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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 July 2004 (01.07.2004)

PCT

(10) International Publication Number
WO 2004/055738 A1

(51) International Patent Classification[7]: G07C 9/00, G06K 9/00

(21) International Application Number: PCT/NO2003/000421

(22) International Filing Date: 17 December 2003 (17.12.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20026097 18 December 2002 (18.12.2002) NO

(71) Applicants and
(72) Inventors: **MATHIASSEN, Svein** [NO/NO]; Homansbyveien 4, N-1389 Heggedal (NO). **MATHIASSEN, Ivar** [NO/NO]; Gaupeveien 21, N-8515 Narvik (NO).

(74) Agent: **ABC-PATENT, SIVILING. ROLF CHR. B. LARSEN A.S**; Postboks 6150 Etterstad, N-0602 Oslo (NO).

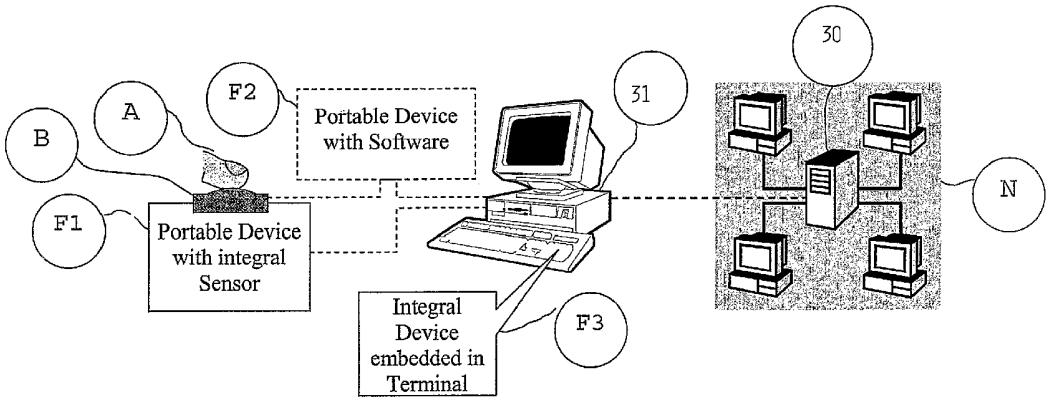
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM,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

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

Published:
— *with international search report*

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.

(54) **Title:** DEVICES FOR COMBINED ACCESS AND INPUT



(57) **Abstract:** A portable or embedded access device is provided for being coupled to, and for allowing only authorized users access to, an access-limited apparatus, device, network or system, e.g. a computer terminal, an internet bank or a corporate or government intranet. The access device comprises an integrated circuit (IC) (1) providing increased security by bridging the functionality of fingerprint input from a user and, upon positive authentication of the user's fingerprint to provide secure communication with the said access-limited apparatus, device, network or system. A corresponding method of using the portable device the embedded device is disclosed for providing a bridge from biometrics input to a computer, into secure communication protocol responses to a non-biometrics network.An embedded access control and user input device or apparatus for being a built-in part of stand alone appliances with some form of access control, e.g. hotel safes, medicine cabinet or the like, and for providing increased security, is also provided. Further, a method of providing secured access control and user input in stand-alone appliances having an embedded access control or user input device according to the invention is also explained.

WO 2004/055738 A1

DEVICES FOR COMBINED ACCESS AND INPUT

This invention is in general related to access and input devices for giving access and allowing user input in access limited devices, apparatuses, appliances, systems or networks.

In particular the invention is related to a portable and an embedded access or input devices and methods of using these in order to obtain a high level of security.

Automated access from a device or terminal to another device or a network / server is subject to authentication of authorized users. Such automated access eliminates manual authentication of the user by human recognition, and has to rely on some form of electronic identification of the user.

One way to resolve such electronic identification of the user is to issue a secret password to the user. Another method is to issue a physical token to the user. In both cases the system relies on the assumption that the person knowing such password, or alternatively carrying such physical token, has proved his identity, assuming that this has authenticated the authorized user. This is not the case, as passwords, or tokens, may intentionally be passed away to a third person, or non-intentionally and illegally acquired by such third person. Despite these obvious shortcomings of such identification by something you know (e.g. a password) or something you carry (e.g. a token) this method is still the dominating method of user identification to networks / servers, etc. because it is practical, but mainly because no better alternative is still commercially available in greater scale.

An alternative identification method is by something you are, meaning some sort of secure identification by biometrics, such as fingerprints. Although biometrics is gaining ground, this happens slowly and is not employed in a greater scale. There are several reasons for this slow growth in biometrics identification for access to networks and

servers;

a. Biometrics has to gain wide public acceptance. This will be the case as soon as the benefit from biometrics identification outranks assumed disadvantages. This includes lack of knowledge about, and lack of available biometrics solutions. Very few users will acquire biometrics solutions per se, if such biometrics do not form part of an overall solution that provides substantial benefits to the user in the form of increased convenience and availability. Basically this item will be resolved when items (b) and (c) are resolved.

b. The unit cost of biometrics sensors still needs to be reduced, to achieve widespread commercial solutions. This is partly pending on cost-efficient designs, which are continuously evolving, but mainly pending on volume. This item will accordingly be resolved when item (c) is resolved.

c. The major obstacle against secure access authentication by biometrics is that the systems and solution providers must embed biometrics access control in their systems. The major obstacle to this is that there are still no commonly accepted international standards of biometrics. A system or solution provider must therefore choose between several alternative emerging biometrics standards, at the risk of choosing the wrong one, or one of the standard proposals that will not be the dominating winner. Most major system providers are reluctant to make a choice on this basis, because of the grave consequences from a wrong selection;

- The costs involved by modifying software on servers etc. are considerable, especially if the non-winning standard is selected, and the software modification process has to be repeated in the near future. The price of biometrics hardware adds to this.

- The negative public relation effects from selecting the non-winning biometrics standard may be serious, and shall not be under-emphasized.
- The time to market will be severely prolonged if selecting a non-winning biometrics standard. This is further aggravated by the lead this will give any major competitors having selected the winning biometrics standard from the outset. This may upset the entire ranking between major solution providers.

Prior-art attempts to resolve this problem have been to enforce biometrics standards. However, there are currently several alternative standards battling side-by-side without any clear winner yet. Some known attempts to resolve the problems have been to use extracted specifics of biometrics to form encryption keys. One such solution is described in US patent 5,995,630 as it requires identical biometrics representation at the receiving end (e.g. a network server). A similar approach is described in US patent 5,991,408. However, none of these resolves the problem of avoiding the need to choose a biometrics standard as they both pose an even more serious problem that will delay biometrics implementation even further; namely proprietary solutions. Other attempts to resolve the problem are focused on improving the communication security by the concept of public key cryptosystems, as e.g. per European patent EP 0 225 010 B1. Though such systems enhances the security of network communication over insecure communication lines, the public key cryptosystems do not prove that the bearer of electronic certificates (checksums of keys and other identity features) is actually the right person. In addition these systems do still require a PIN code for the user to access the PKI system with electronic certificates. This means that yet another PIN code has to be remembered by the user. Moreover, the system security is no better than the protection of this PIN code. As a countermeasure to breaking PIN codes, the

industry tends to make longer and longer PIN codes, making it even more difficult for the user to remember these. The natural response of the users is to write down the PIN codes, leaving the potential security breach wide open.

Accordingly the present two main directions of prior-art attempts to resolve the problems (biometrics encryption, and biometrics representation on servers, on one hand and the concept of public key cryptosystems on the other hand) do not really solve the above problems in network communication, and certainly not for secure access to devices and apparatuses.

Apparent competitors to the portable embodiments of the present invention are so-called USB Dongles with memory onboard (up to 1 Gb). Some of these USB Dongle memory devices are even equipped with fingerprint sensors to prevent unauthorized access to the information stored onboard the USB Dongle. While these devices may physically look somewhat ~~a~~like one of the preferred embodiments of the present invention, there is no similarity in their functionality at all. The USB Dongles presently on the market are purely portable storage means, while the present invention focuses on secure communication triggered by an authorized fingerprint on such portable devices.

On this basis the major solution providers are hesitant to make an early move, though there is a general consensus that biometrics access control is far more secure, and convenient, than password-based or token-based access control. However, when the market leaders are hesitant to provide biometrics access methods widely offered to the market, the lack of availability to the general public will continue to restrain the growth of biometrics access control systems.

It is one object of the present invention to overcome the above limitations by providing a portable access device for being coupled to, and for allowing only authorized users access to, an access-limited apparatus, device, network or

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.