TRANSACTION SECURITY

The present technique relates to security.

Viewed from a first example configuration, there is provided a transaction terminal system comprising: storage circuitry to store information that is indicative of a terminal system currency of the transaction terminal system; input circuitry to receive a token identifier, wherein the token identifier comprises: information that is indicative of a user currency; and information that is associated with user payment account information; processing circuitry to compare the terminal system currency to the user currency, and where there is a difference, to cause a currency choice offering to be provided and in response to selection of the user currency, to transmit a message to cause a transaction to be performed in the user currency in respect of the user payment account, wherein the message comprises the information that is associated with the user payment account information.

Viewed from a second example configuration, there is provided a method comprising: storing information that is indicative of a terminal system currency of a transaction terminal system; receiving a token identifier, wherein the token identifier comprises: information that is indicative of a user currency; and information that is associated with user payment account information; comparing the terminal system currency to the user currency, and where there is a difference, causing a currency choice offering to be displayed; and in response to selection of the user currency, transmitting a message to cause a transaction to be performed in the user currency in respect of the user payment account, wherein the message comprises the information that is associated with the user payment account information.

Viewed from a third example configuration, there is provided a data processing apparatus comprising: input circuitry to receive user payment account information and information indicative of a user currency; processing circuitry to generate a token identifier using the payment account information and the information indicative of the user currency, wherein the token identifier comprises the information indicative of the user currency; and output circuitry to provide the token identifier.

Viewed from a fourth example configuration, there is provided receiving user payment account information and information indicative of a user currency; generating a token identifier using the payment account information and the information indicative of the user currency, wherein the token identifier comprises the information indicative of the user currency; and providing the token identifier.

Viewed from a fifth example configuration, there is provided a server comprising: input circuitry configured to receive a message to cause a transaction to be performed in a user currency in respect of a user payment account, wherein the message comprises information that is associated with the user payment account information; storage circuitry comprising a plurality of mappings from information to user payment account information; and processing circuitry configured, in response to receiving the message, to obtain the user payment account information from the storage circuitry and to cause the transaction to be performed.

Viewed from a sixth example configuration, there is provided a method comprising: receiving a message to cause a transaction to be performed in a user currency in respect of a user payment account, wherein the message comprises information that is associated with the user payment account information; storing a plurality of mappings from information to user payment account information in storage circuitry; and in response to receiving the message, to obtain the user payment account information from the storage circuitry and causing the transaction to be performed.

The present technique will be described further, by way of example only, with reference to embodiments thereof as illustrated in the accompanying drawings, in which:

Figure 1 shows a block diagram representative of the entities that may be involved in a card payment system;

Figure 2 shows a block diagram of an exemplary POS terminal in accordance with some embodiments;

Figure 3 shows a block diagram of an exemplary Payment Services Provider in accordance with some embodiments;

Figure 4 shows a block diagram of an exemplary tokenizer or tokenization data processing apparatus in accordance with some embodiments;

Figure 5A shows an example of a token identifier as generated by the tokenizer or tokenization data processing apparatus;

Figure 5B shows an example of a token identifier as generated by the tokenizer or tokenization data processing apparatus;

Figure 6 illustrates an example communication exchange in accordance with some embodiments;

Figure 7 illustrates another example communication exchange of when a bill is to be settled in accordance with some embodiments;

Figure 8 illustrates a process 700 performed by the POS terminal 70 when performing settlement in some embodiments;

Figure 9 illustrates a process 800 performed by tokenizer 300 for generating a token identifier 400 in accordance with some embodiments; and

Figure 10 illustrates a process 900 performed by the PSP 200 during settlement in accordance with some embodiments.

Before discussing the embodiments with reference to the accompanying figures, the following description of embodiments and associated advantages is provided.

In accordance with one example configuration there is provided a transaction system terminal comprising: storage circuitry to store information that is indicative of a terminal system currency of the transaction terminal system; input circuitry to receive a token identifier, wherein the token identifier comprises: information that is indicative of a user currency; and information that is associated with user payment account information; processing circuitry to compare the terminal system currency to the user currency, and where there is a difference, to cause a currency choice offering to be provided and in response to selection of the user currency, to transmit a message to cause a transaction to be performed in the user currency in respect of the user payment account, wherein the message comprises the information that is associated with the user payment account information.

The transaction terminal may take the form of, for instance, a computer or Point of Sale device (POS device). Using such a device, payment for a service may be taken. The transaction terminal system is configured using storage circuitry to store information that indicates a currency of the transaction terminal system. For instance, a transaction terminal system provided in the UK may be configure to store that a currency of the transactional terminal system is pounds sterling (GBP). Meanwhile, a transaction terminal system configured in Australia may store the fact that the currency of the transaction terminal system is Australian dollars (AUD). The input circuitry is used to receive a token identifier. The token identifier may have been previously obtained as a consequence of a customer providing their card details, for instance during check-in at a hotel a card is presented and a pre-authorisation transaction is performed. By storing and making use of token identifiers rather than Primary Accounts Numbers (PAN), which are typically captured at this time, the organisation using the transaction terminal system is able to absolve itself of the need to securely store PANs and instead need only store token identifiers, which can be returned in the pre-auth response. These can be stored in, for instance, a Property Management System (PMS) or Electronic Cash Register (ECR), which can then use the token at a later time, such as check-out in the case of a hotel. Indeed, since the token identifier is not generally useable, if a hacker were to obtain the token identifiers, the hacker would be able to do very little with these. The token identifier is such that it contains information that is indicative of user currency as well as information that is associated with a user payment account information. The information that is indicative of a user currency could simply be an identifier of the user currency itself. For instance, the abbreviation GBP could be used to indicate that the user currency is British pounds sterling. The user currency can differ from the system currency of the transaction terminal system in that the user currency is a currency in which a user of the payment account wishes to be billed and/or operates their account. Typically, these two currencies will differ when a foreign visitor visits another country. In particular, the visitor's account will operate in one currency while the transaction terminal system itself will operate using the local currency. The user payment account information could be a PAN. The information that is associated with the user payment account information may be such that it is impossible to determine the user payment account information from the information even though there may be a one to one mapping between the information and the user payment account information. The processing circuitry compares the terminal system currency and the

user currency. Where there is a difference between these, a currency choice offering is provided. From here, the user may be able to select whether they wish to be billed using the terminal system currency or the user currency. If the user currency is selected, then a message is transmitted in order to cause a transaction to be performed in the user currency in respect of the user payment account. This is achieved by the message comprising the information that is associated with the user payment account information. In other words, the message need not contain the sensitive user payment account information such as a PAN. As a consequence of this, it is possible for the user to engage in a transaction in their own currency (as opposed to the terminal system currency) without the user payment account information being present at the time the transaction takes place, which may occur at check-out in the case of a hotel. For instance, a retailer may be able to be passed a token or else have previously converted the user payment account information to a token that can subsequently be stored (e.g. at check-in, in the case of a hotel). By virtue of the token identifier comprising information that is indicative of the user currency, it is possible to provide a choice as to whether the ultimate transaction should take place using the user currency or the terminal system currency. A dynamic currency conversion can therefore be performed while the sensitive user payment account information is not present.

In some embodiments, the message comprises the token identifier. The token identifier could contain other information that is passed together with the user payment account information in the message that is sent out to cause the transaction to take place.

In some embodiments, the token identifier comprises a subset of the user payment account information. Providing a subset of the user payment account information in the token identifier may make it possible to immediately perform a sanity check as to whether the token identifier corresponds with the user payment account information. In particular, if the subset of the user payment account information does not match the token identifier, then it can be immediately determined that the token identifier does not correspond with that user payment account information. For example, the user may be able to differentiate between different PANs using the token identifiers.

In some embodiments, the user payment account information is a primary account number; the subset of the user payment account information is a trailing x digits of the user primary account number. Typically the final digit of a PAN is a check some digit used to verify that the other digits in the number are correct. Accordingly, it is convenient to use the trailing digits of a PAN as an indicator or identifier of a particular PAN.

In some embodiments, the token identifier comprises a random or pseudo-random number. By providing a random or pseudo-random number it is possible to effectively remove any ability to translate the token identifier back into the user payment account information. Note that a random number produced by a computer system may not be truly random and may instead therefore be pseudo-random. Such a number may be large enough that it is improbable or effectively impossible that two numbers would have the same random number.

In some embodiments, the token identifier comprises a result of applying a one-way hash to the user payment account information. A one-way hash is a mathematical process used to translate between an input domain and an output domain. The one-way hash function is such that for the same input, the same output will always be produced. As a consequence, it is possible to confirm the token identifier for user account information, but because the hash function is one-way it is mathematical intractable to convert the result of the hash function back into the user payment account information. Although multiple inputs may produce the same result using the hash function (a scenario referred to as “collision”, this is considered to be so unlikely as to be infeasible).

In some embodiments, the token identifier comprises an indicator of an operator of the user payment account. The indicator could take the form, for instance, of a card scheme. Such a token can be used to provide “clues” to, for instance, payment gateways at a time when payment is to be taken, as to which server the transaction request should be issued.

In some embodiments, the token identifier comprises at least one digit; and the token identifier comprises a checksum value in respect of the at least one digit, a check sum value is used to verify the integrity of other characters (e.g. digits). It is achieved by performing a

mathematical function to one or more of the characters in the identifier. Theoretically, a small change to even one of the characters would expect the check sum to change. Accordingly, if the check sum operation is performed in respect of all of the characters and differs from the check sum that makes up part of the token identifier, then it may be assumed that one or more of the characters in the overall identifier is incorrect.

In some embodiments, the checksum value is produced using the Luhn algorithm, the Luhn algorithm (also known as the modulus 10 algorithm) is one of several examples of check sum algorithm. In general, the Luhn algorithm is known to detect any single digit error as well as most transpositions of adjacent digits. Accordingly, such a check sum algorithm is appropriate for confirming the entry of numbers, where a single digit may be an error, or where two digits may be entered transposed.

In some embodiments, the information that is indicative of a user currency comprises a billing currency code identifier, a currency code identifier, or a country code identifier. Currencies could be as identified by, for instance, ISO4217 and country codes could be as identified by, for instance, ISO3166.

In some embodiments, the token identifier comprises one or more leading non-digit characters. By providing, e.g. one leading non-digit character, it is possible to differentiate a token identifier from other account identifiers such as PANs. In some other embodiments, the token identifier is entirely made up from digits.

In some embodiments, the token identifier consists of 16 alphanumeric characters. Many existing systems are configured to accept payment account numbers as 16 alpha numeric characters. For instance, the majority of credit card numbers are 16 digit numbers. Accordingly, by providing the token identifier as 16 alpha numeric characters, it is possible to make use of existing systems that expect payment numbers to be 16 characters long.

In some embodiments, the input circuitry comprises a keypad for entering the token identifier. Such a keypad could be, for instance, an alpha numeric keypad capable of inserting letters and/or numbers. Accordingly, a token identifier can be entered using the keypad.

In some embodiments, the input circuitry comprises an interface for connection to a processing device from which the token identifier is receivable. Input circuitry may be used in order to issue payments via computing system or more complicated sales device. For instance, such a sales device may interface with an inventory system or an ongoing billing system that enables charges accrued by a person over a period of time to be billed. Such a system may keep track of token identifiers such that a user can be billed directly at a later date without further need to either store PANs or require the user to provide payment details multiple times.

In some embodiments an amount of the transaction is determined as a result of input of information for goods or services to be purchased.

In some embodiments, the processing circuitry is configured to operate in at least one of: a sale mode of operation in which the transaction is in respect of a sale; and a refund mode of operation in which the transaction is in respect of a refund. Accordingly, the transaction may be made in respect of a sale in which money is deducted from a PAN for goods or services purchased by a user or a refund in which money is credited back to the PAN as a consequence of a previous transaction being voided – e.g. as a consequence of goods being returned or services being cancelled. In either case, a currency translation may take place. The currency translation in respect of a refund may use the currency translation that occurred in the sale transaction that is to be voided or may take place using more current translation data (e.g. if the period of time or the difference in transaction amounts is greater than a threshold value).

In some embodiments in response to determining that the terminal system currency and the user currency differ, the processing circuitry is configured to cause at least one of: a current currency conversion value from the transaction currency to the user currency, and a converted transaction amount using the current currency conversion value, to be downloaded from a remote server to the transaction terminal system. Accordingly, the transaction terminal system may be able to obtain up-to-date information regarding the conversion of currency between the terminal system currency and the user currency. Accordingly, the translation is

performed on the actual conversion value between the two currencies rather than an old value or an estimated value, which may cause uncertainty in the nature of the transaction being performed.

In some embodiments, the currency choice offering comprises at least one of: the current currency conversion value, and an amount of the transaction converted into the user currency using the current currency conversion value. In the choice offering, a selection may be made based on the current currency conversion value that is available at the transaction terminal system for the translation of the currency between the user selected currency and the transaction terminal system currency. In addition or instead, an amount of the transaction converted into the user selected currency may be provided by providing the amount of the transaction, the user need not determine the amount of the transaction using the current currency conversion value. By providing the current currency conversion value, the user is able to determine whether a good exchange rate is being provided or not. Accordingly, in some embodiments, both pieces of information may be provided during the currency choice offering.

In some embodiments, the input circuitry is adapted to receive the information that is associated with the user payment account information and data relating to the user currency; and the processing circuitry is adapted, in response to receiving the information that is associated with the user payment account information and the data relating to the user currency, to generate encrypted information by encrypting at least the information that is associated with the user payment account information, and to transmit the encrypted information and the data relating to the user currency to a server, wherein the transaction terminal system comprises receiving circuitry to receive the token identifier in response to transmitting the encrypted information; and the transaction terminal system comprises output circuitry to output the token identifier. By presenting payment account information and data relating to the user currency at the transaction terminal system, the transaction terminal system is able to request the corresponding token identifier from a server. The token identifier can then be output, e.g. by displaying it to the user or operator, storing it locally for later use, or outputting it in some other way such as printing it on the merchant's copy of the receipt and/or transmitting it to a PMS or ECR for storage or later use (e.g. check-out of a

hotel). In this way, having initially presented the payment account information it is possible for further payments to be processed using the retrieved token without the card being re-presented. Since the token identifier comprises the information that is indicative of a user currency, which is determined from the data relating to the user currency, DCC can be offered at a later time.

In accordance with another example configuration there is provided a data processing apparatus comprising: input circuitry to receive user payment account information and information indicative of a user currency; processing circuitry to generate a token identifier using the payment account information and the information indicative of the user currency, wherein the token identifier comprises the information indicative of the user currency; and output circuitry to provide the token identifier.

Such a data processing apparatus is capable of generating a token identifier based on user payment account information. The token identifier is subsequently used to perform a transaction in respect of the user payment account information without that user payment account information being provided. In this way, the token identifier can be used as a substitute for the payment account information thus obviating the need for such sensitive information to be transmitted. This also enables the receiver of the token identifier to initiate a transaction without being required to store sensitive information which may be leaked or hacked. The token identifier generated by the data processing apparatus comprises information indicative or the user currency. In this way, it is possible for an initiator of the transaction to determine whether the user should be offered the opportunity to have a transaction converted into the user currency. This determination can be made despite the user payment account information being absent at the time of the transaction. Note that the user payment account information itself might, in some embodiments, be indicative of the user payment account information. Furthermore, in some instances, the data processing apparatus may have card reading capabilities in order to locally read and a card and generate a token. In such a case, those card reading capabilities themselves may be able to receive the information indicative of a user currency from the transaction card.

In some embodiments, the information indicative of the user currency is one of: the user payment account information, a currency code, or an issuer country code. The currency code and/or payment account information (e.g. in the form of a primary account number) and/or issuer country code could be obtained via an EMV chip, for instance.

In some embodiments, the input circuitry comprises magnetic stripe reader circuitry. A magnetic stripe reader circuit is used in order to read a magnetic stripe that can be found on a number of different payment cards. Such a magnetic stripe can be used to store a small amount of information such as the user payment account information and the information indicative of a user currency. Having obtained this data, the processing circuitry can then generate the token identifier, which is stored. The user payment account information then other sensitive information may be discarded.

In some embodiments, the input circuitry comprises EMV circuitry. Europay, Mastercard and Visa (EMV) chips are used to provide so-called "chip-and-PIN" functionality in which a payment card can only be operated in conjunction with a PIN number associated with the card and known to the user. By providing EMV circuitry, information stored in the chip can be accessed when the user presents the card and enters the associated PIN.

In some embodiments, the input circuitry comprises NFC communication circuitry. As above, the input circuitry may comprise Near Field Communication (NFC) communication circuitry that can be used to relay information between a payment card and the data processing apparatus. Such information may include user payment account information as well as information indicative of a user currency. Again, having generated the token identifier, such sensitive information may be discarded.

In some embodiments, the input circuitry comprises a keypad. By providing a keypad, the input circuitry provides the ability for a user to manually enter information. Such information could include the user payment account information and information indicative of the user currency. Having entered such information, as above, it may be discarded once the token identifier has been generated by the processing circuitry.

In some embodiments, the input circuitry comprises communication circuitry to communicate with one or more further data processing devices via a network. By providing communications circuitry as part of the input circuitry, the data processing apparatus is able to receive, for instance, the user payment account information and the information indicative of a user currency. Once a token identifier has been generated by the processing circuitry, such sensitive information (e.g. the user payment account information and/or information indicative of the user currency) may be discarded.

In some embodiments, the output circuitry comprises communication circuitry to communicate with one or more further data processing devices via a network. The output circuitry may be used in order to provide the token identifier that has been generated by the processing circuitry back to a merchant for later use. Since the token identifier is designed to be used with a particular payment services provider, it is of limited use to a third party. In addition, both the token identifier and the user payment account information could be provided to a payment services provider in order to enable a transaction to take place in respect of the payment account information when provided with the token identifier.

In some embodiments, the output circuitry is configured to provide the token identifier to a sender of the user payment account information, e.g. a merchant.

In some embodiments, the user payment account information is provided in encrypted format. The user payment account information may be encrypted by a terminal system using a key that is not available to an operator of the terminal system and only available to the data processing apparatus.

In accordance with another example configuration there is provided a server comprising: input circuitry configured to receive a message to cause a transaction to be performed in a user currency in respect of a user payment account, wherein the message comprises information that is associated with the user payment account information; storage circuitry comprising a plurality of mappings from information to user payment account information; and processing circuitry configured, in response to receiving the message, to

obtain the user payment account information from the storage circuitry and to cause the transaction to be performed.

The server may be used in order to effect the transaction using information that is associated with the user payment account information rather than the user payment account information itself. The information that is associated with the user payment account information could take the form of a token identifier as previously described. The storage circuitry at the server comprises a plurality of mappings between information associated with user payment account information and user payment accounts. In this way, given the information that is associated with the user payment account information it is possible to determine at the server the user payment account information for which the transaction is to be effected. The processing circuitry after receiving the message, uses the storage circuitry to determine the user payment account information given the information that is associated with it and to thereby cause the transaction to be performed in respect of the user payment account information. In this way, a transaction can be effected using only information associated with the user payment account information rather than the user payment account information itself. In addition, by providing data relating to a user currency, it is possible for the transaction to be performed in the user currency.

In some embodiments, the message comprises the user currency.

In some embodiments, the message comprises an indication that the user currency is other than a currency associated with a sender of the message. Accordingly, rather than providing the user currency, which could instead be stored or otherwise obtained by the server, the message could simply comprise an indication that the user currency is other than the currency associated with the sender of the message and that the transaction is to take place in the user currency. It would then be incumbent on the server to determine the currency in which the transaction is to take place i.e. the user currency and then cause the transaction to take place on that currency. This can reduce the band width requirement between the merchant and the server, since the currency in which the transaction is to take place itself needs not be transmitted.

In some embodiments, the message comprises: a transaction amount and a current currency conversion value, or the transaction amount converted into the user currency using the current currency conversion value. By providing a transaction amount and a currency conversion value, the server is able to determine the value and currency of the transaction to take place. Alternatively, by providing the transaction amount that has already been converted, the server need only cause the transaction to take place in respect of the requested amount in respect of the user currency. This latter process has the advantage of reducing the processing load at the server, since the server need not perform the conversion itself.

Particular embodiments will now be described with reference to the figures.

Figure 1 shows a block diagram representative of the entities that may be involved in a card payment system and the information transfer between those entities in a typical card payment system. A cardholder 10 obtains a transaction card 60 from an issuer 40. The issuer 40 may typically be a retail banking or financial institution. Issuers 40 provide transaction cards 60 for use at Point of Sale (POS) terminals 70 located at merchants 20. Transactions initiated by, e.g. a Property Management System (PMS) of a hotel or an Electronic Cash Register (ECR) of a restaurant interface with POS terminals 70 and are acquired and processed by acquirers 30 via card scheme administrators 50. Examples of current card schemes include the MasterCard, VISA, Diners Club and American Express schemes. The cardholder 10 uses their transaction card 60 to make a financial transaction at a merchant 20 (e.g. a hotel). For example, where the cardholder 10 is the holder of a credit card, they may swipe their card through a POS terminal 70 (or insert their card into, or bring their contactless card in proximity to, the terminal) provided at the premises of a merchant 20. The POS terminal 70 extracts account details from the transaction card 60, including the card number that identifies the financial account of the cardholder 10 with the relevant financial institution (i.e. the issuer 40). The POS terminal 70 is connected or connectable to a network 80. For example, smaller scale merchants 20 may connect to the network 80 through a dial-up connection to a PSTN network. Alternative public or private local and/or wide area networks based on industry standard or proprietary wired or wireless technologies and network connections may be used for central handling of transactions. The account details and particulars of the transaction are then sent to and are received by an acquirer 30. The

particulars of the transaction may include the ID of the POS terminal 70, the ID of the merchant 20, the number of the transaction card 60, the value of the requested transaction and the currency of the requested transaction. Upon receipt of the transaction particulars, the acquirer 30 sorts the transactions into groups according to the card scheme and sends the transactions relating to a card scheme to the appropriate card scheme administrator 50 (one only shown in Figure 1). The first digits of the transaction card 60 number typically identify the card scheme. The card scheme administrator 50 then sorts the transactions that it receives by the issuer 40 of the transaction card 60. This may be achieved by examining the Bank Identification Number (BIN), which is often the first six digits of the credit card's Primary Account Number (PAN). Each issuing bank is assigned one or more BINs, so that all cards issued by that issuer 40 commence with one of those BINs. Upon receipt of the transaction particulars, the issuer 40 sends back a response to the card scheme administrator 50. The card scheme administrator 50 forwards this response to the acquirer 30, who in tum returns the response to the POS terminal 70 with an authorisation code.

If the transaction has been successful, the issuer 40 then manages the transfer of funds between the account of the cardholder 10 and the card scheme administrator 50. The card scheme administrator 50 transfers the funds to the acquirer 30 who then settles the funds with the merchant 20. The acquirer 30 sends a statement of account to the merchant 20 and the issuer sends a statement of account to the cardholder 10. Often an acquirer 30 is also an issuer 40. Where the local currency of a merchant 20 does not match the local currency of a cardholder 10, for example where the cardholder 10 has travelled overseas, the cardholder 10 may have difficulty appreciating the true value of the transaction. This is because traditionally the transaction is made in the currency of the merchant 20, with the card scheme administrator 50 attending to the necessary foreign exchange. Dynamic Currency Conversion (DCC) allows a cardholder 10 to conduct a transaction at a merchant 20 in their local currency instead of the local currency of the merchant 20. A fee may be charged for the service. The advantage of DCC, if used in the right circumstances, is that the cardholder 10 can see the exact value that will appear in their statement of account from their respective issuer 40 at the time of the transaction. In DCC transactions, it is the acquirer 30 that attends to the necessary foreign exchange, instead of the card scheme administrator 50 and/or issuer.

In some circumstances, the merchant 20 may keep the account details obtained from the transaction card 60 on file. For instance, in the hotel industry, it is common to obtain the account details in a Property Management System (PMS) so that the card holder 10 can quickly check out of the hotel at the end of their stay. Furthermore, costs accrued during their stay can be kept by the PMS and combined and charged at the end of the guest's stay. The account details can, however, be accidentally leaked or maliciously obtained (hacked) by a third party. More recently, therefore, some merchants 20 have moved to a system of using tokens. In such systems, the POS terminal 70 obtains the account details and sends these (usually in an encrypted format) to a tokenization service, which could be associated with the acquirer 30. The tokenization service uses the account details to generate a token, which is sent back to the merchant 20, for storing in a merchant's PMS. Future transactions (such as check-out) can take place from the merchant 20 at the acquirer 30 using the generated token, and therefore, the merchant 20 need not continue to hold the sensitive account data. The token, however, can only be used with the acquirer 30 by the merchant 20 and so the loss of this information need not be detrimental to the card holder 10 or any of the other entities involved.

The method of performing DCC, explained above, relies on the BIN (and occasionally additional digits of the card number) in order to look up the corresponding user currency. However, if a token is provided in place of user payment account data, then the BIN may not be available. The present embodiments comprises information relating to the user's payment currency into the token, thereby enabling DCC to take place in spite of the user payment account information being absent (e.g. at the time of check-out).

Figure 2 shows a block diagram of an exemplary POS terminal 70. The POS terminal 70 transmits and receives information via a modem 110 or other networking communications system or device. The POS terminal 70 includes a memory 120, which includes a RAM and ROM (e.g. an EEPROM) component; the instructions that control operation of the controller of the POS terminal 70 stored in ROM. Furthermore, a currency of the POS terminal (e.g. the merchant) is stored in ROM.

The POS terminal 70 is responsible for obtaining the PAN of the transaction card and using it to request a token identifier from a tokenization data processing service 300. This can occur during a pre-auth operation in which the issuer is instructed to put a hold on the transaction for 30 days so that the merchant is able to determine that sufficient funds are available. In response to this, the POS terminal may receive the token identifier. By storing the token identifier (e.g. at a PMS or ECR) rather than the PAN itself, security can be improved since the sensitive PAN is not stored by the merchant. Meanwhile, the token identifier is specific to the merchant and Payment Services Provider and thus cannot easily be reused by a third party.

The request to provide a token may include additional data regarding the currency of the card holder 10. In some cases, the user currency is stored on and provided by the transaction card 60. Such information could be acquired by the use of one or more of: a Near Field Communications (NFC) module 140, smart card reader 150, card reader 160, keypad 170, or EMV circuitry 195. In other cases, the RAM may store a table 130 comprising a list of current domestic (DOM) issuers of cards. DOM issuers can be identified by the BIN number on the transaction card. The RAM may also store a list of international (INTL) issuers of cards by their BIN number and a list of the billing currency for that INTL issuer. E.g. for INTL issuer 132459, the issuer 40 may invoice the cardholder 10 in a currency that is not supported by the card scheme administrator 50 so that DCC may not be offered to the cardholder 10. Of course, the RAM may store no entry for the BIN number 132459 with the same effect. Those skilled in the relevant arts will appreciate that some information shown in the table 130 may be stored outside of the POS terminal 70, which may receive the information as required to perform a transaction. For example, a list of DOM issuers may be stored at the POS terminal 70, whereas the list of INTL issuers and the billing currency associated with each INTL issuer may be stored remote from the POS terminal 70, for example in a database of the acquirer 30. Also, further information may be included in the RAM of the POS terminal 70.

In some embodiments, the currency of the card holder 10 is not provided in the request for the token. Instead, this data may be acquired by the tokenization data processing apparatus 300 itself using, for instance, the BIN of the PAN.

The request to provide a token includes the PAN of the transaction card 60 and information identifying the currency of the user (which could by the PAN itself). This information can be acquired by one or more of the NFC module 140, smart card reader 150, card reader 160, keypad 170, or EMV circuitry 195 (one or more of these modules being available on the POS terminal 70). Having acquired this information, the controller 180 encrypts the PAN and transmits it (e.g. via modem 110) as part of the request together with the information identifying the user currency (which may or may not be encrypted). The key could be a shared key or a public key of the tokenization data processing apparatus 300 that is part of a (public key, private key) symmetric key pair. Using a symmetric key pair means that having encrypted the PAN, the POS terminal 70 does not contain the means to decrypt it.

The tokenization data processing apparatus 300 returns the resulting token identifier, which can be output to a merchant's PMS. The token identifier has the user's currency within it (e.g. encoded within it).

Separately, when a transaction (e.g. a payment or a refund) is to be carried out (e.g. during check-out of a hotel or when a restaurant bill is to be paid), the token identifier can be provided, either from the PMS via the input module 190 (which may receive the token from the PMS or ECR) or via one of the NFC module 140, smart card reader 150, card reader 160, keypad 170, or EMV circuitry 195. By comparing the user's currency (provided in the token identifier) with the POS terminal system currency (e.g. stored in the memory 120), the POS terminal 70 can determine whether DCC should be offered. If such an offer is accepted, then the modem 110 can be used to effect a DCC transaction in the selected currency using the token identifier. Otherwise (in either of the previous cases), the modem 110 can be used to effect a regular transaction using the token identifier.

The POS terminal 70 may also receive up-to-date exchange rates via, e.g. the modem 110. These exchange rates can be stored in the memory 120. Accordingly, when DCC is offered, it is possible to show the transaction amount in the user's currency and/or the exchange rate that is being offered at the time of the transaction without the need to request live data.

Figure 3 shows a block diagram of an exemplary Payment Services Provider (PSP) as may be provided by an acquirer 30. The Payment Services Provider 200 is an example of the claimed server. The PSP 200 includes input circuitry 210, which receives a request from the POS terminal 70 to effect either a regular transaction or a DCC transaction. In either case, the request comprises the token identifier as well as information necessary to effect the transaction (an amount, whether the transaction is a sale or a refund, and a selected currency in the case of DCC). This is passed to a controller 220, which uses the token identifier to determine the corresponding PAN from storage circuitry 230. Here it is assumed that the PSP 200 contains a set of translations between PANs and token identifiers, which could be obtained from a tokenization server for instance. In other embodiments, the PSP may send a request for the PAN to, for instance, the tokenization data processing apparatus 300 that generated the token in the first place. In any case, having collected this information, the controller 220 then issues a request via the modem 240 to perform the transaction (either regular or DCC) for the PAN. Since, at this stage in the process, the token identifier has been replaced with a PAN, the process for effecting the transaction can take place as normal.

Figure 4 shows a block diagram of an exemplary tokenizer or tokenization data processing apparatus 300, as may be provided by an acquirer 30. The Tokenizer 300 is an example of the claimed data processing apparatus. The tokenizer 300 receives the encrypted PAN and may also receive information that indicates the currency of the card holder 10 via a modem 310. The tokenizer 300 is able to decrypt the encrypted PAN, e.g. using either a shared key or a private key that is part of a (public key, private key) pair in a symmetric encryption operation. Alternatively, the PAN can be acquired using any of an NFC module 320, smart card reader 330, card reader 340, keypad 350, or EMV circuitry 355 if the transaction card 60 is physically present. Using the PAN, the controller 360 generates the token identifier, which is output by the controller 360 via comms circuitry 370. The controller 360 generates the token identifier such that the token identifier comprises the currency of the card holder 10. The card holder currency can be determined from, e.g. the BIN of PAN (as previously described in relation to the POS terminal) using a memory 380, from data stored on the transaction card 60 if the transaction card 60 is available locally, or from the request to provide a token that is received from the POS terminal 70. Note that in

some embodiments, additional digits of the PAN (beyond just the BIN) are used to more accurately derive the card holder currency.

Figure 5A shows an example of a token identifier 400 as generated by the tokenizer or tokenization data processing apparatus 300. In this embodiment, the token comprises 16 characters, and thus has the same number of characters as a typical PAN. This potentially enables the token identifier 400 to be backwards compatible with systems that permit PANs to be 16 characters long. Here, the token identifier 400 is prefixed by one leading character 410. For example, the character 'T' may be used. This makes it possible to differentiate a token from a real PAN. In some other embodiments, the leading character will be a number so that entirely digits are used (as is the typical convention for primary account numbers). In any event, the leading character is followed by three digits 420 used to help identify the currency of the card holder 10. There are a number of ways that this can be achieved, such as using a textual representation of the country or currency. However, in this embodiment, the numeric 3-digit currency codes represented by ISO4217 are used. In this, the numeric value for the United Kingdom (whose currency is pounds sterling) is 826. The numeric code for the United States of America (whose currency is in American dollars) is 840. Meanwhile, the numeric code for Australia (whose currency is Australian dollars) is 036. Note that in other embodiments, the currency type itself could be encoded using the three digits. In any event, these digits are followed by an eight digit number such as random or pseudo-random digits 430. In some embodiments, the number may be based on the PAN, such as by performing a one-way hash of the PAN using an algorithm like MD5 or SHA-1. Using a one-way hash makes it possible to confirm that the token identifier 400 is associated with the correct PAN. Meanwhile, using a random number makes it possible for the same PAN to be used multiple times. In the suffix of the token identifier 400, the last 3 digits of the PAN 440 are provided, together with a final check digit 450. By including the trailing digits of the PAN 440, it is possible for a user to identify the PAN that the token identifier 400 is associated with, without knowing the PAN itself. This could be useful if a user has multiple different transaction cards 60 for instance. The check digit 450 is provided in order to inhibit incorrectly typed or provided token identifiers from being used. Such an algorithm for performing a check might be Luhn's algorithm. Note that since the token identifier has encoded the user's currency into

the token identifier, it is possible to determine whether DCC should be offered to the user based solely on their token, without the PAN being accessible to the merchant 20.

Figure 5B shows a further example of a token identifier 460 as generated by the tokenizer or tokenization data processing apparatus 300. In this further example, most of the fields remain the same. However, the numeric value 430 is shortened to six characters (e.g. digits). The two digits that are 'saved' are used to encode an IID, which can be used to identify a card issuer and/or scheme (e.g. Visa or Mastercard) or an operator of the payment account. This makes it possible to perform an extra level of validation (to ensure that the token corresponds with the appropriate primary account number) and can be used to help a user identify which primary account number is being used, by looking at the token. Furthermore, knowledge of the card issuer and/or scheme can be used to help the routing of transaction messages when payment is finally to be made. This can be achieved without the need to fully decode the token, thereby maintaining security and permitting more efficient programming logic within the POS terminal and acquirer systems.

Figure 6 illustrates an example communication exchange. Initially, the card 60 provides the PAN to the POS terminal 70. The PAN is encrypted by the POS terminal 70, which then transmits a RequestToken message to the tokenizer 300, including the encrypted PAN. The tokenizer 300 then responds with the corresponding token. Note that in this example, it is assumed that the PAN can be used to determine a currency of the card 60 user. This could be achieved by, for instance, the tokenizer 300 performing an analysis of the PAN to determine the issuer country and, from there, the currency in which the issuer operates (e.g. an issuer based in the UK may operate in pounds sterling). In other examples, the PAN can determine the billing currency itself directly without needing to derive an issuer country first. The determined currency is encoded into the token that is generated (as discussed with reference to Figures 5A and 5B for instance). In other embodiments, additional information can be send along with the PAN. For instance the additional information could take the form of a currency code or an issuer country code, either of which could be deduced by information available on the card 60.

Since the token is not, in isolation, sensitive, there is no need for this to be encrypted. The tokenizer 300 is transmitted to the PMS 500 where it is stored. Charges, etc. can be accumulated against the card holder 10 as appropriate. Once the overall bill is to be settled, a TransactionRequest message can be transmitted from the PMS 500 to the POS terminal 70. This message includes the appropriate token, the amount the transaction is to take place for, and the transaction type (e.g. refund or sale). In some embodiments, an ID of the PoS terminal 70 is also included. The transaction type can be combined with the amount. For example, in the case of a bill being raised, the transaction would be a sale, and thus the amount would be positive. In another example, a refund might be being provided and the amount would be negative. In either case, the POS terminal determines the currency of the card holder 10 from the token. This might take place with the POS terminal 70 storing currencies for each country, by examining characters 2-4 of the token identifier, and determining that that the currency of the listed country differs from the currency of the POS terminal 70. If these do not differ, the transaction proceeds as normal by requesting a transaction is respect of the provided amount for the token identifier. This is sent to the payment service provider 200, which effects the transaction (translating the token identifier in the process). Otherwise, a choice is provided as to whether to charge in currency of the card holder 10 or of the POS terminal 70. One or more of either an exchange rate or a converted amount of the transaction into the currency of the card holder 10 can be provided to guide the user's decision. These can be provided either from a stored set of exchange rates, which are frequently updated by the POS terminal 70 or by requesting a live exchange rate with the payment service provider 200. If the transaction is to proceed in the currency of the POS terminal 70 then the process proceeds as previously discussed. Otherwise, a DCCPaymentRequest message is generated, containing the token identifier, the amount, and the currency the transaction is to take place in. This is sent to the payment service provider 200. As before, the payment service provider 200 obtains the PAN from the token identifier (either via local storage or by making a request to, e.g. the tokenizer 300). The PSP 200 then effects the transaction.

Note that there are various ways in which the DCC transaction can be caused by the POS terminal 70. In some embodiments, for instance, the POS terminal 70 could merely

indicate that DCC is to be used, while the PSP 200 stores or determines the card holder 10's currency.

Figure 7 illustrates another example communication exchange of when a bill is to be settled. The PMS 500 sends a request to the Payment Proxy Server (PPS) to perform a settlement. A PPS can be used to mediate the routing of messages (and any necessary protocol translations between the devices such as the PMS 500, payment terminal 70, Payment DCC Routing Server, and Payment Gateway Server). The PPS forwards the request to the payment terminal 70. From here, the payment terminal 70 issues a DCC Rate Request message, which is forwarded to the PSP via the PPS, which forwards the request to a currency converter service 600. This may be provided by the acquirer 30. The currency converter service responds with a DCC Rate Response, which is provided to the PSP 200, which in turn provides the DCC Rate Response to the payment terminal 70 via the PPS. The DCC Rate Response provides an indication of the currency conversion rate between the currency of the payment terminal 70 and the user's currency. In some other embodiments, the transaction amount can be sent as part of the DCC Rate Request, and the DCC Rate Response returns the converted amount of the transaction. Here, the payment terminal 70 is able to offer DCC if the currency of the card holder 10 and a currency of the payment terminal 70 differ. A Settlement Request is then issued to the PPS based on the result of this choice. At the same time, a receipt may be printed, if this option is enabled and/or requested. At the end of the day the settlements are batched together by the PPS and issued to the PSP 200, which issues Settlements to the acquirer 30. The acquirer responds with Settlement Responses, which are provided back to the PPS via the PSP 200. The Settlement Responses are then provided to the PMS 500. At the end of the day, a batched transaction log file is also provided to the currency converter 600.

Figure 8 illustrates a process 700 performed by the POS terminal 70 when performing settlement in some embodiments. The process starts at a step 710 where an indicator of the terminal currency is stored. Then, at a step 720, a token identifier 400 is received. At step 730, the currency of the card holder 10 is determined from the token identifier 400. At step 740, it is determined whether the terminal currency and the user currency are the same. If so, then at step 750, the transaction is effected using the terminal system currency. Otherwise, at

step 760, a choice of currency is offered. If the user currency is not selected, then again, the transaction occurs in the terminal system currency at step 750. Otherwise, at a step 780, the transaction occurs in the user currency.

Figure 9 illustrates a process 800 performed by tokenizer 300 for generating a token identifier 400. Firstly, at a step 810, the user account information (e.g. a PAN) is received. At a step 820, the user payment currency is received, although in some other embodiments, this may be determined by the tokenizer 300 from, e.g. the PAN. At step 830, a token identifier 400 is generated. The process used for this is illustrated in, for instance, Figures 5A and 5B. Finally, at step 840, the token identifier is provided, e.g. back to the merchant 20 at the POS terminal 70.

Figure 10 illustrates a process 900 performed by the PSP 200 during settlement. At a step 910, information associated with the user account is received. This could, for instance, take the form of a token identifier 400 or part of the token identifier 400. A user currency is then received at step 920. In some embodiments, the user currency can be determined by the PSP 200, for example, if the PSP 200 stores the user currency or can query this information from another device. At a step 930, a lookup is performed in order to obtain the user account. This could, for instance involve using a lookup table to obtain the user account information from a particular token identifier 400. Finally, at a step 940, the transaction is performed on the user account in the user currency. This could involve the exchange of further messages, e.g. to an acquirer 30 or to a card scheme administrator 50 for instance.

Accordingly, it has been shown that even with the use of a token identifier rather than specific user account information, it is possible to offer a user to opportunity to perform DCC. Thus, convenience to a user can be maintained while also maintaining security of the user's financial information.

In the present application, the words "configured to..." are used to mean that an element of an apparatus has a configuration able to carry out the defined operation. In this context, a "configuration" means an arrangement or manner of interconnection of hardware or software. For example, the apparatus may have dedicated hardware which provides the

defined operation, or a processor or other processing device may be programmed to perform the function. "Configured to" does not imply that the apparatus element needs to be changed in any way in order to provide the defined operation.

Although illustrative embodiments of the invention have been described in detail herein with reference to the accompanying drawings, it is to be understood that the invention is not limited to those precise embodiments, and that various changes, additions and modifications can be effected therein by one skilled in the art without departing from the scope and spirit of the invention as defined by the appended claims. For example, various combinations of the features of the dependent claims could be made with the features of the independent claims without departing from the scope of the present invention.