Tokenisation may also be used as a way of securing chip and contactless card transactions, i.e. when a chip or contactless card communicates with a payment terminal, it provides a tokenised PAN as a surrogate for the PAN actually printed/embossed on the card. United States provisional patent application number 62132300 filed 12 March 2015 describes systems and methods which allow payment cards (including contact and contactless chip payment cards and mobile devices) to be personalised in a way which permits the use of payment tokens as well as standard PANs.

United States patent application number 14514290 filed 14 October 2014 is concerned with improving the security of tokenised transactions by providing, along with a token, a token assurance level and data used to generate the token assurance level. As described therein, at the time a token is issued, one or more identification and verification methods are performed to ensure the token is replacing a PAN that was legitimately used by a token requestor and a token assurance level is assigned accordingly.

Summary

According to a first aspect there is provided a method comprising a secondary payment device:

receiving a device primary account number (DPAN) and a funding source proxy (FSP) derived from a funding primary account number (FPAN) of a funding source according to a predetermined algorithm; and

transmitting a secondary payment device transaction request comprising said DPAN and said FSP to a payment terminal. In an embodiment, there is provided a method of identifying the funding source of an electronic transaction, said method comprising a payment terminal: receiving a transaction request comprising one or more credentials from a payment device; and determining whether said credentials comprise a funding source proxy (FSP) and, if not, generating the FSP from one or more of said credentials according to a predetermined algorithm stored on said payment terminal; wherein the FSP is derived from a funding primary account number (FPAN) of a funding source of said payment device.

According to a second aspect there is provided a method comprising a payment terminal:

receiving a secondary payment device transaction request comprising a device primary account number (DPAN) and a funding source proxy (FSP) derived from a funding primary account number (FPAN) of a funding source according to a predetermined algorithm;

responsive thereto, determining that the FSP is not present on a deny list stored at the payment terminal; and

responsive thereto, authorising said secondary payment device transaction request. In an embodiment, there is a method of blocking an electronic transaction, said method comprising a payment terminal: receiving a transaction request comprising one or more credentials from a payment device; determining whether said credentials comprise a funding source proxy (FSP) and, if not, generating the FSP from one or more of said credentials according to a predetermined algorithm stored on said payment terminal; determining that said FSP is present on a deny list stored on the payment terminal; and declining said transaction request; wherein the FSP is derived from a funding primary account number (FPAN) of a funding source of said payment device.

According to a third aspect there is a secondary payment device comprising:

a receiver configured to receive a device primary account number (DPAN) and a funding source proxy (FSP) derived from a funding primary account number (FPAN) of a funding source according to a predetermined algorithm;

a processor, operatively coupled to said receiver, configured to extract said DPAN and said FSP from one or more received messages; and

a transmitter, operatively coupled to said processor, configured to transmit a secondary payment device transaction request comprising the DPAN and the FSP to a payment terminal. In an embodiment, there is provided a method of authorising an electronic transaction, said method comprising a payment terminal: receiving a transaction request comprising one or more credentials from a payment device; determining whether said credentials

comprise a funding source proxy (FSP) and, if not, generating the FSP from one or more of said credentials according to a predetermined algorithm stored on said payment terminal; determining that said FSP is not present on a deny list stored on the payment terminal; and authorising said transaction request; wherein the FSP is derived from a funding primary account number (FPAN) of a funding source of said payment device.

According to a fourth aspect there is a payment terminal comprising:

a receiver configured to receive a secondary payment device transaction request comprising a device primary account number (DPAN) and a funding source proxy (FSP) derived from a funding primary account number (FPAN) of a funding source according to a predetermined algorithm;

a memory storing a deny list; and

a processor, operatively coupled to said receiver and said memory, configured to determine that the FSP is not present on said deny list and, responsive thereto, authorise said secondary payment device transaction request. In an embodiment, there is provided a method comprising a payment terminal: receiving a primary device transaction request comprising a funding primary account number (FPAN) of a funding source; responsive thereto, generating a funding source proxy (FSP) from said FPAN according to a predetermined algorithm stored on the payment terminal; responsive thereto, determining that said generated FSP is not present on a deny list stored at the payment terminal; responsive thereto, authorising said primary device transaction request; issuing a request comprising the FPAN to a payment network for settlement of said transaction; subsequent to issuing said request comprising the FPAN to said payment network, receiving a primary device transaction failed message from the payment network; and responsive thereto, adding the FSP to said deny list; the payment terminal subsequently: receiving a secondary payment device transaction request comprising a device primary account number (DPAN) and the FSP; determining that the received FSP is present on the deny list; and declining said secondary payment device transaction request.

According to an embodiment there is provided a method of provisioning a device with payment capability, said method comprising providing said device with a device primary account number (DPAN) and a funding source proxy (FSP) derived from a funding primary account number (FPAN) of a funding source according to a predetermined algorithm.

According to a an embodiment there is provided a method comprising a secondary payment device: receiving a device primary account number (DPAN) and a funding source proxy (FSP) derived from a funding primary account number (FPAN)

of a funding source according to a predetermined algorithm; and transmitting a secondary payment device transaction request comprising said DPAN and said FSP to a payment terminal.

The DPAN and the FSP could be received in a signed or encrypted record.

The method could further comprise a payment terminal: receiving said secondary payment device transaction request; responsive thereto, determining that the received FSP is not present on a deny list stored at the payment terminal; and responsive thereto, authorising said secondary payment device transaction request.

request comprising said FPAN; responsive thereto, generating the FSP from the received FPAN according to said predetermined algorithm stored on the payment terminal; responsive thereto, determining that the FSP is not present on a deny list stored at the payment terminal; responsive thereto, authorising said primary device transaction request; issuing a request comprising the FPAN to a payment network for settlement of said transaction; subsequent to issuing said request comprising the FPAN to said payment network, receiving a primary device transaction failed message from the payment network; and responsive thereto, adding the FSP to a deny list stored at the payment terminal; the payment terminal subsequently: receiving said secondary payment device transaction request; responsive thereto, determining that the received FSP is present on said deny list; and responsive thereto, declining said secondary payment device transaction request.

The method could further comprise the payment terminal, prior to receiving said secondary payment device transaction request: receiving a primary device transaction request comprising said FPAN; responsive thereto, generating the FSP from the received FPAN according to said predetermined algorithm stored on the payment terminal; responsive thereto, determining that the FSP is not present on a deny list stored at the payment terminal; responsive thereto, authorising said primary device transaction request; issuing a request comprising the FPAN to a payment network for settlement of said transaction; and subsequent to issuing said request comprising the FPAN to said payment network, receiving a primary device transaction approved message from the payment network.

According to an embodiment there is provided a method comprising a payment terminal: receiving a secondary payment device transaction request comprising a device primary account number (DPAN) and a funding source proxy (FSP) derived from a funding primary account number (FPAN) of a funding source according to a predetermined algorithm; responsive thereto, determining that the FSP is not present on a deny list stored at the payment terminal; and responsive thereto, authorising said secondary payment device transaction request.

The method could further comprise said payment terminal issuing a request comprising the DPAN to a payment network for settlement of said transaction.

The method could further comprise the payment terminal: subsequent to issuing said request comprising the DPAN to said payment network, receiving a secondary

comprising the FPAN to a payment network for settlement of said transaction; and subsequent to issuing said request comprising the FPAN to said payment network, receiving a primary device transaction approved message from the payment network.

Said credentials of any of the above aspects could comprise one or more of: a funding PAN (FPAN), a device PAN (DPAN), an expiry date and a serial number.

According to an embodiment there is provided a system comprising a secondary payment device and a payment terminal, configured to perform the method of either of the sixth or seventh aspects.

According to an embodiment there is provided a payment terminal configured to perform the method of either of the sixth or seventh aspects.

Said predetermined algorithm of any of the aspects could generate the FSP in such a way that: said FPAN cannot be determined from the FSP; and/or each possible value of said FPAN uniquely maps to a different FSP. The predetermined algorithm could comprise a cryptographic hash function.

Said predetermined algorithm of any of the aspects could use an expiry date and/or a serial number.

The FSP of any of the aspects could be a payment account reference (PAR) as defined by EMVCo specifications.

Brief Description of the Drawings

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

Figure 1 shows an example multi-party payment transaction system;

Figure 2A illustrates a message flow;

Figure 2B illustrates another message flow;

Figure 3A illustrates the enablement of a secondary device for payments;

Figure 3B illustrates use of a primary payment device at a payment terminal;

Figure 3C illustrates the subsequent attempted use of a secondary payment device;

Figure 3D is a flow chart of a procedure following presentation of a payment device to a terminal;