US008302175B2

(12) **United States Patent**
Thoursie et al.

(10) **Patent No.: US 8,302,175 B2**
(45) **Date of Patent: Oct. 30, 2012**

(54) **METHOD AND SYSTEM FOR ELECTRONIC REAUTHENTICATION OF A COMMUNICATION PARTY**

(75) Inventors: **Anders Thoursie**, Nacka (SE); **Peter Holm**, Sollentuna (SE); **Sven-Håkan Olsson**, Stockholm (SE)

(73) Assignee: **DocAccount AB**, Nacka (SE)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 914 days.

(21) Appl. No.: **11/918,877**

(22) PCT Filed: **Apr. 20, 2005**

(86) PCT No.: **PCT/SE2005/000568**

§ 371 (c)(1),
(2), (4) Date: **Oct. 19, 2007**

(87) PCT Pub. No.: **WO2006/112761**

PCT Pub. Date: **Oct. 26, 2006**

(65) **Prior Publication Data**

US 2009/0106829 A1 Apr. 23, 2009

(51) **Int. Cl.**
G06F 7/04 (2006.01)

(52) **U.S. Cl.** **726/9**

(58) **Field of Classification Search** 726/9
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,588,051	A *	12/1996	Berkowitz et al.	379/243
5,668,876	A *	9/1997	Falk et al.	380/271
6,175,831	B1 *	1/2001	Weinreich et al.	1/1
7,239,688	B1 *	7/2007	Sayko et al.	379/93.02
2002/0004831	A1	1/2002	Woodhill	
2002/0169988	A1 *	11/2002	Vandergeest et al.	713/201
2003/0159031	A1	8/2003	Mueller et al.	
2004/0243832	A1 *	12/2004	Wilf et al.	713/200
2005/0215306	A1 *	9/2005	O'Donnell et al.	463/17

FOREIGN PATENT DOCUMENTS

EP	1 102 150	5/2001

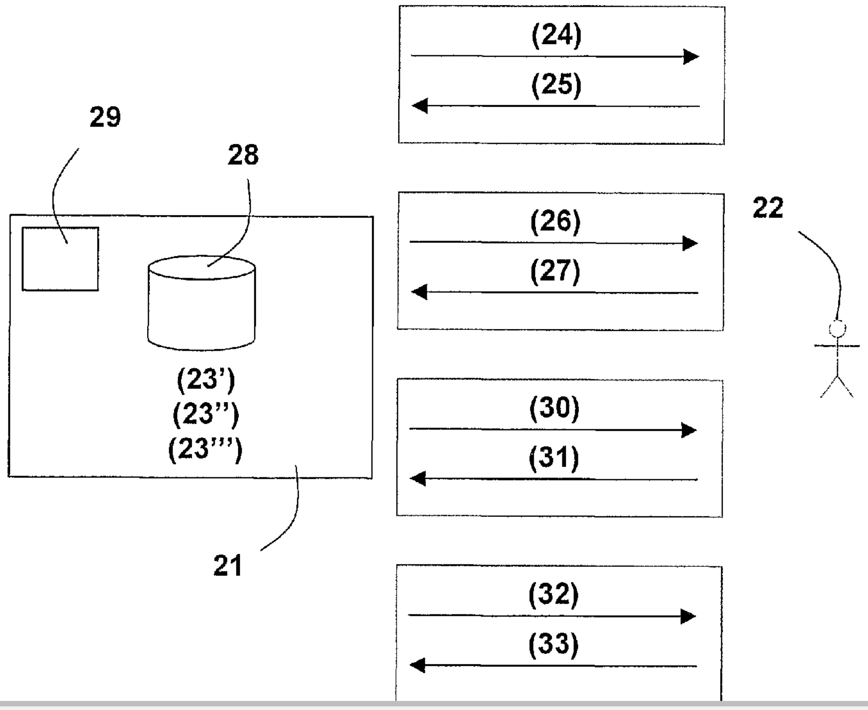
* cited by examiner

Primary Examiner — Cordelia Zecher
(74) *Attorney, Agent, or Firm* — Harness, Dickey & Pierce, P.L.C.

(57) **ABSTRACT**

The present invention relates to a method for electronic reauthentication of a communication party (**12**, **22**). The method further relates to a device for electronic reauthentication of a communication party. A basic idea of the present invention is to have a communication party, which employs a service, state two different communication addresses, one being a telephone number, via which the communicating party may authenticate herself to a provider (**11**, **21**) of the service.

41 Claims, 2 Drawing Sheets



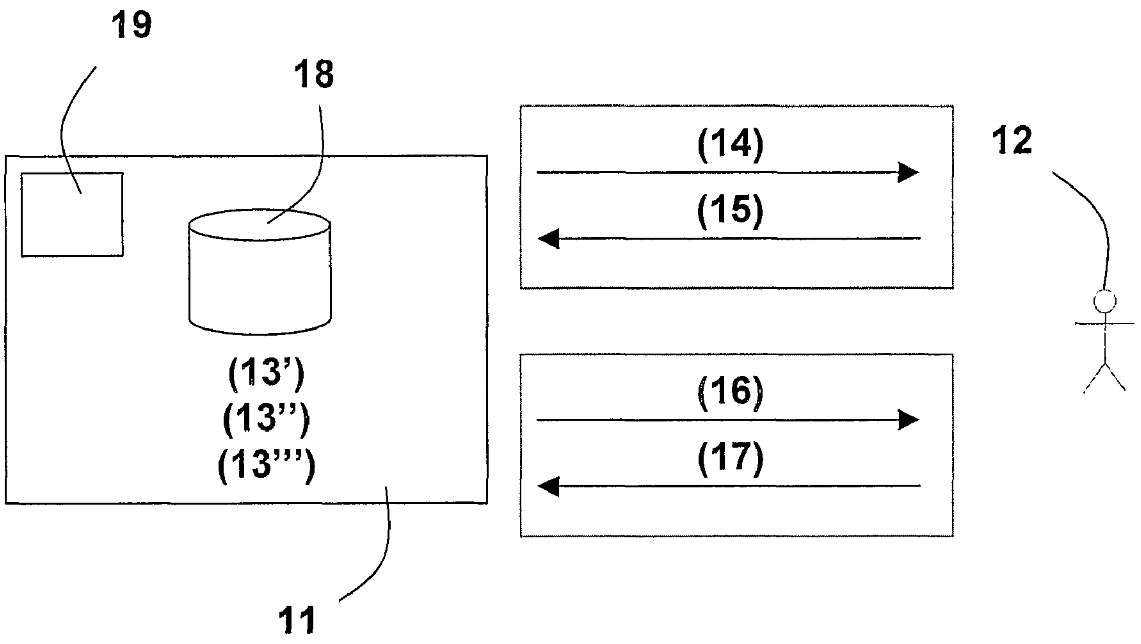


FIG. 1

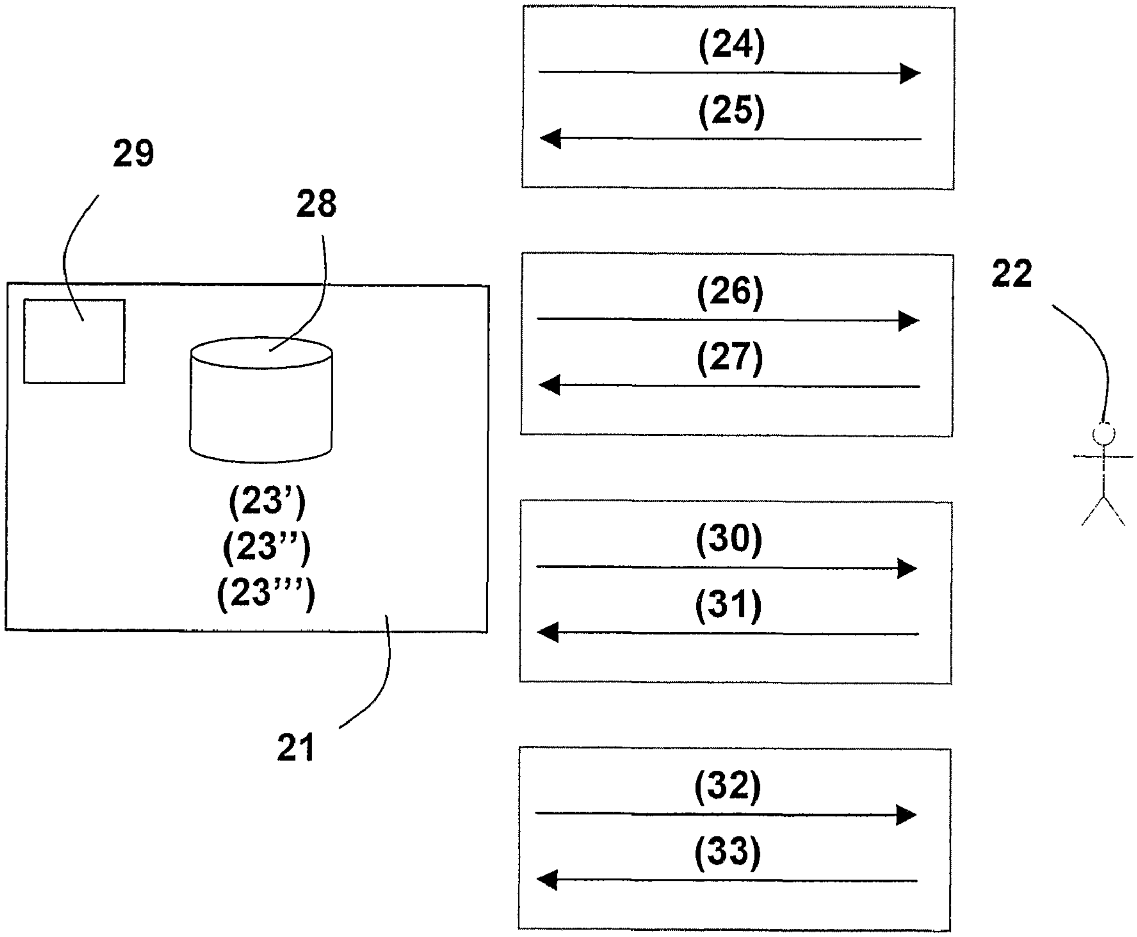


FIG. 2

METHOD AND SYSTEM FOR ELECTRONIC REAUTHENTICATION OF A COMMUNICATION PARTY

This application is a National Phase of PCT Application No. PCT/SE2005/000568 filed on Apr. 20, 2005, which claims priority under 35 U.S.C. §365(c).

TECHNICAL FIELD OF THE INVENTION

The present invention relates to a method for electronic reauthentication of a communication party. The method further relates to a device for electronic reauthentication of a communication party.

BACKGROUND ART

Today companies and organizations communicate with their customers and other parties via the Internet to an ever-increasing extent. In these situations, the companies and organizations need to ensure that a specific party is the same party they communicated with at an earlier occasion.

One way to ensure this is to provide the communication party with a code or a user name and password. If a person is able to replicate the code at a later occasion, this replication is considered to be an indication that it is the same person who previously received the code.

The use of codes or passwords as authenticating means has the disadvantage that there is a risk that an unauthorized person acquires these authenticating means. In today's society, people also need to learn and memorize codes to an ever-increasing extent, e.g. to use various services on the Internet or to use credit cards. This fact increases the risk that people will start to write down codes, making them easier for other people to acquire. It also makes these solutions less user-friendly, since it becomes considerably harder for people to remember all the codes. There is also a risk that so called brute force attacks or dictionary based attacks are used to find out and acquire passwords.

In many situations, code- or password-based solutions are hence considered insufficient. Instead, there is a need to introduce another mechanism which the communication party can control—which is more secure yet easy-to-use. Hence, the following features are desirable for such a mechanism:

The user is able to protect authenticating means, e.g. passwords, from being stolen.

A possible theft of authentication means is easily discovered.

The effect of a possible theft of authenticating means can be reduced, e.g. through a procedure of revoking the authenticating means.

It should be easy for companies to start using the mechanism on a wide basis, e.g. as a means for administering the communication with a great number of communication parties.

The mechanism should be easy-to-use and straightforward from a user perspective.

There are currently available solutions that meet these requirements to some degree. One example is the usage of card-based certificates, based on Public Key Infrastructure, PKI, as a tool for identification. A card-based certificate can be protected. A stolen certificate may easily be identified. If it is stolen, it may be revoked. However, the card-based technology requires an infrastructure that is not yet widely spread,

An alternative is to use file-based certificates based on Public Key Infrastructure. These are more widely spread than card-based certificates, but are still by many considered not sufficiently spread and available to citizens and consumers.

SUMMARY OF THE INVENTION

An object of the invention is to alleviate the problems of prior art through providing a straightforward and easy-to-use method for electronic reauthentication.

This object is accomplished by a method of electronic reauthentication of a communication party in accordance with claim **1**, and a device for electronic reauthentication of a communication party in accordance with claim **21**.

According to a first aspect of the present invention, a method is provided of electronically reauthenticating a communication party. First, an association between a telephone communication address of the communication party, an additional communication address of the communication party and the communication party itself, which association serves as a basis for future authentication of the communication party, is created. Then, a request is received from a requesting communication party and it is verified that an association exists for the requesting communication party. A first confirmation token is distributed to the requesting communication party over a first communication channel and a second confirmation token is received from the requesting communication party over a second communication channel, wherein at least one of the first and the second channel is established by using the telephone communication address of the association for the requesting communication party. Thereafter, correspondence is verified between the first confirmation token and the second confirmation token. A third confirmation token is distributed over a third communication channel to the requesting communication party and a fourth confirmation token is received from the communication party over a fourth communication channel, wherein at least one of the third and the fourth channel is established by using the additional communication address of the association for the requesting communication party. Further, correspondence is verified between the third confirmation token and the fourth confirmation token, wherein the requesting communication party is considered to be authenticated.

If the request comprises a request to create an association for a further telephone communication address, a fifth confirmation token is distributed to the requesting communication party over a fifth communication channel and a sixth confirmation token is received from the requesting communication party over a sixth communication channel, wherein at least one of the fifth and the sixth channel is established by using said further telephone communication address of the request. Then, correspondence is verified between the fifth confirmation token and the sixth confirmation token and an association between said further telephone communication address of the requesting communication party, said additional communication address and the requesting communication party itself is created, which association serves as a basis for future authentication of the requesting communication party.

If the request comprises a request to create an association for a further additional communication address, a seventh confirmation token is distributed to the requesting communication party over a seventh communication channel and an eighth confirmation token is received from the requesting communication party receiving over an eighth communica-

communication address of the request. Correspondence is verified between the seventh confirmation token and the eighth confirmation token and an association between said further additional communication address of the requesting communication party, said telephone communication address and the requesting communication party itself is created, which association serves as a basis for future authentication of the requesting communication party.

According to a second aspect of the present invention, a device is provided for electronic reauthentication of a communication party comprising means for creating an association between a telephone communication address of the communication party, an additional communication address of the communication party and the communication party itself, which association serves as a basis for future authentication of the communication party and means for storing the association. Further, the device comprises means for receiving a request from a requesting communication party, means for verifying that an association exists for the requesting communication party, means for distributing, over a first communication channel, a first confirmation token to the requesting communication party and means for receiving, over a second communication channel, a second confirmation token from the requesting communication party, wherein at least one of the first and the second channel is established by using the telephone communication address of the association for the requesting communication party. Moreover, the device comprises means for verifying correspondence between the first confirmation token and the second confirmation token, means for distributing, over a third communication channel, a third confirmation token to the requesting communication party, means for receiving, over a fourth communication channel, a fourth confirmation token from the communication party, wherein at least one of the third and the fourth channel is established by using the additional communication address of the association for the requesting communication party and means for verifying correspondence between the third confirmation token and the fourth confirmation token, wherein the requesting communication party is considered to be authenticated.

Further, the device comprises means for distributing, if the request comprises a request to create an association for a further telephone communication address, over a fifth communication channel, a fifth confirmation token to the requesting communication party, means for receiving, over a sixth communication channel, a sixth confirmation token from the requesting communication party, wherein at least one of the fifth and the sixth channel is established by using said further telephone communication address of the request, means for verifying correspondence between the fifth confirmation token and the sixth confirmation token, means for creating an association between said further telephone communication ad-dress of the requesting communication party, said additional communication address and the requesting communication party itself, which association serves as a basis for future authentication of the requesting communication party.

Finally, the device comprises means for distributing, if the request comprises a request to create an association for a further additional communication address, over a seventh communication channel, a seventh confirmation token to the requesting communication party, means for receiving, over an eighth communication channel, an eighth confirmation token from the requesting communication party, wherein at least one of the seventh and the eighth channel is established by using said further additional communication address of the

token, means for creating an association between said further additional communication address of the requesting communication party, said telephone communication address and the requesting communication party itself, which association serves as a basis for future authentication of the requesting communication party.

A basic idea of the present invention is to have a communication party, which employs a service, state two different communication addresses, one being a telephone number, via which the communicating party may authenticate herself to a provider of the service.

A relation with the communication party, in the following referred to as a user, is established by confirming user control of the telephone communication address and an additional communication address. Initially, an association between the telephone communication address of the user, the additional communication address of the user and the user herself are created. When receiving a request from a user, which user not necessarily is the same as the user for which an association is created, it must be verified that an association exists for this requesting user. The confirmation of the requesting user's control of the telephone communication address of the association is made by distributing a first confirmation token over a first communication channel to the requesting user, receiving a second confirmation token over a second communication channel from the requesting user and then verifying that the two tokens are the same. At least one of the two communication channels should be established by means of using the telephone communication address of the association of the requesting user. In this way it is ensured that the requesting user is in control of the device which is designated by the telephone communication address. For instance, in case the telephone communication address is a telephone number, the requesting user shows, by sending a second token that is identical to the first token, that she actually is in possession of the telephone linked to the telephone number to which the first token was sent, and authentication of the requesting user is hence made.

To further strengthen authentication validity, confirmation of the requesting user's control of the additional communication address of the association is made by distributing a third confirmation token over a third communication channel to the requesting user, receiving a fourth confirmation token over a fourth communication channel from the requesting user and then verifying that the two tokens are the same. At least one of the two communication channels should be established by means of using the additional communication address of the association of the requesting user. In this way, it is ensured that the requesting user is in control of the means which is designated by the additional communication address. For instance, in case the additional communication address is an e-mail address, the requesting user shows, by sending a fourth token that is identical to the third token, that she actually is in possession of the e-mail account linked to the e-mail address to which the third token was sent, and authentication of the requesting user is hence made again.

The request of the user may for instance be to access an account which the user has at the service provider. The request may also be to create an association for a further telephone communication address and/or a further additional communication address. Alternatively, the request may comprise both an access request and an association request.

If the user request comprises a request to create an association for a further telephone communication address, a fifth confirmation token is distributed to the requesting user over a

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.