PCT
WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 :
H04Q 7/32, H04L 9/00

A1

(11) International Publication Number: WO 00/14984

(43) International Publication Date: 16 March 2000 (16.03.00)

(21) International Application Number: PCT/FI99/00713

(22) International Filing Date: 1 September 1999 (01.09.99)

(30) Priority Data:
981902 4 September 1998 (04.09.98) FI

(71) Applicant *(for all designated States except US)*: SONERA OY [FI/FI]; Teollisuuskatu 15, FIN–00510 Helsinki (FI).

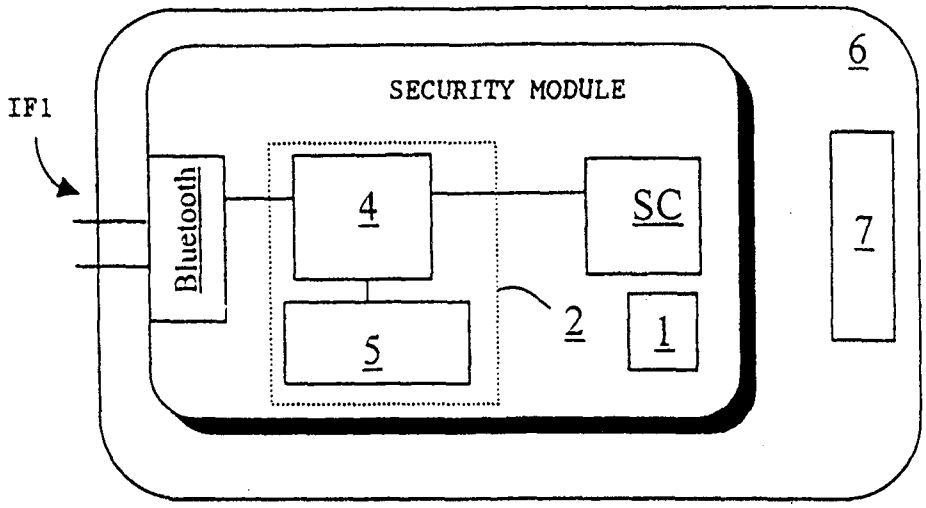
(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: VATANEN, Harri [FI/FI]; Lepolantie 25 A 3, FIN–00660 Helsinki (FI).

(74) Agent: PAPULA REIN LAHTELA OY; Fredrikinkatu 61 A, P.O. Box 981, FIN–00101 Helsinki (FI).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, 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, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
In English translation (filed in Finnish).

(54) Title: SECURITY MODULE, SECURITY SYSTEM AND MOBILE STATION



(57) Abstract

The present invention relates to implementing services and devices affording a high level of data security. In particular, the present invention relates to a security module, a security system and a mobile station for using these. The invention makes it possible to use standard devices easily and without any modifications to implement banking services and other services requiring a high level of data security. In the invention, a security module is formed which uses a standardized local interface for the transmission of the messages to be transmitted. Messages can be transmitted in real time without any delay caused by the telecommunication network.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

SECURITY MODULE, SECURITY SYSTEM AND MOBILE STATION

FIELD OF THE INVENTION

The present invention relates to a security module. In particular, the invention concerns a new and improved security module and a security system for processing and transmitting various messages requiring a high degree of data security. The invention also concerns a mobile station utilizing the security module.

BACKGROUND OF THE INVENTION

In mobile communication networks, e. g. GSM networks (GSM, Global System for Mobile communications), heavy encryption is used in conjunction with the transmission of speech over the radio link between the mobile station and the base station. Besides speech communication, communication using text or data messages has increased. With a rising service level, services relying on text or data communication have gained ground. Text communication can be utilized in various service functions, in paying for services, etc.

At present, a source of difficulties in encrypting messages is the fact that, in mobile telephones consistent with the current standard concerning mobile communication, it is not possible to make any changes to facilitate encryption because the user interfaces used in the telephones are manufacturer-specific. The only component that is sufficiently standardized and sufficiently open in respect of encryption is the subscriber identity module (SIM).

Mobile telephones consistent with a current mobile communication standard, such as the GSM standard, do not directly provide a possibility of en-

crypting text communication via mobile stations. Text communication can be used to implement services, such as bank services, which require a high level of data security. However, services requiring a high level of data security cannot become popular before sufficient encryption of message communication is possible.

A further problem with the use of a mobile communication network is that the message transmission services implemented in it are not necessarily real-time services and the transmission of messages may take time. This may be a problem e.g. when a user wants to pay for his/her shopping at the cash register of a store. In this situation, even a slight delay in message transmission will significantly retard the execution of the payment transaction. At present, no part of the mobile communication standard supports local communication between a mobile station and a cash register terminal.

A group of the world's leading enterprises in telecommunication and information technology has developed a technology that makes it possible to establish a wireless connection between a mobile telephone and e.g. a portable computer. This technology is designated as "Bluetooth" and it is based on short-range radio technology, which can be used to interconnect many types of terminals. A more detailed description of this technology can be found e.g. on the WWW page www.bluetooth.com.

The Bluetooth technology enables devices to be interconnected via a short-range radio link. By using the Bluetooth technology, it is possible to establish a connection e.g. between a mobile station and a portable computer without cumbersome cabling. Printers, work stations, telefax devices, keyboards and virtually any digital apparatus may be parts of a Bluetooth system or network. The technology forms a universal bridge to existing data networks and peripher-

als and provides means for forming small private groups via interconnected devices without a fixed network infrastructure. In addition, encryption and authentication can be used in the communication between the devices, e.g. so that only a given user's mobile telephone may be used in connection with a given portable computer.

Previously known is also a smart card that enables reliable personal authentication and genuine signature. Its sphere of application is unlimited. Examples of possible applications are a national electronic identity card (EID), encryption of files, telecommunication and electronic mail, a means for signing documents, an electronic currency, driver's license, ballot, and so on.

Although the smart card can be used in the ways described above, the problem remains that the smart card still requires a separate reading device for communicating with the smart card. Moreover, the smart card alone is incapable of communicating over any telecommunication network, which means that updating information e.g. using short messages is impossible.

In addition, even if it were possible to connect a mobile station locally to a cash register terminal using Bluetooth technology and thus utilize the mobile station as a payment instrument, there is still the problem of encrypted and secure data communication needed for payment transactions.

In prior art, no general-purpose security module is known which could be connected to different cash register and automated systems, mobile stations or other portable devices and which would be able to safely communicate e.g. with a host device on the one hand and a service provider's device on the other hand utilizing e.g. the Bluetooth technology using encryp-

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.