or ATM device comprising means such as these, to allow interaction with a transaction card).

Trust management becomes extremely challenging when some system elements (payment cards and even terminals) are only intermittently in contact with other the main transaction system, and when it may be necessary for one system element to interact with another system element without a full assurance that this further system element is trustworthy. This may apply, for example, in conflict regions or after a natural disaster, or any other circumstance in which normal communication networks such as the wired or wireless telecommunications infrastructure may be wholly or partially disabled.

Transaction systems using the EMV standards will support offline transactions between a payment card or device and a terminal even when the terminal is not in communication with the main transaction system. Such transactions clearly have added risk as the risk management services provided by the main transaction system are not available, and such financial risk cumulates over time and number of transactions. It is strongly preferable to require terminals and payment devices to make an online connection to the main transaction system sufficiently regularly to control this financial risk. This requirement, however, is difficult to achieve for a conventional transaction card. This is because a conventional transaction card does not have a secure and reliable mechanism to track when online connection is required, or to track any other time or event driven metric.

Summary

In an aspect, the present disclosure provides a method of updating time in a transaction with an offline terminal of a transaction system, comprising: initiating a transaction with the an offline terminal; providing a stored trusted time value and receiving an obtained trusted time value, each trusted time value having been affirmed by a trusted time provider, wherein each trusted time value is affirmed by signature by a private key of an asymmetric key pair; decrypting the obtained signed trusted time value to determine the obtained trusted time value and to confirm that the obtained trusted time value was validly affirmed by the trusted time provider; comparing the

In an aspect, the present disclosure provides a method of updating time at a terminal of a transaction system in a transaction device, comprising, if the terminal is offline: commencing a transaction with the transaction device; providing a stored trusted time value and receiving an obtained trusted time value, each trusted value having been affirmed by a trusted time provider, wherein each trusted time value is affirmed by signature by a private key of an asymmetric key pair; decrypting the obtained signed trusted time value to determine the obtained trusted time value and to confirm that the obtained trusted time value was validly affirmed by the tursted time provider; comparing the obtained trusted time value with the stored trusted time value; and replacing the stored trusted time value with the obtained trusted time value if the obtained trusted time value is more recent than the stored trusted time value. In one embodiment, a method of risk management at a transaction device, wherein the transaction device holds a stored date for a risk related action, wherein the transaction device updates a stored trusted time value by the method described above, and wherein the transaction device takes a risk management action if the updated stored trusted time value is later than the stored date by a predetermined period of time. Risk management rules may be updated by a method substantially similar to the method of updating the trusted time value.

In embodiments, the method steps of the first aspect are performed by the terminal. This terminal may be one of a point of sale terminal and an automated teller machine. Using EMV protocols, such a terminal may request a transaction device trusted time value with a GET DATA command, or may provide a terminal trusted time value with a PUT DATA command. The terminal may also request a transaction device trusted time value or provides a terminal trusted time value with a GENERATE AC command.

In an embodiment, there is provided a method of risk management at a terminal, wherein the terminal holds a stored date for a risk related action, wherein the terminal updates a stored trusted time value by the method described above, and wherein the terminal takes a risk management action if the updated stored trusted time value is later than the stored date by a predetermined period of time. The risk management rules may be updated by a method substantially similar to the method of updating the trusted time value.

In an embodiment of the present disclosure comprises a method of updating time in

a transaction between a transaction device and a terminal, comprising the transaction device and the terminal both performing method steps as described above. For example, at least one method step may be performed at least partly by the offline terminal and at least one method step may be performed at least partly by the transaction device. Preferably, when the terminal is offline the transaction device and the terminal perform these method steps, but wherein the terminal is online and connected to an acquiring bank, the acquiring bank

provides a trusted time value to the terminal and to the transaction device.

In an aspect, the present disclosure provides a trusted time provider for a transaction system, comprising: a clock providing time values; a public/private key pair, comprising a public key for dissemination throughout the transaction system and a private key for signing time values to provide trusted time values; and a module or other means adapted continually to sample time values from the clock, to sign the sampled time values with the private key to form trusted time values, and to disseminate trusted time values throughout the transaction system.

In an aspect, the present disclosure provides a transaction device comprising a memory and a processor, wherein the memory is adapted to store trusted time values, and wherein the processor is programmed to perform the method provided by the first aspect of the invention. In embodiments, the transaction device is a payment card.

It will be appreciated that preferred and/or optional features of any of the preceding aspects of the present disclosure may be combined in any other aspect of the invention, alone or in appropriate combination, unless such features are incompatible.

Brief Description of Figures

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

Figure 1 shows elements of a payment infrastructure in which embodiments of the invention may be used;

Figure 2 shows in schematic form a transaction card adapted for use in embodiments of the invention;

Figure 3 shows in schematic form a terminal adapted for use in embodiments of the invention;

CLAIMS

1. A method of updating time at a transaction device in a transaction with an offline terminal of a transaction system, comprising:

initiating a transaction with the offline terminal;

providing a stored trusted time value and receiving an obtained trusted time value, each trusted time value having been affirmed by a trusted time provider, wherein each trusted time value is affirmed by signature by a private key of an asymmetric key pair;

decrypting the obtained signed trusted time value to determine the obtained trusted time value and to confirm that the obtained trusted time value was validly affirmed by the trusted time provider;

comparing the obtained trusted time value with the stored trusted time value; and

replacing the stored trusted time value with the obtained trusted time value if the obtained trusted time value is more recent than the stored trusted time value.

2. A method as claimed in claim 1, wherein the transaction device is a payment card.

3. A method as claimed in claim 1 or claim 2, wherein the transaction is performed according to EMV protocols.

4. A method as claimed in claim 3, wherein the transaction device requests a terminal stored trusted time value

using CDOL1.

5. A method as claimed in any preceding claim, wherein the transaction device holds a stored date for a risk related action, wherein after replacing the stored trusted time value the transaction device takes a risk management action if the updated stored trusted time value is later than the stored date by a predetermined period of time.

6. A method of updating time at a terminal of a transaction system in a transaction device, comprising, if the terminal is offline:

commencing a transaction with the transaction device;

providing a stored trusted time value and receiving an obtained trusted time value, each trusted value having been affirmed by a trusted time provider, wherein each trusted time value is affirmed by signature by a private key of an asymmetric key pair;

decrypting the obtained signed trusted time value to determine the obtained trusted time value and to confirm that the obtained trusted time value was validly affirmed by the tursted time provider;

comparing the obtained trusted time value with the stored trusted time value; and

replacing the stored trusted time value with the obtained trusted time value if the obtained trusted time value is more recent than the stored trusted time value.

7. A method as claimed in claim 6, wherein the terminal is one of a point of sale terminal and an automated teller machine.

9. A method as claimed in claim 8, wherein the terminal requests a transaction device trusted time value with a GET DATA command.

10. A method as claimed in claim 8 or 9, wherein the terminal provides a terminal trusted time value with a PUT DATA command.

11. A method as claimed in claim 8, wherein the terminal requests a transaction device trusted time value or provides a terminal trusted time value with a GENERATE AC command.

12. A method as claimed in any of claims 6 to 11, wherein the terminal is online and connected to an acquiring bank, the acquiring bank provides a trusted time value to the terminal and to the transaction device.

13. A trusted time provider for a transaction system, comprising:

a clock providing time values;

a public/private key pair, comprising a public key for dissemination throughout the transaction system and a private key for signing time values to provide trusted time values; and

a module adapted continually to sample time values from the clock, to sign the sampled time values with the private key to form trusted time values, and to disseminate trusted time values throughout the transaction system.

14. A transaction device comprising a memory and a processor, wherein the memory is adapted to store trusted time values, and wherein the processor is programmed to initiate a transaction between the transaction device and an offline terminal; provide a stored trusted time value and receive an obtained trusted time value, each trusted time value having been affirmed by a trusted

time provider and wherein each trusted time value is affirmed by signature by a private key of an asymmetric key pair; decrypt the obtained signed trusted time value to determine the obtained trusted time value and to confirm that the obtained trusted time value was validly affirmed by the trusted time provider; compare the obtained trusted time value with the stored trusted time value; and replace the stored trusted time value with the obtained trusted time value if the obtained trusted time value is more recent than the stored trusted time value.

15. A transaction device as claimed in claim 14, wherein the transaction device is a payment card.