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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 March 2001 (08.03.2001)

PCT

(10) International Publication Number
WO 01/16899 A2

(51) International Patent Classification[7]: G07F 7/10

(21) International Application Number: PCT/GB00/03148

(22) International Filing Date: 17 August 2000 (17.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
9920502.3 1 September 1999 (01.09.1999) GB

(71) Applicant *(for all designated States except US)*: **NCR INTERNATIONAL, INC.** [US/US]; 1700 South Patterson Boulevard, Dayton, OH 45479 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **SHIELDS, Adrian** [GB/GB]; 6 Crathes Close, Glenrothes Street, Fife KY7 4SS (GB).

(74) Agent: **WILLIAMSON, Brian**; International Patent Dept., NCR Limited, 206 Marylebone Road, London NW1 6LY (GB).

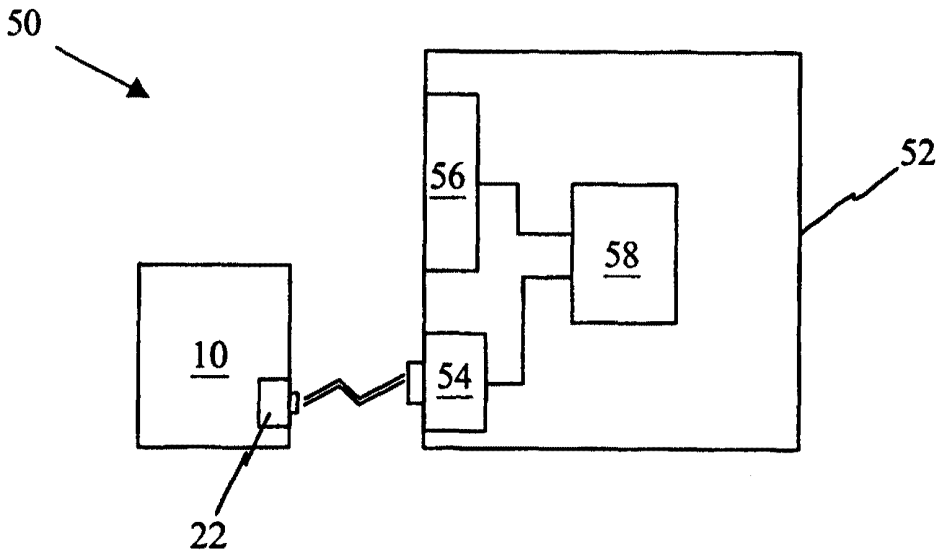
(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, 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:
— *Without international search report and to be republished upon receipt of that report.*

[Continued on next page]

(54) Title: PORTABLE TERMINAL



(57) Abstract: A portable terminal (10) for encrypting information is described. The terminal (10) generates a new key for each transaction, where the new key is generated using one or more properties of the terminal (10). The one or more properties are variable and may include the history of usage of the terminal, and/or the date and time settings. The terminal (10) may generate a unique challenge in addition to the new key so that a unique challenge can be issued for each transaction. A method of encrypting information in a portable terminal, a method of communicating encrypted information between a portable terminal and a self-service terminal, and a transaction system comprising a self-service terminal (52) and a portable terminal (10) are also described.

WO 01/16899 A2

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.

PORTABLE TERMINAL

The present invention relates to a portable terminal. In particular, the invention relates to a portable terminal for encrypting information and to a method of encrypting information in a portable terminal, such as a personal digital assistant (PDA).

PDAs are used for storing personal information and for transferring stored personal information between computer systems. It is also possible to use a PDA to prepare and store highly confidential personal information such as transaction information for execution at a self-service terminal (SST) such as an automated teller machine (ATM).

To provide some security for the transaction information it would be desirable to encrypt the transaction information that is stored on and transmitted from the PDA. However, a conventional PDA is not an inherently secure device; it has minimal tamper resistance, which means that there is no secure area for storing a secret cryptographic key. The lack of secure storage means that industry-standard cryptographic techniques cannot be used with a conventional PDA.

According to a first aspect of the invention there is provided a portable terminal for encrypting information characterised in that the terminal generates a new key for each transaction, where the new key is generated using one or more properties of the portable terminal.

It will be appreciated that the one or more properties of the portable terminal are properties that vary with usage of the terminal or with time; that is, the properties are

variable. This ensures that the new key is unique and unpredictable.

The new key is generated from an unsecure area of memory. Thus, no dedicated security module is required.

The new key may be generated when the transaction is prepared; that is, when the new transaction is entered into the portable terminal. Alternatively, and more preferably, the new key is generated when the transaction is executed; that is, immediately prior to communicating the new transaction from the portable terminal to a self-service terminal.

Preferably, the new key is a symmetric key. Using a symmetric key provides improved performance and ensures compatibility with existing financial systems that generally use symmetric key technology.

A user may enter an identification during preparation of a transaction. Alternatively, the user may enter an identification a short period of time prior to executing the transaction; that is, a short period of time, such as ten seconds, prior to communicating the transaction from the portable terminal to an SST. The identification may be a PIN (personal identification number), or it may be biometrics-based.

Preferably, the one or more properties of the portable terminal include the history of usage of the terminal and/or the date and time settings. The history of usage may include: button selections, pointer movements, data entered, and such like. In some terminals, these properties are stored in system memory. Thus, the system memory is used as

the seed (the starting value used by a pseudo-random number generating routine) from which the new key is generated. As the system memory changes with each keystroke, a unique key is generated for each transaction.

Preferably, the portable terminal generates a unique challenge in addition to the new key so that a unique challenge can be issued for each transaction.

Preferably, the new key and the unique challenge are encrypted using a public key issued by a host.

By virtue of this aspect of the invention a portable terminal uses unpredictable data to generate a new key for each transaction. This new key can be used in association with a public key issued by an ATM owner to provide a secure communications channel between the portable terminal and the ATM. One advantage of this aspect of the invention is that no assumptions are made regarding protected storage areas within the portable terminal.

The portable terminal may be a PDA. Alternatively, the portable terminal may be a portable computer such as a laptop computer, or the terminal may be a portable communication device such as a cellular telephone.

According to a second aspect of the invention there is provided a method of encrypting information in a portable terminal, the method being characterised by the steps of: using one or more properties of the portable terminal to obtain a sequence of values, and generating a new key based on the sequence of values.

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.