as a change in the basic principles under which the system of *Gass* was designed to operate, in order to utilize such received data for authentication purposes, and to provide two-way communication as taught by *Bee*. Therefore, it is respectfully submitted that it is improper to combine *Gass* and *Bee* under § 103(a).

Claims 2-4, 6-7, 9-10, 12-13, and 15

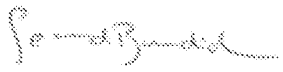
Claims 2-4, 6-7, 9-10, 12-13, and 15 all depend, either directly or indirectly, from an otherwise patentable independent claim 1 or 11. If an independent claim is nonobvious under 35 U.S.C. § 103, then any claim depending therefrom is nonobvious. *In Re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); MPEP § 2143.03. Therefore claims 2-4, 6-7, 9-10, 12-13, and 15 are deemed patentable over *Gass, Kargl, and Bee,* in any combination with *Martin or Kip* at least by the virtue of their dependence on claims 1 or 11. Accordingly, additional reasons for patentability of dependent claims 2-4, 6-7, 9-10, 12-13, and 15 will not be proffered. Reversal of all obviousness rejections is respectfully requested.

Applicant respectfully requests reconsideration of all obviousness rejections and allowance of all claims.

CONCLUSION

It is respectfully urged that the claims of the subject application are patentable over the references cited in the Office Action, and are now in condition for allowance. Applicant requests consideration of the application and allowance of the claims. If there are any outstanding issues that the Examiner feels may be resolved by way of a telephone conference, the Examiner is cordially invited to contact the undersigned attorney at the number below.

Respectfully Submitted,



Sean D. Burdick
Reg. No. 51,513

Uniloc USA, Inc.
7160 N. Dallas Parkway, Suite 380
Plano, TX 75024
(972) 905-9580 x 227

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. no.:	13/734,178	Conf. no.	3155
Applicant:	UNILOC LUXEMBOURG S.A.	Art Unit:	2649
Filed:	January 4, 2013	Examiner:	Ajibola A. Akinyemi

Title: NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENLCOSED CONTENT SOUND WAVES

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicant hereby submits, without admission of prior art effect thereof, form(s) PTO/SB/08 pursuant to the duty of disclosure requirements of 37 CFR §§ 1.56, 1.97 and 1.98.

Applicant has listed publication dates on the attached form(s) PTO/SB/08 based on information presently available to the undersigned. However, the listed publication dates should not be construed as an admission that the information was actually published on the date indicated.

It is respectfully requested that the Examiner initial and return a copy of the enclosed forms PTO/SB/08, and to indicate in the official file wrapper of this patent application that the documents have been considered.

Applicant submits concurrently herewith the fee set forth in § 1.17(p).

Respectfully Submitted,

Sean D. Burdick
Reg. No. 51,513

Uniloc USA, Inc.
7160 N. Dallas Parkway, Suite 380
Plano, TX 75024
972-905-9580 x227

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO
(modified by Applicant)

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	13/734,178
Filing Date	January 4, 2013
First Named Inventor	Craig S. ETCHEGOYEN, et al.
Art Unit	2649
Examiner Name	Ajibola A. Akinyemi
Attorney Docket Number	UN-NP-SC-085

U. S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		8,966,657	02-24-2015	Martinez	
		2007/0235525	10-11-2007	Murch	
		2011/0007901	01-13-2011	Ikeda et al.	
		2013/0212389	08-15-2013	McCreight et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code – Number – Kind Code	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date page(s), volume-issue number(s), publisher, city and/or country where published.	T

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Electronic Patent Application Fee Transmittal					
Application Number:	13734178				
Filing Date:	04-Jan-2013				
Title of Invention:	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES				
First Named Inventor/Applicant Name:	Craig S. ETCHEGOYEN				
Filer:	Sean Dylan Burdick/Tanya Kiatkulpiboone				
Attorney Docket Number:	UN-NP-SC-085				
Filed as Small Entity					
Filing Fees for **Utility under 35 USC 111(a)**					
Description		**Fee Code**	**Quantity**	**Amount**	**Sub-Total in USD($)**
Basic Filing:					
Pages:					
Claims:					
Miscellaneous-Filing:					
Petition:					
Patent-Appeals-and-Interference:					
Post-Allowance-and-Post-Issuance:					
Extension-of-Time:					

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	2806	1	90	90
		Total in USD ($)		**90**

Electronic Acknowledgement Receipt	
EFS ID:	23922260
Application Number:	13734178
International Application Number:	
Confirmation Number:	3155
Title of Invention:	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES
First Named Inventor/Applicant Name:	Craig S. ETCHEGOYEN
Customer Number:	96051
Filer:	Sean Dylan Burdick/Tanya Kiatkulpiboone
Filer Authorized By:	Sean Dylan Burdick
Attorney Docket Number:	UN-NP-SC-085
Receipt Date:	28-OCT-2015
Filing Date:	04-JAN-2013
Time Stamp:	18:02:31
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$90
RAM confirmation Number	5092
Deposit Account	506053
Authorized User	BURDICK, SEAN D
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	SC-085_Response_to_20150813_OA_FINAL.pdf	83192 501a2fda65ec7074d8f75d4d463d2a9ac430e8c6	no	10
Warnings:					
Information:					
2	Transmittal Letter	SC-085_IDS_Transmittal.pdf	62501 010228be01ae6ffd2f756dd50a120f1bfe27059f	no	2
Warnings:					
Information:					
3	Information Disclosure Statement (IDS) Form (SB08)	SC-085_IDS.pdf	27616 14f7fd2a0ab99881ae32fce20f48c54d60ff7011	no	1
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
4	Fee Worksheet (SB06)	fee-info.pdf	31079 3fac02fccb5c3c727b74a4809ac15da292c95bbd	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	204388		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/734,178	01/04/2013	Craig S. ETCHEGOYEN	UN-NP-SC-085	3155

96051 7590 11/06/2015

Uniloc USA Inc.
Legacy Town Center
7160 Dallas Parkway
Suite 380
Plano, TX 75024

EXAMINER
AKINYEMI, AJIBOLA A

ART UNIT	PAPER NUMBER
2649	

NOTIFICATION DATE	DELIVERY MODE
11/06/2015	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

sean.burdick@unilocusa.com
tkiatkulpiboone@unilocusa.com
kris.pangan@unilocusa.com

Office Action Summary	Application No. 13/734,178	Applicant(s) ETCHEGOYEN ET AL.	
	Examiner AJIBOLA AKINYEMI	Art Unit 2649	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10/28/2015*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-4, 6-7, 9-13, 15* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-4,6,7,9-13 and 15* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *01/04/2013* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some * c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

1) The present application is being examined under the pre-AIA first to invent provisions.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained through the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under pre-AIA 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.

2. Ascertaining the differences between the prior art and the claims at issue.

3. Resolving the level of ordinary skill in the pertinent art.

4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

3. Claims 1, 9, 11, 15 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Gass (Pub. No.: US 2004/0038716A1) and further in view of Kargl

(Pub. No.: US 2011/0215158A1), Bee (Pub. No.: US 2008/0080750A1) and Kent (Pub. No.: US 2012/0214416A1).

With respect to claim 1:

Gass discloses a method for near field authentication of a source the source using an audio transceiver computing device comprising scanning a plurality of predetermined frequencies for a free frequency **(parag,0016 discloses scanning plurality of predetermined frequency for a free frequencies);** selecting the free frequency from the plurality of predetermined frequencies **(parag.0016 also discloses selecting free frequency from plurality of frequencies);** generating a periodic enclosed content message; generating a modulated carrier wave representing the periodic enclosed content message and transmitting the modulated carrier wave at the free frequency **(Parag. 0015 also discloses the RDS encoder encodes said frequency or channel information generating a corresponding RDS signal 5 modulated on the RDS sub carrier at 57 KHz);**

wherein the modulated carrier wave comprises a sound wave **(parag. 0016);**

Gass does not explicitly disclose wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication; wherein the content includes at least one of biometric data;

Kargl discloses an enclosed content message includes a begin indication, a content, and an end indication; **(fig.4B, item 402 represent begin indication, item 404 represents end indication and item 400 represent content as in parag. 0038).** It would have been obvious to one of ordinary skill in the art at the time the invention was

made to utilize the teaching of Kargl into the teaching of Gass in order to reduce the hardware complexity and increase data rate.

Gass and Kargl do not disclose content to include at least one of biometric data;

Bee discloses transmitting content with biometric data via all kinds of transmission frequencies or wireless transmission/reception technologies such as a general car-use frequency channel or transmission/reception module of Bluetooth wireless communication, 802.11a/b/g **(parag. 0025).**

It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the teaching of Bee into teaching of Gass in view of Kargl so as to promote system's security and convenience of wireless remote control.

With respect to claims 9, 15:

Kargl discloses the method wherein the carrier wave is modulated by the periodic enclosed content message (abst. parag. 0005).

With respect to claim 11:

Gass discloses a method for near field authentication of a source, the source using an audio transceiver computing device, the method comprising scanning a plurality of predetermined frequencies for a free frequency **(parag,0016 discloses scanning plurality of predetermined frequency for a free frequencies);** selecting the free frequency from the plurality of predetermined frequencies **(parag.0016 also discloses selecting free frequency from plurality of frequencies);** generating a periodic enclosed content message; generating a modulated carrier wave representing the periodic enclosed content message; and transmitting the modulated carrier wave at the

free frequency **(Parag. 0015 also discloses the RDS encoder encodes said frequency or channel information generating a corresponding RDS signal 5 modulated on the RDS sub carrier at 57 KHz);**

wherein the modulated carrier wave comprises a sound wave **(parag. 0016);**

Gass does not explicitly disclose wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication; and wherein the content includes device identification data including a bit string or bit array derived from user-configurable and non-user-configurable data specific to the audio transceiver computing device.

Kargl discloses an enclosed content message includes a begin indication, a content, and an end indication; **(fig.4B, item 402 represent begin indication, item 404 represents end indication and item 400 represent content as in parag. 0038).** It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the teaching of Kargl into the teaching of Gass in order to reduce the hardware complexity and increase data rate.

Bee discloses content includes device identification data including a bit string or bit array derived from user-configurable and non-user-configurable data specific to the audio transceiver computing device (**parag. 0024-0025 discloses a fingerprint image processing and control unit 12 for providing the functions of fingerprint image processing, fingerprint template extraction, and identification; transmitting content with biometric data via all kinds of transmission frequencies or wireless transmission/reception technologies such as a general car-use frequency**

channel or transmission/reception module of Bluetooth wireless communication, 802.11a/b/g).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the teaching of Bee into teaching of Gass in view of Kargl so as to promote system's security and convenience of wireless remote control.

4. Claim 2 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Gass (Pub. No.: US 2004/0038716A1), Kargl (Pub. No. No. US 2011/0215158A1), Bee (Pub. No.: US 2008/0080750A1) as applied to claim 1 above and further in view of Martin (Pub. No.: US 2007/0198850A1).

With respect to claim 2:

The rejection of claim 1 is incorporated; Gass, Karl and Bee do not explicitly disclose the method further comprising displaying a user interface on the audio transceiver computing device requesting the biometric data from a user; and responsive to receiving the biometric data, generating the periodic enclosed content message, wherein the content in each period of the periodic enclosed content message includes the biometric data.

Martin discloses this limitation (parag. 0062-0063 discloses a user interface on the audio transceiver computing device requesting the biometric data from a user). It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the teaching of Martin into the teaching of Gass in view of Karlg and Bee in order to provide a security system wherein the user is provided with dual layered verification system in addition to a unique identifier given to the user.

5. Claims 3-4, 12-13 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Gass (Pub. No.: US 2004/0038716A1), Kargl (Pub. No. No. US 2011/0215158A1), Bee (Pub. No.: US 2008/0080750A1) as applied to claim 1 above and further in view of Kip (Patent No.: US 5019813).

With respect to claims 3, 12:

The rejection of claim 1 is incorporated; Gass, Kargl and Bee do not explicitly disclose wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

Kip discloses this above limitations (col.5, line 39-44). It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the teaching of Kip into the teaching of Gass view of Karlg and Bee in order to provide a universally applicable data exchange system operating in a contactless manner.

With respect to claims 4, 13:

Kip discloses the method wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user (fig.5b, col.5, line 39-44).

6. Claims 6-7 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Gass (Pub. No.: US 2004/0038716A1), Kargl (Pub. No. No. US 2011/0215158A1),

Bee (Pub. No.: US 2008/0080750A1), Martin (Pub. No.: US 2007/0198850A1) as applied to claim 2 above and further in view of Kip (Patent No.: US 5019813).

With respect to claim 6:

The rejection of claim 2 is incorporated; Gass, Kargl, Bee and Martin do not disclose wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

Kip discloses this above limitations (col.5, line 39-44). It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the teaching of Kip into the teaching of Gass in view of Kargl, Bee and Martin in order to provide a universally applicable data exchange system operating in a contactless manner.

With respect to claim 7:

Kip discloses the method wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user (fig.5b, col.5, line 39-44).

Response to Arguments

Applicant's arguments filed 10/28/2015 have been fully considered but they are not persuasive. Regarding claims 1, 11, applicant argued that none of the cited prior art disclose wherein the modulated carrier wave comprises a sound wave.

Examiner respectfully disagrees with this statement because using a modulated carrier wave to comprise a sound wave is a broad term, Gass discloses in parag. 0016,

0018 that when a called is received on a mobile terminal MT, The ringing tone is transmitted over FM radio to audio system AU and then outputted through the loudspeaker LS which is inform of sound wave.

RELEVANT REFERENCE…….Kent Pub. No.: US 2012/0214416A1 …**parag. 0046 for modulating carrier wave to comprise a sound waves.**

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to AJIBOLA AKINYEMI whose telephone number is

(571)270-1846. The examiner can normally be reached on monday- friday (8.30-5pm) Est.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, YUWEN PAN can be reached on (571) 272-7855. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/AJIBOLA AKINYEMI/
Primary Examiner, Art Unit 2649

Notice of References Cited	Application/Control No. 13/734,178	Applicant(s)/Patent Under Reexamination ETCHEGOYEN ET AL.	
	Examiner AJIBOLA AKINYEMI	Art Unit 2649	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-5,019,813 A	05-1991	Kip; Harm J.	A01K11/006	340/10.51
*	B	US-2004/0038716 A1	02-2004	Gass, Vincent	H04M1/6091	455/569.1
*	C	US-2007/0198850 A1	08-2007	Martin; Christopher D.	G07C9/00087	713/186
*	D	US-2008/0080750 A1	04-2008	Bee; Chap-Meng	G06K9/00006	382/124
*	E	US-2010/0208899 A1	08-2010	Kasargod; Sudhir K.	H04S1/002	381/1
*	F	US-2011/0215158 A1	09-2011	Kargl; Walter	H04L27/04	235/492
*	G	US-2012/0216262 A1	08-2012	Bardsley; Jeffrey Scott	H04L63/0861	726/5
*	H	US-2012/0214416 A1	08-2012	Kent; Jonathan Douglas	H04L63/18	455/41.2
*	I	US-2013/0159701 A1	06-2013	PHILLIPS, II; Eugene B.	H04L63/045	713/155
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO
(modified by Applicant)

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	13/734,178
Filing Date	January 4, 2013
First Named Inventor	Craig S. ETCHEGOYEN, et al.
Art Unit	2649
Examiner Name	Ajibola A. Akinyemi
Attorney Docket Number	UN-NP-SC-085

U. S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		8,966,657	02-24-2015	Martinez	
		2007/0235525	10-11-2007	Murch	
		2011/0007901	01-13-2011	Ikeda et al.	
		2013/0212389	08-15-2013	McCreight et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code – Number – Kind Code	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date page(s), volume-issue number(s), publisher, city and/or country where published.	T

Examiner Signature	/Ajibola Akinyemi/	Date Considered	11/03/2015

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A./

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13734178	ETCHEGOYEN ET AL.
	Examiner	Art Unit
	AJIBOLA AKINYEMI	2649

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	08/30/2013	01/14/2014	10/28/2014	02/25/2015	08/07/2015	11/03/2015			
	1	✓	✓	✓	✓	✓	✓			
	2	✓	✓	✓	✓	✓	✓			
	3	✓	✓	✓	✓	✓	✓			
	4	✓	✓	✓	✓	✓	✓			
	5	✓	✓	✓	✓	✓	-			
	6	✓	✓	✓	✓	✓	✓			
	7	✓	✓	✓	✓	✓	✓			
	8	✓	✓	✓	✓	✓	-			
	9		✓	✓	✓	✓	✓			
	10					✓	✓			
	11					✓	✓			
	12					✓	✓			
	13					✓	✓			
	14					✓	-			
	15					✓	✓			

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13734178	ETCHEGOYEN ET AL.
	Examiner	Art Unit
	AJIBOLA AKINYEMI	2649

CPC- SEARCHED		
Symbol	Date	Examiner
H04B1/034; H04B1/205; H04B5/0031; H04B5/02	11/3/2015	AA

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
455	41.1	11/3/2015	AA

SEARCH NOTES		
Search Notes	Date	Examiner
H04B1/034; H04B1/205; H04B5/0031; H04B5/02	11/3/2015	AA

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. no.:	13/734,178	Conf. no.	3155
Applicant:	Craig S. ETCHEGOYEN	Art Unit:	2649
Filed:	January 4, 2013	Examiner:	Ajibola A. Akinyemi

Title: NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES

RESPONSE TO FINAL OFFICE ACTION

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir,

In response to the Final Office Action ("Action") mailed November 6, 2015, Applicant respectfully requests reconsideration of all pending claims in view of the following remarks.

REMARKS

Applicant thanks Examiner Akinyemi for his thorough review of the application papers, considering the IDS references of record, and opinion on patentability. Claims 1-4, 6, 7, 9-13, and 15 are pending in the application.

Response to Rejections Under 35 U.S.C. §103

Claims 1 and 11

In the most recent Action, independent claims 1 and 11 were rejected under Pre-AIA 35 U.S.C. § 103(a) as being unpatentable over U.S. Application Pub. 2004/0038716 ("*Gass*") and further in view of U.S. Application Pub. 2011/0215158 ("*Kargl*"), U.S. Application Pub. 2008/0080750 ("*Bee*"), and U.S. Application Pub. 2012/0214416 ("*Kent*"). Applicant respectfully traverses.

A. The Sound Waves Outputted By Loudspeakers As Taught By *Gass* Are Neither Modulated Nor Serving As Carrier Waves.

Claims 1 and 11 recite a limitation of "wherein the modulated carrier wave comprises a sound wave." In the most recent Action, the Examiner cites to *Gass* at ¶¶ 0016-0018 for allegedly disclosing a modulated carrier wave comprising a sound wave. Action at 8-9. Specifically, the Examiner states that, "Gass discloses in parag. 0016, 0018 that when a call is received on a mobile terminal MT, the ringing tone is transmitted over FM radio to audio system AU and then outputted through the loudspeaker LS which is in form of sound wave." Action at 8-9.

Applicant agrees with the Examiner that *Gass* teaches the output of a sound wave through a loudspeaker but respectfully disagrees that *Gass* discloses or suggests that such a sound wave acts as a modulated carrier wave as required by Applicant's claims 1 and 11 as previously amended. In fact, *Gass* teaches just the opposite. Namely, to the extent that *Gass* teaches that any wave is modulated or acts as a carrier wave, it is a radio wave and not a sound wave. In fact, *Gass* teaches that a FM radio signal is demodulated before such signal is fed to an amplifier that outputs audio data to a loudspeaker that in turn outputs sound waves. In particular, *Gass* teaches, with reference to Figure 1, that "[b]ased on said channel information, the tuner TR is advised by advising information 8 to switch to the corresponding frequency for **demodulating** the received

FM signal 7. The **demodulated** FM signal 10 is fed to the amplifier AMP, that outputs corresponding audio data to the loudspeaker LS." *Gass* at ¶ 0016 (emphasis added.) **Therefore, by the time the sound waves are outputted through a loudspeaker as taught by *Gass,* such sound waves are neither modulated, nor serving as carrier waves as required by Applicant's claims 1 and 11.**

In addition to requiring that the modulated carrier wave comprise a sound wave, Claims 1 and 11 further recite a limitation of "transmitting the modulated carrier wave at the free frequency." Accordingly, claims 1 and 11 require the transmitting of sound waves at a free frequency. In the most recent Action, the Examiner cites to *Gass* to satisfy such limitation. Action at 3. Applicant respectfully disagrees with the Examiner's reliance on *Gass*, as *Gass* does not teach or suggest that transmission of sound waves at a free frequency as required by the claims. As discussed above, *Gass* teaches the output of sound waves from a loudspeaker. *Gass* includes no discussion regarding the frequency at which such sound waves are transmitted, and does not even suggest that such transmission of sound waves would be on a "free" frequency (which is logical given that the purpose of the loudspeaker is to merely transmit the sound to a human ear). As such, Applicant respectfully submits that the Examiner's reliance on *Gass* is misplaced in that *Gass* does not disclose at least two of the limitations recited in claims 1 and 11.

B. It is Unclear Whether The Examiner Relies Upon *Kent* In Making The Obviousness Rejection.

"To facilitate review, [an obviousness] analysis should be made explicit." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006). Here, it is not clear whether the Examiner is relying upon *Kent* in making the obviousness rejection of the pending claims. The Examiner first identifies *Kent* as a reference relied upon in rejecting claims 1, 9, 11, and 15 under 35 U.S.C. § 103 (see top of page 3 of Action). However, no other mention of *Kent* is made again in the Examiner's discussion of how the combination of the cited prior art renders the pending claims obvious. In fact, the Examiner appears to rely solely on *Gass* for its alleged teaching of "where the modulated carrier wave comprises a sounds wave" (see end of first full paragraph of page 3 of Action). In the section of the Action entitled, "Response to Arguments," the Examiner then identifies *Kent* as a "RELEVANT REFERENCE" and alleges that *Kent* teaches modulating a carrier wave to comprise a sound wave (page 9 of

Action). No assertion is made however, that *Kent* is actually relied upon in the Examiner's obviousness analysis. Applicant respectfully requests clarification regarding whether the Examiner is in fact relying on *Kent* in making the obviousness rejection of the pending claims and, as discussed further below, requests that the finality of the most recent action be withdrawn.

C. Applicant Requests Withdrawal Of Finality.

Section 706.07(a) of the MPEP specifies the conditions under which the finality of a second or subsequent office action is proper, providing that, "[s]econd or any subsequent actions on the merits shall be final, except where the examiner introduces a new ground of rejection that is neither necessitated by applicant's amendment of the claims, nor based on information submitted in an information disclosure statement filed during the period set forth in 37 C.F.R. 1.97(c) with the fee set forth in 37 CFR 1.17(p)." To the extent that the Examiner is in fact relying upon *Kent*, a newly cited reference, in making the obviousness rejection of the pending claims, Applicant respectfully submits that the finality of the subject Office Action is premature and therefore requests withdrawal of that finality, pursuant to Section 706.07(d) of the MPEP.

In particular, the sole amendment made to claims 1 and 11 in connection with Applicant's reply filed on October 28, 2015, was to incorporate the limitations of cancelled dependent claims 5 and 14 into the independent claims. The limitations of claims 5 and 14 ("wherein the modulated carrier wave comprises a sound wave") that are now recited in claims 1 and 11, respectively, were previously presented for examination. Thus, the limitations could have been rejected based on *Kent* in an earlier office action but were not. Because the limitations added to independent claims 1 and 11 were presented for examination in the preceding office action, any new ground of rejection of claims 1 and 11 based on the newly cited *Kent* reference in the Final Office Action, cannot reasonably be said to be either necessitated by claim amendment or an information disclosure statement. Accordingly, the finality of the Final Office Action should be withdrawn.

D. The Office Has Not Met Its Burden In Setting Forth A *Prima Facie* Case Of Obviousness.

To the extent that the Examiner is in fact relying upon *Kent* in making the obviousness

rejection of the pending claims, Applicant respectfully submits that the a *prima facie* case of obviousness has not been made. As noted above, the Examiner refers to *Kent* as a "Relevant Reference" and identifies a paragraph of the specification of *Kent* that allegedly teaches modulating a carrier wave to comprise sound waves. However, the Examiner has not articulated any reasoning for why a person of ordinary skill in the art would have combined *Kent* with the other cited references. *See* MPEP § 706.02(j) ("the examiner should set forth in the office action: (D) an explanation as to why the claimed invention would have been obvious to one of ordinary skill in the art at the time the invention was made"). "[A] patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art. ... it can be important to identify a reason that would have prompted a person of ordinary skill . . . to combine the elements in the way the claimed new invention does." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007). Accordingly, the Office has not met its burden of setting forth a *prima facie* case of unpatentability.

Even if the Office does not seek to rely upon *Kent*, Applicant respectfully submits, for the reasons discussed herein, a prima facie basis for obviousness has not been set forth with respect to obviousness combinations involving other prior art as the proposed combinations still fail to yield or disclose all limitations of the claimed invention, and no sufficient basis for why such combinations would have been made by a person of ordinary skill in the art has been sufficiently articulated.

E. The Combination Of *Gass* And *Kent* Would Be Improper As Such A Combination Would Alter The Principle Of Operation Of The Radio Transmission/Reception System By Which The Invention In *Gass* Was Designed To Operate.

It is not clear, as stated above, whether the Examiner relies upon *Kent* in rejecting Applicant's pending claims 1 and 11. However, to the extent that the Examiner does rely upon *Kent* in making an obviousness rejection under 35 U.S.C. § 103 in combination with *Gass*, the Applicant respectfully objects to such a ground of rejection for the reasons set forth below. More specifically, Applicant would object to such a combination as being improper as such a hypothetical combination would fundamentally alter the principle of operation of the system of

Gass, which relies upon the transmission and reception of radio waves, and relies primarily upon existing car radio receivers to operate.

"[C]ombinations that change the basic principles under which the prior art was designed to operate, or that render the prior art inoperable for its intended purpose, may fail to support a conclusion of obviousness." *Plas-Pak Industries v. Sulzer Mixpac AG*, 2015 U.S. App. LEXIS 1456, at *5 (Fed. Cir. 2015) (citations omitted). "If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious." MPEP 2143.01 VI (citing *In re Ratti*, 270 F.2d 810, 813 (C.C.P.A. 1959)). Similarly, "[i]f proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification." MPEP 2143.01 V (citing *In re Gordon*, 733 F.2d 900 (Fed. Cir. 1984)).

In this case, the basic "principle of operation" of *Gass* is explicitly set forth in the specification, which states, "[t]he basic principle of the invention is, that unused frequency channels are continuously determined, i.e. by carrying out periodically frequency scanning runs, in a hands free communication system comprising a mobile terminal and an audio system, **equipped with a radio sender and a radio receiver respectively**." *Gass* at ¶ 0007 (emphasis added). In fact, the specification of *Gass* is rife with statements defining the invention to include a mobile terminal with a radio sender and an audio system equipped with broadcast radio receiver to receive radio waves. *See Gass* at ¶ 0002. In fact, *Gass* notes that the solution that he teaches "does not require any change on existing car radios capable of receiving RDS information to serve as an audio system AU." *Gass* at ¶ 0017.

In contrast, the system taught by *Kent* requires the detection and decoding of sound waves. *Kent* at ¶ 0051. *Kent* notes that existing devices having microphones could be used to receive sound waves using the technology. *Kent* at ¶ 0041. However, the implementation of such technology needed for the transmission and reception of sound waves in the systems taught in *Gass*, would fundamentally alter the basic principles of operation of such off-the-shelf radio transmitter/receiver technology described in *Gass*. Because combining *Gass* and *Kent* would fundamentally alter *Gass*'s "principle of operation," such a combination would not support a conclusion of obviousness.

F. The Obviousness Rejection Of Claims 1 And 11, Based On A Combination Of *Gass* And *Bee,* Is Improper Because Such Combination Would Render The Invention of *Gass* Unsuitable for Its Intended Purpose.

Applicant maintains its previously submitted arguments that it is improper to combine *Gass* and *Bee*. Specifically, claim 1 recites, with the context of a method for near field authentication of a source, the limitations of "generating a periodic enclosed content message . . . wherein the content includes at least one of biometric data." Claim 11 recites, with the context of a method for near field authentication of a source, the limitations of "generating a periodic enclosed content message . . . wherein the content includes device identification data including a bit string or bit array derived from user-configurable and non-user-configurable data specific to the audio transceiver computing device." The Examiner acknowledges that *Gass* and *Kargl* fail to disclose the foregoing limitations and instead relies upon *Bee* to supply the disclosure. Applicant respectfully submits that it would be improper to combine the teachings of *Bee* with the teachings of *Gass* because it would render the invention taught in *Gass* unsuitable for its intended purpose.

If a proposal for modifying the prior art in an effort to attain the claimed invention causes the art to become inoperable or destroys its intended function, then the requisite motivation to make the modification would not have existed. *See In re Fritch*, 972 F.2d 1260, 1265 n. 12 ("A proposed modification [is] inappropriate for an obviousness inquiry when the modification render[s] the prior art reference inoperable for its intended purpose"); *see also, In re Ratti*, 270 F.2d 810, 813 (CCPA 1959) (holding the suggested combination of references improper under § 103 because it "would require a substantial reconstruction and redesign of the elements shown in [a prior art reference] as well as change in the basic principles under which [that reference's] construction was designed to operate").

In the present case, *Gass* teaches the use of a radio transmitter on a mobile terminal to broadcast information to an audio system such as a car radio receiver including a radio data system (RDS) receiver. As discussed above, the thrust of the system taught by *Gass* is to provide for the broadcast of information from a mobile terminal to a car radio receiver (with RDS receiver) that can then amplify the volume of the communications over the car's speakers, thus allowing for hands free communications while driving. (*Gass* at ¶¶ 0001-0007.)

The use of biometric data and the authentication of such data taught by *Bee*, requires the storage of biometric identification information on a database, which must further be analyzed and associated with a user in order to authenticate the identity of the source user. Likewise, the utilization of a bit string or bit array derived from user-configurable and non-user-configurable data specific to the audio transceiver computing device for authentication purposes would also require the storage of corresponding data to authenticate the source device. Even to the extent that the mobile terminal taught by *Gass* could be modified to transmit such biometric information or user-configurable and non-user-configurable data to the audio system (car radio receiver and speakers), the audio system (AU) taught by *Gass* would be rendered inoperable for its intended purpose – hands free mobile communications.

In short, the audio system taught by *Gass* does not include a database or any other suitable structure for storing biometric data or user-configurable and non-user-configurable data so that it could associate any incoming data with the user of the mobile terminal. Not only that, but the audio system taught by *Gass* has no means for analyzing any received biometric data (or user-configurable and non-user-configurable data) even if such transmissions could be received.

Claims 2-4, 6-7, 9-10, 12-13 and 15

Claims 2-4, 6-7, 9-10, 12-13 and 15 all depend, either directly or indirectly, from an otherwise patentable independent claim 1 or 11. If an independent claim is nonobvious under 35 U.S.C. § 103, then any claim depending therefrom is nonobvious. *In Re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); MPEP § 2143.03. Therefore, claims 2-4, 6-7, 9-10, 12-13 and 15 are deemed patentable over *Gass, Kargl, Bee, and Kent,* in any combination with *Martin or Kip* at least by the virtue of their dependence on claims 1 or 11. Accordingly, additional reasons for patentability of dependent claims 2-4, 6-7, 9-10, 12-13 and 15 will not be proffered. Reversal of all obviousness rejections is respectfully requested.

Applicant respectfully requests reconsideration of all obviousness rejections and allowance of all claims.

CONCLUSION

It is respectfully urged that the claims of the subject application are patentable over the references cited in the Office Action, and are now in condition for allowance. Applicant requests consideration of the application and allowance of the claims. If there are any outstanding issues that the Examiner feels may be resolved by way of a telephone conference, the Examiner is cordially invited to contact the undersigned attorney at the number below.

Respectfully Submitted,

Sean D. Burdick
Reg. No. 51,513

Uniloc USA, Inc.
7160 N. Dallas Parkway, Suite 380
Plano, TX 75024
(972) 905-9580 x 227

Electronic Acknowledgement Receipt	
EFS ID:	24386836
Application Number:	13734178
International Application Number:	
Confirmation Number:	3155
Title of Invention:	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES
First Named Inventor/Applicant Name:	Craig S. ETCHEGOYEN
Customer Number:	96051
Filer:	Sean Dylan Burdick/Tanya Kiatkulpiboone
Filer Authorized By:	Sean Dylan Burdick
Attorney Docket Number:	UN-NP-SC-085
Receipt Date:	16-DEC-2015
Filing Date:	04-JAN-2013
Time Stamp:	18:39:35
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Response After Final Action	SC-085_Response_to_20151106_FOA_FINAL.pdf	99494 43ad05d4b42860d95dab1a3f321932d883e264ee	no	9
Warnings:					
Information:					

Total Files Size (in bytes):	99494

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/734,178	01/04/2013	Craig S. ETCHEGOYEN	UN-NP-SC-085	3155

96051 7590 01/05/2016

Uniloc USA Inc.
Legacy Town Center
7160 Dallas Parkway
Suite 380
Plano, TX 75024

EXAMINER
AKINYEMI, AJIBOLA A

ART UNIT	PAPER NUMBER
2649	

NOTIFICATION DATE	DELIVERY MODE
01/05/2016	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

sean.burdick@unilocusa.com
tkiatkulpiboone@unilocusa.com
kris.pangan@unilocusa.com

Advisory Action Before the Filing of an Appeal Brief	**Application No.** 13/734,178	**Applicant(s)** ETCHEGOYEN ET AL.	
	Examiner AJIBOLA AKINYEMI	**Art Unit** 2649	**AIA (First Inventor to File) Status** No

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 16 December 2015 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

NO NOTICE OF APPEAL FILED

1. ☒ The reply was filed after a final rejection. No Notice of Appeal has been filed. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114 if this is a utility or plant application. Note that RCEs are not permitted in design applications. The reply must be filed within one of the following time periods:
   a) ☐ The period for reply expires _____months from the mailing date of the final rejection.
   b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action; or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.
   c) ☐ A prior Advisory Action was mailed more than 3 months after the mailing date of the final rejection in response to a first after-final reply filed within 2 months of the mailing date of the final rejection. The current period for reply expires months from the mailing date of *the prior Advisory Action* or SIX MONTHS from the mailing date of the final rejection, whichever is earlier.
   Examiner Note: If box 1 is checked, check either box (a), (b) or (c). ONLY CHECK BOX (b) WHEN THIS ADVISORY ACTION IS THE FIRST RESPONSE TO APPLICANT'S FIRST AFTER-FINAL REPLY WHICH WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. ONLY CHECK BOX (c) IN THE LIMITED SITUATION SET FORTH UNDER BOX (c). See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) or (c) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendments filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   b) ☐ They raise the issue of new matter (see NOTE below);
   c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.
   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): (a) ☐ will not be entered, or (b) ☒ will be entered, and an explanation of how the new or amended claims would be rejected is provided below or appended.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.
9. ☐ The affidavit or other evidence filed after final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
10. ☐ The affidavit or other evidence filed after the date of filing the Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
11. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

12. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
13. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____
14. ☐ Other: _____.

STATUS OF CLAIMS

15. The status of the claim(s) is (or will be) as follows:
    Claim(s) allowed: .
    Claim(s) objected to: .
    Claim(s) rejected: 1-4,6,7,9-13 and 15.
    Claim(s) withdrawn from consideration: .

/AJIBOLA AKINYEMI/
Primary Examiner, Art Unit 2649

Continuation of 12. does NOT place the application in condition for allowance because: Applicant argued that none of the reference discloses wherein the modulated carrier wave comprises a sound wave. Examiner respectfully disagrees with this statement and will like to explain as follows: Firstly, applicant acknowledge in his argument that the examiner's reference has FM radio signal as in page 2 of the argument. Gass has FM radio signal but FM radio signal ALWAYS contain carrier wave and sound wave. When a call is coming in to the mobile terminal, said mobile terminal sends an RDS information to the radio set to advise said radio set to receive FM-MODULATED information of a certain carrier frequency from the mobile terminal. The FM receiver of the radio set then switches to the advised frequency and the audio output of the car radio is switched to said FM-receiver for distributing the received information to the loudspeakers connected.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. no.:	13/734,178	Conf. no.	3155
Applicant:	Craig S. ETCHEGOYEN	Art Unit:	2649
Filed:	January 4, 2013	Examiner:	Ajibola A. Akinyemi

Title: NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES

RESPONSE TO FINAL OFFICE ACTION

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir,

In response to the Final Office Action ("Action") mailed November 6, 2015, Applicant respectfully requests reconsideration of all pending claims in view of the following remarks.

OK TO ENTER: /A.A./

PTO/AIA/31 (03-14)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

NOTICE OF APPEAL FROM THE EXAMINER TO THE PATENT TRIAL AND APPEAL BOARD

Docket Number (Optional): UN-NP-SC-085

I hereby certify that this correspondence is being facsimile transmitted to the USPTO, EFS-Web transmitted to the USPTO, or deposited with the United States Postal Service with sufficient postage in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, on Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on _____.

Signature _____

Typed or printed name _____

In re Application of: Craig S. ETCHEGOYEN et al.

Application Number	Filed
13/734,178	

For: NEAR FIELD AUTHENTICATION...

Art Unit	Examiner
2649	Ajibola A. Akinyemi

Applicant hereby **appeals** to the Patent Trial and Appeal Board from the last decision of the examiner.

The fee for this Notice of Appeal is (37 CFR 41.20(b)(1)) $ 800.00

☑ Applicant asserts small entity status. See 37 CFR 1.27. Therefore, the fee shown above is reduced by 50%, and the resulting fee is: $ 400.00

(previously paid on June 23, 2014)

☐ Applicant certifies micro entity status. See 37 CFR 1.29. Therefore, the fee shown above is reduced by 75%, and the resulting fee is: $ _____
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 50-6053.

☐ Payment made via EFS-Web.

☐ A petition for an extension of time under 37 CFR 1.136(a) (PTO/AIA/22 or equivalent) is enclosed.
For extensions of time in reexamination proceedings, see 37 CFR 1.550.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant

☑ attorney or agent of record Registration number 51,513

☐ attorney or agent acting under 37 CFR 1.34 Registration number _____

Signature /Sean D. Burdick/

Typed or printed name Sean D. Burdick

Telephone Number 972-905-9580 x227

Date February 8, 2016

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☑ * Total of 1 forms are submitted.

This collection of information is required by 37 CFR 41.20(b)(1) and 41.31. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. no.:	13/734,178	Conf. no.	3155
Applicant:	Uniloc Luxembourg S.A.	Art Unit:	2649
Filed:	January 4, 2013	Examiner:	Ajibola A. Akinyemi

Title: NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENLCOSED CONTENT SOUND WAVES

SECOND REINSTATEMENT OF APPEAL

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir,

Applicant hereby requests a Reinstatement of Appeal for Notices of Appeal previously filed on June 23, 2014 and May 19, 2015. Applicant also requests the $400 Notice of Appeal fee previously paid on June 23, 2014 to be applied to this reinstatement. No additional fee is due.

Respectfully Submitted,

Sean D. Burdick
Reg. No. 51,513

Uniloc USA, Inc.
7160 N. Dallas Parkway, Suite 380
Plano, Texas 75024
(972) 905-9580 x227

Electronic Acknowledgement Receipt	
EFS ID:	24850009
Application Number:	13734178
International Application Number:	
Confirmation Number:	3155
Title of Invention:	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES
First Named Inventor/Applicant Name:	Craig S. ETCHEGOYEN
Customer Number:	96051
Filer:	Sean Dylan Burdick/Kris Pangan
Filer Authorized By:	Sean Dylan Burdick
Attorney Docket Number:	UN-NP-SC-085
Receipt Date:	08-FEB-2016
Filing Date:	04-JAN-2013
Time Stamp:	13:40:49
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Notice of Appeal Filed	SC-085_Notice_of_Appeal.pdf	141092 b3a30c6acef7aa2d4573599127f0d2c896a47a86	no	1

Warnings:
Information:

2	Notice of Appeal Filed	SC-085_Reinstatement_of_Appeal.pdf	58359 e91b1f15c91c7415d3aad38fc0cc8cc9f7115bb4	no	1
Warnings:					
Information:					
			Total Files Size (in bytes):	199451	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Before the Patent Trial and Appeal Board

In re Application of: Etchegoyen, Craig S. Serial No.: 13/734,178 Filed: January 4, 2013 For: NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES	Patent Examiner: Ajibola A. Akinyemi Group Art Unit: 2649 Confirmation No.: 3155 *April 8, 2016*

Applicant respectfully requests that the Patent Trial and Appeal Board ("the Board") review the final rejection in the above-captioned application. The review is requested in view of clear errors identified below in the Final Office Action mailed November 6, 2015 ("Final Action"). These errors are summarized on the following pages.

Applicant filed a Notice of Appeal (Form PTO/SB/31) on February 8, 2016.

Table of Contents

I. REAL PARTY IN INTEREST

The real parties in interest are the assignee Uniloc Luxembourg S. A., and its exclusive licensee Uniloc USA, Inc.

II. RELATED APPEALS, INTERFERENCES, AND TRIALS

The instant application was previously the subject of an appeal before the Board, Applicant having filed an appeal brief on August 25, 2014. In response to Applicant's aforesaid appeal brief, the Office reopened prosecution as set forth in an action mailed on November 3, 2014. No related application has been appealed to the Board or other tribunal.

III. SUMMARY OF CLAIMED SUBJECT MATTER

The present invention provides a method for near field authentication of a computing device, such as a cell phone, using sound waves. The invention may be used with any computing device that has audio transceiving capability, e.g. a speaker and a microphone. Specification ("Spec.") at paragraph ("¶") 0007.[1] An inventive feature that is the focus of this appeal is a claim limitation wherein the computing device transmits an acoustic carrier wave modulated by a periodic enclosed content message, wherein the enclosed content includes a

[1] References are made to the Specification as filed.

digital representation of biometric data of a user of the computing device, or device identification data for the computing the device itself, or both. Spec. at ¶ 0008; 0032. A receiving device, e.g., a server authenticating a secure transaction, is configured to scan for and receive the periodic enclosed content message, demodulate it, and recover digital data representing the biometric or device identification data. Spec. at ¶ 0011; 0033; 0043; 0054.

Claim 1 recites a method for near field authentication of a source, the source using an audio transceiver computing device, the method comprising (Spec. at ¶ 0007): scanning a plurality of predetermined frequencies for a free frequency (Spec. at ¶ 0007); selecting the free frequency from the plurality of predetermined frequencies (Spec. at ¶ 0007); generating a periodic enclosed content message (Spec. at ¶ 0007); generating a modulated carrier wave representing the periodic enclosed content message (Spec. at ¶ 0007); and transmitting the modulated carrier wave at the free frequency (Spec. at ¶ 0007); wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication (Spec. at ¶ 0008); and wherein the content includes at least one of biometric data, or device identification data (Spec. at ¶ 0008).

IV. ARGUMENT

In the most recent Action, independent claims 1 and 11 were rejected under Pre-AIA 35 U.S.C. § 103(a) as being unpatentable over U.S. Application Pub. 2004/0038716 ("*Gass*") and further in view of U.S. Application Pub. 2011/0215158 ("*Kargl*"), and U.S. Application Pub. 2008/0080750 ("*Bee*"). As noted by Applicant in its Response to Final Action filed on December 16, 2015, and discussed further herein, it is unclear whether the Office relies upon U.S. Application Pub. 2012/0214416 ("*Kent*") in rejecting claims 1 and 11. Applicant respectfully traverses.

A. The Sound Waves Outputted By Loudspeakers As Taught By *Gass* Are Neither Modulated Nor Serving As Carrier Waves.

Claims 1 and 11 recite a limitation of "wherein the modulated carrier wave comprises a sound wave." The primary point of disagreement between Applicant and the Examiner is whether radio waves are the same as, or "contain," sound waves. The Examiner, in the Advisory Action mailed on January 5, 2016, states that "Gass has FM radio signal but FM radio signal ALWAYS contain carrier wave and sound wave." Examiner's foregoing statement is simply not an accurate description of the properties of radio waves, which those of ordinary skill in the art will recognize are

electromagnetic in nature, which are materially different from sound waves (which are mechanical waves and not electromagnetic waves), and do not "contain" sound waves. Applicant suspects that the Examiner is inadvertently associating "sound waves" with radio waves encoded with audio data, which those of ordinary skill in the art will recognize as being materially different than sound waves.

In the Final Action dated November 6, 2015, the Examiner cites to *Gass* at ¶¶ 0016-0018 for allegedly disclosing a modulated carrier wave comprising a sound wave. Action at 8-9. Specifically, the Examiner states that, "Gass discloses in parag. 0016, 0018 that when a call is received on a mobile terminal MT, the ringing tone is transmitted over FM radio to audio system AU and then outputted through the loudspeaker LS which is in form of sound wave." Action at 8-9.

Applicant agrees with the Examiner that *Gass* teaches the output of a sound wave through a loudspeaker but respectfully disagrees that *Gass* discloses or suggests that such a sound wave acts as a modulated carrier wave as required by Applicant's claims 1 and 11 as previously amended. In fact, *Gass* teaches just the opposite. Namely, to the extent that *Gass* teaches that any wave is modulated or acts as a carrier wave, it is a radio wave and not a

sound wave. In fact, *Gass* teaches that a FM radio signal is demodulated before such signal is fed to an amplifier that outputs audio data to a loudspeaker that in turn outputs sound waves. In particular, *Gass* teaches, with reference to Figure 1, that "[b]ased on said channel information, the tuner TR is advised by advising information 8 to switch to the corresponding frequency for **demodulating** the received FM signal 7. The **demodulated** FM signal 10 is fed to the amplifier AMP, that outputs corresponding audio data to the loudspeaker LS." *Gass* at ¶ 0016 (emphasis added.) **Therefore, by the time the sound waves are outputted through a loudspeaker as taught by *Gass*, such sound waves are neither modulated, nor serving as carrier waves as required by Applicant's claims 1 and 11.**

Applicant respectfully disagrees with the Examiner's assertion in the Advisory Action dated January 6, 2016, stating that, "Gass has FM radio signal but FM radio signal ALWAYS contain carrier wave and sound wave." Those of ordinary skill in the art will recognize that radio waves are neither equivalent to, nor do they contain, sound waves. Radio waves and sound waves are materially different from one another. Specifically, radio waves are electromagnetic waves composed of electric and magnetic fields oscillating at right angles to each other, and do not require a medium through which to

propagate (they can travel through a vacuum such as space). In contrast, sound waves are longitudinal mechanical waves and require a medium through which to propagate (for example, air). Moreover, Applicant describes in its specification how radio waves differ from sound waves with respect to their usage in near field communication. In particular, Applicant notes that there are certain drawbacks (range limitations) associated with using radio waves in conventional near field communications. (Spec. at ¶ 0004.) In contrast, Applicant describes how sound waves are capable of accurately transmitting information over a very short distance (near field communications) using inexpensive equipment. (Spec. at ¶ 0026.) Therefore, in view of the foregoing, it is clear that *Gass's* teaching of a modulated radio wave does not anticipate the limitation of, "wherein the modulated carrier wave comprises a sound wave," as recited in claims 1 and 11.

In addition to requiring that the modulated carrier wave comprise a sound wave, Claims 1 and 11 further recite a limitation of "transmitting the modulated carrier wave at the free frequency." Accordingly, claims 1 and 11 require the transmitting of sound waves at a free frequency. In the most recent Action, the Examiner cites to *Gass* to satisfy such limitation. Action at 3. Applicant respectfully disagrees with the Examiner's reliance on *Gass*, as *Gass*

does not teach or suggest that transmission of sound waves at a free frequency as required by the claims. As discussed above, *Gass* teaches the output of sound waves from a loudspeaker. *Gass* includes no discussion regarding the frequency at which such sound waves are transmitted, and does not even suggest that such transmission of sound waves would be on a "free" frequency (which is logical given that the purpose of the loudspeaker is to merely transmit the sound to a human ear). As such, Applicant respectfully submits that the Examiner's reliance on *Gass* is misplaced in that *Gass* does not disclose at least two of the limitations recited in claims 1 and 11.

B. It Is Unclear Whether The Examiner Relies Upon *Kent* In Making The Obviousness Rejection.

"To facilitate review, [an obviousness] analysis should be made explicit." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006). In the Final Action, it is not clear whether the Examiner is relying upon *Kent* in making the obviousness rejection of the pending claims. The Examiner first identifies *Kent* as a reference relied upon in rejecting claims 1, 9, 11, and 15 under 35 U.S.C. § 103 (see top of page 3 of Action). However, no other mention of *Kent* is made again in the Examiner's discussion of how the combination of the cited prior art renders the pending claims obvious. In

fact, the Examiner appears to rely solely on *Gass* for its alleged teaching of "where the modulated carrier wave comprises a sounds wave" (see end of first full paragraph of page 3 of Action). In the section of the Action entitled, "Response to Arguments," the Examiner then identifies *Kent* as a "RELEVANT REFERENCE" and alleges that *Kent* teaches modulating a carrier wave to comprise a sound wave (page 9 of Action). No assertion is made however, that *Kent* is actually relied upon in the Examiner's obviousness analysis.

C. The Office Has Not Met Its Burden In Setting Forth A *Prima Facie* Case Of Obviousness.

To the extent that the Board determines that the Examiner is in fact relying upon *Kent* in making the obviousness rejection of the pending claims, Applicant respectfully submits that the a *prima facie* case of obviousness has not been made. As noted above, the Examiner refers to *Kent* as a "Relevant Reference" and identifies a paragraph of the specification of *Kent* that allegedly teaches modulating a carrier wave to comprise sound waves. However, the Examiner has not articulated any reasoning for why a person of ordinary skill in the art would have combined *Kent* with the other cited references. *See* MPEP § 706.02(j) ("the examiner should set forth in the office action: (D) an explanation as to why the claimed invention would

have been obvious to one of ordinary skill in the art at the time the invention was made"). "[A] patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art. … it can be important to identify a reason that would have prompted a person of ordinary skill . . . to combine the elements in the way the claimed new invention does." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007). Accordingly, the Office has not met its burden of setting forth a *prima facie* case of unpatentability.

Even if the Office does not seek to rely upon *Kent*, Applicant respectfully submits, for the reasons discussed herein, a prima facie basis for obviousness has not been set forth with respect to obviousness combinations involving other prior art as the proposed combinations still fail to yield or disclose all limitations of the claimed invention, and no sufficient basis for why such combinations would have been made by a person of ordinary skill in the art has been sufficiently articulated.

D. The Combination Of *Gass* And *Kent* Would Be Improper As Such A Combination Would Alter The Principle Of Operation Of The Radio Transmission/Reception System By Which The Invention In *Gass* Was Designed To Operate.

It is not clear, as stated above, whether the Examiner relies upon *Kent* in rejecting Applicant's pending claims 1 and 11. However, to the extent that the Board determines that the Examiner does rely upon *Kent* in making an obviousness rejection under 35 U.S.C. § 103 in combination with *Gass*, the Applicant respectfully objects to such a ground of rejection for the reasons set forth below. More specifically, Applicant would object to such a combination as being improper as such a hypothetical combination would fundamentally alter the principle of operation of the system of *Gass*, which relies upon the transmission and reception of radio waves, and relies primarily upon existing car radio receivers to operate.

"[C]ombinations that change the basic principles under which the prior art was designed to operate, or that render the prior art inoperable for its intended purpose, may fail to support a conclusion of obviousness." *Plas-Pak Industries v. Sulzer Mixpac AG*, 2015 U.S. App. LEXIS 1456, at *5 (Fed. Cir. 2015) (citations omitted). "If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render

the claims prima facie obvious." MPEP 2143.01 VI (citing *In re Ratti*, 270 F.2d 810, 813 (C.C.P.A. 1959)). Similarly, "[i]f proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification." MPEP 2143.01 V (citing *In re Gordon*, 733 F.2d 900 (Fed. Cir. 1984)).

In this case, the basic "principle of operation" of *Gass* is explicitly set forth in the specification, which states, "[t]he basic principle of the invention is, that unused frequency channels are continuously determined, i.e. by carrying out periodically frequency scanning runs, in a hands free communication system comprising a mobile terminal and an audio system, **equipped with a radio sender and a radio receiver respectively**." *Gass* at ¶ 0007 (emphasis added). In fact, the specification of *Gass* is rife with statements defining the invention to include a mobile terminal with a radio sender and an audio system equipped with broadcast radio receiver to receive radio waves. *See Gass* at ¶ 0002. In fact, *Gass* notes that the solution that he teaches "does not require any change on existing car radios capable of receiving RDS information to serve as an audio system AU." *Gass* at ¶ 0017.

In contrast, the system taught by *Kent* requires the detection and

decoding of sound waves. *Kent* at ¶ 0051. *Kent* notes that existing devices having microphones could be used to receive sound waves using the technology. *Kent* at ¶ 0041. However, the implementation of such technology needed for the transmission and reception of sound waves in the systems taught in *Gass*, would fundamentally alter the basic principles of operation of such off-the-shelf radio transmitter/receiver technology described in *Gass*. Because combining *Gass* and *Kent* would fundamentally alter *Gass*'s "principle of operation," such a combination would not support a conclusion of obviousness.

E. The Obviousness Rejection Of Claims 1 And 11, Based On A Combination Of *Gass* And *Bee*, Is Improper Because Such Combination Would Render The Invention of *Gass* Unsuitable for Its Intended Purpose.

Applicant respectfully submits that it would be improper to combine the teachings of *Bee* with the teachings of *Gass* because it would render the invention taught in *Gass* unsuitable for its intended purpose. *Gass* teaches the use of a radio transmitter on a mobile terminal to broadcast information to an audio system such as a car radio receiver including a radio data system (RDS) receiver. As discussed above, the thrust of the system taught by *Gass* is to provide for the broadcast of information from a mobile terminal to a car radio receiver (with RDS receiver) that can then amplify the volume of the

communications over the car's speakers, thus allowing for hands free communications while driving. (*Gass* at ¶¶ 0001-0007.)

The use of biometric data and the authentication of such data taught by *Bee*, requires the storage of biometric identification information on a database, which must further be analyzed and associated with a user in order to authenticate the identity of the source user. Likewise, the utilization of a bit string or bit array derived from user-configurable and non-user-configurable data specific to the audio transceiver computing device for authentication purposes would also require the storage of corresponding data to authenticate the source device. Even to the extent that the mobile terminal taught by *Gass* could be modified to transmit such biometric information or user-configurable and non-user-configurable data to the audio system (car radio receiver and speakers), the audio system (AU) taught by *Gass* would be rendered inoperable for its intended purpose – hands free mobile communications.

In short, the audio system taught by *Gass* does not include a database or any other suitable structure for storing biometric data or user-configurable and non-user-configurable data so that it could associate any incoming data with the user of the mobile terminal. Not only that, but the audio system taught by *Gass* has no means for analyzing any received biometric data (or user-

configurable and non-user-configurable data) even if such transmissions could be received.

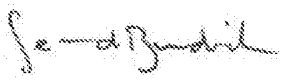
F. The Obviousness Rejection Of The Dependent Claims Should Be Reversed Based On Dependency From Claims 1 or 11.

Claims 2-4, 6-7, 9-10, 12-13 and 15 all depend, either directly or indirectly, from an otherwise patentable independent claim 1 or 11. If an independent claim is nonobvious under 35 U.S.C. § 103, then any claim depending therefrom is nonobvious. *In Re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); MPEP § 2143.03. Therefore, claims 2-4, 6-7, 9-10, 12-13 and 15 are deemed patentable over *Gass, Kargl, Bee, and Kent,* in any combination with *Martin or Kip* at least by the virtue of their dependence on claims 1 or 11. Accordingly, additional reasons for patentability of dependent claims 2-4, 6-7, 9-10, 12-13 and 15 will not be proffered.

Conclusion

Applicant respectfully submits that the rejections in this application are improper and should be overturned.

Very truly yours,



Sean Burdick
Registration No. 51,513
Attorney for Applicant

IV. CLAIMS APPENDIX

1. A method for near field authentication of a source, the source using an audio transceiver computing device, the method comprising:

scanning a plurality of predetermined frequencies for a free frequency;

selecting the free frequency from the plurality of predetermined frequencies;

generating a periodic enclosed content message;

generating a modulated carrier wave representing the periodic enclosed content message; and

transmitting the modulated carrier wave at the free frequency;

wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication; and

wherein the content includes at least one of biometric data; and

wherein the modulated carrier wave comprises a sound wave.

2. The method of claim 1 further comprising:

displaying a user interface on the audio transceiver computing device requesting the biometric data from a user; and

responsive to receiving the biometric data, generating the periodic

enclosed content message, wherein the content in each period of the periodic enclosed content message includes the biometric data.

3. The method of claim 1, wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

4. The method of claim 1, wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.

5. (canceled)

6. The method of claim 2, wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

7. The method of claim 2, wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.

8. (canceled)

9. The method of claim 1 wherein the carrier wave is modulated by the periodic enclosed content message.

10. The method of claim 1, wherein the non-user-configurable data comprises hardware component numbers, serial numbers, and version numbers.

11. A method for near field authentication of a source, the source using an audio transceiver computing device, the method comprising:

scanning a plurality of predetermined frequencies for a free frequency;

selecting the free frequency from the plurality of predetermined frequencies;

generating a periodic enclosed content message;

generating a modulated carrier wave representing the periodic enclosed content message; and

transmitting the modulated carrier wave at the free frequency;

wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication;

wherein the content includes device identification data including a bit string or bit array derived from user-configurable and non-user-configurable data specific to the audio transceiver computing device; and

wherein the modulated carrier wave comprises a sound wave.

12. The method of claim 11, wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

13. The method of claim 11, wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.

14. (canceled)

15. The method of claim 11 wherein the carrier wave is modulated by the periodic enclosed content message.

Electronic Acknowledgement Receipt	
EFS ID:	25443930
Application Number:	13734178
International Application Number:	
Confirmation Number:	3155
Title of Invention:	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES
First Named Inventor/Applicant Name:	Craig S. ETCHEGOYEN
Customer Number:	96051
Filer:	Sean Dylan Burdick/Tanya Kiatkulpiboone
Filer Authorized By:	Sean Dylan Burdick
Attorney Docket Number:	UN-NP-SC-085
Receipt Date:	08-APR-2016
Filing Date:	04-JAN-2013
Time Stamp:	17:48:01
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Appeal Brief Filed	SC-085_Appeal_Brief_FINAL.pdf	111858 dcc67ea3277b840e0bfbd29b8cb14bf6faded6d0	no	22
Warnings:					
Information:					

Total Files Size (in bytes):	111858

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/734,178	01/04/2013	Craig S. ETCHEGOYEN	UN-NP-SC-085	3155

96051 7590 07/26/2016

Uniloc USA Inc.
Legacy Town Center
7160 Dallas Parkway
Suite 380
Plano, TX 75024

EXAMINER	
ART UNIT	PAPER NUMBER

DATE MAILED: 07/26/2016

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

Notification of Non-Compliant Appeal Brief (37 CFR 41.37)	Application No.	Applicant(s)	
	13/734,178	Etchegoyen. Craig S.	
	Examiner	Art Unit	
	Akinyemi, Ajibola A.	2649	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

The Appeal Brief filed on *April 8, 2016* is defective for failure to comply with one or more provisions of 37 CFR 41.37(c).

To avoid dismissal of the appeal, applicant must file an amended brief or other appropriate correction (see MPEP 1205.03) within **ONE MONTH or THIRTY DAYS** from the mailing date of this Notification, whichever is longer. **EXTENSIONS OF THIS TIME PERIOD MAY BE GRANTED UNDER 37 CFR 1.136.**

1. ☐ The brief does not contain the items required under 37 CFR 41.37(c), or the items are not under the proper heading or in the proper order.

2. ☐ (a) The brief does not contain a concise explanation of the subject matter defined in each of the rejected independent claims, referring to the specification in the Record by page and line number or by paragraph number and to the drawings, if any, by reference characters; and/or (b) the brief fails to identify, for each rejected independent claim and for each dependent claim argued separately that contains a means plus function or step plus function recitation under 35 U.S.C. 112, sixth paragraph, the structure, material, or acts described in the specification as corresponding to each claimed function with reference to the specification in the Record by page and line number or paragraph number, and to the drawings, if any, by reference characters (37 CFR 41.37(c)(1)(iii)).

3. ☒ The brief does not contain a correct copy of the appealed claims as an appendix thereto (37 CFR 41.37(c)(1)(v)).

4. ☒ Other (including any explanation in support of the above items):

The Claims Appendix is non-compliant as it does not match the last entered amendment, specifically at least claim 1. The last entered amendment was filed on 10/28/15. An entirely new Appeal Brief is not necessary, only the corrected section.

Sonja Despertt, Supervisory Paralegal Specialist
(571) 272-9797

IV. CLAIMS APPENDIX

1. A method for near field authentication of a source, the source using an audio transceiver computing device, the method comprising:

scanning a plurality of predetermined frequencies for a free frequency;

selecting the free frequency from the plurality of predetermined frequencies;

generating a periodic enclosed content message;

generating a modulated carrier wave representing the periodic enclosed content message; and

transmitting the modulated carrier wave at the free frequency;

wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication;

wherein the content includes biometric data; and

wherein the modulated carrier wave comprises a sound wave.

2. The method of claim 1 further comprising:

displaying a user interface on the audio transceiver computing device requesting the biometric data from a user; and

responsive to receiving the biometric data, generating the periodic enclosed content message, wherein the content in each period of the periodic enclosed content message includes the biometric data.

3. The method of claim 1, wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

4. The method of claim 1, wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.

5. (canceled)

6. The method of claim 2, wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

7. The method of claim 2, wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.

8. (canceled).

9. The method of claim 1 wherein the carrier wave is modulated by the periodic enclosed content message.

10. The method of claim 11, wherein the non-user-configurable data comprises hardware component numbers, serial numbers, and version numbers.

11. A method for near field authentication of a source, the source using an audio transceiver computing device, the method comprising:

scanning a plurality of predetermined frequencies for a free frequency;

selecting the free frequency from the plurality of predetermined frequencies;

generating a periodic enclosed content message;

generating a modulated carrier wave representing the periodic enclosed content message; and

transmitting the modulated carrier wave at the free frequency;

wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication;

wherein the content includes device identification data including a bit string or bit array derived from user-configurable and non-user-configurable data specific to the audio transceiver computing device; and

wherein the modulated carrier wave comprises a sound wave.

12. The method of claim 11, wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

13. The method of claim 11, wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.

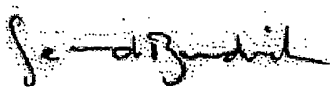
14. (canceled).

15. The method of claim 11 wherein the carrier wave is modulated by the periodic enclosed content message.

The foregoing amended Claims Appendix reflects the last entered amendment filed on October 28, 2015. Applicant respectfully requests entry of this amended section in the Appeal Brief.

A one-month extension of time is believed to be due. The Commissioner is authorized to charge this fee or credit any overpayment to our Deposit Account No. 50-6053.

Respectfully Submitted,



Sean D. Burdick
Reg. No. 51,513

Uniloc USA, Inc.
7160 N. Dallas Parkway, Suite 380
Plano, Texas 75024
(972) 905-9580 x227

RECEIVED
CENTRAL FAX CENTER

AUG 3 0 2016

FAX

Date:	08/30/2016
Pages including cover sheet:	7

To:	5712738300@rcfax.com
Phone	
Fax Number	*+15712738300*

From:	Sarah Gallegos
	Uniloc USA
	7160 N. Dallas Parkway, Ste
	Plano
	TX 75024
Phone	*19729059579*
Fax Number	*(972) 905-4254*

NOTE:

US Patent Application No. 13/734,178 (Our ref.: UN-NP-SC-085)

Unlloc USA, Inc.
7160 N. Dallas Pkwy, Suite 380
Plano, TX 75024
972.905.9580

FAX COVER SHEET

TO: Commissioner of Patents
U.S. Patent & Trademark Office

571.273.8300

FROM: Kris Pangan

DATE: August 30, 2016

PAGES: 6 (including cover)

RE: U.S. Patent Application No. 13/734,178
Title: NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES
Inventor: Craig S. ETCHEGOYEN et al.
Our Ref.: UN-NP-SC-085

RECEIVED
CENTRAL FAX CENTER

AUG 3 0 2016

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. no.:	13/734,178	Conf. no.	3155
Applicant:	Craig S. ETCHEGOYEN	Art Unit:	2649
Filed:	January 4, 2013	Examiner:	Ajibola A. Akinyemi

Title: NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES

RESPONSE TO NON-COMPLIANT APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir,

In response to the Notice of Non-Compliant Amendment dated July 29, 2016, please amend the Appeal Brief filed April 8, 2014 ("Appeal Brief") by replacing the Claims Appendix in its entirety with the following amended Claims Appendix:

Certificate of Facsimile Transmission

I hereby certify that this correspondence is being facsimile-transmitted to the U.S. Patent and Trademark Office (Fax No. 571-273-8300) on August 30, 2016.

Kristina Pangan

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

96051 7590 12/16/2016

Uniloc USA Inc.
Legacy Town Center
7160 Dallas Parkway
Suite 380
Plano, TX 75024

EXAMINER
AKINYEMI, AJIBOLA A

ART UNIT	PAPER NUMBER
2649	

DATE MAILED: 12/16/2016

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/734,178	01/04/2013	Craig S. ETCHEGOYEN	UN-NP-SC-085	3155

TITLE OF INVENTION: NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	03/16/2017

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

96051 7590 12/16/2016

Uniloc USA Inc.
Legacy Town Center
7160 Dallas Parkway
Suite 380
Plano, TX 75024

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/734,178	01/04/2013	Craig S. ETCHEGOYEN	UN-NP-SC-085	3155

TITLE OF INVENTION: NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	03/16/2017

EXAMINER	ART UNIT	CLASS-SUBCLASS
AKINYEMI, AJIBOLA A	2649	455-041100

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:

❑ Issue Fee

❑ Publication Fee (No small entity discount permitted)

❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): (**Please first reapply any previously paid issue fee shown above**)

❑ A check is enclosed.

❑ Payment by credit card. Form PTO-2038 is attached.

❑ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

❑ Applicant asserting small entity status. See 37 CFR 1.27

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

❑ Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/734,178	01/04/2013	Craig S. ETCHEGOYEN	UN-NP-SC-085	3155

96051 7590 12/16/2016

Uniloc USA Inc.
Legacy Town Center
7160 Dallas Parkway
Suite 380
Plano, TX 75024

EXAMINER	
AKINYEMI, AJIBOLA A	
ART UNIT	PAPER NUMBER
2649	

DATE MAILED: 12/16/2016

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Examiner-Initiated Interview Summary	Application No.	Applicant(s)	
	13/734,178	ETCHEGOYEN ET AL.	
	Examiner	Art Unit	
	AJIBOLA AKINYEMI	2649	

All participants (applicant, applicant's representative, PTO personnel):

(1) *AJIBOLA AKINYEMI*. (3)_____.

(2) *SEAN D. BURDICK*. (4)_____.

Date of Interview: *07 December 2016*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☐103 ☒Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1 and 11*.

Identification of prior art discussed: *N/A*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Office called attorney of record Mr. Sean Burdick and asked him to amend claim 1 and 11. An agreement was reached at this time.

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/AJIBOLA AKINYEMI/ Primary Examiner, Art Unit 2649	

Notice of Allowability	Application No. 13/734,178	Applicant(s) ETCHEGOYEN ET AL.	
	Examiner AJIBOLA AKINYEMI	Art Unit 2649	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *12/07/2016*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1-4,6,7,9-13 and 15*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☒ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☒ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/AJIBOLA AKINYEMI/
Primary Examiner, Art Unit 2649

1. The present application is being examined under the pre-AIA first to invent provisions.

EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in an interview with Mr. Sean D. Burdick on December 07, 2016.

Please amend claim as below:

1. (currently amended) A method for near field authentication of a source, the source using an audio transceiver computing device, the method comprising:

scanning a plurality of predetermined frequencies for a free frequency;

selecting the free frequency from the plurality of predetermined frequencies;

generating a periodic enclosed content message;

generating a modulated carrier wave representing the periodic enclosed content message; and

transmitting the modulated carrier wave at the free frequency;

wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication;

wherein the content includes biometric data and a bit array, the bit array being derived from user-configurable and non-user-configurable data specific to the audio transceiver computing device; and

wherein the modulated carrier wave comprises a sound wave.

10. (currently amended) The method of claim ~~11~~ 1, wherein the non-user-configurable data comprises hardware component numbers, serial numbers, and version numbers.

11. (currently amended) A method for near field authentication of a source, the source using an audio transceiver computing device, the method comprising:

scanning a plurality of predetermined frequencies for a free frequency;

selecting the free frequency from the plurality of predetermined frequencies;

generating a periodic enclosed content message;

generating a modulated carrier wave representing the periodic enclosed content message; and

transmitting the modulated carrier wave at the free frequency;

wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication;

wherein the content includes device identification data including a ~~bit string or~~ bit array derived from user-configurable and non-user-configurable data specific to the audio transceiver computing device; and wherein the modulated carrier wave comprises a sound wave.

REASON FOR ALLOWANCE

This communication warrants no examiner's reason for allowance, as applicant's reply makes evident the reason for allowance, satisfying the record as whole as required by rule 37 CFR 1.104(e). In this case, the substance of applicant's remarks filed on 04/08/2016 and additional limitation on 12/07/2016 with respect to the added claim limitations point out the reason claims are patentable over the prior art of record. Thus, the reason for allowance is in all probability evident from the record and no statement for examiner's reason for allowance is necessary (see MPEP 1302.14).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to AJIBOLA AKINYEMI whose telephone number is (571)270-1846. The examiner can normally be reached on monday- friday (8.30-5pm) Est.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, YUWEN PAN can be reached on (571) 272-7855. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/AJIBOLA AKINYEMI/
Primary Examiner, Art Unit 2649

Examiner-Initiated Interview Summary	Application No.	Applicant(s)	
	13/734,178	ETCHEGOYEN ET AL.	
	Examiner	Art Unit	
	AJIBOLA AKINYEMI	2649	

All participants (applicant, applicant's representative, PTO personnel):

(1) *AJIBOLA AKINYEMI*. (3)_____.

(2) *SEAN D. BURDICK*. (4)_____.

Date of Interview: *07 December 2016*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☐103 ☒Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1 and 11*.

Identification of prior art discussed: *N/A*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Office called attorney of record Mr. Sean Burdick and asked him to amend claim 1 and 11. An agreement was reached at this time.

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/AJIBOLA AKINYEMI/ Primary Examiner, Art Unit 2649	

Notice of References Cited	Application/Control No. 13/734,178	Applicant(s)/Patent Under Reexamination ETCHEGOYEN ET AL.	
	Examiner AJIBOLA AKINYEMI	Art Unit 2649	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-5,019,813 A	05-1991	Kip; Harm J.	A01K11/006	340/10.51
*	B	US-2004/0038716 A1	02-2004	Gass, Vincent	H04M1/6091	455/569.1
*	C	US-2007/0198850 A1	08-2007	Martin; Christopher D.	G07C9/00087	713/186
*	D	US-2008/0080750 A1	04-2008	Bee; Chap-Meng	G06K9/00006	382/124
*	E	US-2010/0208899 A1	08-2010	Kasargod; Sudhir K.	H04S1/002	381/1
*	F	US-2011/0215158 A1	09-2011	Kargl; Walter	H04L27/04	235/492
*	G	US-2012/0216262 A1	08-2012	Bardsley; Jeffrey Scott	H04L63/0861	726/5
*	H	US-2012/0214416 A1	08-2012	Kent; Jonathan Douglas	H04L63/18	455/41.2
*	I	US-2013/0159701 A1	06-2013	PHILLIPS, II; Eugene B.	H04L63/045	713/155
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13734178	ETCHEGOYEN ET AL.
	Examiner	Art Unit
	AJIBOLA AKINYEMI	2649

CPC- SEARCHED		
Symbol	Date	Examiner
H04B1/034; H04B1/205; H04B5/0031; H04B5/02	12/7/2016	AA

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
455	41.1	12/7/2016	AA

SEARCH NOTES		
Search Notes	Date	Examiner
H04B1/034; H04B1/205; H04B5/0031; H04B5/02	12/7/2016	AA

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
See PgPub. Text Search		12/7/2016	AA

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13734178	ETCHEGOYEN ET AL.
	Examiner	**Art Unit**
	AJIBOLA AKINYEMI	2649

CPC							
Symbol						**Type**	**Version**
H04B		5	/	02		F	2013-01-01
H04B		5	/	0031		I	2013-01-01
			/				
			/				
			/				
			/				
			/				
			/				
			/				
			/				
			/				
			/				
			/				
			/				

CPC Combination Sets							
Symbol					**Type**	**Set**	**Ranking**	**Version**
			/					
			/					

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 12	
/AJIBOLA AKINYEMI/ Primary Examiner.Art Unit 2649 (Primary Examiner)	12/07/2016 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure Fig. 3

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13734178	ETCHEGOYEN ET AL.
	Examiner	Art Unit
	AJIBOLA AKINYEMI	2649

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION									
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED				
455	41.2	H	0	4	B	7 / 00 (2006.01.01)					
CROSS REFERENCE(S)											
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)										
455	569.1										

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	12	
/AJIBOLA AKINYEMI/ Primary Examiner.Art Unit 2649	12/07/2016	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	Fig. 3

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13734178	ETCHEGOYEN ET AL.
	Examiner	**Art Unit**
	AJIBOLA AKINYEMI	2649

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1														
2	2														
5	3														
6	4														
-	5														
3	6														
4	7														
-	8														
7	9														
8	10														
9	11														
10	12														
11	13														
-	14														
12	15														

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 12	
/AJIBOLA AKINYEMI/ Primary Examiner.Art Unit 2649 (Primary Examiner)	12/07/2016 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure Fig. 3

U.S. Patent and Trademark Office Part of Paper No. 20161207

Akinyemi, Ajibola A.

From: Sean Burdick <sean.burdick@unilocusa.com>
Sent: Thursday, December 08, 2016 2:12 PM
To: Akinyemi, Ajibola A.
Subject: proposed Examiner's Amendment for 13/734,178
Attachments: proposed Examiner's amendment 13734178.docx

Dear Mr. Akinyemi,

Here is the proposed Examiner's Amendment based on our phone call yesterday.

Best Regards,

Sean D. Burdick, P.E. | Unilloc USA, Inc.
President & General Counsel
Legacy Town Center I | 7160 N. Dallas Parkway Suite 380 | Plano, Texas 75024
sean.burdick@unilocusa.com | 972 905 9580 x227

Preserving Intellectual Property Rights

EAST Search History

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1	(scan$4 and frequencies and free and select$3 and predetermined and generat$3 and periodic and content adj message and indication).clm.	US-PGPUB	OR	OFF	2016/12/09 10:31

12/9/2016 10:32:19 AM
C:\Users\aakinyemi\Documents\EAST\Workspaces\15044606.wsp

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. no.:	13/734,178	Conf. no.	3155
Applicant:	Craig S. ETCHEGOYEN	Art Unit:	2649
Filed:	January 4, 2013	Examiner:	Ajibola A. Akinyemi

Title: NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES

PROPOSED EXAMINER'S AMENDMENT

Dear Mr. Akinyemi,

Please consider the following claim amendments for entry as an Examiner's Amendment.

IN THE CLAIMS:

1. (currently amended) A method for near field authentication of a source, the source using an audio transceiver computing device, the method comprising:

scanning a plurality of predetermined frequencies for a free frequency;

selecting the free frequency from the plurality of predetermined frequencies;

generating a periodic enclosed content message;

generating a modulated carrier wave representing the periodic enclosed content message; and

transmitting the modulated carrier wave at the free frequency;

wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication;

wherein the content includes biometric data and a bit array, the bit array being derived from user-configurable and non-user-configurable data specific to the audio transceiver computing device; and

wherein the modulated carrier wave comprises a sound wave.

2. (original) The method of claim 1 further comprising:

displaying a user interface on the audio transceiver computing device requesting the biometric data from a user; and

responsive to receiving the biometric data, generating the periodic enclosed content message, wherein the content in each period of the periodic enclosed content message includes the biometric data.

3. (previously presented) The method of claim 1, wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

4. (previously presented) The method of claim 1, wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.

5. (canceled)

6. (previously presented) The method of claim 2, wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

7. (previously presented) The method of claim 2, wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.

8. (canceled).

9. (previously presented) The method of claim 1 wherein the carrier wave is modulated by the periodic enclosed content message.

10. (currently amended) The method of claim ~~11~~ 1, wherein the non-user-configurable data comprises hardware component numbers, serial numbers, and version numbers.

11. (currently amended) A method for near field authentication of a source, the source using an audio transceiver computing device, the method comprising:

scanning a plurality of predetermined frequencies for a free frequency;

selecting the free frequency from the plurality of predetermined frequencies;

generating a periodic enclosed content message;

generating a modulated carrier wave representing the periodic enclosed content message; and

transmitting the modulated carrier wave at the free frequency;

wherein each period of the periodic enclosed content message includes a begin indication, a content, and an end indication;

wherein the content includes device identification data including a ~~bit string or~~ bit array derived from user-configurable and non-user-configurable data specific to the audio transceiver computing device; and

wherein the modulated carrier wave comprises a sound wave.

12. (previously presented) The method of claim 11, wherein the transmitting step further comprises transmitting the modulated carrier wave for a predetermined number of periods, or a predetermined period of time.

13. (previously presented) The method of claim 11, wherein the transmitting step further comprises transmitting the modulated carrier wave until a stop indication is received from a user.

14. (canceled).

15. (previously presented) The method of claim 11 wherein the carrier wave is modulated by the periodic enclosed content message.

REMARKS

Applicant proposes the foregoing claim amendments for entry as an Examiner's Amendment.

Respectfully Submitted,

Sean D. Burdick
Reg. No. 51,513

Uniloc USA, Inc.
7160 N. Dallas Parkway, Suite 380
Plano, TX 75024
(972) 905-9580 x 227

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13734178	ETCHEGOYEN ET AL.
	Examiner	**Art Unit**
	AJIBOLA AKINYEMI	2649

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	08/30/2013	01/14/2014	10/28/2014	02/25/2015	08/07/2015	11/03/2015	12/07/2016		
1	1	✓	✓	✓	✓	✓	✓	=		
2	2	✓	✓	✓	✓	✓	✓	=		
5	3	✓	✓	✓	✓	✓	✓	=		
6	4	✓	✓	✓	✓	✓	✓	=		
-	5	✓	✓	✓	✓	✓	-	-		
3	6	✓	✓	✓	✓	✓	✓	=		
4	7	✓	✓	✓	✓	✓	✓	=		
-	8	✓	✓	✓	✓	✓	-	-		
7	9		✓	✓	✓	✓	✓	=		
8	10					✓	✓	=		
9	11					✓	✓	=		
10	12					✓	✓	=		
11	13					✓	✓	=		
-	14					✓	-	-		
12	15					✓	✓	=		

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

96051 7590 12/16/2016

Uniloc USA Inc.
Legacy Town Center
7160 Dallas Parkway
Suite 380
Plano, TX 75024

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/734,178	01/04/2013	Craig S. ETCHEGOYEN	UN-NP-SC-085	3155

TITLE OF INVENTION: NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	03/16/2017

EXAMINER	ART UNIT	CLASS-SUBCLASS
AKINYEMI, AJIBOLA A	2649	455-041100

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Sean D. Burdick
2
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: Uniloc Luxembourg S.A.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Luxembourg, Luxembourg

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☑ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

☑ Issue Fee

☐ Publication Fee (No small entity discount permitted)

☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): (**Please first reapply any previously paid issue fee shown above**)

☐ A check is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☑ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number 50-6053 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

☐ Applicant asserting small entity status. See 37 CFR 1.27

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

☐ Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date December 20, 2016

Typed or printed name Sean D. Burdick Registration No. 51,513

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Electronic Patent Application Fee Transmittal

Application Number:	13734178
Filing Date:	04-Jan-2013
Title of Invention:	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES
First Named Inventor/Applicant Name:	Craig S. ETCHEGOYEN
Filer:	Sean Dylan Burdick/Kris Pangan
Attorney Docket Number:	UN-NP-SC-085

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
UTILITY APPL ISSUE FEE	2501	1	480	480

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**480**

Electronic Acknowledgement Receipt	
EFS ID:	27844462
Application Number:	13734178
International Application Number:	
Confirmation Number:	3155
Title of Invention:	NEAR FIELD AUTHENTICATION THROUGH COMMUNICATION OF ENCLOSED CONTENT SOUND WAVES
First Named Inventor/Applicant Name:	Craig S. ETCHEGOYEN
Customer Number:	96051
Filer:	Sean Dylan Burdick/Kris Pangan
Filer Authorized By:	Sean Dylan Burdick
Attorney Docket Number:	UN-NP-SC-085
Receipt Date:	20-DEC-2016
Filing Date:	04-JAN-2013
Time Stamp:	11:47:32
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$480
RAM confirmation Number	122016INTEFSW00010962506053
Deposit Account	506053
Authorized User	Kristina Pangan
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	SC-085_Issue_Fee_Transmittal.pdf	211971 ae0b297eda2b9a20fefe76c4ffe9a6ea24ccf7ad	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30594 365be0db70b7a51ac7bb0a2461f0421798aa6f13	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	242565		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/734,178	01/04/2013	Craig S. ETCHEGOYEN	UN-NP-SC-085	3155

7590 12/21/2016

Uniloc USA Inc.
Legacy Town Center
7160 Dallas Parkway
Suite 380
Plano, TX 75024

EXAMINER	
AKINYEMI, AJIBOLA A	
ART UNIT	PAPER NUMBER
2649	

DATE MAILED: 12/21/2016

PRIORITY ACKNOWLEDGMENT

☒ 1. Receipt is acknowledged of priority papers submitted under 35 U.S.C. 119. The papers have been placed of record in the file.

☐ 2. Applicant's claim for priority, based on papers filed in parent Application Number _____ submitted under 35 U.S.C. 119, is acknowledged.

☐ 3. The priority papers, submitted _____, after payment of the issue fee are

- ☐ acknowledged
  While the priority claim or certified copy filed will be placed in the file record, neither will be reviewed and the patent when published will not include the priority claim.
  See 37 CFR 1.55(a)(2).
- ☐ not acknowledged since the processing fee in 37 CFR 1.17(i) has not been received.

☐ 4. For utility and plant applications filed on or after November 29, 2000, the priority claim is not entered because the claim was not presented within the time limit required by 37 CFR 1.55(a)(1). A petition to accept a delayed claim for priority under 35 U.S.C. 119(a) - (d) or (f), or 365(a) may be filed. See 37 CFR 1.55(c) and MPEP 201.14(a).

FOR

571-272-4200 or 1-888-786-0101
Application Assistance Unit
Office of Data Management

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/734,178	02/07/2017	9564952	UN-NP-SC-085	3155

96051 7590 01/18/2017

Uniloc USA Inc.
Legacy Town Center
7160 Dallas Parkway
Suite 380
Plano, TX 75024

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Craig S. ETCHEGOYEN, Newport Beach, CA;
Dono HARJANTO, Irvine, CA;
Sean D. BURDICK, Dallas, TX;
UNILOC LUXEMBOURG S.A., Luxembourg, LUXEMBOURG

AO 120 (Rev. 08/10)

TO:	**Mail Stop 8** **Director of the U.S. Patent and Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:18-cv-0341	8/5/2018	Eastern District of Texas

PLAINTIFF	DEFENDANT
Uniloc USA, Inc.; Uniloc Luxembourg S.A. and Uniloc 2017, LLC	Amazon.com, Inc.; Amazon Web Services, Inc.; Amazon Digital Services, LLC.; Amazon Digital Services, Inc.; and Amazon Fulfillment Services, Inc.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	9,564,952	2/7/2017	Uniloc 2017, LLC
2			
3			
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO:	**Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450**	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:18-cv-0341	8/5/2018	Eastern District of Texas

PLAINTIFF	DEFENDANT
Uniloc USA, Inc.; Uniloc Luxembourg S.A. and Uniloc 2017, LLC	Amazon.com, Inc.; Amazon Web Services, Inc.; Amazon Digital Services, LLC.; Amazon Digital Services, Inc.; and Amazon Fulfillment Services, Inc.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	9,564,952	2/7/2017	Uniloc 2017, LLC
2			
3			
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy