(12) UK Patent Application (19) GB (11) 2525426 (13) A

(43) Date of A Publication 28.10.2015

(21) Application No: 1407258.1

(22) Date of Filing: 24.04.2014

(71) Applicant(s):
Vodafone IP Licensing Limited
(Incorporated in the United Kingdom)
Vodafone House, The Connection, NEWBURY,
Berkshire, RG14 2FN, United Kingdom

(72) Inventor(s):
Jaime Antonio Abril Dovalo
Rebecca Claire Higley
Cristina Elena Vintila
Nikolai Strasding
Selin Özsoy
Sebastiaan Adrianus Alphonsus Petrus Hoeksel

(74) Agent and/or Address for Service:
Boult Wade Tennant
Verulam Gardens, 70 Gray's Inn Road, LONDON,
WC1X 8BT, United Kingdom

(51) INT CL:
G06Q 20/32 (2012.01) ***G06Q 20/36*** (2012.01)
G06Q 20/38 (2012.01) ***H04L 9/32*** (2006.01)
H04L 29/06 (2006.01)

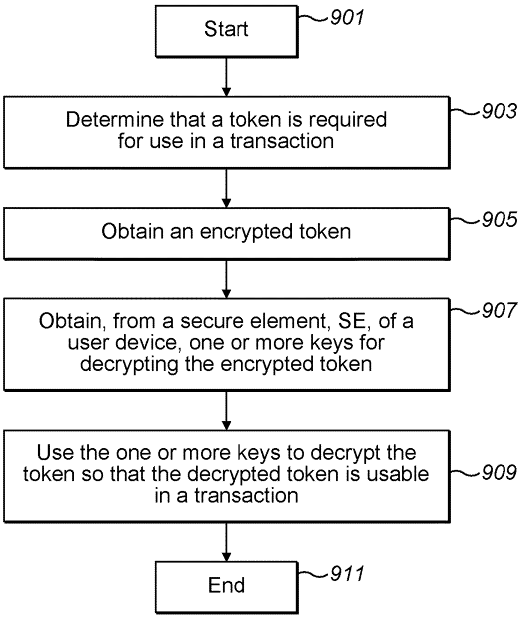
(56) Documents Cited:
None

(58) Field of Search:
Other: **No search performed: 17(5)(b) report issued**

(54) Title of the Invention: **Secure token implementation**
Abstract Title: **Use of encrypted token in e-commerce transactions**

(57) A method for obtaining a token for use in a transaction comprising the steps of: determining that a token is required for use in a transaction 903; obtaining an encrypted token 905; obtaining, from a secure element, SE, of a user device, one or more keys for decrypting the encrypted token 907; and using the one or more keys to decrypt the token so that the decrypted token is usable in a transaction 909. Advantageously, security is improved since if malicious activity results in tokens being retrieved from the user device, the encrypted tokens are unusable.

FIG. 9


Start
901
Determine that a token is required for use in a transaction
903
Obtain an encrypted token
905
Obtain, from a secure element, SE, of a user device, one or more keys for decrypting the encrypted token
907
Use the one or more keys to decrypt the token so that the decrypted token is usable in a transaction
909
End
911

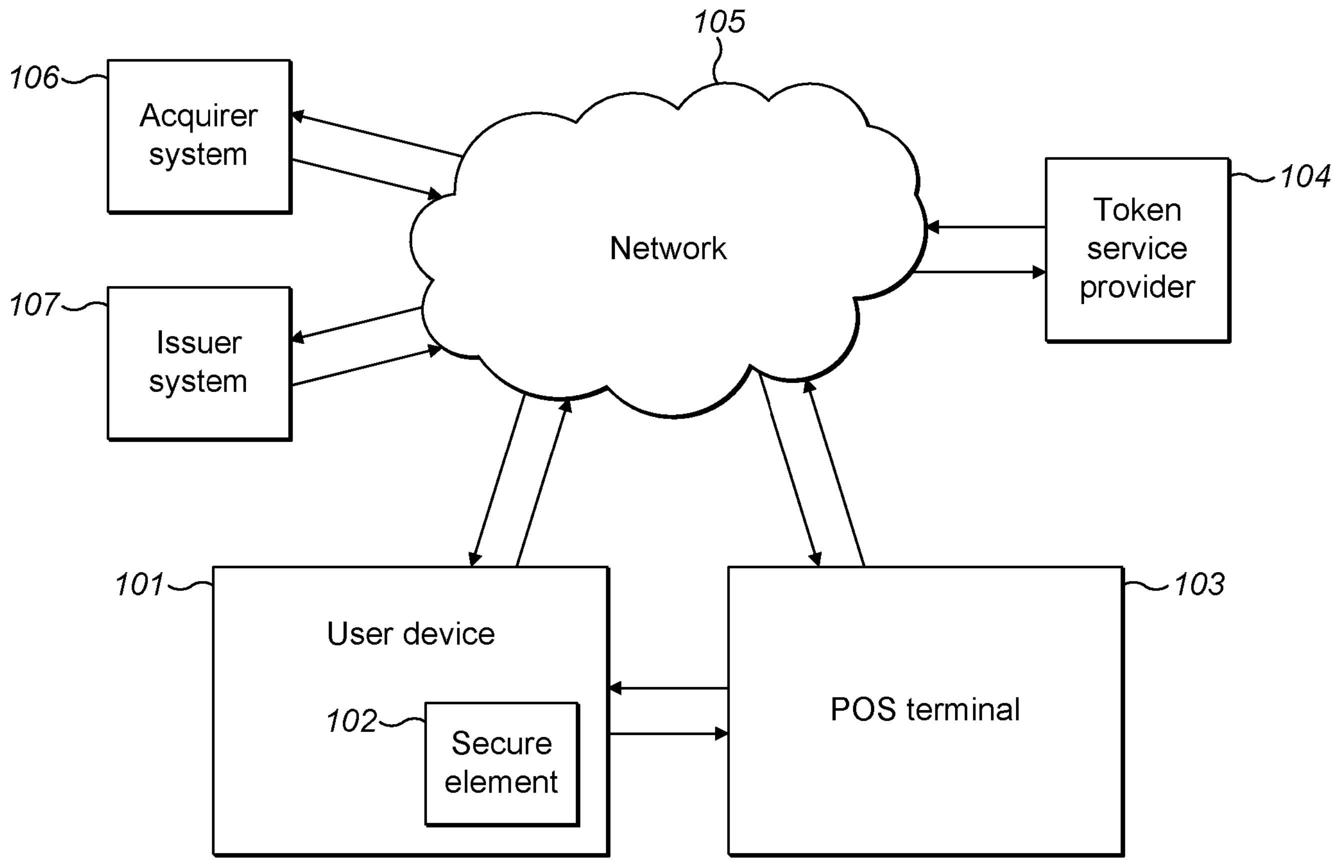

105
106
Acquirer system
Network
104
Token service provider
107
Issuer system
101
User device
103
POS terminal
102
Secure element

FIG. 1

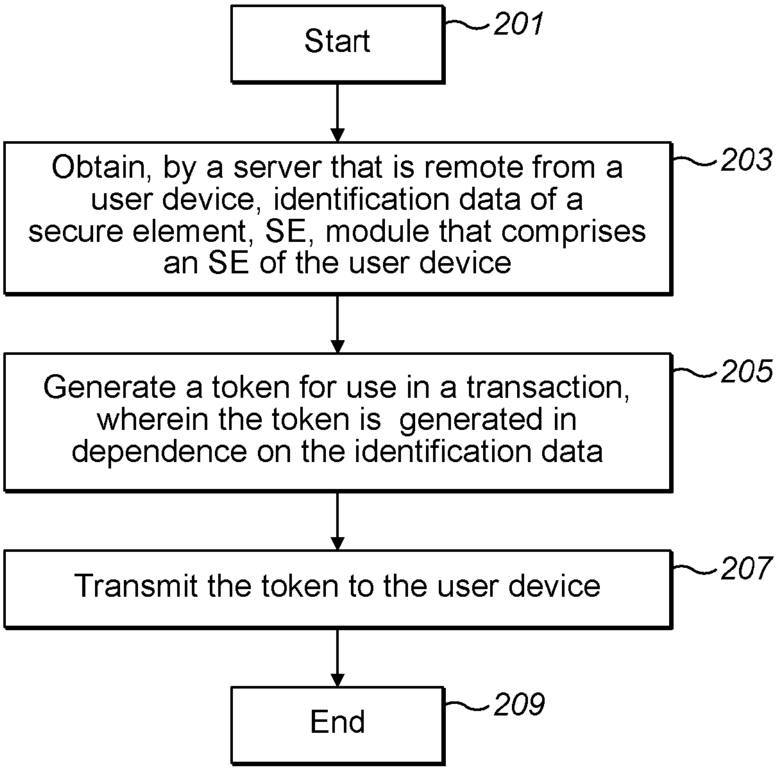

Start
201
Obtain, by a server that is remote from a user device, identification data of a secure element, SE, module that comprises an SE of the user device
203
Generate a token for use in a transaction, wherein the token is generated in dependence on the identification data
205
Transmit the token to the user device
207
End
209

FIG. 2

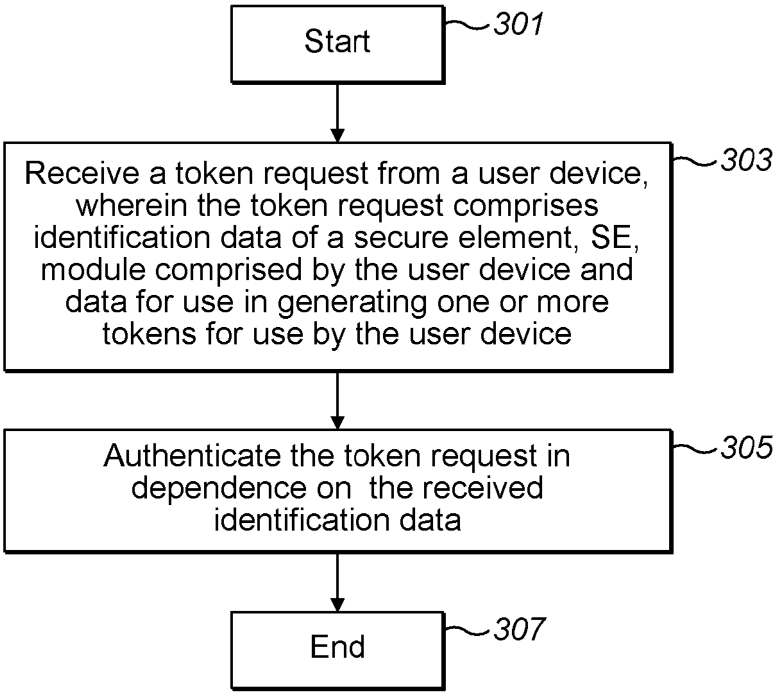

Start
301
Receive a token request from a user device, wherein the token request comprises identification data of a secure element, SE, module comprised by the user device and data for use in generating one or more tokens for use by the user device
303
Authenticate the token request in dependence on the received identification data
305
End
307

FIG. 3

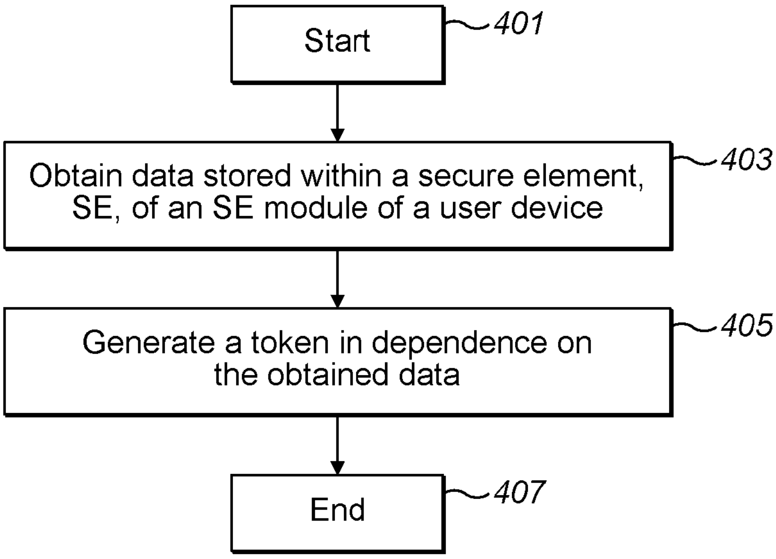

Start
401
Obtain data stored within a secure element, SE, of an SE module of a user device
403
Generate a token in dependence on the obtained data
405
End
407

FIG. 4

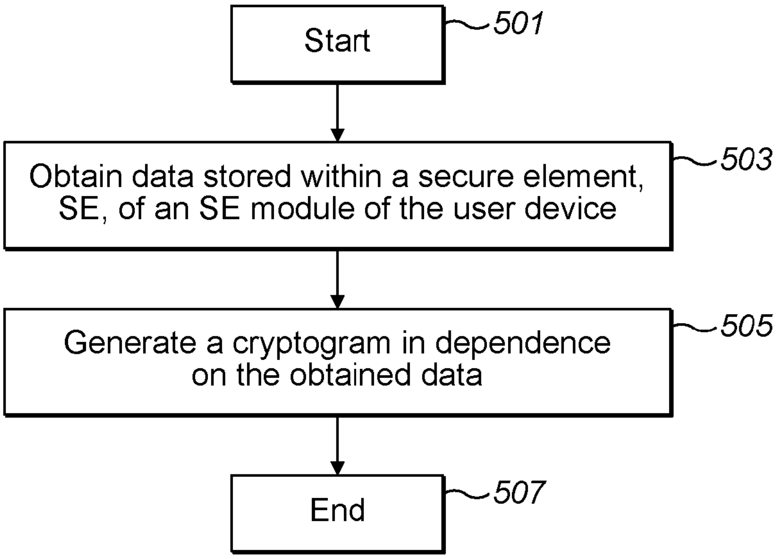

Start
501
Obtain data stored within a secure element, SE, of an SE module of the user device
503
Generate a cryptogram in dependence on the obtained data
505
End
507

FIG. 5

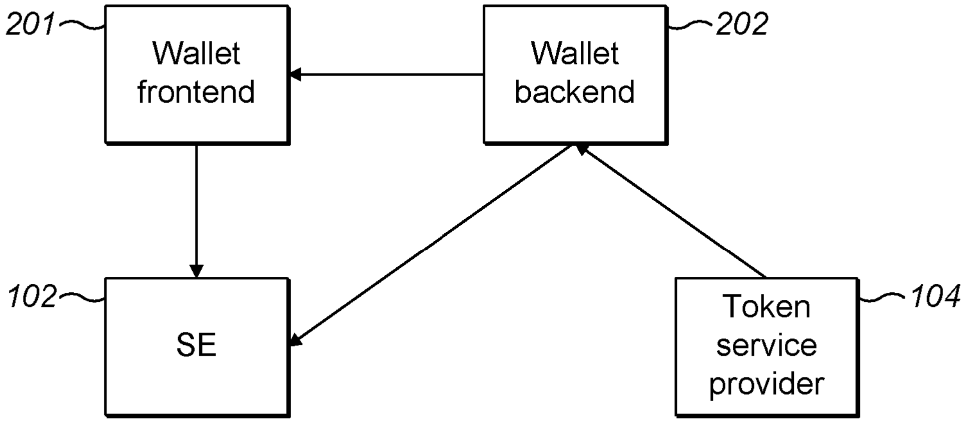

201
Wallet frontend
202
Wallet backend
102
SE
104
Token service provider

FIG. 6

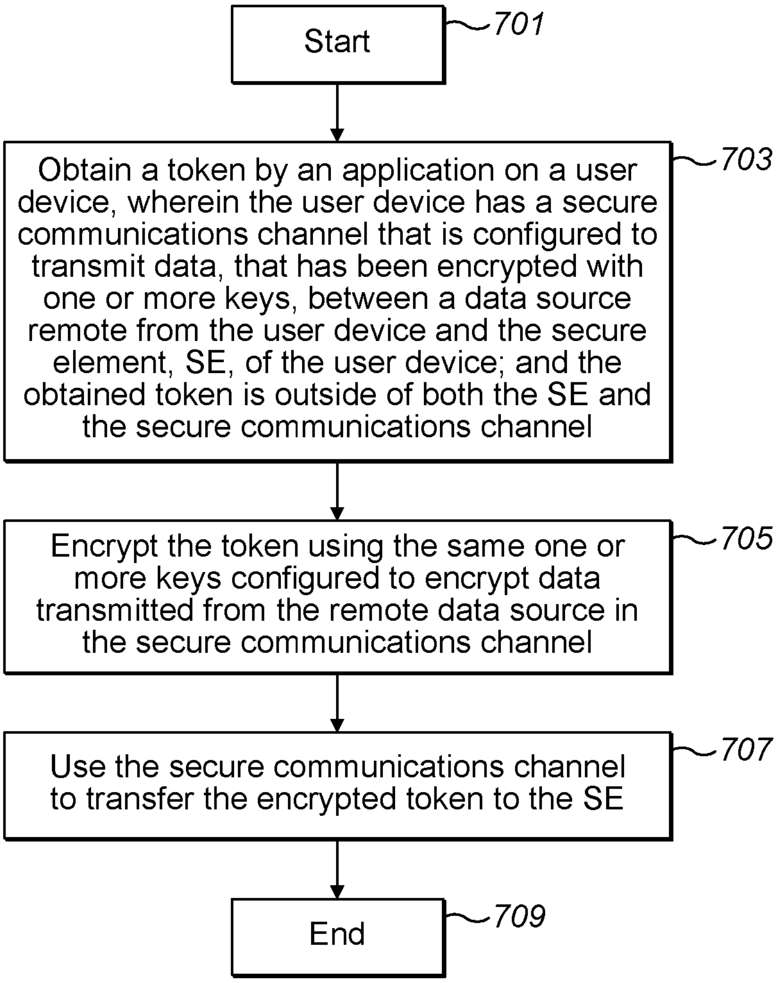

Start
701
Obtain a token by an application on a user device, wherein the user device has a secure communications channel that is configured to transmit data, that has been encrypted with one or more keys, between a data source remote from the user device and the secure element, SE, of the user device; and the obtained token is outside of both the SE and the secure communications channel
703
Encrypt the token using the same one or more keys configured to encrypt data transmitted from the remote data source in the secure communications channel
705
Use the secure communications channel to transfer the encrypted token to the SE
707
End
709

FIG. 7

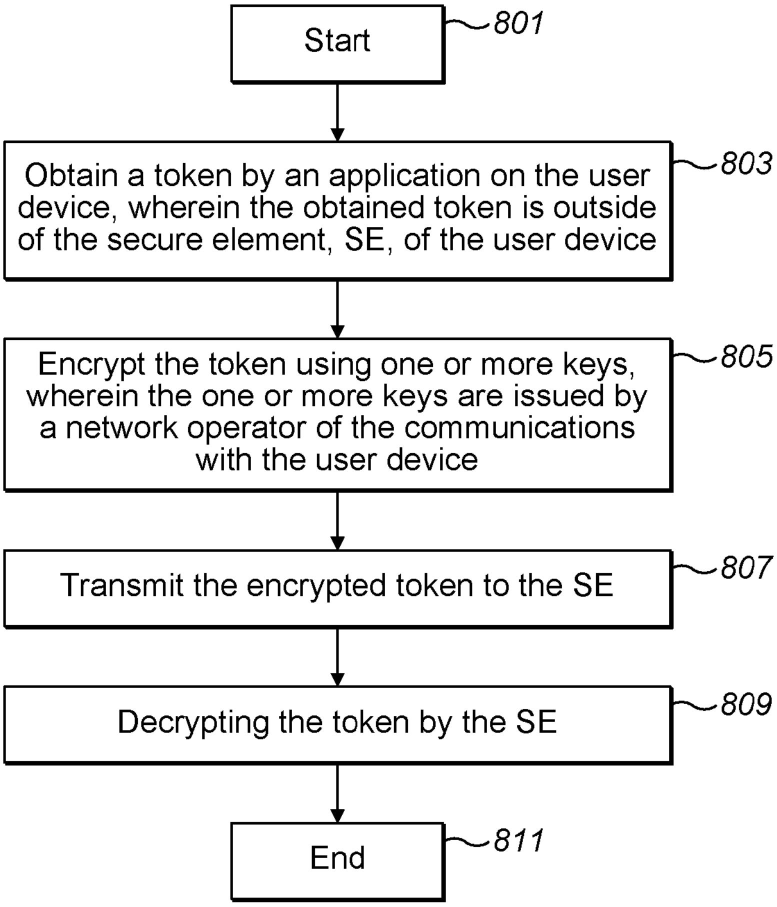

Start
801
Obtain a token by an application on the user device, wherein the obtained token is outside of the secure element, SE, of the user device
803
Encrypt the token using one or more keys, wherein the one or more keys are issued by a network operator of the communications with the user device
805
Transmit the encrypted token to the SE
807
Decrypting the token by the SE
809
End
811

FIG. 8

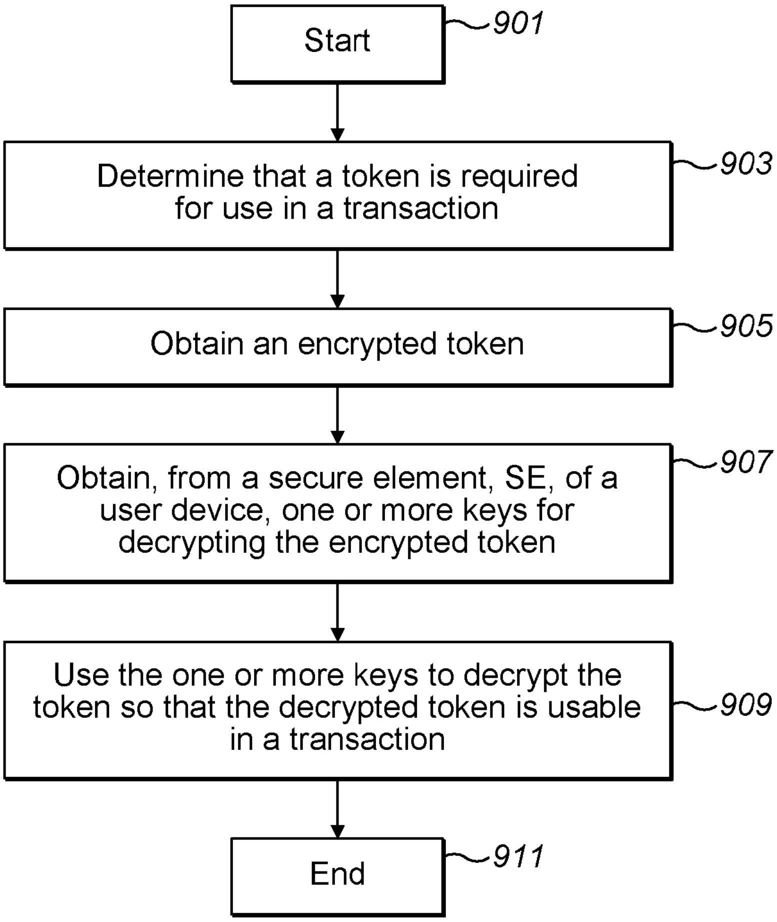

Start
901
Determine that a token is required for use in a transaction
903
Obtain an encrypted token
905
Obtain, from a secure element, SE, of a user device, one or more keys for decrypting the encrypted token
907
Use the one or more keys to decrypt the token so that the decrypted token is usable in a transaction
909
End
911

FIG. 9

SECURE TOKEN IMPLEMENTATION

Field of the Invention

The present invention relates to a method for improving the security of transactions by user devices. More particularly, embodiments of the invention improve the security of token based transactions. According to embodiments, the use of tokens is dependent on data stored in the secure element of a user's device. Advantageously, security is improved over known techniques.

Background to the Invention

Chip card technology for payments is well established. Problems experienced by chip cards include the cards being vulnerable to fraud in e-commerce and card not present transactions. The required data for performing such transactions are the user's Primary Account Number, PAN, the expiry data and CVV, and all of this data is printed on the card. In addition, the cards are limited to having a single purpose.

There has therefore been a lot of interest in replacing payments by chip cards with user devices, such as mobile telephones, that are able to function as payment devices in addition to providing other services. Important for the effective implementation of payments by such user devices is ensuring the security of sensitive personal data during transactions. In particular, the transfer of the payment data from the user device to a merchant's point-of-sale terminal and then to the issuer host needs to be robust.

A known technique for improving the security of personal data in a payment system is to use tokens. Tokens are surrogate values that are used instead of personal data, such as a user's PAN. Tokens may be used for implementing payment transactions as well as non-financial purposes, such as loyalty tracking. An advantage of using tokens is that the potential loss due to malicious activity is greatly reduced. For example, a token may be limited to use with a specific merchant, use in a specific country or use within a predetermined time period. Tokens may also be limited to just a single use. The potential loss resulting from the loss of a token with such use restrictions is less than that of fraudulent chip card payments that can be made in an almost unrestricted manner until the fraudulent activity has been detected and the functioning of the chip card stopped. Accordingly, even if a token is intercepted when it is transferred from a user device to a point-of sale terminal, the potential loss is greatly reduced.

The provisioning and using of tokens is described in EMV Payment Tokenisation Specification, Technical Framework, Version 1.0, March 2014, the entire contents of which are incorporated into the present document by reference.

Tokens are generated by a token service provider, that is remote from a user device, and transmitted to the user device. The token service provider generates payment tokens for a particular user in response to receiving a token request. The token request comprises personal data of the user, such as the user's PAN and its expiry date. The token service provider performs an identification and verification, ID&V, check on the received personal data in the token request and then generates tokens in dependence on the provided data in the token request.

Known token systems are implemented by Host Card Emulation, HCE, solutions. In HCE solutions, the user device is capable of emulating a chip card with token data stored in the user device. The token system has a server that is remote from both the user device and the token service provider. In order to obtain tokens to make payments, the user first needs to register his card details, which contain personal data, such as PAN, expiry date, etc., with the remote server. The server stores the personal data and uses it to request tokens from the token service provider every time tokens are needed.

A number of problems are experienced by the above-described operation of a token system.

A user's personal data is stored by the remote server. The user therefore has less control over their personal data as the personal data has been provided to a third party and malicious activity may result in personal data being stolen from the third party's server.

In addition, obtaining data from a remote server in order to generate a token request is a slow process that can only be performed when the user device has network connectivity. This results in a poor user experience.

Malicious activity may also result in tokens being intercepted when the tokens are transmitted to the user device, or tokens that are stored in the user device being retrieved from the user device. The obtained tokens may then be fraudulently used in transactions.

In order to limit the potential loss due to the lack of security, both the value of tokens, and the number of tokens that can be generated in response to a token request, are restricted. In addition, or alternatively, a validation through a PIN may be requested every time a token is used. These again result in a poor user experience.

Accordingly, known implementations of tokens by user devices experience a number of problems.

Summary of the Invention

According to a first aspect of the invention, there is provided a method for obtaining a token for use in a transaction, the method comprising: determining that a token is required for use in a transaction; obtaining an encrypted token; obtaining, from a secure element, SE, of a user device, one or more keys for decrypting the encrypted token; and using the one or more keys to decrypt the token so that the decrypted token is usable in a transaction.

Preferably, the method further comprises: obtaining a token; obtaining one or more keys for encrypting the token; and using the one or more keys to encrypt the token so that the token is not usable in a transaction.

Preferably, the encrypted token is stored on the user device but outside of the SE of the user device.

Preferably, the one or more keys are keys issued by a network operator of the communications with the user device and/or a payment service provider.

Preferably, the token is for paying for a transaction and is for use in one or more systems and methods according to an EMV Payment Tokenisation Specification.

Preferably, the token comprises one or more of identification data of the SE, a primary account number and an expiry date of a primary account number.

Preferably, the token comprises identification data and the identification data is an integrated circuit card identifier.

Preferably, the obtained token has been generated by the user device.

Preferably, the user device is a mobile telephone or a mobile computing device.

Preferably, the SE is a smart card of the user device or a subscriber identification module, SIM, of the user device.

According to a second aspect of the invention, there is provided a user device for using a token in a transaction, wherein the user device is configured to perform the method as set out in the first aspect.

Brief Description of the Drawings

Embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 shows a system according to an embodiment of the invention;

Figure 2 shows a process according a first embodiment of the invention;

Figure 3 shows another process according a first embodiment of the invention;

Figure 4 shows a process according a second embodiment of the invention;

Figure 5 shows a process according a third embodiment of the invention;

Figure 6 shows communication paths according to a fourth embodiment of the invention;

Figure 7 shows a process according a first implementation of the fourth embodiment of the invention;

Figure 8 shows a process according a second implementation of the fourth embodiment of the invention; and

Figure 9 shows a process according a fifth embodiment of the invention.

Detailed Description

Embodiments of the invention solve at least some of the above-described problems and improve the security of the implementation of tokens on user devices.

According to embodiments, the use of tokens is dependent on data stored in the Secure Element, SE, of a user device. The stored data may be the personal data of a user.

In a first embodiment, tokens are generated in dependence on identification data of the SE module that supports the SE. Advantageously, the tokens are dependent on identification data related to the user device that they were intended for use by. Security is improved by generating tokens that can be easily prevented from being used by any other user device.

In a second embodiment, personal data for generating a token request is stored in the SE. Advantageously, there is no need for a remote server to store this personal data and either to generate a token request itself or to provide it to the user device in order for the user device to generate a token request.

In a third embodiment, data in the SE is used to generate a cryptogram. Advantageously, the cryptogram improves the security of transactions performed by the user device.

In a fourth embodiment, the SE stores one or more tokens and a token is not retrieved from the SE until it is required for use during a transaction. Advantageously, this prevents malicious activity from stealing tokens from the user device.

In a fifth embodiment, the user device stores encrypted tokens. The SE is required to decrypt the tokens. Advantageously, even if malicious activity does result in tokens being retrieved from the user device, the encrypted tokens are unusable.

Embodiments are described in more detail below.

Figure 1 shows a system according to an embodiment. The system comprises a user device, a network, an issuer system, an acquirer system, a token service provider and a merchant's point-of-sale terminal.

The user device may be, for example, a mobile device such as a mobile telephone or computing tablet or any type of computing device for making token based payments. The user device comprises a communications interface for communicating with the network. The same, or an additional, communications interface may also be used for communicating with the terminal.

The network shown in Figure 1 may comprise a plurality of networks. For example, the network may comprise a wireless communications network for communications with the mobile device as well as a payment network for communications with the issuer system, acquirer system, token service provider and the terminal.

The issuer system is provided by the bank of the user of the user device and controls the transfer of money from the user's account during a financial transaction.

The acquirer system is the bank of the merchant that the user is making a payment to and controls the transfer of money into the merchant's account during a financial transaction.

The token service provider is a server system for generating tokens in response to receiving a token request triggered by a user device. After the token service provider has generated one or more tokens, the tokens are transmitted to the user device.

The terminal is any type of merchant's point-of-sale terminal that is capable of accepting a token-based payment. Suitable communications links for transferring token-based payments from the user device to the terminal include near field communication, NFC, Bluetooth and WiFi. In addition, or alternatively, a user device may transfer a token-based payment to the terminal by the user device generating a computer readable code, such as a QR code, in dependence on the token-based payment. To transfer the token-based payment, the user device displays the computer readable code and the code is read by a computer readable code reader of the terminal. The terminal may also be capable of transmitting data to the user device. This may be used by the terminal to provide the user device with acknowledgements of accepted token-based payments.

The operation, and communication between, such a user device, issuer system, acquirer system, token service provider and merchant's terminal in order to implement a payment is well known in the art and the skilled person would be aware of a number of ways in which these techniques can be implemented.

The user device comprises a Secure Element, SE. An SE is a tamper resistant component which provides a secure and confidential operating environment in the user device. The SE may run multiple applications for a variety of purposes. The SE may be all or part of an SE module. Suitable from factors include an universal integrated circuit card (UICC), eUICC, an embedded SE, a smartSD, a smart microSD, and others known in the art.

Implementations and operations of an SE are described in VISA MOBILE, Proximity Payment Testing & Compliance Requirements for MicroSD and Mobile Accessories, Version 3.1, February 2014, the entire contents of which are incorporated herein by reference.

Communications with a SE are described in GlobalPlatform Device Technology, Secure Element Access Control, Version 1.0.20, March 2014, the entire contents of which are incorporated herein by reference.

SEs, and communication with SEs over an NFC interface in order to pay for a transaction, is described in 'Mobile/NFC Security Fundamentals', Secure Elements 101, Smart Card Alliance Webinar, March 28, 2013, http://www.smartcardalliance.org/resources/webinars/Secure_Elements_101_FINAL3_0

32813.pdf viewed on 14 April 2014, the entire contents of which are incorporated herein by reference.

According to embodiments, the SE may store personal data, such as a PAN and its expiry date, identification data of the SE module that supports the SE, such as an integrated circuit card identifier, ICCID, and other data for use in token based transactions. The SE may also store tokens that have either been generated by the SE itself or generated elsewhere and provided to the SE.

Preferably, the user device functions as an electronic/digital wallet that provides a payment token whenever needed by the user to pay for a transaction. The wallet has a frontend for communicating with the SE of the user device and a backend for communicating with other applications on the user device, a remote token service provider and/or interface to a remote point-of-sale terminal. The number of tokens available from the wallet is monitored and, if the number of tokens has decreased to a predetermined threshold amount, a request for one or more tokens is automatically generated. The monitoring of the number of tokens in the wallet may be by the wallet backend, wallet frontend (which can be a wallet client application), or SE module on the user device.

In a first embodiment, the tokens are generated by a token service provider remote from the user device. The user device generates and sends a token request to the token service provider.

In a preferred implementation, the wallet frontend automatically determines that a token request should be generated due to the number of available tokens being at or below a predetermined threshold level. The wallet frontend generates and sends a message to the SE module that is a request for the SE module to sign a token request. The token request is a request for one or more tokens and comprises token request data, i.e. the data required by a remote token service provider to generate one or more tokens, such as a PAN and its expiry date. The above-described determination that a token request should be generated, and sending a message to the SE module, may alternatively be performed by the wallet backend.

The SE module receives the message comprising a token request from the wallet frontend. In response to receiving the message, the SE module obtains identification data stored in the SE and inserts the identification data into the token request. The token request is entirely hashed and is signed for the requested number of tokens with a private key of the SE module. The private key used to sign the token request is stored in the SE.

Advantageously, a token request for transmission to a remote token service provider is generated with the token request comprising identification data of the SE module. The token service provider is able to verify the authenticity and integrity of the token request by determining that the request comprises the identification data of the SE module and checking the hash and signature.

In an alternative implementation, the token request sent to the token service provider does not comprise identification data of the SE module and the token service provider obtains the identification data by other means. For example, the identification data may be already known by the token service provider and stored therein. The token service provider may alternatively obtain the identification data by directly, or indirectly via the user device or other means, requesting the identification data from another server that is remote from both the token service provider and the user device. The token request received from the user device is still hashed and signed for the requested number of tokens with a private key of the SE module.

The token service provider generates one or more tokens in dependence on the identification data and the token request sent from the user device. The token service provider transmits the one or more generated tokens to the wallet backend and/or frontend.

Advantageously, by generating the tokens in dependence on the identification data, the generated tokens may be easily made usable only by a specific user device and so there is no value in a malicious party attempting to intercept tokens for use by any other device. In addition, the user device does not have the computational burden of generating tokens and it is not necessary for the user device to be provided with any additional data required for generating tokens.

Figure 2 is a flow chart of a process according to the first embodiment.

In step 201, the process begins.

In step 203, a server that is remote from a user device obtains identification data of a secure element, SE, module that comprises an SE of the user device.

In step 205, a token is generated for use in a transaction, wherein the token is generated in dependence on the identification data.

In step 207, the token is transmitted to the user device.

In step 209, the process ends.

Figure 3 is a flow chart of another process according to the first embodiment.

In step 301, the process begins.

In step 303, a token request is received from a user device, wherein the token request comprises identification data of a secure element, SE, module comprised by the user device and data for use in generating one or more tokens for use by the user device.

In step 305, the token request is authenticated in dependence on the received identification data.

In step 307, the process ends.

In a second embodiment, the SE stores personal data for generating a token request.

A user enters their personal data to the user device. The personal data preferably includes the user's real PAN and its expiry date. The personal data is stored in the SE only after an ID&V operation on the personal data has been performed and the result has been positive. A preferred implementation of the ID&V operation is for the personal data to be provided to the wallet frontend. The wallet frontend determines that an ID&V operation is required and transmits, via the wallet backend, the personal data to the user's issuer system that is remote from the user device. The issuer system verifies the personal data, according to known verification techniques in the art, and transmits, via the wallet backend, an ID&V verification response back to the wallet frontend. The wallet frontend then transmits the ID&V verification response to the SE module that stores the ID&V verification response in the SE. The ID&V operations are preferably implemented by 3-D Secure techniques, as is known in the art.

Once the personal data is stored in the SE, it is not necessary for another ID&V operation to be performed on the data. The ID&V verification response is preferably used to generate a token assurance level that is applied to tokens that are generated in dependence on the verified personal data. Token assurance levels are described in the above-cited EMV Payment Tokenisation Specification.

Token requests are generated in dependence on the personal data stored in the SE and, optionally, ID&V verification response data also stored therein. A token request may be generated entirely by operations within the SE itself or the personal data may be retrieved from the SE and the token request generated by wallet applications on the user device, that operate outside of the SE. The token request is hashed and signed by a private key obtained from the SE module as described for the first embodiment. Optionally, the token request is also generated in dependence on identification data of the SE module and is a token request as described for the first embodiment.

The generated token request is transmitted by the user device to a token service provider for generating a token. The token service provider that receives the token request may operate according to the first embodiment as described in the present document.

Advantageously, token service providers are not required to perform ID&V checks on the personal data provided by token requests. It is also not necessary to store personal data on the server of a third party and to perform the slow and unreliable process of either requesting a remote server to generate a token request or for a user device to request personal data from a remote server whenever generating a token request.

In another implementation applications on the user device itself operates as the token service provider and there is no token request sent from the user device. Any additional data required for generating tokens is transmitted to the user device. The user device uses wallet applications outside of the SE and, optionally, applications executed within the SE, to generate one or more tokens in dependence on the personal data and, optionally, SE module identification data that is stored in the SE.

Advantageously, security is improved by maintaining the personal data on the user device during token generation. The data involved in token generation is not transmitted at all over the network and remains on the user device. Preferably, the personal data is stored securely on, and never leaves, the SE during the token generation process.

In another implementation, applications only on the SE operate as the token service provider, without any applications outside of the SE being used to generate a token. Any additional data required for generating tokens is provided to the SE. Preferably, the generated tokens are stored in the SE and are never present outside of the SE until required for use during a transaction.

Advantageously, security is further improved by maintaining the personal data as well as all other data for generating a token in the SE of the user device during token generation.

Figure 4 is a flow chart of a process according to the second embodiment.

In step 401, the process begins.

In step 403, data stored within a secure element, SE, of an SE module of a user device is obtained.

In step 405, a token is generated in dependence on the obtained data.

In step 407, the process ends.

According to a third embodiment, a cryptogram is generated in dependence on data stored in the SE. The cryptogram functions as a token cryptogram as described in the above-cited EMV Payment Tokenisation Specification.

By generating the cryptogram in dependence on data stored in the SE, it is possible to determine from the cryptogram that a payment with a token is being performed by a token that has been stored in the same SE. The data in the SE used to generate the cryptogram is secret to the SE and can be used to perform identification and authorisation operations on the cryptogram. Preferably, the data is a private key of the SE module. The data may also be an additional data value, such as an application transaction counter, ATC. The additional data value may be known to be only derived from the SE such that it can be shown that cryptogram was generated by that SE. Alternatively, or in addition, the data that the cryptogram is generated in dependence upon includes personal data of the user, such as a PAN and its expiry date, identification data of the SE module, or any other data.

Advantageously, security is improved since the cryptogram is identifiable as being created by the SE of the user device. A token that uses the cryptogram can be determined to have been stored in the SE.

Figure 5 is a flow chart of a process according to the third embodiment.

In step 501, the process begins.

In step 503, data stored within a secure element, SE, of an SE module of the user device is obtained.

In step 505, a cryptogram is generated in dependence on the obtained data.

In step 507, the process ends.

According to a fourth embodiment, tokens received by the wallet backend and/or frontend from a remote token service provider are securely transmitted to the SE and stored in the SE until required for use.

In a first implementation, the wallet backend uses a secure channel to transport the tokens to the SE.

Trusted Service Manager, TSM, is a known technique for securely performing the provisioning and lifecycle management of service provider credentials e.g. payment, transport, etc. The TSM acts as a connection point between service providers, such as banks, transit operators and merchants, and SE modules, that are issued by mobile network operators. NFC payments by mobile devices using UICC or device SE can use the TSM model and how to implement the secure channel required for this would be known by the skilled person.

The TSM is described in the White Paper: The Role of the Trusted Service Manager in Mobile Commerce, December 2013, http://www.gsma.com/digitalcommerce/wp-content/uploads/2013/12/GSMA-TSM-White-Paper-FINAL-DEC-2013.pdf, viewed on 11th April 2014, the entire contents of which are incorporated herein by reference.

The joint GSMA and European Payments Council publication, EPC – GSMA: Mobile Contactless Payments Service Management Roles: Requirements and Specifications: DocEPC 220-08, Ver 2.0, October 2010, describes the role of a TSM in managing secure card emulation services and is also incorporated in its entirety herein by reference.

The above-cited document 'Mobile/NFC Security Fundamentals' describes how a TSM is used to enable payments over an NFC interface.

In a first implementation, the wallet backend uses existing OTA and/or OTI (or other mechanisms in place that achieve the goal of communication to the SE) capabilities of the TSM to open a channel to the SE and to transmit the received tokens to the SE for storage therein. The channel is preferably direct between the wallet backend and the SE. This direct channel is an end-to-end secure channel, opened on top of the actual communication/transport channel between the OTA/OTI (or other mechanisms in place that achieve the goal of communication to the SE) platform and the SE. The wallet backend is provisioned with, or obtains, any keys or other data required for transmitting the tokens via the TSM communication system. The keys may be the existing mobile network operator keys and/or those of a payment service provider and/or any other keys that are used to create a secure end-to-end communication channel between the wallet backend and the SE. The keys are preferably specific to the mobile network operator. The keys may be provisioned to the SE and/or the wallet backend at the time of their manufacture. The wallet backend uses the one or more keys to encrypt the token so that the token is encrypted in the same way as if it had been transmitted to the user device from a remote data source using the TSM OTA/OTI capabilities, or any other TSM communication technique. The encrypted token is then provided to the communication channel and transmitted to the SE.

Advantageously, this method of provisioning the tokens on the SE makes use of the existing TSM infrastructures in a simplified manner.

According to a second implementation, the wallet backend is provisioned with one or more keys. The wallet backend encrypts received tokens using the one or more keys. The tokens are then transmitted to the SE via the wallet frontend. The keys are preferably issued by the mobile network operator that supports communication with the user device and private keys. The keys may be existing keys used for TSM communications. The keys may be provisioned to the SE and/or the wallet backend at the time of their manufacture. The wallet backend to wallet frontend communication is secure and the transmission of tokens to the wallet frontend is done securely. On top of that, by sharing a common secret key or, alternatively, by using an asymmetric key mechanism, the wallet backend and the SE ensure end-to-end security of the token transmission.

Advantageously, the transfer of the tokens to the SE is secure.

Figure 6 shows the communication paths between the wallet backend and the SE in the above-described first and second implementations of the fourth embodiment.

In the first implementation, the tokens are preferably transmitted directly from the wallet backend to the SE via a secure channel (opened by the TSM or OTA directly from the wallet backend, if the wallet backend has OTA capabilities) and the tokens are preferably not transmitted via the wallet frontend or any other applications.

In the second implementation, the encrypted tokens are transmitted from the wallet backend to the wallet frontend, and then from the wallet frontend to the SE.

Figure 7 is a flow chart of a process according to the first implementation of the fourth embodiment.

In step 701, the process begins.

In step 703, a token is obtained by an application on a user device, wherein the user device has a secure communications channel that is configured to transmit data, that has been encrypted with one or more keys, between a data source remote from the user device and the secure element, SE, of the user device; and the obtained token is outside of both the SE and the secure communications channel.

In step 705, the token is encrypted using the same one or more keys configured to encrypt data transmitted from the remote data source in the secure communications channel.

In step 707, the secure communications channel is used to transfer the encrypted token to the SE.

In step 709, the process ends.

Figure 8 is a flow chart of a process according to the second implementation of the fourth embodiment.

In step 801, the process begins.

In step 803, a token is obtained by an application on the user device, wherein the obtained token is outside of the secure element, SE, of the user device.

In step 805, the token is encrypted using one or more keys, wherein the one or more keys are issued by a network operator of the communications with the user device.

In step 807, the encrypted token is transmitted to the SE.

In step 809, the token is decrypted by the SE.

In step 811, the process ends.

In a fifth embodiment, tokens are stored on the user device but outside of the SE. When one or more tokens transmitted by the token service provider are received by the wallet backend, the tokens are encrypted with a public key. The public key may be stored in the wallet backend or the SE. The private key for decrypting the encrypted tokens is only stored in the SE.

In response to determining that token is required for use in a transaction, an encrypted token is obtained and decrypted. Accordingly, a token is only decrypted just before it is required for use during a payment transaction.

Advantages include not needing to perform a process for transferring a token to the SE and not requiring a storage area on the SE for the token. The encryption and decryption process can be performed without requiring any network connectivity.

Figure 9 is a flow chart of a process according to the second implementation of the fifth embodiment.

In step 901, the process begins.

In step 903, it is determined that a token is required for use in a transaction.

In step 905, an encrypted token is obtained.

In step 907, one or more keys for decrypting the encrypted token are obtained from a secure element, SE, of a user device.

In step 909, one or more keys are used to decrypt the token so that the decrypted token is usable in a transaction.

In step 911, the process ends.

In the above-described embodiments, one or more tokens and/or cryptograms are obtained by a user device for use in one or more transactions. The use of the token(s) in a transaction may be based on any known techniques, such as those described in the above-cited EMV Payment Tokenisation Specification.

Embodiments also include a number of modifications and variations that can be made to the embodiments as described above.

In the above-described embodiments, identification data of a SE module is referred to. This identification data may be identification data of only the SE. Alternatively, the identification data may not be identification of either the SE or the SE module, but other data.

The SE module may be the physical hardware that the SE is provided by. Alternatively, the SE module may be just the SE itself.

Embodiments have been generally described with reference to payment transactions. Embodiments also include applying the disclosed techniques for ensuring security of tokens that are not used for payments.

In an embodiment, whether or not a token is stored in the SE is dependent on the use restrictions of the token. If the token is valid to use for a long period of time or is suitable for high value transactions, then the token is stored in the SE. Otherwise, it is determined to store the token outside of the SE, preferably encrypted in accordance with the fifth embodiment.

In the first embodiment, it is not necessary for the token request to be sent by the user device that the token(s) are to be generated for. The token request may alternatively be sent by another entity that is requesting the token(s) on behalf of the user device that is to be provided with the token(s).

Figure 1 shows a system according to an embodiment. Embodiments also include alternative system architectures, such as system architectures for e-commerce and card not present transactions and it is not essential for a token to be directly transferred to a merchant's point-of-sale terminal as described above.

The techniques of first implementation of the fourth embodiment are in no way restricted to use with just TSM channels are applicable to any type of secure channels between an OTA interface and the SE. Suitable implementations of a secure channel are described in the above-cited Secure Element Access Control document.

In the fourth embodiment, it is not necessary for the tokens to be received by the wallet backend from a remote token service provider and the token may have been generated on the user device.

In the fifth embodiment, tokens are stored on the user device but outside of the SE. It is not necessary for the stored tokens to have been transmitted to the wallet backend by a token service provider and the stored tokens may have been generated on the user device or in the SE.

In the fifth embodiment, tokens are described as being stored on the user device but outside of the SE. It is not necessary for the tokens to be stored outside of the SE and the tokens may be stored in the SE for improved security.

All of the described operations of embodiments may be automated and methods of embodiments computer implemented.

The flow charts and descriptions thereof herein should not be understood to prescribe a fixed order of performing the method steps described therein. Rather, the method steps may be performed in any order that is practicable. Although the present invention has been described in connection with specific exemplary embodiments, it should be understood that various changes, substitutions, and alterations apparent to those skilled in the art can be made to the disclosed embodiments without departing from the spirit and scope of the invention as set forth in the appended claims.

CLAIMS:

1. A method for obtaining a token for use in a transaction, the method comprising:

   determining that a token is required for use in a transaction;

   obtaining an encrypted token;

   obtaining, from a secure element, SE, of a user device, one or more keys for decrypting the encrypted token; and

   using the one or more keys to decrypt the token so that the decrypted token is usable in a transaction.

2. The method according to claim 1, further comprising:

   obtaining a token;

   obtaining one or more keys for encrypting the token; and

   using the one or more keys to encrypt the token so that the token is not usable in a transaction.

3. The method according to claim 1 or 2, wherein the encrypted token is stored on the user device but outside of the SE of the user device.

4. The method according to any preceding claim, wherein the one or more keys are keys issued by a network operator of the communications with the user device and/or a payment service provider.

5. The method according to any preceding claim, wherein the token is for paying for a transaction and is for use in one or more systems and methods according to an EMV Payment Tokenisation Specification.

6. The method according to any preceding claim, wherein the token comprises one or more of identification data of the SE, a primary account number and an expiry date of a primary account number.

7. The method according to claim 6, wherein the token comprises identification data and the identification data is an integrated circuit card identifier.

8. The method according to any preceding claim, wherein the obtained token has been generated by the user device.

9. The method according to any preceding claim, wherein the user device is a mobile telephone or a mobile computing device.

10. The method according to any preceding claim, wherein the SE is a smart card of the user device or a subscriber identification module, SIM, of the user device.

11. A user device for using a token in a transaction, wherein the user device is configured to perform the method as set out in any preceding claim.