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:



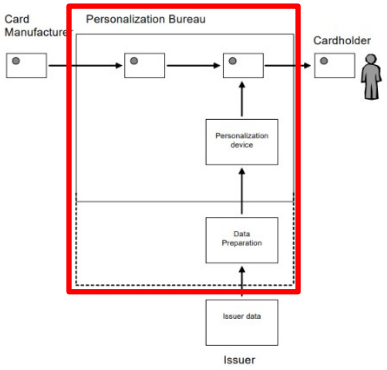
Cards and Packaging

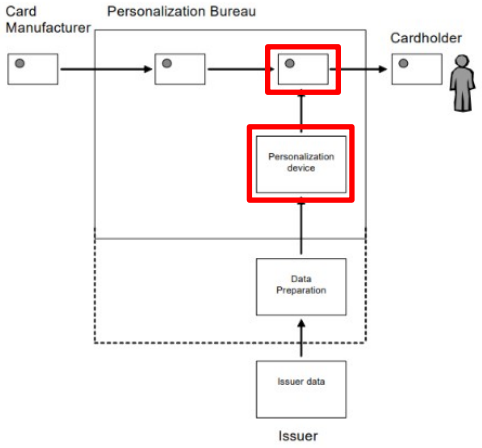
A wide range of payment card manufacturing, packaging and fulfillment options – including complete end-to-end EMV®, magnetic stripe, dual interface, high-content upcycled and recovered ocean-bound plastic, and metal card solutions.

Source: https://www.cpicardgroup.com/

Evidence of Use

Claim Language	Evidence of Infringement
1.A system for personalizing an authentication token comprising:	CPI card group 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. cpi card group® Cards and Packaging A wide range of payment card manufacturing, packaging and fulfillment options – including complete end-to-end EMV®, magnetic stripe, dual interface, high-content upcycled and recovered ocean-bound plastic, and metal card solutions. Source: https://www.cpicardgroup.com/ **1. Purpose** 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.

Claim Language	Evidence of Infringement
	2. Scope 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. **Involved Entities**  Source: EMV Card Personalization Specification, at page 8 & 9 of 104
an interface device, the authentication token, and a personalization device,	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. **Involved Entities**

Claim Language	Evidence of Infringement
	 **5.5 Encryption** This section describes the encryption of secret data during personalization. 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. Source: EMV Card Personalization Specification, at page 9 & 81 of 104

Claim Language	Evidence of Infringement
the system configured to establish an encrypted session between the authentication token and the personalization device using a transport key;	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"). **5.3 Session Keys** 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_{ENC}, SKU_{MAC}, and SKU_{DEK}. Source: EMV Card Personalization Specification, at page 75 of 104

Claim Language	Evidence of Infringement
the interface device including a processor, a user interface, and an interface for communication with the authentication token;	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") **5.5 Encryption** This section describes the encryption of secret data during personalization. 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. Source: EMV Card Personalization Specification, at page 81 of 104
the authentication token including a personalization mode, and having a serial number; and	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"). **1. Purpose**

<table>
<tr><th>Claim Language</th><th>Evidence of Infringement</th></tr>
<tr><td></td><td>
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.

Source: EMV Card Personalization Specification, at page 8 of 104

Table 14 – Response to INITIALIZE UPDATE command
<table>
<tr><th>Field</th><th>Length</th></tr>
<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 (RCARD)</td><td>6</td></tr>
<tr><td>Card cryptogram</td><td>8</td></tr>
<tr><td>SW1 SW2</td><td>2</td></tr>
</table>
Source: EMV Card Personalization Specification, at page 55 of 104

6.27 RCARD (Pseudo-Random Number from the IC Card)
Purpose: 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.
Format: Binary, 6 bytes

Source: EMV Card Personalization Specification, at page 88 of 104
</td></tr>
<tr><td>the personalization device being configured to encrypt the serial number</td><td>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</td></tr>
</table>

Claim Language	Evidence of Infringement
of the authentication token using a personalization key, and being configured to forward the encrypted serial number to the authentication token;	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. 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. **6.17 KMC (DES Master Key for Personalization Session Keys)** *Purpose:* This DES key is used for generating derived keys to generate MACs and encrypt and decrypt DES keys and secret data during personalization (K_{ENC}, K_{MAC} and K_{DEK}). *Format:* Binary, 16 bytes *Notes:* Must be generated with odd parity. Source: EMV Card Personalization Specification, at page 86 of 104 **4 IC Card Personalization Processing** **4.1 Preparation for Personalization (Pre-Personalization)** 4.1.1.5 The version number of the personalization master key (KMC) used to generate the initial personalization keys (the K_{ENC}, the K_{MAC} and the K_{DEK}) for each application must be on the IC card. Source: EMV Card Personalization Specification, at page 68 of 104 **3.2.5 INITIALIZE UPDATE Command**

Claim Language	Evidence of Infringement
	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_{ENC}, the K_{MAC} and the K_{DEK} 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. Source: EMV Card Personalization Specification, at page 54 & 56 of 104 **1.3 Secure Messaging** Two derived keys on the IC card are used during the establishment of the secure channel. These are the K_{ENC}, used to generate a session key SKU_{ENC} which is in turn used to create and validate authentication cryptograms, and the K_{MAC}, used to generate a session key SKU_{MAC} which is in turn used to compute the MAC of the EXTERNAL AUTHENTICATE command. Both of these keys (K_{ENC} and K_{MAC}) are derived from the same master key, the KMC. When the secure channel is to be Source: EMV Card Personalization Specification, at page 22 of 104 **3.2.6 EXTERNAL AUTHENTICATE Command** 3.2.6.6 The host cryptogram must be created by generating a MAC as described in section 5.4.1 using SKU_{ENC}. The data to be MACed is = Sequence Counter (2 bytes) || R_{CARD} (6 bytes) || R_{TERM} (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. Source: EMV Card Personalization Specification, at page 58 & 59 of 104 **5.4 MACs**

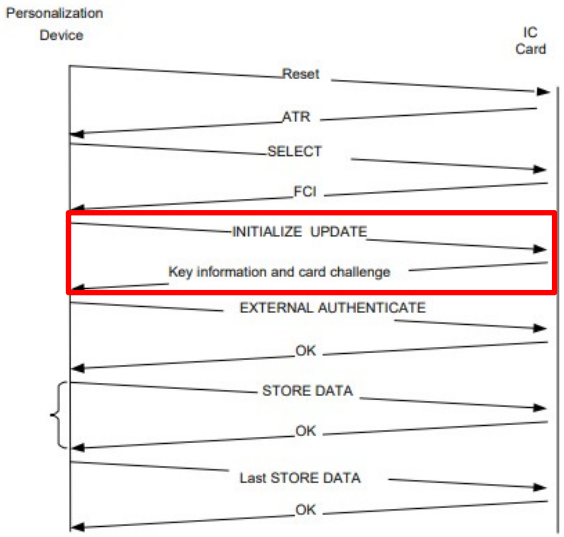
Claim Language	Evidence of Infringement
	The personalization process creates MACs for three purposes: 1. During the IC personalization process (INITIALIZE UPDATE command and EXTERNAL AUTHENTICATE command) the IC card returns a MAC (the card cryptogram) and the personalization device sends a MAC (the host cryptogram) to the IC card. The IC card and the personalization device authenticate each other using these cryptograms. The process of creating the Source: EMV Card Personalization Specification, at page 75 & 76 of 104
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;	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. **3.2.5 INITIALIZE UPDATE Command** 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 K_{ENC}, the K_{MAC} and the K_{DEK} for the application are also returned. 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. **Table 14 – Response to INITIALIZE UPDATE command**

Claim Language	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 (R_{CARD})	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
	Source: EMV Card Personalization Specification, at page 50 of 104 **6.27 R_{CARD} (Pseudo-Random Number from the IC Card)** *Purpose:* 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. *Format:* Binary, 6 bytes Source: EMV Card Personalization Specification, at page 88 of 104
decrypt the encrypted serial number forwarded from the personalization device, and validate that the personalization key is correct;	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. **4 IC Card Personalization Processing** **4.1 Preparation for Personalization (Pre-Personalization)**

Claim Language	Evidence of Infringement
	4.1.1.5 The version number of the personalization master key (KMC) used to generate the initial personalization keys (the K_{ENC}, the K_{MAC} and the K_{DEK}) for each application must be on the IC card. 4.1.1.6 A derived key (K_{ENC}) 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. Source: EMV Card Personalization Specification, at page 68 of 104 **5.4 MACs** The personalization process creates MACs for three purposes: 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 Source: EMV Card Personalization Specification, at page 75 & 76 of 104 **1.3 Secure Messaging**

Claim Language	Evidence of Infringement
	Two derived keys on the IC card are used during the establishment of the secure channel. These are the K_{ENC}, used to generate a session key SKU_{ENC} which is in turn used to create and validate authentication cryptograms, and the K_{MAC}, used to generate a session key SKU_{MAC} which is in turn used to compute the MAC of the EXTERNAL AUTHENTICATE command. Both of these keys (K_{ENC} and K_{MAC}) are derived from the same master key, the KMC. When the secure channel is to be **3.2.6 EXTERNAL AUTHENTICATE Command** 3.2.6.6 The host cryptogram must be created by generating a MAC as described in section 5.4.1 using SKU_{ENC}. The data to be MACed is = Sequence Counter (2 bytes)|| R_{CARD} (6 bytes)|| R_{TERM} (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. Source: EMV Card Personalization Specification, at page 22, 58 & 59 of 104
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	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. **1.4 The STORE DATA Command** The STORE DATA command is used to send personalization data to the card application; it is described in detail in section 3.2.7. **5.3 Session Keys**

Claim Language	Evidence of Infringement
	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_{ENC}, SKU_{MAC}, and SKU_{DEK}. **5.6 Decryption** 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. **5.5 Encryption** This section describes the encryption of secret data during personalization. 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. Source: EMV Card Personalization Specification, at page 22, 75 & 81 of 104
store the initial seed value and the initial secret key after decryption thereof using the transport key;	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 (SKUdek). The data is stored in an assigned location by the IC card. **5.6 Decryption** 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. Source: EMV Card Personalization Specification, at page 81 of 104

Claim Language	Evidence of Infringement
	6.33 SKU_{DEK} (Personalization Session Key for Key and PIN Encryption) *Purpose:* This DES key is created during the personalization process and is used to encrypt and decrypt secret data in ECB mode. *Format:* Binary, 16 bytes *Content:* Derived as described in section 5.3. *Remarks:* Parity convention not required **5.6.1 Decryption Using ECB Mode** 5.6.1.2 The IC card must use SKU_{DEK} for decryption of encrypted data grouping values. Source: EMV Card Personalization Specification, at page 82 & 89 of 104
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.	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. **5.6 Decryption** 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. **The IC Card Application**

Claim Language	Evidence of Infringement
	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. Source: EMV Card Personalization Specification, at page 21 & 81 of 104 **6.33 SKU_{DEK} (Personalization Session Key for Key and PIN Encryption)** *Purpose:* This DES key is created during the personalization process and is used to encrypt and decrypt secret data in ECB mode. *Format:* Binary, 16 bytes *Content:* Derived as described in section 5.3. *Remarks:* Parity convention not required **5.6.1 Decryption Using ECB Mode** 5.6.1.2 The IC card must use SKU_{DEK} for decryption of encrypted data grouping values. Source: EMV Card Personalization Specification, at page 82 & 89 of 104 **3.2.4 SELECT Command** 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. The SELECT command will be issued once for each IC card application to be personalized. Source: EMV Card Personalization Specification, at page 53 of 104