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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 June 2010 (24.06.2010)

PCT

(10) International Publication Number
WO 2010/071904 A2

(51) International Patent Classification:
G06Q 20/00 (2006.01) *G06F 21/00* (2006.01)

(21) International Application Number:
PCT/ZA2009/000111

(22) International Filing Date:
17 December 2009 (17.12.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2008/10812 17 December 2008 (17.12.2008) ZA

(71) Applicant *(for all designated States except US)*: **RADIO SURVEILLANCE SECURITY SA (PTY) LTD** [ZA/ZA]; Douglas Saunders Drive, Block A, Sunbury Park, La Lucia, Kwa Zulu Natal 4019 Durban (ZA).

(72) Inventors: **WEIDEMAN, Grant, Paul**; Douglas Saunders Drive, Block A, Sunbury Park, La Lucia, Kwa Zulu Natal 4019 Durban (ZA). **NARAINSAMY, Selvanathan**; Douglas Saunders Drive, Block A, Sunbury Park, La Lucia, Kwa Zulu Natal 4019 Durban (ZA).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **WEIDEMAN, Grant, Paul** [ZA/ZA]; Douglas Saunders Drive, Block A, Sunbury Park, La Lucia, Kwa Zulu Natal 4019 Durban (ZA).

(74) Agent: **MORRISON FORSTER INC.**; 9 Sunbury Park, Douglas Saunders Drive, La Lucia Ridge, Kwa Zulu Natal, P O Box 5147, Sunbury Park, Kwa Zulu Natal, 4019 Durban (ZA).

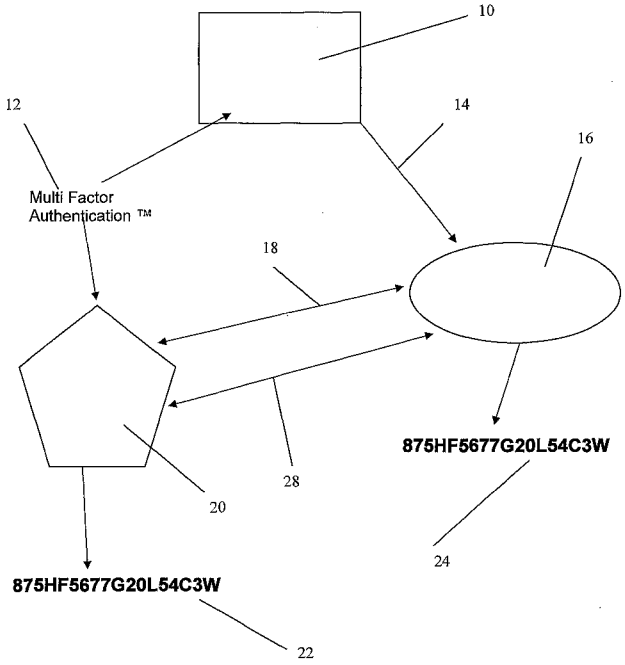
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG,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

[Continued on next page]

(54) Title: SECURITY MEASURES FOR CREDIT CARD

FIGURE 1



(57) Abstract: A method for generating a code on card related transactions such as credit card transactions includes loading multi-factor authentication software onto the card itself. The software is read by a card transaction terminal such as an ATM or a similar payment station which generates a time and/or date specific code which is verified with a code generated on a remote CPU running similar or identical multi-factor authentication software. The two codes need not be identical, but should be similar to a sufficient tolerance to ensure that there is no security breach. Once the code is verified the transaction may proceed as it would normally.

WO 2010/071904 A2

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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

SECURITY MEASURES FOR CREDIT CARD

TECHNICAL FIELD OF THE INVENTION

This invention relates to security measures for bank card related transactions.

For purposes of this specification the term 'card' as applied to card related transactions shall be understood to include any type of 'smartcard' which includes any form of electronic processor and/or electronic memory and/or electronic storage capacity.

BACKGROUND ART

Card related fraud is a well documented worldwide problem. In recent studies credit card fraud was estimated to amount to 52 billion US dollars in the United States in 2007.

Diverse methods have been devised to commit card fraud including intercepting the cards, copying the secure information contained on the card and using that information to either directly make purchases or clones the card.

One of the most important steps during this process is to obtain the confidential authorization code which verifies the authenticity and detail on the card with a card reading machine. This code is unique to each card and is stored in the magnetic strip or the electronic chip on the card.

Current practise is for the code to be programmed onto the card when it is issued, and for that code to remain unchanged during the lifetime of the card.

This unchanging or static code has many drawbacks, the most important being that once it is intercepted, a would-be fraudster is free to clone the card and is capable of validating the authenticity thereof for any transaction.

The code is usually intercepted while being verified by a card reading machine. This may be accomplished by adding software to the machine (or another handheld device) which reads the card and intercepts/copies the code without otherwise affecting the transaction. The user is therefore unaware of this interception.

It is an object of this invention to provide an alternative to the single programmed static authentication code on credit and debit cards or similar card related transactions.

DISCLOSURE OF THE INVENTION

According to the invention a method of generating a dynamic authentication code for card related transactions includes the steps of loading algorithm generating software onto the card to generate a time and/or date specific code when used in combination with a card transaction machine, and synchronising the generated code with one similarly generated at a remote terminal.

In the preferred form of the invention, suitable algorithm-generating and/or multifactor authentication software is loaded onto a card such as a credit card. The software may be loaded onto the micro-chip or any similar storage means and/or memory of the card, or wherever suitable.

The software may be interpreted by a card reading machine such as an ATM or a card transacting terminal to generate a time and date specific code. This code may be sent to a remote terminal, on which the same software may be running and on which an identical code may be generated on similar terms.

The remote terminal may verify the authenticity of the card and allow the transaction to proceed as it would normally.

In the preferred form of the invention the software loaded onto the card may be any suitable multi factor authentication software.

In a refinement of the invention the card transaction terminal transmits a signal to the remote terminal which responds by sending a time and/or the date according to the terminal or the time zone in which the remote terminal is located.

This signal and subsequent time and date ensures that the time and/or date on the remote terminal and the card transaction terminal are identical so that an identical or suitably matched code may be generated.

The method may be adapted to generate a new code for each new transaction, which may be valid for a specific time interval, for instance three minutes. This variation

should negate any delays caused by time-and-date verification or similar communication interruptions and should ensure that the codes are always identical.

BRIEF DESCRIPTION OF THE DRAWINGS

An embodiment of the invention is described below with reference to the accompanying flow diagram.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

In the drawing multi-factor authentication software 12 is loaded onto a credit or debit card 10. In this embodiment multi factor authentication software is used but any suitable algorithm generating authentication software may be used.

The software may be loaded onto the microchip (not shown) of the card. It may be possible and necessary for the software to be loaded on other storage means in future depending on the evolution of card transactions.

The software is also loaded onto a remote terminal 20.

When the card is used 14 with a card reading machine 16 such as an ATM or a credit card transaction terminal the following two steps occur:

Firstly the card terminal transmits a signal or a 'ping' 18 to the remote terminal 20 located at a banking institution or the like (not shown). The remote terminal responds by sending back a signal 18 containing the time and/or date to the card terminal

The reasoning behind this step is to ensure that the terminals are synchronised with regards to the time and date, irrespective of time zone differences or whether the machine's time and date are set accurately.

In the next step that the card terminal reads the software from the card and interprets it, taking the time and date into account, to generate a code 24 unique to the card for that specific time and/or date.

Once the card terminal has generated the code it transmits the code 28 to the remote terminal where it is decrypted and interpreted to verify whether it is valid or not. If the codes satisfies the necessary criteria the remote terminal transmits a signal for receipt by the card terminal to authorise the transaction.

In the preferred form of the invention this whole method takes place in a matter of seconds. It is however envisioned that a code may be time interval generated and that a code will be valid for a few minutes to ensure that communication delays or transaction traffic does not affect the generation and verification of codes.

This time interval may for instance be three minutes.

CLAIMS

1. A method of generating a dynamic authentication code for card related transactions characterised in that it includes the steps of loading algorithm generating software onto the card to generate a time and date specific code when used in combination with a card transaction machine,
and synchronising the generated code with one similarly generated at a remote terminal.

2. A method of generating a dynamic authentication code for card related transactions according to claim 1 characterised in that algorithm-generating and/or multifactor authentication software is loaded onto a card such as a credit card.

3. A method of generating a dynamic authentication code for card related transactions according to claim 1 or 2 characterised in that the software is loaded onto the micro-chip memory of the card.

4. A method of generating a dynamic authentication code for card related transactions according to any of claims 1 to 3 characterised in that the software is interpreted by a card transacting terminal to generate a time and date specific code.

5. A method of generating a dynamic authentication code for card related transactions according to claim 4 characterised in that the card transaction terminal is an ATM (Automatic Teller Machine).

6. A method of generating a dynamic authentication code for card related transactions according to any of the above claims characterised in that the code is sent to a remote terminal, on which the same software is running and on which an identical code is generated on similar terms.

7. A method of generating a dynamic authentication code for card related transactions according to claim 6 characterised in that the code is negligibly similar to the code generated by the card transaction terminal.

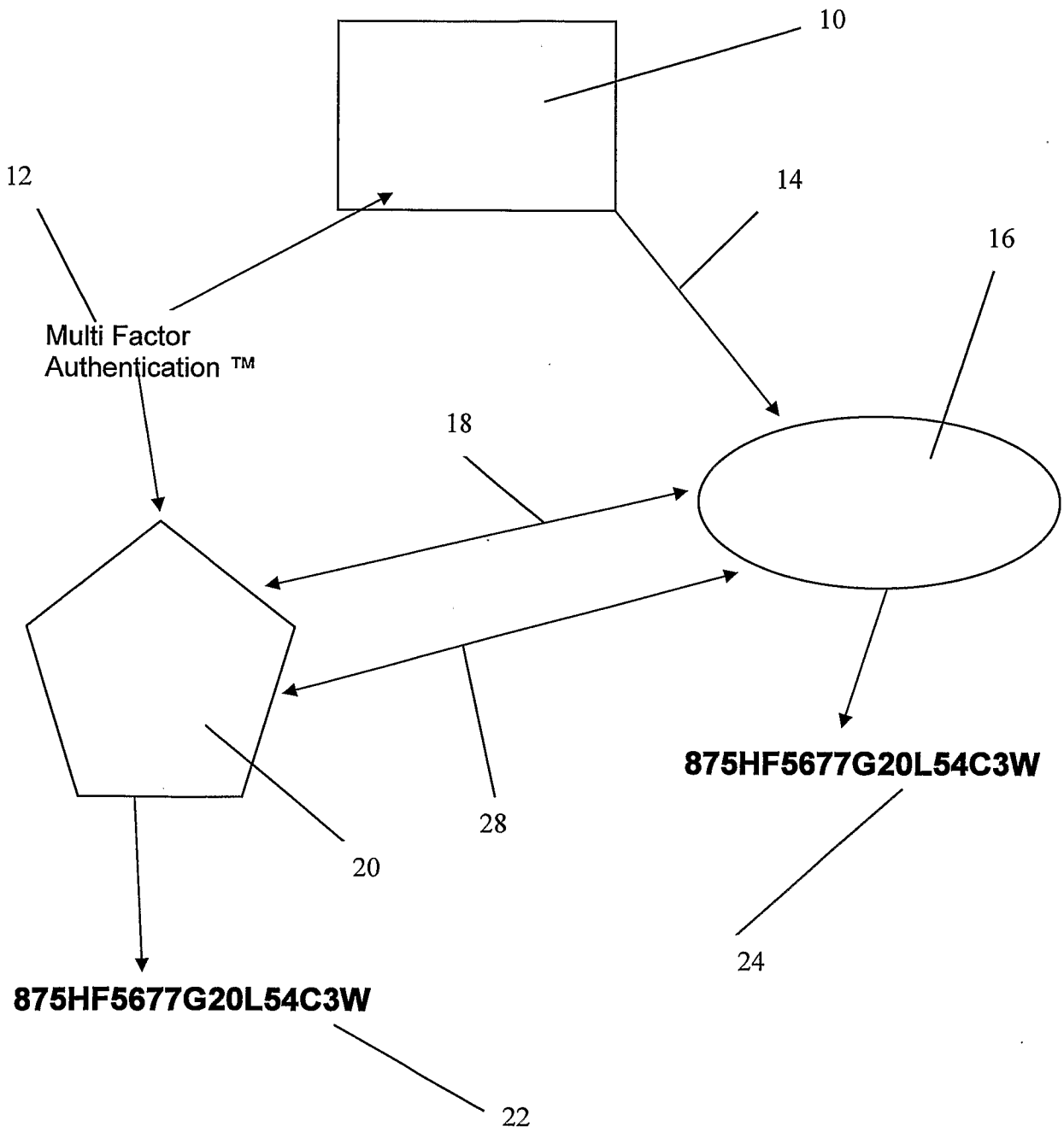
8. A method of generating a dynamic authentication code for card related transactions according to any of the above claims characterised in that the remote terminal verifies the authenticity of the card and allows the transaction to proceed.

9. A method of generating a dynamic authentication code for card related transactions according to any of the above claims characterised in that the card transaction terminal transmits a signal to the remote terminal which responds by sending a time and/or the date according to the terminal or the time zone in which the remote terminal is located.

10. A method of generating a dynamic authentication code for card related transactions according to any of the above claims characterised in that method is adapted to generate a new code for each new transaction, which is valid for a specific time interval.

11. A method of generating a dynamic authentication code for card related transactions according to claim 10 characterised in that the time interval is three minutes.

FIGURE 1


10
12
14
16
Multi Factor
Authentication ™
18
875HF5677G20L54C3W
28
20
24
875HF5677G20L54C3W
22