

1 Michael J. Glenn, SBN 89654  
2 LAW OFFICES OF JAMES M. DONOVAN  
3 915 Wilshire Blvd., Suite 1610  
4 Los Angeles, CA 90017-3474  
5 213-629-4861  
6 mglenn@thedonovanoffices.com

7 Howard L. Wernow (*Pro hac vice* forthcoming)  
8 Sand, Sebolt & Wernow Co., LPA  
9 Aegis Tower – Suite 1100  
10 4940 Munson Street NW  
11 Canton, OH 44718-3684  
12 330-244-1174  
13 howard.wernow@sswip.com

14  
15  
16 **IN THE UNITED STATES DISTRICT COURT**  
17 **FOR THE CENTRAL DISTRICT OF CALIFORNIA**  
18 **SOUTHERN DIVISION**  
19

20 **AUTH TOKEN LLC,**

Case No.

21 Plaintiff,

Patent Case

22 v.

Jury Trial Demanded

23 **CARDLOGIX CORPORATION,**

24 Defendant.

25 **COMPLAINT FOR PATENT INFRINGEMENT**

26 1. Plaintiff Auth Token LLC (“Plaintiff”), through its attorneys,  
27 complains of CardLogix Corporation (“Defendant”), and alleges the following:  
28

**PARTIES**

1  
2 2. Plaintiff Auth Token LLC is a corporation organized and existing  
3 under the laws of Delaware that maintains its principal place of business at 261  
4 West 35th St, Suite 1003, New York, NY 10001.

5  
6 3. Defendant CardLogix Corporation is a corporation organized and  
7 existing under the laws of California that maintains an established place of  
8 business at 16 Hughes Dr #100, Irvine, CA 92618.

**JURISDICTION**

9  
10  
11 4. This is an action for patent infringement arising under the patent laws  
12 of the United States, Title 35 of the United States Code.

13  
14 5. This Court has exclusive subject matter jurisdiction under 28 U.S.C.  
15 §§ 1331 and 1338(a).

16  
17 6. This Court has personal jurisdiction over Defendant because it has  
18 engaged in systematic and continuous business activities in this District and is  
19 incorporated in this District's state. As described below, Defendant has committed  
20 acts of patent infringement giving rise to this action within this District.

**VENUE**

21  
22  
23 7. Venue is proper in this District under 28 U.S.C. § 1400(b) because  
24 Defendant has an established place of business in this District. In addition,  
25 Defendant has committed acts of patent infringement in this District, and Plaintiff  
26 has suffered harm in this district.  
27  
28

**PATENTS-IN-SUIT**

1  
2 8. Plaintiff is the assignee of all right, title and interest in United States  
3 Patent Nos. 8,375,212; and 8,688,990 (the “Patents-in-Suit”); including all rights to  
4 enforce and prosecute actions for infringement and to collect damages for all  
5 relevant times against infringers of the Patents-in-Suit. Accordingly, Plaintiff  
6 possesses the exclusive right and standing to prosecute the present action for  
7 infringement of the Patents-in-Suit by Defendant.  
8  
9

**THE '212 PATENT**

10  
11 9. The '212 Patent is entitled “Method for personalizing an  
12 authentication token,” and issued 2013-02-12. The application leading to the '212  
13 Patent was filed on 2010-12-27. A true and correct copy of the '212 Patent is  
14 attached hereto as Exhibit 1 and incorporated herein by reference.  
15

**THE '990 PATENT**

16  
17 10. The '990 Patent is entitled “Method for personalizing an  
18 authentication token,” and issued 2014-04-01. The application leading to the '990  
19 Patent was filed on 2013-02-12. A true and correct copy of the '990 Patent is  
20 attached hereto as Exhibit 2 and incorporated herein by reference.  
21  
22

**COUNT 1: INFRINGEMENT OF THE '212 PATENT**

23  
24 11. Plaintiff incorporates the above paragraphs herein by reference.

25  
26 12. **Direct Infringement.** Defendant has been and continues to directly  
27 infringe one or more claims of the '212 Patent in at least this District by making,  
28

1 using, offering to sell, selling and/or importing, without limitation, at least the  
2 Defendant products identified in the charts incorporated into this Count below  
3 (among the “Exemplary Defendant Products”) that infringe at least the exemplary  
4 claims of the ’212 Patent also identified in the charts incorporated into this Count  
5 below (the “Exemplary ’212 Patent Claims”) literally or by the doctrine of  
6 equivalents. On information and belief, numerous other devices that infringe the  
7 claims of the ’212 Patent have been made, used, sold, imported, and offered for  
8 sale by Defendant and/or its customers.  
9

10  
11 13. Defendant also has and continues to directly infringe, literally or  
12 under the doctrine of equivalents, the Exemplary ’212 Patent Claims, by having its  
13 employees internally test and use these Exemplary Products.  
14

15 14. **Actual Knowledge of Infringement.** The service of this Complaint,  
16 in conjunction with the attached claim charts and references cited, constitutes  
17 actual knowledge of infringement as alleged here.  
18

19 15. Despite such actual knowledge, Defendant continues to make, use,  
20 test, sell, offer for sale, market, and/or import into the United States, products that  
21 infringe the ’212 Patent. On information and belief, Defendant has also continued  
22 to sell the Exemplary Defendant Products and distribute product literature and  
23 website materials inducing end users and others to use its products in the  
24 customary and intended manner that infringes the ’212 Patent. See Exhibit 3  
25  
26  
27  
28

1 (extensively referencing these materials to demonstrate how they direct end users  
2 to commit patent infringement).

3           16. **Induced Infringement.** At least since being served by this Complaint  
4 and corresponding claim charts, Defendant has actively, knowingly, and  
5 intentionally continued to induce infringement of the '212 Patent, literally or by the  
6 doctrine of equivalents, by selling Exemplary Defendant Products to their  
7 customers for use in end-user products in a manner that infringes one or more  
8 claims of the '212 Patent.  
9

10  
11           17. Exhibit 3 includes charts comparing the Exemplary '212 Patent  
12 Claims to the Exemplary Defendant Products. As set forth in these charts, the  
13 Exemplary Defendant Products practice the technology claimed by the '212 Patent.  
14 Accordingly, the Exemplary Defendant Products incorporated in these charts  
15 satisfy all elements of the Exemplary '212 Patent Claims.  
16  
17

18           18. Plaintiff therefore incorporates by reference in its allegations herein  
19 the claim charts of Exhibit 3.  
20

21           19. Plaintiff is entitled to recover damages adequate to compensate for  
22 Defendant's infringement.  
23

24                           **COUNT 2: INFRINGEMENT OF THE '990 PATENT**

25           20. Plaintiff incorporates the above paragraphs herein by reference.  
26  
27  
28

1           21. **Direct Infringement.** Defendant has been and continues to directly  
2 infringe one or more claims of the '990 Patent in at least this District by making,  
3 using, offering to sell, selling and/or importing, without limitation, at least the  
4 Defendant products identified in the charts incorporated into this Court below  
5 (among the "Exemplary Defendant Products") that infringe at least the exemplary  
6 claims of the '990 Patent also identified in the charts incorporated into this Court  
7 below (the "Exemplary '990 Patent Claims") literally or by the doctrine of  
8 equivalents. On information and belief, numerous other devices that infringe the  
9 claims of the '990 Patent have been made, used, sold, imported, and offered for  
10 sale by Defendant and/or its customers.

11           22. Defendant also has and continues to directly infringe, literally or  
12 under the doctrine of equivalents, the Exemplary '990 Patent Claims, by having its  
13 employees internally test and use these Exemplary Products.

14           23. **Actual Knowledge of Infringement.** The service of this Complaint,  
15 in conjunction with the attached claim charts and references cited, constitutes  
16 actual knowledge of infringement as alleged here.

17           24. Despite such actual knowledge, Defendant continues to make, use,  
18 test, sell, offer for sale, market, and/or import into the United States, products that  
19 infringe the '990 Patent. On information and belief, Defendant has also continued  
20 to sell the Exemplary Defendant Products and distribute product literature and  
21

1 website materials inducing end users and others to use its products in the  
2 customary and intended manner that infringes the '990 Patent. See Exhibit 4  
3 (extensively referencing these materials to demonstrate how they direct end users  
4 to commit patent infringement).  
5

6       **25. Induced Infringement.** At least since being served by this Complaint  
7 and corresponding claim charts, Defendant has actively, knowingly, and  
8 intentionally continued to induce infringement of the '990 Patent, literally or by the  
9 doctrine of equivalents, by selling Exemplary Defendant Products to their  
10 customers for use in end-user products in a manner that infringes one or more  
11 claims of the '990 Patent.  
12  
13

14       26. Exhibit 4 includes charts comparing the Exemplary '990 Patent  
15 Claims to the Exemplary Defendant Products. As set forth in these charts, the  
16 Exemplary Defendant Products practice the technology claimed by the '990 Patent.  
17 Accordingly, the Exemplary Defendant Products incorporated in these charts  
18 satisfy all elements of the Exemplary '990 Patent Claims.  
19  
20

21       27. Plaintiff therefore incorporates by reference in its allegations herein  
22 the claim charts of Exhibit 4.  
23

24       28. Plaintiff is entitled to recover damages adequate to compensate for  
25 Defendant's infringement.  
26  
27  
28

**JURY DEMAND**

29. Under Rule 38(b) of the Federal Rules of Civil Procedure, Plaintiff respectfully requests a trial by jury on all issues so triable.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff respectfully requests the following relief:

- A. A judgment that the '212 Patent is valid and enforceable
- B. A judgment that Defendant has infringed directly and indirectly one or more claims of the '212 Patent;
- C. A judgment that the '990 Patent is valid and enforceable
- D. A judgment that Defendant has infringed directly and indirectly one or more claims of the '990 Patent;
- E. An accounting of all damages not presented at trial;
- F. A judgment that awards Plaintiff all appropriate damages under 35 U.S.C. § 284 for Defendant's continuing or future infringement, up until the date such judgment is entered with respect to the '212; and '990 Patents, including pre- or post-judgment interest, costs, and disbursements as justified under 35 U.S.C. § 284;
- G. And, if necessary, to adequately compensate Plaintiff for Defendant's infringement, an accounting:



- i. that this case be declared exceptional within the meaning of 35 U.S.C. § 285 and that Plaintiff be awarded its reasonable attorneys' fees against Defendant that it incurs in prosecuting this action;
- ii. that Plaintiff be awarded costs, and expenses that it incurs in prosecuting this action; and
- iii. that Plaintiff be awarded such further relief at law or in equity as the Court deems just and proper.

Dated: March 8, 2022

Respectfully submitted,

/s/ Michael J. Glenn, SBN 89654  
Michael J. Glenn, SBN 89654  
LAW OFFICES OF JAMES M. DONOVAN  
915 Wilshire Blvd., Suite 1610  
Los Angeles, CA 90017-3474  
213-629-4861  
mglenn@thedonovanoffices.com

Howard L. Wernow (*Pro hac vice* forthcoming)  
Sand, Sebolt & Wernow Co., LPA  
Aegis Tower – Suite 1100  
4940 Munson Street NW  
Canton, OH 44718-3684  
330-244-1174  
howard.wernow@sswip.com

**Counsel for Plaintiff**  
**Auth Token LLC**

# Exhibit 1



US008375212B2

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

(10) **Patent No.:** **US 8,375,212 B2**  
(45) **Date of Patent:** **Feb. 12, 2013**

(54) **METHOD FOR PERSONALIZING AN AUTHENTICATION TOKEN**

(75) Inventors: **Peter Buck**, London (GB); **Peter Newport**, London (GB)

(73) Assignee: **Prism Technologies LLC**, Omaha, NE (US)

(\*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

4,800,590	A	1/1989	Vaughan
5,060,263	A	10/1991	Bosen et al.
5,200,999	A	4/1993	Matyas et al.
5,317,636	A	5/1994	Vizcaino
5,343,529	A	8/1994	Goldfine et al.
5,577,121	A *	11/1996	Davis et al. .... 705/67
5,586,260	A	12/1996	Hu
5,592,553	A	1/1997	Guski et al.
5,638,444	A	6/1997	Chou et al.
5,657,388	A	8/1997	Weiss
5,699,528	A	12/1997	Hogan
5,737,421	A	4/1998	Audebert
5,745,571	A	4/1998	Zuk
5,802,176	A	9/1998	Audebert
5,887,065	A	3/1999	Audebert
5,903,721	A	5/1999	Sixtus
5,913,203	A	6/1999	Wong et al.

(21) Appl. No.: **12/978,754**

(22) Filed: **Dec. 27, 2010**

(65) **Prior Publication Data**  
US 2011/0093708 A1 Apr. 21, 2011

**Related U.S. Application Data**

(62) Division of application No. 10/176,974, filed on Jun. 20, 2002, now Pat. No. 7,865,738.

(30) **Foreign Application Priority Data**  
May 10, 2002 (GB) ..... 0210692.0

(51) **Int. Cl.**  
**H04L 9/32** (2006.01)

(52) **U.S. Cl.** ..... **713/173; 705/66**

(58) **Field of Classification Search** ..... **713/168-173, 713/181-184; 705/65-67; 726/9, 10, 20; 235/380, 382; 340/5.81, 5.85**

See application file for complete search history.

(56) **References Cited**

**U.S. PATENT DOCUMENTS**

3,764,742 A 10/1973 Abbott et al.  
4,605,820 A 8/1986 Campbell, Jr.  
4,697,072 A 9/1987 Kawana

**FOREIGN PATENT DOCUMENTS**

EP 0 174 016 3/1986  
EP 1 028 401 8/2000

(Continued)

**OTHER PUBLICATIONS**

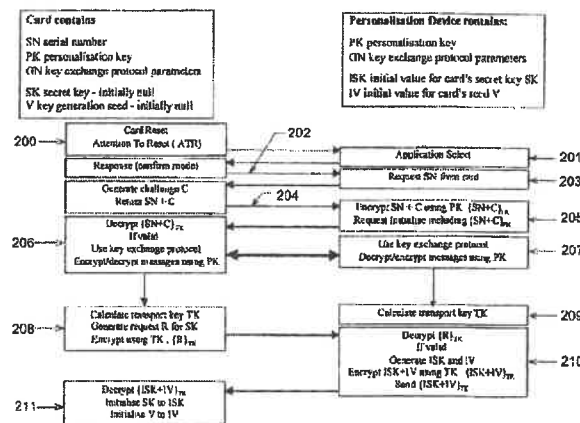
"The SecurID Mechanism," Nystrom at al., Jan. 1999.

*Primary Examiner* — Nirav B Patel  
(74) *Attorney, Agent, or Firm* — Martin & Ferraro, LLP

(57) **ABSTRACT**

An authentication token using a smart card that an organization would issue to its customer, the smart card having a processor for executing a software application that is responsive to a user input to generate a one-time password as an output. The smart card co-operates with an interface device for inputting the user input and displaying the one-time password. The authentication token may be used in combination with a remote authentication server for validation of the password and hence authentication of the user.

**4 Claims, 3 Drawing Sheets**



**US 8,375,212 B2**

Page 2

U.S. PATENT DOCUMENTS

5,937,068 A 8/1999 Audebert  
 5,937,394 A 8/1999 Wong et al.  
 5,956,699 A 9/1999 Wong et al.  
 5,963,915 A 10/1999 Kirsch  
 5,987,232 A 11/1999 Tabuki  
 6,000,832 A 12/1999 Franklin et al.  
 6,067,621 A 5/2000 Yu et al.  
 6,088,450 A \* 7/2000 Davis et al. .... 713/182  
 6,148,404 A 11/2000 Yatsukawa  
 6,163,771 A 12/2000 Walker et al.  
 6,168,077 B1 1/2001 Gray et al.  
 6,194,991 B1 2/2001 Barrs et al.  
 6,230,267 B1 \* 5/2001 Richards et al. .... 713/172  
 6,377,994 B1 4/2002 Ault et al.  
 6,385,723 B1 \* 5/2002 Richards ..... 713/160  
 6,434,561 B1 8/2002 Durst et al.  
 6,442,690 B1 8/2002 Howard et al.  
 6,751,733 B1 6/2004 Nakamura et al.  
 6,757,825 B1 \* 6/2004 MacKenzie et al. .... 713/169  
 6,785,661 B1 8/2004 Mandler et al.  
 6,904,526 B1 \* 6/2005 Hongwei ..... 713/182  
 6,904,626 B1 6/2005 Hongwei

6,910,131 B1 \* 6/2005 Yamada et al. .... 713/186  
 6,940,980 B2 \* 9/2005 Sandhu et al. .... 380/282  
 7,007,050 B2 2/2006 Saarinen  
 7,080,078 B1 7/2006 Slaughter et al.  
 7,281,128 B2 \* 10/2007 Mikel et al. .... 713/155  
 7,386,878 B2 \* 6/2008 Fernando et al. .... 726/3  
 7,430,668 B1 \* 9/2008 Chen et al. .... 713/187  
 7,865,738 B2 1/2011 Buck et al.  
 2001/0047335 A1 11/2001 Arndt et al.  
 2001/0054148 A1 12/2001 Hoomaert et al.  
 2002/0002678 A1 1/2002 Chow et al.  
 2002/0010863 A1 1/2002 Mankefors  
 2002/0046169 A1 4/2002 Keresman, III et al.  
 2003/0112972 A1 6/2003 Hattick et al.  
 2004/0059952 A1 3/2004 Newport et al.

FOREIGN PATENT DOCUMENTS

GB 2 317 983 4/1998  
 GB 2 361 790 10/2001  
 WO WO 00/62214 10/2000  
 WO WO 01/26062 4/2001

\* cited by examiner

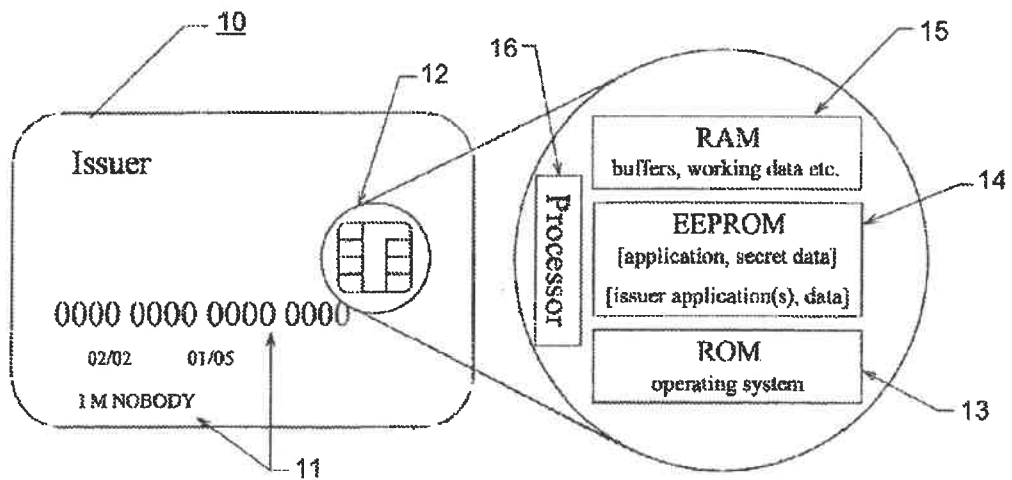


Figure 1

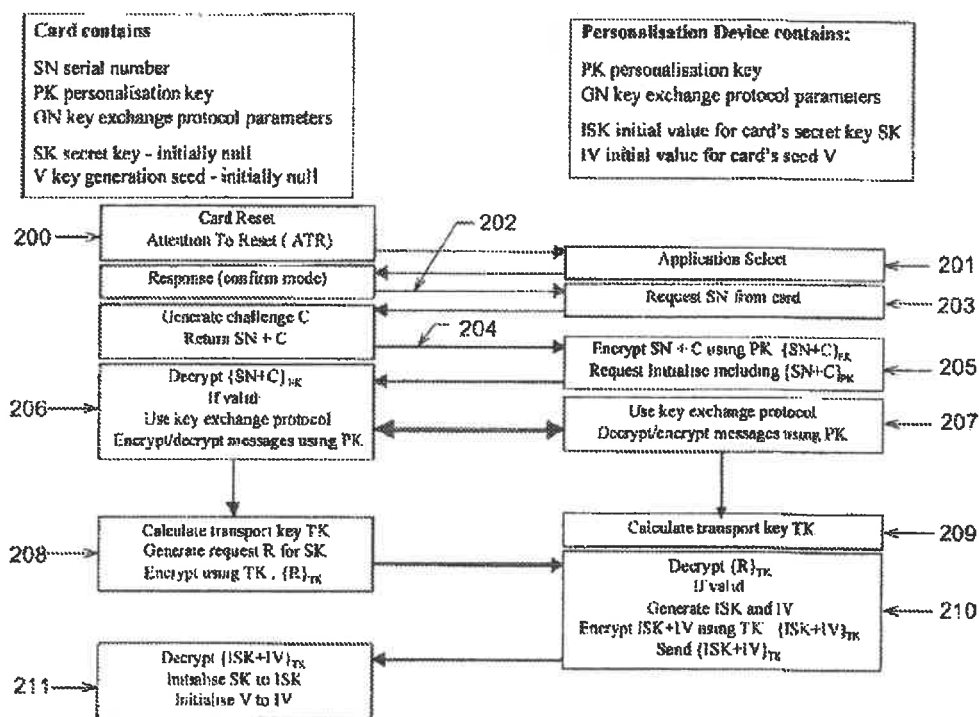


Figure 2

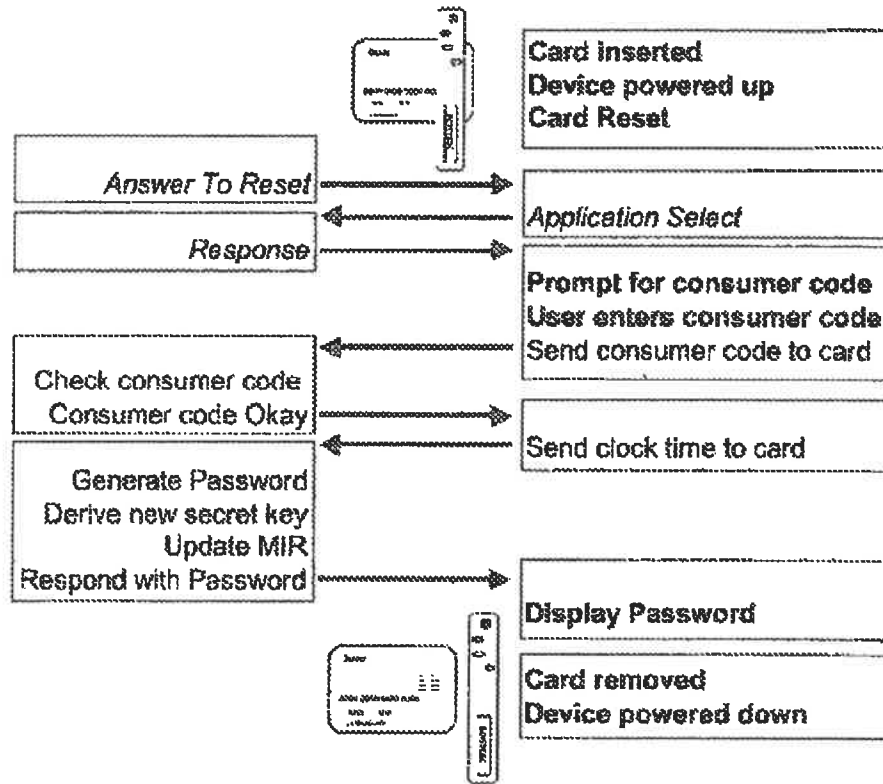


Figure 3

METHOD FOR PERSONALIZING AN AUTHENTICATION TOKEN

The present application is a divisional of U.S. application Ser. No. 10/176,974, filed Jun. 20, 2002 (U.S. Pat. No. 7,865, 738); which claims priority to Great Britain Patent Application No. 0210692.0, filed May 10, 2002; all of which are incorporated by reference herein.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to an authentication token using a smart card.

2. Description of the Prior Art

There are a variety of technologies available to authenticate remote users in order to enforce secure access control. These range from simple, single factor authentication (such as use of a password) to multiple factor authentication (such as use of a physical token in conjunction with a Personal Identification Number (PIN)). It is widely accepted that single factor authentication offers limited assurance as it is vulnerable to a wide range of attacks, many of which are neither sophisticated nor expensive to mount (such as 'shoulder surfing' or eavesdropping). Most online services, however, still rely on single factor authentication because it appears to be the cheapest to implement—although this is usually because the subsequent cost of dealing with systematic attacks has not been considered.

Dual factor authentication systems are, however, widely used to protect remote access by support staff to these same online services. Many organisations also protect access to their critical corporate systems, both remotely and locally, using such authentication mechanisms. The essence of a dual factor mechanism is that it requires both 'something you know', for example, a PIN or passcode, and 'something you have', for example a physical token that can be authenticated itself. Increasingly, research is being done to add a third type of factor, 'something you are' i.e. biometrics such as retina scan, iris scan or fingerprint, but this is not yet available in a reliable cost-effective way that can be used reliably in a mass-market type environment.

There are a variety of tokens available that can fulfil the role of the second factor ('something you have'), but many of them rely on an infrastructure of interface devices to be able to authenticate them. Thus, use of a smart card requires a card reader to be available to enable the system to interact with the application resident on the smart card. New form factors have been explored to reduce this reliance, such as Universal Serial Bus (USB) tokens that can plug directly into a USB port on a computer. Many new PCs are being shipped with USB ports instead of the older style serial ports or parallel ports, most notebook computers now only have USB ports and all Apple computers have had easily accessible USB ports since the launch of the iMac in 1998.

To remove the dependence on an external infrastructure and to enable the token to be used in as wide a range of channels as possible, a number of manufacturers have developed stand-alone tokens that do not need to be connected to the remote computer system. They interact with the user via a screen and keypad. The user then interacts with the remote system through whatever channel they are using i.e. web, Wireless Application Protocol (WAP) phone, voice, TV set-top box.

Stand-alone tokens generally offer one or more mechanisms by which they can authenticate themselves to the remote system. One approach is for the system to issue a

'challenge' to be entered into the token, for example an apparently meaningless string of numbers. The token applies a cryptographic process, using the challenge and other information that is kept secret inside the token. As a result, it generates a 'response', which is displayed to the user to be sent back to the remote system. The remote system can check that the response received is the correct response from that token to the challenge sent and hence ascertain the authenticity or otherwise of the token. This process may use a symmetric cryptographic process with keys that are shared between the token and the remote system. Alternatively, it may use an asymmetric cryptographic process, removing the need for shared secret keys but requiring significantly more processing capability in the token. In most cases, the remote system does not generate the challenge and authenticate the token's response itself but uses a dedicated local authentication server which is especially established for that purpose and can provide the facility to multiple systems within the same organisation.

There is a variant on this approach where the challenge is generated internally to the token, based on a combination of static data, deterministically varying data (such as an event counter), and dynamic data (such as time). The authentication server must be maintained in synchronisation with the token so that it can reproduce the same challenge when it attempts to validate the response.

An alternative approach has been to use a modern version of the old tried and tested method of having a series of passwords each of which can only be used once. This approach was used by the military for many years, supplying a pad of slips of paper, each of which had a one-time password printed on it. As each password was used it was ripped from the pad and discarded. A matching pad was maintained at the other end to enable messages to be validated. The modern approach is to use a cryptographic process to generate a one-time password dynamically when it is needed. The token and the authentication server share secret information that can be combined with dynamic information available to both (for real-time systems this can be the time) enabling the authentication server to be able to generate the same one-time password that the token has generated and thus validate it. This mechanism uses a symmetric cryptographic process, which enables it to be carried out quickly and cost-effectively in the token. It does not require as much processing at the authentication server as no challenge needs to be generated at the outset, hence only a single interaction is needed between the protected system and the authentication server to authenticate the user.

Smart cards are in use worldwide for a variety of purposes. They have long been in use for financial products (credit, debit and loyalty cards), especially in France where they were invented. With the advent of GSM mobile phones, the smart card market has significantly increased with the need for Subscriber Identification Modules (SIMs). The technology used on smart cards lags leading edge semiconductor technology by 2 or 3 years, thus the speed and power of the processors are relatively low and memory is restricted. As more ambitious uses are devised for smart cards, the technology required is becoming more complex and hence the cost of the cards is increasing. Conversely, the increasing size of the market has led to economies of scale in the most widely used technologies (such as those required for GSM SIMs or memory chips as used in digital cameras and MP3 players).

Asymmetric cryptographic functions are heavily processor intensive and hence significantly slower than symmetric functions (of the order of 100 times slower). The limited processing capability of most smart card chips has restricted



US 8,375,212 B2

3

their practical use to symmetric cryptographic functions. However, smart card chips are now available with cryptographic co-processors that can execute asymmetric cryptographic functions much more quickly enabling such functions to become a practical option. The newest versions of specifications such as EMV (credit/debit card functionality defined jointly by Europay/Mastercard/Visa) take advantage of these improved capabilities to provide better security features.

Most smart cards have in the past been produced with a specific single application hardwired into Read Only Memory (ROM). International standards (specifically ISO 7816) have established common specifications for smart cards, ranging from size and shape and where the contacts should be, through the electrical characteristics, to the basic communications protocol to interact with the card and the underlying filing system structure that should be implemented on it. Some manufacturers have produced simple proprietary operating systems to handle all the standard activities (like the interface protocol) on behalf of the applications. However, the smart card still has to be hardwired at manufacture with the operating system software and the application software in the ROM. The standards allow for the application software on the card to offer multiple separate 'applications' (such as a credit card, loyalty card and electronic purse) selectable by the interface device with which the card is used. The required application is selected when the card is powered up and 'reset' by the interface device and the appropriate interaction is then conducted with the card. However, these separate applications must all reside together in the smart card's ROM and share the same data areas. Accordingly, they must all trust each other to ensure that the data for one is not read or overwritten by another. Generally, therefore, such cards will only have separate applications that have all been developed by (or for) the same organisation that is issuing the card.

To address these shortcomings, some multi-application smart card operating systems have been developed. These require only the operating system to be hardwired into the smart card's ROM. Applications can be loaded into the card's Electrically Erasable Programmable Read Only Memory (EEPROM) after manufacture. Indeed, they can be subsequently removed or replaced allowing upgraded applications to be delivered onto the smart cards even after they have been issued to end users. To ensure that the applications can not interfere with each other, the applications themselves are written in an interpreted language (such as Java) and the actual execution is under the control of the card's operating system, thus allowing address range checking and other mechanisms to be used to isolate each application and its data. The initial cost of using such cards has led to a slow take up of the technology, but increasing capability of the card processors and larger memory is increasing their practical applicability. New GSM SIMs will be available on multi-application cards, allowing service operators to offer customisable functionality on the SIM independent of the particular phone in use, including value-added services.

The Applicant offers a remote authentication service under the name QUIZID to enable users of a protected computer system (internal users or external customers) to be securely authenticated before being allowed access to the protected system. The current authentication mechanism relies on a device (which must be 'personalised' and securely delivered to the user) that generates one-time passwords; use of the device itself is secured by the use of a colour-coded unique consumer code that must be entered by the user in order to obtain a password. The password and a user ID, entered into

4

the protected system, are sent to QUIZID for validation and if a successful response is received the system can allow access to the user. A more detailed description of this can be found in PCT/GB01/05507. How the QUIZID service is used in relation to other identifying information such as account names or user identification is up to the designers of the protected system. The QUIZID service is designed to be used for protecting access to corporate systems as well as publicly accessible systems such as e-tailers or financial services.

SUMMARY OF THE INVENTION

The present invention provides a design for a remote authentication token using a smart card that an organisation would issue to its customer, along with an interface device to display the one-time password. In a preferred implementation, the invention is used in combination with a remote authentication server for validation of the password and is thus interoperable with the current QUIZID service.

As described above, many financial services are now issuing 'smart' credit or debit cards which have already been personalised and securely delivered to the customer. These same organisations are offering online services that need effective user authentication to protect access to customer data as required by legislation. Consequently, for authentication purposes, use of a smart card that has already been delivered to the customer is cost-effective and will help to reinforce both the organisation's brand and its commitment to security.

These and other objects of the present invention will be apparent from review of the following specification and the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Examples of the present invention will now be described in detail with reference to the accompanying drawings, in which:

FIG. 1 shows the distribution of components across the memory of a multi-application smart card;

FIG. 2 shows the interaction between a smart card and a personalisation device; and,

FIG. 3 shows the interaction between a smart card, an interface device and a user.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

With reference to FIGS. 1 to 3 generally, we now describe the proposed token, including the components of the token, namely the smart card itself and the interface device. We also describe the operation of the token, including the end-user interaction with the token in normal use, the operation of the various components and the interaction between them, and the handling of error conditions. The remote authentication token proposed here combines the functionality of authentication technology, including that provided by the existing QUIZID remote authentication service (described in more detail in PCT/GB01/05507), with the convenience of smart card technology. This type of technology is either already in use or about to be launched by many organisations, especially in the financial services sector.

FIG. 1 shows an example of a smart card 10, which in common with many types of payment card displays account and issuer information 11, and also contains a microchip 12. The chip 12 comprises various types of on board memory, including ROM 13, EEPROM 14 and RAM 15, and also a

US 8,375,212 B2

5

processor 16. Thus, not only can information be stored on the card, but also an application can be loaded onto the card issued by an organisation to an end-user, for example a credit card with the EMV application. The card has already been personalised for the end-user by the issuer and has been delivered to them by some secure means.

The smart card also contains the authentication application itself. This includes the secret data that is used to generate the passwords and the colour coded unique consumer code. Since the issuing organisation will already be incurring the costs associated with issuing the smart card the additional costs to include the authentication application would be relatively low. The smart card may also contain one or more of the issuer's applications.

The authentication application may be loaded onto the card in one of two ways, depending on the type of smart card.

A 'single application' smart card will have the application and a limited operating system 'burnt' into the ROM 13 at chip manufacture. In this case a version of the authentication application will have been developed in the appropriate language for the card's processor (which may be assembler or a higher level language depending on the chip and tool support). This version of the authentication application will be supplied to the issuer for examination and integration into the ROM mask to be hardwired into the card's chip 12. It may also be combined with the issuer's application(s) prior to manufacture to make the ROM mask. Cards with the application already in the ROM 13 are delivered to the issuer. The card itself is then personalised by the issuer (embossing etc.) and the authentication application is personalised using a specific personalisation device.

If the card is a multi-application card, the operating system will be 'burnt' into the ROM 13 at chip manufacture. The authentication application and any issuer applications will be subsequently loaded onto card. Cards containing only the operating system are delivered to the issuer. The issuer's applications are loaded onto the card through an interaction with the operating system. A version of the authentication application will have been developed in the appropriate language for the card's operating system (such as Java for Javacard or MEL for Multos) and then signed and certified. This version can be loaded at the same time, separately or even subsequently, for example during personalisation by the issuer. Once the authentication application has been loaded it is personalised using a specific personalisation device. Although the multi-application operating systems allow for the loading and personalisation of the authentication application after the card has been issued, in the preferred embodiment it is not intended to issue cards prior to establishing the authentication application on them.

As indicated, whichever type of smart card 10 is used, the application will be personalised to ensure the correct secret data is in the card's EEPROM 14 along with an initial colour coded unique consumer code. Until the application is personalised it cannot be used. Once personalised it cannot be re-personalised. In the following embodiment, the application, once personalised will contain the following elements:

- a secret key (SK) stored in EEPROM, used by the cryptographic algorithm to generate passwords;
- a unique consumer code stored in EEPROM, used to validate the code entered by the user;
- a monotonically increasing register (MIR) stored in EEPROM, used by the cryptographic algorithm to generate passwords;
- a seed value (V) stored in EEPROM, used by the key generation algorithm; and,

6

application software to respond to application commands, generate a password and generate a new key.

The application that is loaded onto the smart card operates in three modes. Each mode allows a different limited range of interactions. When the application is first loaded it is in Personalisation mode. In this mode it will respond only to a personalisation command. After personalisation the application is in Normal mode. In this mode it will interact with an interface device to generate passwords when presented with a valid colour coded unique consumer code. If the incorrect unique consumer code is entered in sequential attempts (beyond a pre-set limit) the application enters Locked mode. In this mode the application will only accept (a limited number of) attempts to enter the correct unlock code. If the correct unlock code is entered, the application reverts to Normal mode. The application can never be returned to Personalisation mode.

When the application is loaded onto the smart card it is in a non-personalised state. The secret data has been set to starting values, but the unique key for the card has not been set. The card itself does, however, have a unique serial number. The application is in Personalisation mode. It will not accept any commands from a user's interface device in this mode. It will, however, accept a personalisation command from a personalisation device. The personalisation device requests the serial number, and establishes a private communications channel with the application to enable it to issue the application with seed values for the secret key and the key generation algorithm. The same data is stored securely by the personalisation device for subsequent loading into the authentication server. The card serial number can be used to determine the username that the issuer will associate with the card. Once the seed has been used by the application to set the initial secret key, the application switches to Normal mode.

While there are a variety of suitable mechanisms to secure the communications between the personalisation device and the application, the preferred implementation is to use a key exchange protocol to establish a transport key, supplemented by a pre-defined personalisation key to protect against 'man in the middle' attacks. This is necessary because, although the card may be personalised at the same time that it is loaded with the application, in a multi-application card environment this may be subsequent to the manufacture or issuer personalisation of the card. It may even be performed remotely from the personalisation device, which could be at (or incorporated into) the authentication server, and must therefore be protected against interception.

An example of a personalisation interaction is illustrated in FIG. 2 and the steps involved are described below:

- initially, the card is reset (step 200) and responds with an Attention to Reset (ATR).
- the personalisation device selects (step 201) the authentication application and determines (step 202) that it is in personalisation mode.
- the personalisation device requests (step 203) the card serial number and receives (step 204) the serial number (SN) and a challenge (C) from the card application.
- using the pre-defined Personalisation Key (PK) the personalisation device encrypts (step 205) SN and C and returns the encrypted value to the card in a request to commence initialisation.
- the card application decrypts (step 206) the received data using PK and validates it as correct. This demonstrates that both the card application and the personalisation device are using the correct PK.
- if successful, the card application uses (step 206) the key exchange protocol to generate messages to send back to

the personalisation device. The key exchange protocol itself is inherently protected against interception, but the messages are also encrypted (step 206) using PK to protect against 'man in the middle' attacks.

the personalisation device responds (step 207) with the appropriate key exchange protocol messages, encrypted using PK.

at the end of the key exchange, both the card application (step 208) and the personalisation device (step 209) have a unique shared key that is unknown to anyone else including eavesdroppers. This key is used as a Transport Key (TK) for the rest of the personalisation process.

the card application generates a request (step 208) (R) for its Secret Key (SK), encrypts (step 208) the request using TK and sends it to the personalisation device.

the personalisation device decrypts (step 210) the request using TK and validates it as correct. This demonstrates that both the card application and the personalisation device are using the same TK and hence that the key exchange process has worked correctly.

if successful, the personalisation device generates (step 210), or obtains from a pre-generated list, the Initial Secret Key (ISK) and the Initial Value (IV) for the card application's key generation seed (V). ISK and IV are encrypted (step 210) using TK and sent to the card.

the card application decrypts (step 211) the received data using TK, initialises (step 211) its SK to ISK and initialises (step 211) its V to IV. The card application now enters Normal mode.

the personalisation device delivers (step 210) the ISK and IV to the authentication server (if they were not pre-generated and hence already in the authentication server) securely.

Although there may be a number of suitable key exchange protocols available, the preferred implementation is to use the Diffie-Hellman exchange which is within the processing capabilities of the card and does not rely on out of band secure communications to pre-establish any shared secret. The Diffie-Hellman exchange operates as follows:

the card application and personalisation device both know the pre-defined values 'n' (a large prime number) and 'g' (a small single digit number that is primitive mod n). These don't need to be kept secret and can be common to all cards, therefore are included in the application that is loaded onto the card;

the card application generates a large random integer 'x';

the card application calculates  $A=g.\text{sup}.x \text{ mod } n$ ;

the card application sends A to the personalisation device;

the personalisation device generates a large random integer 'y';

the personalisation device calculates  $P=g.\text{sup}.Y \text{ mod } n$ ;

the personalisation device send P to the card application;

the card application calculates  $K1=P.\text{sup}.x \text{ mod } n$ ;

the personalisation device calculates  $K2=A.\text{sup}.y \text{ mod } n$ ;

and,

both K1 and K2 are equal to  $g.\text{sup}.xy \text{ mod } n$  and hence the card application and the personalisation device have calculated the same key which can now be used as the Transport Key (TK).

The second main component of the authentication token is the interface device provided to the end-user. The interface device is a device that can be used with a user's smart card to enable the generation of a password. The device could take a variety of forms, for example a pen or a calculator or a mobile phone battery pack. When the smart card is inserted into the interface device, the user is prompted to enter their colour coded unique consumer code and, if correct, the output

response from the interface device is a one-time password. A password so generated can then be entered into the access device, such as a PC, a telephone, a WAP phone, or even by voice, for the service that requires the authentication.

As the smart card is personalised to the customer, the interface device does not need to be. Users, therefore, can share an interface device, for example one at home for use by all members of a family. Equally, users can have more than one, for example one at home, one in the office. Users can even, safely, borrow an interface device from a stranger, for example in a cybercaf or a restaurant. Therefore, in one embodiment, the interface devices are preferably generic, hence all identical and requiring no personalisation for each customer. As they do not need to be personalisable or securely delivered to users (they could even be available over the counter if the issuing organisation has a branch network), it should be possible to keep the associated cost significantly low.

The interface device provides the power to the smart card to enable it to operate. It also includes a real-time clock to enable time to be used as a dynamic input into the password generation process. It therefore includes a battery, which has a reasonably long life but is not accessible by the user. After manufacture, the device's clock can be synchronised with the service's system-wide time through the smart card interface. When battery replacement is required, the device's clock must once again be synchronised (which is why the battery is not user-replaceable). When no smart card is inserted in the slot, the device only provides power to the real-time clock. When a smart card is inserted, the device powers up and applies power to the smart card and to itself. When the smart card is removed the device powers down. For this reason, the device needs no user accessible power switch.

Although the interface device may take one of many forms, it will typically include the following five elements:

- i. an interface to the token, initially a set of smart card contacts, but other interfaces would be possible, such as Bluetooth;
- ii. an input mechanism, such as a keypad for entry of the colour coded unique consumer code and for menu selection;
- iii. an output mechanism, such as a display screen, although other mechanisms could be provided such as voice output for the blind;
- iv. a source of a dynamic input to the password generation, such as a battery operated real-time clock; and,
- v. a processor with application software to handle the interfaces.

Once the user has received the smart card and an interface device they can use the combination to authenticate themselves to the issuer's services, as and when required. The authentication is assured either by an authentication server operated by the issuer themselves or by a shared authentication server such as described in PCT/GB01/05507.

There are many different business models within which strong authentication would be advantageous. An example is given below of a typical interaction, where the issuer provides an online e-commerce service requiring the users to authenticate themselves when they place an order.

1. User browses issuer's online service on their PC.
2. User places order on service.
3. Service prompts user for authentication password in secure form.
4. User inserts smart card into an interface device.
5. Interface device prompts for colour coded unique consumer code entry.

US 8,375,212 B2

9

- 6. User enters colour coded unique consumer code into the interface device.
- 7. Interface device displays password.
- 8. User enters password into secure form on issuer's online service on their PC.
- 9. Service authenticates password with remote authentication service.
- 10. Service confirms authentication to user, accepts order.
- 11. User removes the smart card from the interface device.

When the smart card is issued to the user, the application will have been personalised and will be in Normal mode. The user can then use a generic interface device to change the colour coded unique consumer code from the pre-set initial value to one of their own choice. The card will now be able to interact with a generic interface device to generate a password. An example of this type of interaction is shown in FIG. 3.

The process used to generate the one-time password relies on the use of a secret key (SK) in conjunction with a tried and tested cryptographic algorithm. The data that is processed by the algorithm to generate the password is derived from a Monotonically Increasing Register (MIR) that is maintained within the card application and tracked at the authentication server, along with a Dynamic Variable (DV) that can be validated or reproduced at the authentication server. To increase the variability of the passwords and the difficulty of an attempt to spoof the password generation, the secret key is itself modified after each password generation using a key generation algorithm. The authentication server must apply the same algorithms to validate the password and keep in synchronisation with the MIR, SK and V on the card.

The process for password generation is as follows:

the MIR is concatenated with the DV to produce a payload (L);

L is encrypted using the cryptographic algorithm with SK to produce G;

the least significant bits of G are used to generate an integer I;

the least 2 significant bits of DV, concatenated with the least significant bit of MIR, are used to generate an integer D;

I is combined with D to produce the password;

the key generation algorithm uses MIR and SK and a seed V to generate a new key NK and a new seed NV;

SK is replaced with NK;

V is replaced with NV; and

MIR is incremented.

The inclusion of the 3 bits that are used to create D, enables the authentication server to detect loss of synchronisation with the application on the card. The authentication server will be maintaining its own copy of the MIR for each card. When the password arrives to be validated at the authentication server, the least significant bit of the MIR on the card, as included in the password via D, should match that of the MIR in the server. If not, there may have been a previous password generated that did not arrive at the server, in which case the server increments the MIR and executes the key generation algorithm to obtain the appropriate SK. Similarly, the 2 least significant bits of the DV included in the password via D can be compared with those of the DV reproduced at the authentication server, allowing for a discrepancy to be detected and corrected before the password is validated. Parameters can be established at the authentication server to determine whether (and how many) subsequent values of the MIR should be tried if the validation fails.

The combination of I and D can be achieved in a variety of ways. The 3 bits of D can be interspersed at pre-determined

10

positions in I, the resulting value then being interpreted as a decimal value. Any length password can be generated by selecting the appropriate number of bits of the output of the cryptographic algorithm, for example an eight digit password would be produced from a 26 bit value composed of the 3 bits of D and 23 bits of I. Alternatively, I can be interpreted as a decimal value (the length depending on the number of bits used) and D interpreted as a decimal value (one digit in length as only 3 bits are used). The resulting password would be created by concatenating the digits derived from I with the digit derived from D (or inserting the digit from D into the digits from I). Again, any length password can be generated by selecting the appropriate number of bits of the output of the cryptographic algorithm. An eight digit password would require 23 bits to be used to produce I which would be 7 digits long, with D providing the eighth digit. In the preferred embodiment, an eight digit password will be generated by interpreting 23 bits of the cryptogram as a 7 digit decimal integer I and appending a decimal digit interpreted from the 3 bits of D.

The preferred implementation is to use the Advanced Encryption Standard (AES) with 128 bit keys as the cryptographic algorithm, along with a key generation algorithm based on ANSI X9.17 but using AES and generating 128 bit keys. One of the strengths of AES is that there are no known weak keys, so all keys generated by the key generation algorithm would be acceptable.

As each card must work with any one of the interface devices, the source of the DV in the initial embodiment will be a real-time clock in the interface device. In future embodiments, when the smart card may have its own source of power, there will be other sources of dynamic variable that could be maintained within the card itself.

The example shown in FIG. 3 illustrates the case where the user enters the unique consumer code correctly first time. If the unique consumer code entered is incorrect the application will respond 'code incorrect' and the interface device will re-prompt for the unique consumer code. This can happen repeatedly up to a preset limit, for example three attempts. If the unique consumer code has not been entered correctly within the limited number of attempts, the application will respond 'Locked' and the interface device will inform the user that the application is locked. The application will enter Locked mode.

When the application is in Locked mode it will not accept commands to generate a password. It will not respond to the normal interactions. When the interface device attempts to interact with the application, it is told (in the Answer To Reset) that the application is locked and informs the user that the application is locked. If the user then enters a sequence of colour codes the interface device will send them to the application as an unlock command. The correct sequence will cause the application to unlock and revert to Normal mode. To obtain the correct sequence the user will have to contact a customer support function. The unlock sequence will only work once. If the application is subsequently locked again a different unlock sequence will be required.

Other embodiments of the invention will be apparent to those skilled in the art from consideration of the specification and practice of the invention disclosed herein. It is intended that the specification and examples be considered as exemplary only, with a true scope and spirit of the invention being indicated by the following claims.

We claim:

- 1. A method for personalizing an authentication token comprising:

US 8,375,212 B2

11

entering by the authentication token into personalization mode;  
 requesting from the authentication token, by a personalization device in communication with the authentication token, a serial number of the authentication token;  
 5 encrypting by the personalization device the serial number using a personalization key, and forwarding the encrypted serial number to the authentication token from the personalization device;  
 decrypting by the authentication token of the encrypted serial number, and validating by the authentication token that the personalization key is correct;  
 10 establishing an encrypted session between the authentication token and the personalization device using a transport key;  
 sending to the authentication token, by the personalization device, an initial seed value and an initial secret key using the transport key to encrypt the initial seed value and the initial secret key, the initial seed value and the initial secret key for facilitating an initial interaction  
 20 between the authentication token and an interface device; and

12

storing by the authentication token the initial seed value and the initial secret key after decryption thereof by the authentication token using the transport key, wherein, once the authentication token is personalized with the initial seed value and the initial secret key, the authentication token can no longer enter the personalization mode.  
 2. The method of claim 1, wherein after the authentication token is provided the initial seed value and the initial secret key, the initial seed value stored in a memory in the authentication token can be used to generate a key for use in generating a secure password used in interacting with the interface device.  
 3. The method of claim 2, wherein data exchanged between  
 15 the authentication token and the personalization device for use in generating the secure password is stored by the personalization device for subsequent transfer to a third party.  
 4. The method of claim 2, further comprising entering by the authentication token into normal mode after said storing  
 20 the initial seed value and the initial secret key.

\* \* \* \* \*

# Exhibit 2



US008688990B2

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

(10) **Patent No.:** **US 8,688,990 B2**  
(45) **Date of Patent:** **\*Apr. 1, 2014**

- (54) **METHOD FOR PERSONALIZING AN AUTHENTICATION TOKEN**
- (71) Applicant: **Prism Technologies LLC**, Omaha, NE (US)
- (72) Inventors: **Peter Buck**, Dartford (GB); **Peter Newport**, Devonport (NZ)
- (73) Assignee: **Prism Technologies LLC**, Omaha, NE (US)
- (\* ) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.  
This patent is subject to a terminal disclaimer.

- (58) **Field of Classification Search**  
USPC ..... 713/172-173, 182-184; 726/9, 10, 20; 340/5.81, 5.85; 705/65-67  
See application file for complete search history.

(56) **References Cited**

**U.S. PATENT DOCUMENTS**

3,764,742	A	10/1973	Abbott et al.
4,605,820	A	8/1986	Campbell, Jr.
4,697,072	A	9/1987	Kawana
4,800,590	A	1/1989	Vaughan
5,060,263	A	10/1991	Bosen et al.
5,200,999	A	4/1993	Matyas et al.
5,317,636	A	5/1994	Vizzaino
5,343,529	A	8/1994	Goldfine et al.
5,577,121	A	* 11/1996	Davis et al. .... 705/67

(Continued)

**FOREIGN PATENT DOCUMENTS**

EP	0 174 016	3/1986
EP	1 028 401	8/2000

(Continued)

**OTHER PUBLICATIONS**

"The SecurID Mechanism," Nystrom et al., Jan. 1999.

*Primary Examiner* — Nirav B Patel

(74) *Attorney, Agent, or Firm* — Martin & Ferraro, LLP

(57) **ABSTRACT**

An authentication token using a smart card that an organization would issue to its customer, the smart card having a processor for executing a software application that is responsive to a user input to generate a one-time password as an output. The smart card co-operates with an interface device for inputting the user input and displaying the one-time password. The authentication token may be used in combination with a remote authentication server for validation of the password and hence authentication of the user.

**4 Claims, 3 Drawing Sheets**

- (21) Appl. No.: **13/765,351**
- (22) Filed: **Feb. 12, 2013**
- (65) **Prior Publication Data**  
US 2013/0159716 A1 Jun. 20, 2013

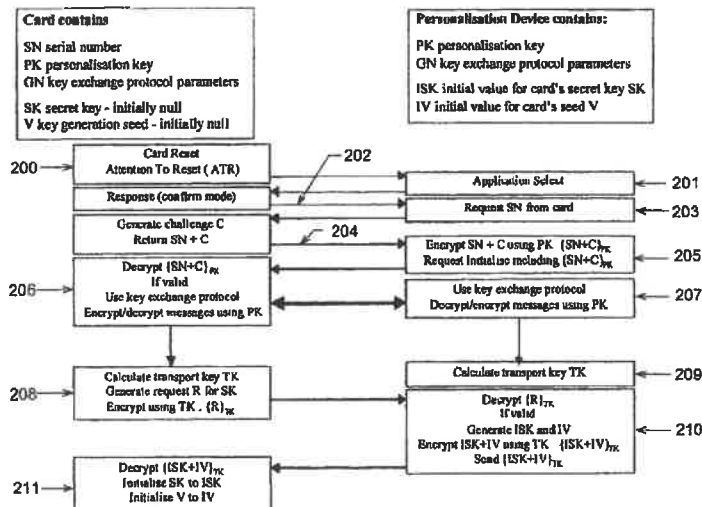
**Related U.S. Application Data**

- (60) Continuation of application No. 12/978,754, filed on Dec. 27, 2010, now Pat. No. 8,375,212, which is a division of application No. 10/176,974, filed on Jun. 20, 2002, now Pat. No. 7,865,738.

**Foreign Application Priority Data**

May 10, 2002 (GB) ..... 0210692.0

- (51) **Int. Cl.**  
**H04L 9/32** (2006.01)
- (52) **U.S. Cl.**  
USPC ..... 713/173; 705/66



**US 8,688,990 B2**

Page 2

(56)

**References Cited**

**U.S. PATENT DOCUMENTS**

5,586,260 A 12/1996 Hu  
 5,592,553 A 1/1997 Guski et al.  
 5,638,444 A 6/1997 Chou et al.  
 5,657,388 A 8/1997 Weiss  
 5,699,528 A 12/1997 Hogan  
 5,737,421 A 4/1998 Audebert  
 5,745,571 A 4/1998 Zuk  
 5,802,176 A 9/1998 Audebert  
 5,887,065 A 3/1999 Audebert  
 5,903,721 A 5/1999 Sixtus  
 5,913,203 A 6/1999 Wong et al.  
 5,937,068 A 8/1999 Audebert  
 5,937,394 A 8/1999 Wong et al.  
 5,956,699 A 9/1999 Wong et al.  
 5,963,915 A 10/1999 Kirsch  
 5,987,232 A 11/1999 Tabuki  
 6,000,832 A 12/1999 Franklin et al.  
 6,067,621 A 5/2000 Yu et al.  
 6,088,450 A \* 7/2000 Davis et al. .... 713/182  
 6,148,404 A 11/2000 Yatsukawa  
 6,163,771 A 12/2000 Walker et al.  
 6,168,077 B1 1/2001 Gray et al.  
 6,194,991 B1 2/2001 Barrs et al.  
 6,230,267 B1 5/2001 Richards et al.  
 6,377,994 B1 4/2002 Ault et al.  
 6,385,723 B1 5/2002 Richards  
 6,434,561 B1 8/2002 Durst et al.

6,442,690 B1 8/2002 Howard et al.  
 6,751,733 B1 6/2004 Nakamura et al.  
 6,757,825 B1 6/2004 MacKenzie et al.  
 6,785,661 B1 8/2004 Mandler et al.  
 6,904,526 B1 \* 6/2005 Hongwei ..... 713/182  
 6,910,131 B1 \* 6/2005 Yamada et al. .... 713/186  
 6,940,980 B2 9/2005 Sandhu et al.  
 7,007,050 B2 2/2006 Saarinen  
 7,080,078 B1 7/2006 Slaughter et al.  
 7,281,128 B2 \* 10/2007 Mikel et al. .... 713/155  
 7,386,878 B2 \* 6/2008 Fernando et al. .... 726/3  
 7,430,668 B1 \* 9/2008 Chen et al. .... 713/187  
 7,865,738 B2 \* 1/2011 Buck et al. .... 713/184  
 8,375,212 B2 2/2013 Buck et al.  
 2001/0047335 A1 11/2001 Arndt et al.  
 2001/0054148 A1 12/2001 Hoormaert et al.  
 2002/0002678 A1 1/2002 Chow et al.  
 2002/0010863 A1 1/2002 Mankefors  
 2002/0046169 A1 4/2002 Keresman, III et al.  
 2003/0112972 A1 6/2003 Hattick et al.  
 2004/0059952 A1 \* 3/2004 Newport et al. .... 713/202

**FOREIGN PATENT DOCUMENTS**

GB 2 317 983 4/1998  
 GB 2 361 790 10/2001  
 WO WO 00/62214 10/2000  
 WO WO 01/26062 4/2001

\* cited by examiner



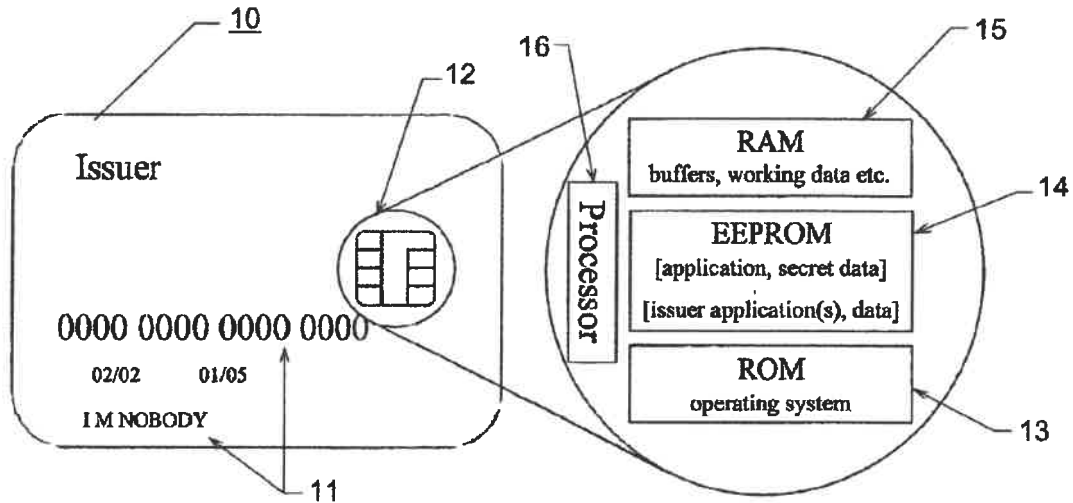


Figure 1

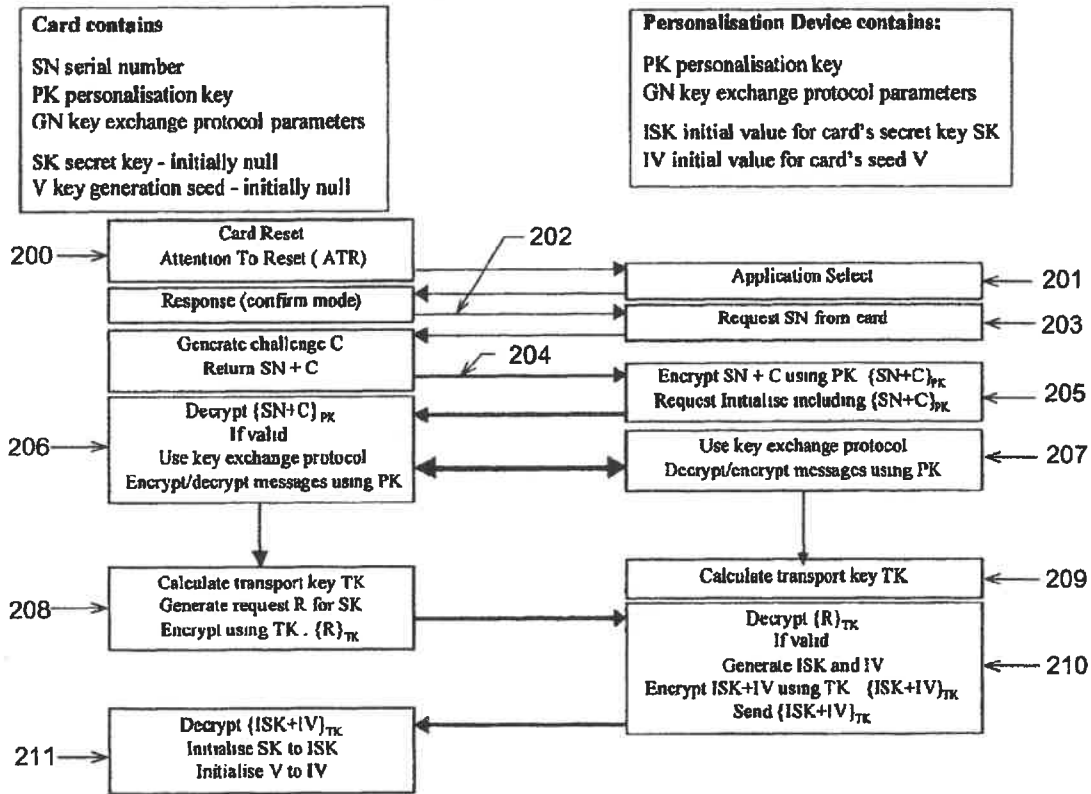


Figure 2

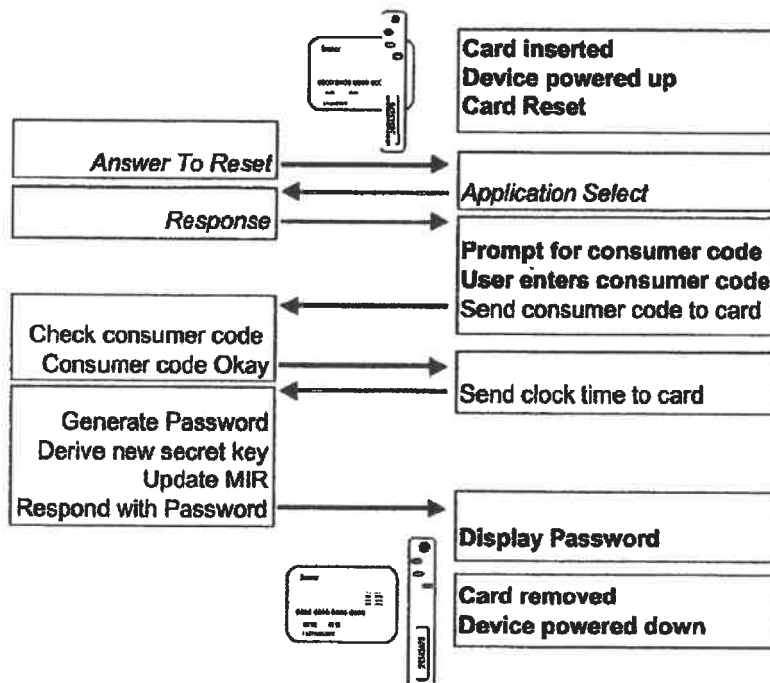


Figure 3

1

METHOD FOR PERSONALIZING AN AUTHENTICATION TOKEN

The present application is a continuation of U.S. application Ser. No. 12/978,754, filed Dec. 27, 2010 (U.S. Pat. No. 8,375,212); which is a divisional of U.S. application Ser. No. 10/176,974, filed Jun. 20, 2002 (U.S. Pat. No. 7,865,738); which claims priority to Great Britain Patent Application No. 0210692.0, filed May 10, 2002; all of which are incorporated by reference herein.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to an authentication token using a smart card.

2. Description of the Prior Art

There are a variety of technologies available to authenticate remote users in order to enforce secure access control. These range from simple, single factor authentication (such as use of a password) to multiple factor authentication (such as use of a physical token in conjunction with a Personal Identification Number (PIN)). It is widely accepted that single factor authentication offers limited assurance as it is vulnerable to a wide range of attacks, many of which are neither sophisticated nor expensive to mount (such as 'shoulder surfing' or eavesdropping). Most online services, however, still rely on single factor authentication because it appears to be the cheapest to implement—although this is usually because the subsequent cost of dealing with systematic attacks has not been considered.

Dual factor authentication systems are, however, widely used to protect remote access by support staff to these same online services. Many organisations also protect access to their critical corporate systems, both remotely and locally, using such authentication mechanisms. The essence of a dual factor mechanism is that it requires both 'something you know', for example, a PIN or passcode, and 'something you have', for example a physical token that can be authenticated itself. Increasingly, research is being done to add a third type of factor, 'something you are' i.e. biometrics such as retina scan, iris scan or fingerprint, but this is not yet available in a reliable cost-effective way that can be used reliably in a mass-market type environment.

There are a variety of tokens available that can fulfill the role of the second factor ('something you have'), but many of them rely on an infrastructure of interface devices to be able to authenticate them. Thus, use of a smart card requires a card reader to be available to enable the system to interact with the application resident on the smart card. New form factors have been explored to reduce this reliance, such as Universal Serial Bus (USB) tokens that can plug directly into a USB port on a computer. Many new PCs are being shipped with USB ports instead of the older style serial ports or parallel ports, most notebook computers now only have USB ports and all Apple computers have had easily accessible USB ports since the launch of the iMac in 1998.

To remove the dependence on an external infrastructure and to enable the token to be used in as wide a range of channels as possible, a number of manufacturers have developed stand-alone tokens that do not need to be connected to the remote computer system. They interact with the user via a screen and keypad. The user then interacts with the remote system through whatever channel they are using i.e. web, Wireless Application Protocol (WAP) phone, voice, TV set-top box.

2

Stand-alone tokens generally offer one or more mechanisms by which they can authenticate themselves to the remote system. One approach is for the system to issue a 'challenge' to be entered into the token, for example an apparently meaningless string of numbers. The token applies a cryptographic process, using the challenge and other information that is kept secret inside the token. As a result, it generates a 'response', which is displayed to the user to be sent back to the remote system. The remote system can check that the response received is the correct response from that token to the challenge sent and hence ascertain the authenticity or otherwise of the token. This process may use a symmetric cryptographic process with keys that are shared between the token and the remote system. Alternatively, it may use an asymmetric cryptographic process, removing the need for shared secret keys but requiring significantly more processing capability in the token. In most cases, the remote system does not generate the challenge and authenticate the token's response itself but uses a dedicated local authentication server which is especially established for that purpose and can provide the facility to multiple systems within the same organisation.

There is a variant on this approach where the challenge is generated internally to the token, based on a combination of static data, deterministically varying data (such as an event counter), and dynamic data (such as time). The authentication server must be maintained in synchronisation with the token so that it can reproduce the same challenge when it attempts to validate the response.

An alternative approach has been to use a modern version of the old tried and tested method of having a series of passwords each of which can only be used once. This approach was used by the military for many years, supplying a pad of slips of paper, each of which had a one-time password printed on it. As each password was used it was ripped from the pad and discarded. A matching pad was maintained at the other end to enable messages to be validated. The modern approach is to use a cryptographic process to generate a one-time password dynamically when it is needed. The token and the authentication server share secret information that can be combined with dynamic information available to both (for real-time systems this can be the time) enabling the authentication server to be able to generate the same one-time password that the token has generated and thus validate it. This mechanism uses a symmetric cryptographic process, which enables it to be carried out quickly and cost-effectively in the token. It does not require as much processing at the authentication server as no challenge needs to be generated at the outset, hence only a single interaction is needed between the protected system and the authentication server to authenticate the user.

Smart cards are in use worldwide for a variety of purposes. They have long been in use for financial products (credit, debit and loyalty cards), especially in France where they were invented. With the advent of GSM mobile phones, the smart card market has significantly increased with the need for Subscriber Identification Modules (SIMs). The technology used on smart cards lags leading edge semiconductor technology by 2 or 3 years, thus the speed and power of the processors are relatively low and memory is restricted. As more ambitious uses are devised for smart cards, the technology required is becoming more complex and hence the cost of the cards is increasing. Conversely, the increasing size of the market has led to economics of scale in the most widely used technologies (such as those required for GSM SIMs or memory chips as used in digital cameras and MP3 players).

3

Asymmetric cryptographic functions are heavily processor intensive and hence significantly slower than symmetric functions (of the order of 100 times slower). The limited processing capability of most smart card chips has restricted their practical use to symmetric cryptographic functions. However, smart card chips are now available with cryptographic co-processors that can execute asymmetric cryptographic functions much more quickly enabling such functions to become a practical option. The newest versions of specifications such as EMV (credit/debit card functionality defined jointly by Europay/Mastercard/Visa) take advantage of these improved capabilities to provide better security features.

Most smart cards have in the past been produced with a specific single application hardwired into Read Only Memory (ROM). International standards (specifically ISO 7816) have established common specifications for smart cards, ranging from size and shape and where the contacts should be, through the electrical characteristics, to the basic communications protocol to interact with the card and the underlying filing system structure that should be implemented on it. Some manufacturers have produced simple proprietary operating systems to handle all the standard activities (like the interface protocol) on behalf of the applications. However, the smart card still has to be hardwired at manufacture with the operating system software and the application software in the ROM. The standards allow for the application software on the card to offer multiple separate 'applications' (such as a credit card, loyalty card and electronic purse) selectable by the interface device with which the card is used. The required application is selected when the card is powered up and 'reset' by the interface device and the appropriate interaction is then conducted with the card. However, these separate applications must all reside together in the smart card's ROM and share the same data areas. Accordingly, they must all trust each other to ensure that the data for one is not read or overwritten by another. Generally, therefore, such cards will only have separate applications that have all been developed by (or for) the same organisation that is issuing the card.

To address these shortcomings, some multi-application smart card operating systems have been developed. These require only the operating system to be hardwired into the smart card's ROM. Applications can be loaded into the card's Electrically Erasable Programmable Read Only Memory (EEPROM) after manufacture. Indeed, they can be subsequently removed or replaced allowing upgraded applications to be delivered onto the smart cards even after they have been issued to end users. To ensure that the applications can not interfere with each other, the applications themselves are written in an interpreted language (such as Java) and the actual execution is under the control of the card's operating system, thus allowing address range checking and other mechanisms to be used to isolate each application and its data. The initial cost of using such cards has led to a slow take up of the technology, but increasing capability of the card processors and larger memory is increasing their practical applicability. New GSM SIMs will be available on multi-application cards, allowing service operators to offer customisable functionality on the SIM independent of the particular phone in use, including value-added services.

The Applicant offers a remote authentication service under the name QUIZID to enable users of a protected computer system (internal users or external customers) to be securely authenticated before being allowed access to the protected system. The current authentication mechanism relies on a device (which must be 'personalised' and securely delivered

4

to the user) that generates one-time passwords; use of the device itself is secured by the use of a colour-coded unique consumer code that must be entered by the user in order to obtain a password. The password and a user ID, entered into the protected system, are sent to QUIZID for validation and if a successful response is received the system can allow access to the user. A more detailed description of this can be found in PCT/GB01/05507. How the QUIZID service is used in relation to other identifying information such as account names or user identification is up to the designers of the protected system. The QUIZID service is designed to be used for protecting access to corporate systems as well as publicly accessible systems such as e-tailers or financial services.

SUMMARY OF THE INVENTION

The present invention provides a design for a remote authentication token using a smart card that an organisation would issue to its customer, along with an interface device to display the one-time password. In a preferred implementation, the invention is used in combination with a remote authentication server for validation of the password and is thus interoperable with the current QUIZID service.

As described above, many financial services are now issuing 'smart' credit or debit cards which have already been personalised and securely delivered to the customer. These same organisations are offering online services that need effective user authentication to protect access to customer data as required by legislation. Consequently, for authentication purposes, use of a smart card that has already been delivered to the customer is cost-effective and will help to reinforce both the organisation's brand and its commitment to security.

These and other objects of the present invention will be apparent from review of the following specification and the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Examples of the present invention will now be described in detail with reference to the accompanying drawings, in which:

FIG. 1 shows the distribution of components across the memory of a multi-application smart card;

FIG. 2 shows the interaction between a smart card and a personalisation device; and,

FIG. 3 shows the interaction between a smart card, an interface device and a user.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

With reference to FIGS. 1 to 3 generally, we now describe the proposed token, including the components of the token, namely the smart card itself and the interface device. We also describe the operation of the token, including the end-user interaction with the token in normal use, the operation of the various components and the interaction between them, and the handling of error conditions. The remote authentication token proposed here combines the functionality of authentication technology, including that provided by the existing QUIZID remote authentication service (described in more detail in PCT/GB01/05507), with the convenience of smart card technology. This type of technology is either already in use or about to be launched by many organisations, especially in the financial services sector.

US 8,688,990 B2

5

FIG. 1 shows an example of a smart card 10, which in common with many types of payment card displays account and issuer information 11, and also contains a microchip 12. The chip 12 comprises various types of on board memory, including ROM 13, EEPROM 14 and RAM 15, and also a processor 16. Thus, not only can information be stored on the card, but also an application can be loaded onto the card issued by an organisation to an end-user, for example a credit card with the EMV application. The card has already been personalised for the end-user by the issuer and has been delivered to them by some secure means.

The smart card also contains the authentication application itself. This includes the secret data that is used to generate the passwords and the colour coded unique consumer code. Since the issuing organisation will already be incurring the costs associated with issuing the smart card the additional costs to include the authentication application would be relatively low. The smart card may also contain one or more of the issuer's applications.

The authentication application may be loaded onto the card in one of two ways, depending on the type of smart card.

A 'single application' smart card will have the application and a limited operating system 'burnt' into the ROM 13 at chip manufacture. In this case a version of the authentication application will have been developed in the appropriate language for the card's processor (which may be assembler or a higher level language depending on the chip and tool support). This version of the authentication application will be supplied to the issuer for examination and integration into the ROM mask to be hardwired into the card's chip 12. It may also be combined with the issuer's application(s) prior to manufacture to make the ROM mask. Cards with the application already in the ROM 13 are delivered to the issuer. The card itself is then personalised by the issuer (embossing etc.) and the authentication application is personalised using a specific personalisation device.

If the card is a multi-application card, the operating system will be 'burnt' into the ROM 13 at chip manufacture. The authentication application and any issuer applications will be subsequently loaded onto card. Cards containing only the operating system are delivered to the issuer. The issuer's applications are loaded onto the card through an interaction with the operating system. A version of the authentication application will have been developed in the appropriate language for the card's operating system (such as Java for Javacard or MEL for Multos) and then signed and certified. This version can be loaded at the same time, separately or even subsequently, for example during personalisation by the issuer. Once the authentication application has been loaded it is personalised using a specific personalisation device. Although the multi-application operating systems allow for the loading and personalisation of the authentication application after the card has been issued, in the preferred embodiment it is not intended to issue cards prior to establishing the authentication application on them.

As indicated, whichever type of smart card 10 is used, the application will be personalised to ensure the correct secret data is in the card's EEPROM 14 along with an initial colour coded unique consumer code. Until the application is personalised it cannot be used. Once personalised it cannot be re-personalised. In the following embodiment, the application, once personalised will contain the following elements:

- a secret key (SK) stored in EEPROM, used by the cryptographic algorithm to generate passwords;
- a unique consumer code stored in EEPROM, used to validate the code entered by the user;

6

a monotonically increasing register (MIR) stored in EEPROM, used by the cryptographic algorithm to generate passwords;

a seed value (V) stored in EEPROM, used by the key generation algorithm; and,

application software to respond to application commands, generate a password and generate a new key.

The application that is loaded onto the smart card operates in three modes. Each mode allows a different limited range of interactions. When the application is first loaded it is in Personalisation mode. In this mode it will respond only to a personalisation command. After personalisation the application is in Normal mode. In this mode it will interact with an interface device to generate passwords when presented with a valid colour coded unique consumer code. If the incorrect unique consumer code is entered in sequential attempts (beyond a pre-set limit) the application enters Locked mode. In this mode the application will only accept (a limited number of) attempts to enter the correct unlock code. If the correct unlock code is entered, the application reverts to Normal mode. The application can never be returned to Personalisation mode.

When the application is loaded onto the smart card it is in a non-personalised state. The secret data has been set to starting values, but the unique key for the card has not been set. The card itself does, however, have a unique serial number. The application is in Personalisation mode. It will not accept any commands from a user's interface device in this mode. It will, however, accept a personalisation command from a personalisation device. The personalisation device requests the serial number, and establishes a private communications channel with the application to enable it to issue the application with seed values for the secret key and the key generation algorithm. The same data is stored securely by the personalisation device for subsequent loading into the authentication server. The card serial number can be used to determine the username that the issuer will associate with the card. Once the seed has been used by the application to set the initial secret key, the application switches to Normal mode.

While there are a variety of suitable mechanisms to secure the communications between the personalisation device and the application, the preferred implementation is to use a key exchange protocol to establish a transport key, supplemented by a pre-defined personalisation key to protect against 'man in the middle' attacks. This is necessary because, although the card may be personalised at the same time that it is loaded with the application, in a multi-application card environment this may be subsequent to the manufacture or issuer personalisation of the card. It may even be performed remotely from the personalisation device, which could be at (or incorporated into) the authentication server, and must therefore be protected against interception.

An example of a personalisation interaction is illustrated in FIG. 2 and the steps involved are described below:

initially, the card is reset (step 200) and responds with an Attention to Reset (ATR).

the personalisation device selects (step 201) the authentication application and determines (step 202) that it is in personalisation mode.

the personalisation device requests (step 203) the card serial number and receives (step 204) the serial number (SN) and a challenge (C) from the card application.

using the pre-defined Personalisation Key (PK) the personalisation device encrypts (step 205) SN and C and returns the encrypted value to the card in a request to commence initialisation.

US 8,688,990 B2

7

the card application decrypts (step 206) the received data using PK and validates it as correct. This demonstrates that both the card application and the personalisation device are using the correct PK.

if successful, the card application uses (step 206) the key exchange protocol to generate messages to send back to the personalisation device. The key exchange protocol itself is inherently protected against interception, but the messages are also encrypted (step 206) using PK to protect against 'man in the middle' attacks.

the personalisation device responds (step 207) with the appropriate key exchange protocol messages, encrypted using PK.

at the end of the key exchange, both the card application (step 208) and the personalisation device (step 209) have a unique shared key that is unknown to anyone else including eavesdroppers. This key is used as a Transport Key (TK) for the rest of the personalisation process.

the card application generates a request (step 208) (R) for its Secret Key (SK), encrypts (step 208) the request using TK and sends it to the personalisation device.

the personalisation device decrypts (step 210) the request using TK and validates it as correct. This demonstrates that both the card application and the personalisation device are using the same TK and hence that the key exchange process has worked correctly.

if successful, the personalisation device generates (step 210), or obtains from a pre-generated list, the Initial Secret Key (ISK) and the Initial Value (IV) for the card application's key generation seed (V). ISK and IV are encrypted (step 210) using TK and sent to the card.

the card application decrypts (step 211) the received data using TK, initialises (step 211) its SK to ISK and initialises (step 211) its V to IV. The card application now enters Normal mode.

the personalisation device delivers (step 210) the ISK and IV to the authentication server (if they were not pre-generated and hence already in the authentication server) securely.

Although there may be a number of suitable key exchange protocols available, the preferred implementation is to use the Diffie-Hellman exchange which is within the processing capabilities of the card and does not rely on out of band secure communications to pre-establish any shared secret. The Diffie-Hellman exchange operates as follows:

the card application and personalisation device both know the pre-defined values 'n' (a large prime number) and 'g' (a small single digit number that is primitive mod n). These don't need to be kept secret and can be common to all cards, therefore are included in the application that is loaded onto the card;

the card application generates a large random integer 'x';

the card application calculates  $A = g.\text{sup}.x \text{ mod } n$ ;

the card application sends A to the personalisation device;

the personalisation device generates a large random integer 'y';

the personalisation device calculates  $P = g.\text{sup}.Y \text{ mod } n$ ;

the personalisation device send P to the card application;

the card application calculates  $K1 = P.\text{sup}.x \text{ mod } n$ ;

the personalisation device calculates  $K2 = A.\text{sup}.y \text{ mod } n$ ;

and,

both K1 and K2 are equal to  $g.\text{sup}.xy \text{ mod } n$  and hence the card application and the personalisation device have calculated the same key which can now be used as the Transport Key (TK).

The second main component of the authentication token is the interface device provided to the end-user. The interface

8

device is a device that can be used with a user's smart card to enable the generation of a password. The device could take a variety of forms, for example a pen or a calculator or a mobile phone battery pack. When the smart card is inserted into the interface device, the user is prompted to enter their colour coded unique consumer code and, if correct, the output response from the interface device is a one-time password. A password so generated can then be entered into the access device, such as a PC, a telephone, a WAP phone, or even by voice, for the service that requires the authentication.

As the smart card is personalised to the customer, the interface device does not need to be. Users, therefore, can share an interface device, for example one at home for use by all members of a family. Equally, users can have more than one, for example one at home, one in the office. Users can even, safely, borrow an interface device from a stranger, for example in a cybercaf or a restaurant. Therefore, in one embodiment, the interface devices are preferably generic, hence all identical and requiring no personalisation for each customer. As they do not need to be personalisable or securely delivered to users (they could even be available over the counter if the issuing organisation has a branch network), it should be possible to keep the associated cost significantly low.

The interface device provides the power to the smart card to enable it to operate. It also includes a real-time clock to enable time to be used as a dynamic input into the password generation process. It therefore includes a battery, which has a reasonably long life but is not accessible by the user. After manufacture, the device's clock can be synchronised with the service's system-wide time through the smart card interface. When battery replacement is required, the device's clock must once again be synchronised (which is why the battery is not user-replaceable). When no smart card is inserted in the slot, the device only provides power to the real-time clock. When a smart card is inserted, the device powers up and applies power to the smart card and to itself. When the smart card is removed the device powers down. For this reason, the device needs no user accessible power switch.

Although the interface device may take one of many forms, it will typically include the following five elements:

- i. an interface to the token, initially a set of smart card contacts, but other interfaces would be possible, such as Bluetooth;
- ii. an input mechanism, such as a keypad for entry of the colour coded unique consumer code and for menu selection;
- iii. an output mechanism, such as a display screen, although other mechanisms could be provided such as voice output for the blind;
- iv. a source of a dynamic input to the password generation, such as a battery operated real-time clock; and,
- v. a processor with application software to handle the interfaces.

Once the user has received the smart card and an interface device they can use the combination to authenticate themselves to the issuer's services, as and when required. The authentication is assured either by an authentication server operated by the issuer themselves or by a shared authentication server such as described in PCT/GB01/05507.

There are many different business models within which strong authentication would be advantageous. An example is given below of a typical interaction, where the issuer provides an online e-commerce service requiring the users to authenticate themselves when they place an order.

1. User browses issuer's online service on their PC.
2. User places order on service.

3. Service prompts user for authentication password in secure form.
4. User inserts smart card into an interface device.
5. Interface device prompts for colour coded unique consumer code entry.
6. User enters colour coded unique consumer code into the interface device.
7. Interface device displays password.
8. User enters password into secure form on issuer's online service on their PC.
9. Service authenticates password with remote authentication service.
10. Service confirms authentication to user, accepts order.
11. User removes the smart card from the interface device.

When the smart card is issued to the user, the application will have been personalised and will be in Normal mode. The user can then use a generic interface device to change the colour coded unique consumer code from the pre-set initial value to one of their own choice. The card will now be able to interact with a generic interface device to generate a password. An example of this type of interaction is shown in FIG. 3.

The process used to generate the one-time password relies on the use of a secret key (SK) in conjunction with a tried and tested cryptographic algorithm. The data that is processed by the algorithm to generate the password is derived from a Monotonically Increasing Register (MIR) that is maintained within the card application and tracked at the authentication server, along with a Dynamic Variable (DV) that can be validated or reproduced at the authentication server. To increase the variability of the passwords and the difficulty of an attempt to spoof the password generation, the secret key is itself modified after each password generation using a key generation algorithm. The authentication server must apply the same algorithms to validate the password and keep in synchronisation with the MIR, SK and V on the card.

The process for password generation is as follows:

- the MIR is concatenated with the DV to produce a payload (L);
- L is encrypted using the cryptographic algorithm with SK to produce G;
- the least significant bits of G are used to generate an integer I;
- the least 2 significant bits of DV, concatenated with the least significant bit of MIR, are used to generate an integer D;
- I is combined with D to produce the password;
- the key generation algorithm uses MIR and SK and a seed V to generate a new key NK and a new seed NV;
- SK is replaced with NK;
- V is replaced with NV; and,
- MIR is incremented.

The inclusion of the 3 bits that are used to create D, enables the authentication server to detect loss of synchronisation with the application on the card. The authentication server will be maintaining its own copy of the MIR for each card. When the password arrives to be validated at the authentication server, the least significant bit of the MIR on the card, as included in the password via D, should match that of the MIR in the server. If not, there may have been a previous password generated that did not arrive at the server, in which case the server increments the MIR and executes the key generation algorithm to obtain the appropriate SK. Similarly, the 2 least significant bits of the DV included in the password via D can be compared with those of the DV reproduced at the authentication server, allowing for a discrepancy to be detected and corrected before the password is validated. Parameters can be

established at the authentication server to determine whether (and how many) subsequent values of the MIR should be tried if the validation fails.

The combination of I and D can be achieved in a variety of ways. The 3 bits of D can be interspersed at pre-determined positions in I, the resulting value then being interpreted as a decimal value. Any length password can be generated by selecting the appropriate number of bits of the output of the cryptographic algorithm, for example an eight digit password would be produced from a 26 bit value composed of the 3 bits of D and 23 bits of I. Alternatively, I can be interpreted as a decimal value (the length depending on the number of bits used) and D interpreted as a decimal value (one digit in length as only 3 bits are used). The resulting password would be created by concatenating the digits derived from I with the digit derived from D (or inserting the digit from D into the digits from I). Again, any length password can be generated by selecting the appropriate number of bits of the output of the cryptographic algorithm. An eight digit password would require 23 bits to be used to produce I which would be 7 digits long, with D providing the eighth digit. In the preferred embodiment, an eight digit password will be generated by interpreting 23 bits of the cryptogram as a 7 digit decimal integer I and appending a decimal digit interpreted from the 3 bits of D.

The preferred implementation is to use the Advanced Encryption Standard (AES) with 128 bit keys as the cryptographic algorithm, along with a key generation algorithm based on ANSI X9.17 but using AES and generating 128 bit keys. One of the strengths of AES is that there are no known weak keys, so all keys generated by the key generation algorithm would be acceptable.

As each card must work with any one of the interface devices, the source of the DV in the initial embodiment will be a real-time clock in the interface device. In future embodiments, when the smart card may have its own source of power, there will be other sources of dynamic variable that could be maintained within the card itself.

The example shown in FIG. 3 illustrates the case where the user enters the unique consumer code correctly first time. If the unique consumer code entered is incorrect the application will respond 'code incorrect' and the interface device will re-prompt for the unique consumer code. This can happen repeatedly up to a preset limit, for example three attempts. If the unique consumer code has not been entered correctly within the limited number of attempts, the application will respond 'Locked' and the interface device will inform the user that the application is locked. The application will enter Locked mode.

When the application is in Locked mode it will not accept commands to generate a password. It will not respond to the normal interactions. When the interface device attempts to interact with the application, it is told (in the Answer To Reset) that the application is locked and informs the user that the application is locked. If the user then enters a sequence of colour codes the interface device will send them to the application as an unlock command. The correct sequence will cause the application to unlock and revert to Normal mode. To obtain the correct sequence the user will have to contact a customer support function. The unlock sequence will only work once. If the application is subsequently locked again a different unlock sequence will be required.

Other embodiments of the invention will be apparent to those skilled in the art from consideration of the specification and practice of the invention disclosed herein. It is intended that the specification and examples be considered as exem-



US 8,688,990 B2

11

plary only, with a true scope and spirit of the invention being indicated by the following claims.

We claim:

1. A system for personalizing an authentication token comprising: 5

an interface device, the authentication token, and a personalization device, the system configured to establish an encrypted session between the authentication token and the personalization device using a transport key;

the interface device including a processor, a user interface, 10 and an interface for communication with the authentication token;

the authentication token including a personalization mode, and having a serial number; and

the personalization device being configured to encrypt the 15 serial number of the authentication token using a personalization key, and being configured to forward the encrypted serial number to the authentication token;

the authentication token, when in the personalization mode, being configured to: 20

receive, from the personalization device, a request for the serial number, and return the serial number to the personalization device;

decrypt the encrypted serial number forwarded from the 25 personalization device, and validate that the personalization key is correct;

12

receive, from said personalization device through the encrypted session, an initial seed value and initial secret key, the initial seed value and the initial secret key being configured to facilitate an initial interaction between the authentication token and the interface device; and

store the initial seed value and the initial secret key after decryption thereof using the transport key;

wherein, once said authentication token is personalized with the initial seed value and the initial secret key, the authentication token is configured to be unable to again enter to the personalization mode.

2. The system of claim 1, wherein the authentication token is further configured to generate a key for use in generating a secure password used in interacting with the interface device using the initial seed value stored in a memory in the authentication token.

3. The system of claim 2, wherein the personalization device is further configured to store, for subsequent transfer to a third party, data exchanged between the authentication token and the personalization device for use in generating the secure password.

4. The method of claim 2, wherein the authentication token is further configured to enter into normal mode after the initial seed value and the initial secret key are stored.

\* \* \* \* \*

# Exhibit 3

**EVIDENCE OF USE FOR U.S. PATENT NO. 8,375,212**

Title: Method for personalizing an authentication token

Application No.: US 12/978,754


Filing Date: December 27, 2010

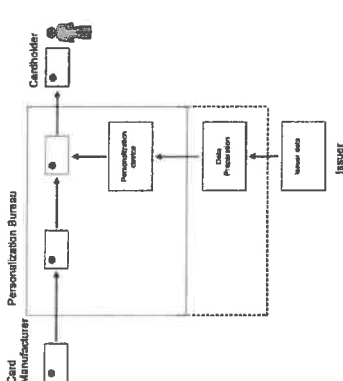
Issue Date: February 12, 2013

**Accused Product:**

EMV stands for Europay, Mastercard and Visa — is a global standard for cards equipped with computer chips and the technology used to authenticate chip-card transactions. EMV cards are smart cards (also called chip cards or IC cards) that store their data on integrated circuits in addition to magnetic stripes (for backward compatibility). These include cards that must be physically inserted (or "dipped") into a reader and contactless cards that can be read over a short distance using radio-frequency identification (RFID) technology. Payment cards that comply with the EMV standard are often called Chip and PIN or Chip and Signature cards, depending on the authentication methods employed by the card issuer.

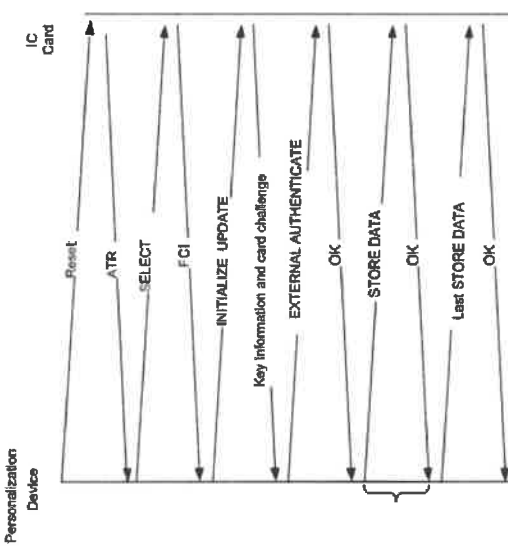
Source: <https://www.cardlogix.com/glossary/emv-europay-mastercard-visa-smart-card/>

Evidence of Use	Evidence of Infringement
<p>Claim Language</p> <p>1. A method for personalizing an authentication token comprising:</p>	<p>CardLogix card enables EMV chip cards and terminals to exchange authentication data which is based on EMV specification. EMV specification provides a method for personalizing an authentication token. For example, as per EMV Card Personalization specification, card (“authentication token”) personalization (“personalizing”) is one of the major parts in the production of EMV cards.</p> <div data-bbox="646 1094 748 1472" style="text-align: center;">  </div> <p>EMV stands for Europay, Mastercard and Visa — is a global standard for cards equipped with computer chips and the technology used to authenticate chip-card transactions. EMV cards are smart cards (also called chip cards or IC cards) that store their data on integrated circuits in addition to magnetic stripes (for backward compatibility). These include cards that must be physically inserted (or “dipped”) into a reader and contactless cards that can be read over a short distance using radio-frequency identification (RFID) technology. Payment cards that comply with the EMV standard are often called Chip and PIN or Chip and Signature cards, depending on the authentication methods employed by the card issuer.</p> <p>Source: <a href="https://www.cardlogix.com/glossary/emv-europay-mastercard-visa-smart-card/">https://www.cardlogix.com/glossary/emv-europay-mastercard-visa-smart-card/</a></p> <p><b>1. Purpose</b></p> <p>Card personalization is one of the major cost components in the production of EMV cards. This specification standardizes the EMV card personalization process with the objective of reducing the cost of personalization thus facilitating the migration to chip.</p>

Claim Language	Evidence of Infringement
	<p><b>2. Scope</b></p> <p>In this specification, card personalization means the use of data personalization commands that are sent to a card that already contains the basic EMV application. This is sometimes referred to as “on-card” personalization. The specification does not cover cards where an application load file is personalized before being loaded onto the card.</p> <p><b>Involved Entities</b></p>  <pre> graph TD     CM[Card Manufacturer] --&gt; PB[Personalization Bureau]     PB --&gt; CH[Cardholder]     PB --&gt; PC[Personalization Center]     PC --&gt; DP[Data Preparation]     DP --&gt; I[Issuer]     </pre> <p>Source: <u>EMV Card Personalization Specification</u>, at page 8 &amp; 9 of 104</p>
<p>entering by the authentication token into personalization mode;</p>	<p>EMV specification allows the authentication token to be entered into personalization mode. For example, a personalization device activates the IC card (“authentication token”) and the IC card responds with “Answer To Reset” (ATR). This can be considered as equivalent to the authentication token entering the personalization mode.</p> <p><b>1 Card Personalization Data Processing</b></p> <p><b>1.1 Overview of the Process</b></p>

Claim Language	Evidence of Infringement
<p>requesting from the authentication token, by a personalization device in communication with the authentication token, a serial number of the authentication token;</p>	<p>Within a personalization bureau environment the processing of Personalization Device Instructions (PDI) and IC card personalization data processing requires the following three functional steps:</p> <ol style="list-style-type: none"> <li>1. Data preparation</li> <li>2. <u>Personalization device set-up and processing</u></li> <li>3. <u>IC card application processing.</u></li> </ol> <p><b>3 Personalization Device-ICC Interface</b></p> <p><b>3.1 Processing Step '0F'</b></p> <p>For the Processing Step '0F' the personalization device activates the IC card (Reset) and the IC card responds with <u>Answer To Reset (ATR)</u>. At this point protocol selection and a warm reset may be used to allow more efficient communications to speed up personalization.</p> <p><u>Source:</u> EMV Card Personalization Specification, at page 20 &amp; 48 of 104</p>
<p>requesting from the authentication token, by a personalization device in communication with the authentication token, a serial number of the authentication token;</p>	<p>EMV specification allows the personalization device to request serial number of the authentication token. For example, the personalization device sends an Initialize Update Command ("request") to the card ("authentication token") and in response to the update command, the card sends a Card Challenge ("serial number") to the personalization device. Rcard is a random number that is generated by the IC card or the IC card application.</p> <p><b>3.2.5 INITIALIZE UPDATE Command</b></p>

Claim Language	Evidence of Infringement																
	<p>The INITIALIZE UPDATE command is the first command issued to the IC card after the personalization device selects the application. INITIALIZE UPDATE is used to establish the Secure Channel Session to be used during personalization. The data to perform mutual authentication is exchanged. The identifier and version number for the KMC and the data to be used to derive the <math>K_{ENC}</math>, the <math>K_{MAC}</math> and the <math>K_{DEK}</math> for the application are also returned.</p> <p>The INITIALIZE UPDATE command will be issued once for each secure channel initiation. It shall be issued at least once for each IC card application to be personalized.</p> <p><b>Table 14 – Response to INITIALIZE UPDATE command</b></p> <table border="1"> <thead> <tr> <th>Field</th> <th>Length</th> </tr> </thead> <tbody> <tr> <td>KEYDATA (See Table 15)</td> <td>10</td> </tr> <tr> <td>Version number of the master key (KMC)</td> <td>1</td> </tr> <tr> <td>Identifier for Secure Channel Protocol (ALGSCP = '02')</td> <td>1</td> </tr> <tr> <td>Sequence Counter</td> <td>2</td> </tr> <tr> <td>Card challenge (<math>R_{CARD}</math>)</td> <td>6</td> </tr> <tr> <td>Card cryptogram</td> <td>8</td> </tr> <tr> <td>\$W1 SW2</td> <td>2</td> </tr> </tbody> </table> <p>Source: EMV Card Personalization Specification, at page 54 &amp; 55 of 104</p> <p><b>Figure 6 – Personalization Command Flow</b></p>	Field	Length	KEYDATA (See Table 15)	10	Version number of the master key (KMC)	1	Identifier for Secure Channel Protocol (ALGSCP = '02')	1	Sequence Counter	2	Card challenge ( $R_{CARD}$ )	6	Card cryptogram	8	\$W1 SW2	2
Field	Length																
KEYDATA (See Table 15)	10																
Version number of the master key (KMC)	1																
Identifier for Secure Channel Protocol (ALGSCP = '02')	1																
Sequence Counter	2																
Card challenge ( $R_{CARD}$ )	6																
Card cryptogram	8																
\$W1 SW2	2																

Claim Language	Evidence of Infringement
	 <p><b>Source:</b> EMV Card Personalization Specification, at page 50 of 104</p> <p><b>6.27 Rcard (Pseudo-Random Number from the IC Card)</b></p> <p><b>Purpose:</b> A pseudo-random number (see 3.2.5.9) generated by the IC card or the IC card application. Used in the creation of the host and card cryptograms.</p> <p><b>Format:</b> Binary, 6 bytes</p> <p><b>Source:</b> EMV Card Personalization Specification, at page 88 of 104</p>



Claim Language	Evidence of Infringement
<p>encrypting by the personalization device the serial number using a personalization key, and forwarding the encrypted serial number to the authentication token from the personalization device;</p>	<p>EMV specification allows the personalization device to encrypt the serial number and then forward the encrypted serial number to the authentication token. For example, the personalization device uses the master key i.e., KMC to generate the personalization keys i.e., Kenc, Kmac and Kdek. The Kenc is used to generate a session key SKUenc which is used for creating and validating cryptograms. The SKUenc is used to create the host cryptogram by generating a MAC, which is then sent by the personalization device to the card.</p> <p>The data that is MACed to create the host cryptogram consists of the Rcard. Thus, it can be said that the serial number (Rcard) is encrypted by the Kenc (“the personalization key”) using SKUenc and forwarded to card (“authentication token”). Here, we have considered the Kenc as the personalization key because, it creates the SKUenc which then generates the MAC (host cryptogram) and sends to the card.</p> <p><b>6.17 KMC (DES Master Key for Personalization Session Keys)</b></p> <p><i>Purpose:</i> This DES key is used for generating derived keys to generate MACs and encrypt and decrypt DES keys and secret data during personalization (Kenc, Kmac and Kdek).</p> <p><i>Format:</i> Binary, 16 bytes</p> <p><i>Notes:</i> Must be generated with odd parity.</p> <p><u>Source:</u> EMV Card Personalization Specification, at page 86 of 104</p> <p><b>4 IC Card Personalization Processing</b></p> <p><b>4.1 Preparation for Personalization (Pre-Personalization)</b></p> <p>4.1.1.5 The version number of the personalization master key (KMC) used to generate the initial personalization keys (the Kenc, the Kmac and the Kdek) for each application must be on the IC card.</p> <p><u>Source:</u> EMV Card Personalization Specification, at page 68 of 104</p>

Claim Language	Evidence of Infringement
	<p><b>3.2.5 INITIALIZE UPDATE Command</b></p> <p>3.2.5.7 The first 6 bytes of KEYDATA returned from the INITIALIZE UPDATE command are used to identify the master key for secure messaging (KMC). The six least significant bytes of KEYDATA are used as key diversification data. The personalization device must use the KMC and KEYDATA to generate the <math>K_{ENC}</math>, the <math>K_{MAC}</math> and the <math>K_{DEK}</math> for this IC card, as defined in section 4.1. These keys must have been placed in the IC card prior to the start of the personalization process.</p> <p><u>Source:</u> EMV Card Personalization Specification, at page 54 &amp; 56 of 104</p> <p><b>1.3 Secure Messaging</b></p> <p>Two derived keys on the IC card are used during the establishment of the secure channel. These are the <math>K_{ENC}</math>, used to generate a session key <math>SKU_{ENC}</math> which is in turn used to create and validate authentication cryptograms, and the <math>K_{MAC}</math>, used to generate a session key <math>SKU_{MAC}</math> which is in turn used to compute the MAC of the EXTERNAL AUTHENTICATE command. Both of these keys (<math>K_{ENC}</math> and <math>K_{MAC}</math>) are derived from the same master key, the KMC. When the secure channel is to be</p> <p><u>Source:</u> EMV Card Personalization Specification, at page 22 of 104</p> <p><b>3.2.6 EXTERNAL AUTHENTICATE Command</b></p> <p>3.2.6.6 The host cryptogram must be created by generating a MAC as described in section 5.4.1 using <math>SKU_{ENC}</math>. The data to be MACed is = Sequence Counter (2 bytes)    <math>R_{CARD}</math> (6 bytes)    <math>R_{TERM}</math> (8 bytes). The IC card must verify the host cryptogram by generating a duplicate cryptogram and comparing it to the value received in the command data field.</p> <p><u>Source:</u> EMV Card Personalization Specification, at page 58 &amp; 59 of 104</p>

Claim Language	Evidence of Infringement
<p>decrypting by the authentication token of the encrypted serial number, and validating by the authentication token that the personalization key is correct;</p>	<p><b>5.4 MACs</b></p> <p>The personalization process creates MACs for three purposes:</p> <ol style="list-style-type: none"> <li>1. During the IC personalization process (INITIALIZE UPDATE command and EXTERNAL AUTHENTICATE command) the IC card returns a MAC (the card cryptogram) and the personalization device sends a MAC (the host cryptogram) to the IC card. The IC card and the personalization device authenticate each other using these cryptograms. The process of creating the</li> </ol> <p>Source: EMV Card Personalization Specification, at page 75 &amp; 76 of 104</p> <p>EMV specification allows the authentication token to decrypt the encrypted serial number and validate that the personalization key is correct. For example, the personalization keys such as Kenc is created by the IC card using the personalization master key (KMC) and Kenc is used in verifying the host cryptogram. The Kenc key is used by the IC card to generate a session key SKUenc which helps to create and validate authentication cryptograms. The IC card can generate a duplicate cryptogram and compare it to the value (host cryptogram) received to validate the same. As per the claim clause, the authentication token decrypts the encrypted serial number. In the EMV standard, the validation of the host cryptogram which is a MAC consisting of Rcard ("serial number") is done by the card. As per patent specifications, the card application decrypts the received data using the personalization key and validates it as correct. Since the Kenc personalization key can be used to verify the host cryptogram thus it could be said that decryption process could occur at the card.</p> <p><b>4 IC Card Personalization Processing</b></p>

Claim Language	Evidence of Infringement
	<p><b>4.1 Preparation for Personalization (Pre-Personalization)</b></p> <p><b>4.1.1.5</b> The version number of the personalization master key (K<sub>MC</sub>) used to generate the initial personalization keys (the K<sub>ENC</sub>, the K<sub>MAC</sub> and the K<sub>DEK</sub>) for each application must be on the IC card.</p> <p><b>4.1.1.6</b> A derived key (K<sub>ENC</sub>) must be generated for each IC card and placed into the application. This key is used to generate the card cryptogram and to verify the host cryptogram. This key is also used to decrypt the STORE DATA command data field in CBC mode if the security level of secure messaging requires the command data field to be encrypted.</p> <p><u>Source: EMV Card Personalization Specification, at page 68 of 104</u></p> <p><b>5.4 MACs</b></p> <p>The personalization process creates MACs for three purposes:</p> <ol style="list-style-type: none"><li>1. During the IC personalization process (INITIALIZE UPDATE command and EXTERNAL AUTHENTICATE command) the IC card returns a MAC (the card cryptogram) and the personalization device sends a MAC (the host cryptogram) to the IC card. The IC card and the personalization device authenticate each other using these cryptograms. The process of creating the</li></ol> <p><u>Source: EMV Card Personalization Specification, at page 75 &amp; 76 of 104</u></p> <p><b>1.3 Secure Messaging</b></p>

Claim Language	Evidence of Infringement
	<p>Two derived keys on the IC card are used during the establishment of the secure channel. These are the <math>K_{ENC}</math>, used to generate a session key <math>SKU_{ENC}</math> which is in turn used to create and validate authentication cryptograms, and the <math>K_{MAC}</math>, used to generate a session key <math>SKU_{MAC}</math> which is in turn used to compute the MAC of the EXTERNAL AUTHENTICATE command. Both of these keys (<math>K_{ENC}</math> and <math>K_{MAC}</math>) are derived from the same master key, the KMC. When the secure channel is to be</p> <p><b>3.2.6 EXTERNAL AUTHENTICATE Command</b></p> <p>3.2.6.6 The host cryptogram must be created by generating a MAC as described in section 5.4.1 using <math>SKU_{ENC}</math>. The data to be MACed is = Sequence Counter (2 bytes)    <math>R_{CARD}</math> (6 bytes)    <math>R_{TERM}</math> (8 bytes). The IC card must verify the host cryptogram by generating a duplicate cryptogram and comparing it to the value received in the command data field.</p> <p><u>Source:</u> EMV Card Personalization Specification, at page 22, 58 &amp; 59 of 104</p>

Claim Language	Evidence of Infringement
<p>establishing an encrypted session between the authentication token and the personalization device using a transport key;</p>	<p>EMV specification allows to establish an encrypted session between the authentication token and the personalization device using a transport key. For example, whenever a secure channel is created ("encrypted session"), DES session keys are generated and one of them include SKUdek ("transport key").</p> <p><b>5.3 Session Keys</b></p> <p><u>DES session keys are generated every time a secure channel is initiated. These session keys may be used for subsequent commands if secure messaging is required. Up to three session keys may be generated, namely SKU<sub>ENC</sub>, SKU<sub>MAC</sub>, and SKU<sub>DK</sub>.</u></p> <p><u>Source: EMV Card Personalization Specification, at page 75 of 104</u></p>

Claim Language	Evidence of Infringement
<p>sending to the authentication token, by the personalization device, an initial seed value and an initial secret key using the transport key to encrypt the initial seed value and the initial secret key, the initial seed value and the initial secret key for facilitating an initial interaction between the authentication token and an interface device; and</p>	<p>EMV specification allows to send an initial seed value and an initial secret key by encrypting using a transport key such that the seed value and the secret key are used for facilitating initial interaction between the authentication token and an interface device. For example, the Store Data command is used for sending secret data or personalization data to the IC card. The SKUdek (“transport key”) is used to encrypt secret data (“initial seed value and initial secret key”) that is sent to an IC card. The data preparation process sends encrypted secret data to the personalization device, which then re-encrypts that data using the SKUdek which is then sent to the IC card. The secret data (“initial seed value and initial secret key”) is used for data exchange between the terminal (“interface device”) and the IC card. In the standard, the data exchanged between the authentication token and the terminal could include a PIN that form a part of the secret data. Here, we have considered the initial seed value and initial secret key as equivalent to the secret data.</p> <p><b>1.4 The STORE DATA Command</b></p> <p>The STORE DATA command is used to send personalization data to the card application; it is described in detail in section 3.2.7.</p> <p><b>5.3 Session Keys</b></p> <p>DES session keys are generated every time a secure channel is initiated. These session keys may be used for subsequent commands if secure messaging is required. Up to three session keys may be generated, namely SKU<sub>ENC</sub>, SKU<sub>MAC</sub>, and SKU<sub>DEK</sub>.</p> <p><u>Source:</u> EMV Card Personalization Specification, at page 22 &amp; 75 of 104</p> <p><b>6.36 TK (Transport Key)</b></p> <p><i>Purpose:</i> A DES key used to encrypt other key values for transmission between the data preparation system and the personalization device.</p> <p><i>Format:</i> Binary, 16 bytes</p> <p><i>Remarks:</i> This key is not related to the K<sub>DEK</sub> and the SKU<sub>DEK</sub> used to encrypt secret data sent to an IC card.</p> <p><u>Source:</u> EMV Card Personalization Specification, at page 90 of 104</p>

Claim Language	Evidence of Infringement
	<p><b>5.6 Decryption</b></p> <p>The personalization device must decrypt secret data encrypted by the data preparation process. This secret data will then be re-encrypted prior to sending to the IC card. The IC card should decrypt the secret data prior to storing it for future use. This section describes the decryption of secret data during personalization.</p> <p><b>5.5 Encryption</b></p> <p>This section describes the encryption of secret data during personalization.</p> <p>After personalization, confidential or secret data may be exchanged between a terminal and an IC card application. For example, a PIN may be changed between a terminal and an IC card during an online transaction. This section does not apply to encryption of secret data after personalization. Post personalization encryption is covered in application specific documents.</p> <p><u>Source:</u> EMV Card Personalization Specification, at page 81 of 104</p>



Claim Language	Evidence of Infringement
<p>storing by the authentication token the initial seed value and the initial secret key after decryption thereof by the authentication token using the transport key, wherein, once the authentication token is personalized with the initial seed value and the initial secret key, the authentication token can no longer enter the personalization mode.</p>	<p>EMV specification allows the authentication token to store the seed value and secret key. Also, the authentication token can no longer enter the personalization mode. As per the specification, the secret data is stored by the IC card and before storing, the secret data is decrypted using the transport key (SKUdek). The data is stored in an assigned location by the IC card. The Select command is used to select IC card application that is to be personalized and it is issued only once for each IC card application. Thus, it can be said that the authentication token can no longer enter the personalization mode once personalized.</p> <p><b>5.6 Decryption</b></p> <p>The personalization device must decrypt secret data encrypted by the data preparation process. This secret data will then be re-encrypted prior to sending to the IC card. The IC card should decrypt the secret data prior to storing it for future use. This section describes the decryption of secret data during personalization.</p> <p><b>The IC Card Application</b></p> <p>The IC card application receives the personalization data from the personalization device and stores it in its assigned location, for use when the EMV card application becomes operational.</p> <p>Source: EMV Card Personalization Specification, at page 21 &amp; 81 of 104</p> <p><b>6.33 SKU<sub>DEK</sub> (Personalization Session Key for Key and PIN Encryption)</b></p> <p><i>Purpose:</i> This DES key is created during the personalization process and is used to encrypt and decrypt secret data in ECB mode.</p> <p><i>Format:</i> Binary, 16 bytes</p> <p><i>Content:</i> Derived as described in section 5.3.</p> <p><i>Remarks:</i> Parity convention not required</p> <p><b>5.6.1 Decryption Using ECB Mode</b></p>

Claim Language	Evidence of Infringement
	<p>5.6.1.2 <u>The IC card must use SKU<sub>DEX</sub> for decryption of encrypted data grouping values.</u></p> <p><u>Source: EMV Card Personalization Specification, at page 82 &amp; 89 of 104</u></p> <p><b>3.2.4 SELECT Command</b></p> <p><u>The SELECT command is used to select each IC card application to be personalized. Application selection is described in EMV Version 4.1 Book 1.</u></p> <p><u>The SELECT command will be issued once for each IC card application to be personalized.</u></p> <p><u>Source: EMV Card Personalization Specification, at page 53 of 104</u></p>

# Exhibit 4

**EVIDENCE OF USE FOR U.S. PATENT NO. US8,688,990**

Title: Method for personalizing an authentication token

Application No.: US 13/765,351

Filing Date: February 12, 2013

Issue Date: April 01, 2014


**Accused Product:**

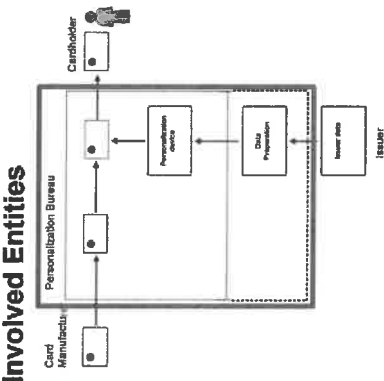


EMV stands for Europay, Mastercard and Visa — is a global standard for cards equipped with computer chips and the technology used to authenticate chip-card transactions. EMV cards are smart cards (also called chip cards or IC cards) that store their data on integrated circuits in addition to magnetic stripes (for backward compatibility). These include cards that must be physically inserted (or “dipped”) into a reader and contactless cards that can be read over a short distance using radio-frequency identification (RFID) technology. Payment cards that comply with the EMV standard are often called Chip and PIN or Chip and Signature cards, depending on the authentication methods employed by the card issuer.

Source: <https://www.cardlogix.com/glossary/emv-europay-mastercard-visa-smart-card/>

**Evidence of Use**

Claim Language	Evidence of Infringement
<p>1. A system for personalizing an authentication token comprising:</p>	<p>CardLogix enables EMV chip cards and terminals to exchange authentication data which is based on EMV specification. EMV specification provides a method for personalizing an authentication token. For example, as per EMV Card Personalization specification, card (“authentication token”) personalization (“personalizing”) is one of the major parts in the production of EMV cards.</p>  <p>EMV stands for <u>Europay, Mastercard and Visa</u> — is a global standard for cards equipped with computer chips and the technology used to authenticate chip-card transactions. EMV cards are smart cards (also called chip cards or IC cards) that store their data on <u>integrated circuits in addition to magnetic stripes (for backward compatibility)</u>. These include cards that must be physically inserted (or “dipped”) into a reader and contactless cards that can be read over a short distance using radio-frequency identification (RFID) technology. Payment cards that comply with the EMV standard are often called Chip and PIN or Chip and Signature cards, depending on the authentication methods employed by the card issuer.</p> <p><u>Source: <a href="https://www.cardlogix.com/glossary/emv-europay-mastercard-visa-smart-card/">https://www.cardlogix.com/glossary/emv-europay-mastercard-visa-smart-card/</a></u></p> <p><b>1. Purpose</b></p> <p>Card personalization is one of the major cost components in the production of EMV cards. <u>This specification standardizes the EMV card personalization process with the objective of reducing the cost of personalization thus facilitating the migration to chip.</u></p> <p><b>2. Scope</b></p>

Claim Language	Evidence of Infringement
<p>an interface device, the authentication token, and a personalization device,</p>	<p>In this specification, <u>card personalization means the use of data personalization commands that are sent to a card that already contains the basic EMV application. This is sometimes referred to as "on-card" personalization. The specification does not cover cards where an application load file is personalized before being loaded onto the card.</u></p> <p><b>Involved Entities</b></p>  <p><b>Involved Entities</b></p> <p>Source: EMV Card Personalization Specification, at page 8 &amp; 9 of 104</p>
<p>an interface device, the authentication token, and a personalization device,</p>	<p>EMV specification allows the authentication token to be entered into personalization mode. The personalization is carried out on an IC card ("authentication token") by a personalization device. After personalization, the IC card is handed over to a cardholder who can use the IC card at a terminal (such as POS device) ("an interface device") for initiating payments.</p> <p><b>Involved Entities</b></p>

Claim Language	Evidence of Infringement
	<div data-bbox="308 1008 747 1491" data-label="Diagram"> <pre> graph TD     CM[Card Manufacturer] --&gt; PB[Personalization Bureau]     subgraph PB [Personalization Bureau]         PS[Personalization Service]         DP[Data Preparation]     end     PS --&gt; CH[Cardholder]     I[Issuer] -- Issuer data --&gt; DP     </pre> </div> <div data-bbox="747 1260 787 1501" data-label="Section-Header"> <h3>5.5 Encryption</h3> </div> <div data-bbox="795 630 836 1501" data-label="Text"> <p>This section describes the encryption of secret data during personalization.</p> </div> <div data-bbox="852 525 1015 1501" data-label="Text"> <p><u>After personalization, confidential or secret data may be exchanged between a terminal and an IC card application. For example, a PIN may be changed between a terminal and an IC card during an online transaction. This section does not apply to encryption of secret data after personalization. Post personalization encryption is covered in application specific documents.</u></p> </div> <div data-bbox="1039 588 1079 1501" data-label="Text"> <p><u>Source: EMV Card Personalization Specification, at page 9 &amp; 81 of 104</u></p> </div>

Claim Language	Evidence of Infringement
<p>the system configured to establish an encrypted session between the authentication token and the personalization device using a transport key;</p>	<p>EMV specification allows establishing an encrypted session between the authentication token and the personalization device using a transport key. For example, whenever a secure channel is created (“encrypted session”), DES session keys are generated and one of them includes SKUdek (“transport key”).</p> <p><b>5.3 Session Keys</b></p> <p><u>DES session keys are generated every time a secure channel is initiated. These session keys may be used for subsequent commands if secure messaging is required. Up to three session keys may be generated, namely SKU<sub>ENG</sub>, SKU<sub>MAC</sub>, and SKU<sub>DK</sub>.</u></p> <p><u>Source: EMV Card Personalization Specification, at page 75 of 104</u></p>



Claim Language	Evidence of Infringement
<p>the interface device including a processor, a user interface, and an interface for communication with the authentication token;</p>	<p>The terminal such as a Point-of-Sale (POS) device ("interface device") should possess the enablement of a processor, a user interface, and an interface for communication with the IC card ("authentication token")</p> <p><b>5.5 Encryption</b></p> <p>This section describes the encryption of secret data during personalization.</p> <p><u>After personalization, confidential or secret data may be exchanged between a terminal and an IC card application. For example, a PIN may be changed between a terminal and an IC card during an online transaction. This section does not apply to encryption of secret data after personalization. Post personalization encryption is covered in application specific documents.</u></p> <p><u>Source: EMV Card Personalization Specification, at page 81 of 104</u></p>
<p>the authentication token including a personalization mode, and having a serial number; and</p>	<p>EMV specification allows the authentication token have a serial number. For example, the IC card ("authentication token") has an Rcard number which is the card challenge ("serial number").</p> <p><b>1. Purpose</b></p>

Claim Language	Evidence of Infringement																
	<p>Card personalization is one of the major cost components in the production of EMV cards. This specification standardizes the EMV card personalization process with the objective of reducing the cost of personalization thus facilitating the migration to chip.</p> <p>Source: EMV Card Personalization Specification, at page 8 of 104</p> <p><b>Table 14 - Response to INITIALIZE UPDATE command</b></p> <table border="1"> <thead> <tr> <th>Field</th> <th>Length</th> </tr> </thead> <tbody> <tr> <td>KEYDATA (See Table 15)</td> <td>10</td> </tr> <tr> <td>Version number of the master key (KMC)</td> <td>1</td> </tr> <tr> <td>Identifier for Secure Channel Protocol (ALGSCP = '02')</td> <td>1</td> </tr> <tr> <td>Sequence Counter</td> <td>2</td> </tr> <tr> <td>Card challenge (R<sub>CARD</sub>)</td> <td>6</td> </tr> <tr> <td>Card cryptogram</td> <td>8</td> </tr> <tr> <td>SW1 SW2</td> <td>2</td> </tr> </tbody> </table> <p>Source: EMV Card Personalization Specification, at page 55 of 104</p> <p><b>6.27 R<sub>CARD</sub> (Pseudo-Random Number from the IC Card)</b></p> <p><i>Purpose:</i> A pseudo-random number (see 3.2.5.9) generated by the IC card or the IC card application. Used in the creation of the host and card cryptograms.</p> <p><i>Format:</i> Binary, 6 bytes</p> <p>Source: EMV Card Personalization Specification, at page 88 of 104</p>	Field	Length	KEYDATA (See Table 15)	10	Version number of the master key (KMC)	1	Identifier for Secure Channel Protocol (ALGSCP = '02')	1	Sequence Counter	2	Card challenge (R <sub>CARD</sub> )	6	Card cryptogram	8	SW1 SW2	2
Field	Length																
KEYDATA (See Table 15)	10																
Version number of the master key (KMC)	1																
Identifier for Secure Channel Protocol (ALGSCP = '02')	1																
Sequence Counter	2																
Card challenge (R <sub>CARD</sub> )	6																
Card cryptogram	8																
SW1 SW2	2																
the personalization device being configured to encrypt the serial number	EMV specification allows the personalization device to encrypt the serial number and then forward the encrypted serial number to the authentication token. For example, the personalization device uses the master key i.e., KMC to generate the personalization keys i.e., Kenc, Kmac and Kdek. The																

Claim Language	Evidence of Infringement
<p>of the authentication token using a personalization key, and being configured to forward the encrypted serial number to the authentication token;</p>	<p>Kenc is used to generate a session key SKUenc which is used for creating and validating cryptograms. The SKUenc is used to create the host cryptogram by generating a MAC, which is then sent by the personalization device to the card.</p> <p>The data that is MACed to create the host cryptogram consists of the Rcard. Thus, it can be said that the serial number (Rcard) is encrypted by the Kenc (“the personalization key”) using SKUenc and forwarded to card (“authentication token”). Here, we have considered the Kenc as the personalization key because, it creates the SKUenc which then generates the MAC (host cryptogram) and sends to the card.</p> <div data-bbox="667 695 727 1472" style="border: 1px solid black; padding: 5px;"> <p><b>6.17 KMC (DES Master Key for Personalization Session Keys)</b></p> </div> <p><i>Purpose:</i> This DES key is used for generating derived keys to generate MACs and encrypt and decrypt DES keys and secret data during personalization (Kenc, Kmac and Knew).</p> <p><i>Format:</i> Binary, 16 bytes</p> <p><i>Notes:</i> Must be generated with odd parity.</p> <p><u>Source:</u> EMV Card Personalization Specification, at page 86 of 104</p> <p><b>4 IC Card Personalization Processing</b></p> <p><b>4.1 Preparation for Personalization (Pre-Personalization)</b></p> <div data-bbox="1138 575 1240 1415" style="border: 1px solid black; padding: 5px;"> <p>4.1.1.5 The version number of the personalization master key (KMC) used to generate the initial personalization keys (the Kenc, the Kmac and the Knew) for each application must be on the IC card.</p> </div> <p><u>Source:</u> EMV Card Personalization Specification, at page 68 of 104</p> <p><b>3.2.5 INITIALIZE UPDATE Command</b></p>

Claim Language	Evidence of Infringement
	<p>3.2.5.7 The first 6 bytes of KEYDATA returned from the INITIALIZE UPDATE command are used to identify the master key for secure messaging (KMC). The six least significant bytes of KEYDATA are used as key diversification data. The personalization device must use the KMC and KEYDATA to generate the K<sub>ENC</sub>, the K<sub>MAC</sub> and the K<sub>NEK</sub> for this IC card, as defined in section 4.1. These keys must have been placed in the IC card prior to the start of the personalization process.</p> <p><u>Source:</u> EMV Card Personalization Specification, at page 54 &amp; 56 of 104</p> <p><b>1.3 Secure Messaging</b></p> <p>Two derived keys on the IC card are used during the establishment of the secure channel. These are the K<sub>ENC</sub>, used to generate a session key SKU<sub>ENC</sub> which is in turn used to create and validate authentication cryptograms, and the K<sub>MAC</sub>, used to generate a session key SKU<sub>MAC</sub> which is in turn used to compute the MAC of the EXTERNAL AUTHENTICATE command. Both of these keys (K<sub>ENC</sub> and K<sub>MAC</sub>) are derived from the same master key, the KMC. When the secure channel is to be</p> <p><u>Source:</u> EMV Card Personalization Specification, at page 22 of 104</p> <p><b>3.2.6 EXTERNAL AUTHENTICATE Command</b></p> <p>3.2.6.6 The host cryptogram must be created by generating a MAC as described in section 5.4.1 using SKU<sub>ENC</sub>. The data to be MACed is = Sequence Counter (2 bytes)    R<sub>CARD</sub> (6 bytes)    R<sub>TERM</sub> (8 bytes). The IC card must verify the host cryptogram by generating a duplicate cryptogram and comparing it to the value received in the command data field.</p> <p><u>Source:</u> EMV Card Personalization Specification, at page 58 &amp; 59 of 104</p> <p><b>5.4 MACs</b></p>

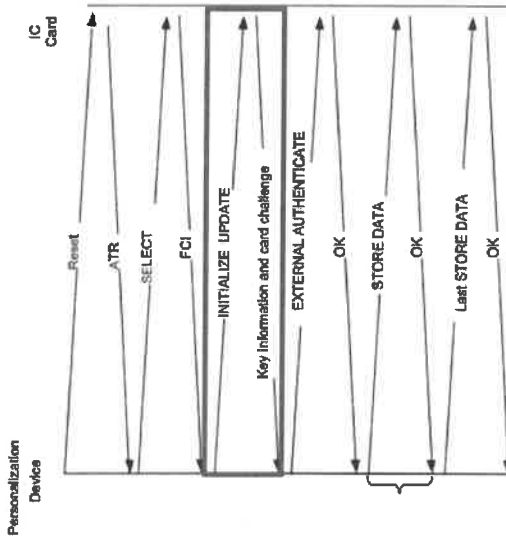
Claim Language	Evidence of Infringement
<p>the authentication token, when in the personalization mode, being configured to: receive, from the personalization device, a request for the serial number, and return the serial number to the personalization device;</p>	<p>The personalization process creates MACs for three purposes:</p> <ol style="list-style-type: none"> <li>1. During the IC personalization process (INITIALIZE UPDATE command and EXTERNAL AUTHENTICATE command) the IC card returns a MAC (the card cryptogram) and the personalization device sends a MAC (the host cryptogram) to the IC card. The IC card and the personalization device authenticate each other using these cryptograms. The process of creating the</li> </ol> <p>Source: EMV Card Personalization Specification, at page 75 &amp; 76 of 104</p> <p>EMV specification allows the personalization device to request serial number of the authentication token. For example, the personalization device sends an Initialize Update Command to the card ("authentication token") and in response to the update command; the card sends a Card Challenge ("serial number") to the personalization device. Rcard is a random number that is generated by the IC card or the IC card application.</p> <p><b>3.2.5 INITIALIZE UPDATE Command</b></p> <p>The INITIALIZE UPDATE command is the first command issued to the IC card after the personalization device selects the application. INITIALIZE UPDATE is used to establish the Secure Channel Session to be used during personalization. The data to perform mutual authentication is exchanged. The identifier and version number for the KMC and the data to be used to derive the Kenc, the KMAC and the KDK for the application are also returned.</p> <p>The INITIALIZE UPDATE command will be issued once for each secure channel initiation. It shall be issued at least once for each IC card application to be personalized.</p> <p>Table 14 – Response to INITIALIZE UPDATE command</p>

Evidence of Infringement

Field	Length
KEYDATA (See Table 15)	10
Version number of the master key (KMC)	1
Identifier for Secure Channel Protocol (ALGSCP = '02')	1
Sequence Counter	2
Card challenge (RCARD)	6
Card cryptogram	8
SW1 SW2	2

Source: EMV Card Personalization Specification, at page 54 & 55 of 104

Figure 6 - Personalization Command Flow



Claim Language	Evidence of Infringement
	<p>Source: EMV Card Personalization Specification, at page 50 of 104</p> <p><b>6.27 R<sub>CARD</sub> (Pseudo-Random Number from the IC Card)</b></p> <p><i>Purpose:</i> A pseudo-random number (see 3.2.5.9) generated by the IC card or the IC card application. Used in the creation of the host and card cryptograms.</p> <p><i>Format:</i> Binary, 6 bytes</p> <p>Source: EMV Card Personalization Specification, at page 88 of 104</p>
<p>decrypt the encrypted serial number forwarded from the personalization device, and validate that the personalization key is correct;</p>	<p>EMV specification allows the authentication token to decrypt the encrypted serial number and validate that the personalization key is correct. For example, the personalization keys such as Kenc is created by the IC card using the personalization master key (KMC) and Kenc is used in verifying the host cryptogram. The Kenc key is used by the IC card to generate a session key SKUenc which helps to create and validate authentication cryptograms. The IC card can generate a duplicate cryptogram and compare it to the value (host cryptogram) received to validate the same. As per the claim clause, the authentication token decrypts the encrypted serial number. In the EMV standard, the validation of the host cryptogram which is a MAC consisting of Rcard ("serial number") is done by the card. As per patent specifications, the card application decrypts the received data using the personalization key and validates it as correct. Since the Kenc personalization key can be used to verify the host cryptogram thus it could be said that decryption process could occur at the card.</p> <p><b>4 IC Card Personalization Processing</b></p> <p><b>4.1 Preparation for Personalization (Pre-Personalization)</b></p>

Claim Language	Evidence of Infringement
	<p><b>4.1.1.5</b> The version number of the personalization master key (K<sub>MCM</sub>) used to generate the initial personalization keys (the K<sub>ENC</sub>, the K<sub>MAC</sub> and the K<sub>DEK</sub>) for each application must be on the IC card.</p> <p><b>4.1.1.6</b> A derived key (K<sub>ENC</sub>) must be generated for each IC card and placed into the application. This key is used to generate the card cryptogram and to verify the host cryptogram. This key is also used to decrypt the STORE DATA command data field in CBC mode if the security level of secure messaging requires the command data field to be encrypted.</p> <p>Source: EMV Card Personalization Specification, at page 68 of 104</p> <p><b>5.4 MACs</b></p> <p>The personalization process creates MACs for three purposes:</p> <ol style="list-style-type: none"><li>1. During the IC personalization process (INITIALIZE UPDATE command and EXTERNAL AUTHENTICATE command) the IC card returns a MAC (the card cryptogram) and the personalization device sends a MAC (the host cryptogram) to the IC card. The IC card and the personalization device authenticate each other using these cryptograms. The process of creating the</li></ol> <p>Source: EMV Card Personalization Specification, at page 75 &amp; 76 of 104</p> <p><b>1.3 Secure Messaging</b></p>



Claim Language	Evidence of Infringement
<p>receive, from said personalization device through the encrypted session, an initial seed value and initial secret key, the initial seed value and the initial secret key being configured to facilitate an initial interaction between the authentication token and the interface device; and</p>	<p>Two derived keys on the IC card are used during the establishment of the secure channel. <u>These are the <math>K_{ENC}</math>, used to generate a session key <math>SK_{U_{ENC}}</math> which is in turn used to create and validate authentication cryptograms, and the <math>K_{MAC}</math>, used to generate a session key <math>SK_{U_{MAC}}</math> which is in turn used to compute the MAC of the EXTERNAL_AUTHENTICATE command. Both of these keys (<math>K_{ENC}</math> and <math>K_{MAC}</math>) are derived from the same master key, the KMC. When the secure channel is to be</u></p> <p><b>3.2.6 EXTERNAL AUTHENTICATE Command</b></p> <p>3.2.6.6 The host cryptogram must be created by generating a MAC as described in section 5.4.1 using <math>SK_{U_{ENC}}</math>. The data to be MACed is = Sequence Counter (2 bytes)    <math>R_{CARD}</math> (6 bytes)    <math>R_{TERM}</math> (8 bytes). <u>The IC card must verify the host cryptogram by generating a duplicate cryptogram and comparing it to the value received in the command data field.</u></p> <p>Source: EMV Card Personalization Specification, at page 22, 58 &amp; 59 of 104</p>
<p>receive, from said personalization device through the encrypted session, an initial seed value and initial secret key, the initial seed value and the initial secret key being configured to facilitate an initial interaction between the authentication token and the interface device; and</p>	<p>EMV specification allows reception of an initial seed value and an initial secret key such that the seed value and the secret key are used for facilitating initial interaction between the authentication token and the interface device. For example, the Store Data command is used for sending secret data or personalization data to the IC card. The secret data (“initial seed value and initial secret key”) is used for data exchange between the terminal (“interface device”) and the IC card. In the standard, the data exchanged between the authentication token and the terminal could include a PIN that form a part of the secret data. Here, we have considered the initial seed value and initial secret key as equivalent to the secret data.</p> <p><b>1.4 The STORE DATA Command</b></p> <p><u>The STORE DATA command is used to send personalization data to the card application; it is described in detail in section 3.2.7.</u></p> <p><b>5.3 Session Keys</b></p>

Claim Language	Evidence of Infringement
	<p>DES session keys are generated every time a secure channel is initiated. These session keys may be used for subsequent commands if secure messaging is required. Up to three session keys may be generated, namely <math>SKU_{ENC}</math>, <math>SKU_{MAC}</math>, and <math>SKU_{DEK}</math>.</p> <p><b>5.6 Decryption</b></p> <p><u>The personalization device must decrypt secret data encrypted by the data preparation process. This secret data will then be re-encrypted prior to sending to the IC card. The IC card should decrypt the secret data prior to storing it for future use. This section describes the decryption of secret data during personalization.</u></p> <p><b>5.5 Encryption</b></p> <p>This section describes the encryption of secret data during personalization.</p> <p><u>After personalization, confidential or secret data may be exchanged between a terminal and an IC card application. For example, a PIN may be changed between a terminal and an IC card during an online transaction. This section does not apply to encryption of secret data after personalization. Post personalization encryption is covered in application specific documents.</u></p> <p><u>Source: EMV Card Personalization Specification, at page 22, 75 &amp; 81 of 104</u></p>
<p>store the initial seed value and the initial secret key after decryption thereof using the transport key;</p>	<p>EMV specification allows the authentication token to store the seed value and secret key. As per the specification, the secret data is stored by the IC card and before storing, the secret data is decrypted using the transport key (<math>SKU_{DEK}</math>). The data is stored in an assigned location by the IC card.</p> <p><b>5.6 Decryption</b></p> <p><u>The personalization device must decrypt secret data encrypted by the data preparation process. This secret data will then be re-encrypted prior to sending to the IC card. The IC card should decrypt the secret data prior to storing it for future use. This section describes the decryption of secret data during personalization.</u></p> <p><u>Source: EMV Card Personalization Specification, at page 81 of 104</u></p>

Claim Language	Evidence of Infringement
	<p><b>6.33 SKU<sub>DEK</sub> (Personalization Session Key for Key and PIN Encryption)</b></p> <p><i>Purpose:</i> <u>This DES key is created during the personalization process and is used to encrypt and decrypt secret data in ECB mode.</u></p> <p><i>Format:</i> Binary, 16 bytes</p> <p><i>Content:</i> Derived as described in section 5.3.</p> <p><i>Remarks:</i> Parity convention not required</p> <p><b>5.6.1 Decryption Using ECB Mode</b></p> <p>5.6.1.2 <u>The IC card must use SKU<sub>DEK</sub> for decryption of encrypted data grouping values.</u></p> <p><u>Source:</u> EMV Card Personalization Specification, at page 82 &amp; 89 of 104</p>
<p>wherein, once said authentication token is personalized with the initial seed value and the initial secret key, the authentication token is configured to be unable to again enter to the personalization mode.</p>	<p>EMV specification allows the authentication token to store the seed value and secret key. Also, the authentication token can no longer enter the personalization mode. As per the specification, the secret data is stored by the IC card and before storing, the secret data is decrypted using the transport key (SKU<sub>DEK</sub>). The data is stored in an assigned location by the IC card. The Select command is used to select IC card application that is to be personalized and it is issued only once for each IC card application. Thus, it can be said that the authentication token can no longer enter the personalization mode once personalized.</p> <p><b>5.6 Decryption</b></p> <p><u>The personalization device must decrypt secret data encrypted by the data preparation process. This secret data will then be re-encrypted prior to sending to the IC card. The IC card should decrypt the secret data prior to storing it for future use. This section describes the decryption of secret data during personalization.</u></p> <p><b>The IC Card Application</b></p>

Claim Language	Evidence of Infringement
	<p>The IC card application receives the personalization data from the personalization device and stores it in its assigned location, for use when the EMV card application becomes operational.</p> <p>Source: EMV Card Personalization Specification, at page 21 &amp; 81 of 104</p> <p><b>6.33 <u>SKU<sub>oEK</sub></u> (Personalization Session Key for Key and PIN Encryption)</b></p> <p><i>Purpose:</i> This DES key is created during the personalization process and is used to encrypt and decrypt secret data in ECB mode.</p> <p><i>Format:</i> Binary, 16 bytes</p> <p><i>Content:</i> Derived as described in section 5.3.</p> <p><i>Remarks:</i> Parity convention not required</p> <p><b>5.6.1 Decryption Using ECB Mode</b></p> <p>5.6.1.2 The IC card must use SKU<sub>oEK</sub> for decryption of encrypted data grouping values.</p> <p>Source: EMV Card Personalization Specification, at page 82 &amp; 89 of 104</p> <p><b>3.2.4 SELECT Command</b></p> <p>The SELECT command is used to select each IC card application to be personalized. Application selection is described in EMV Version 4.1 Book 1.</p> <p>The SELECT command will be issued once for each IC card application to be personalized.</p> <p>Source: EMV Card Personalization Specification, at page 53 of 104</p>

52

