CLAIMS

1. A method of authenticating products, the method comprising:

receiving, by an authentication card, authentication data including information about a product and sale information associated with the product from a merchant terminal associated with a merchant during a sale of the product, wherein the authentication card is associated with a card issuer communicably connected to the merchant terminal and the authentication card is not associated with the product prior to the sale of the product;

once the information about the product has been received, generating, by the authentication card, a signed message at the authentication card, the signed message comprising information about the authentication card and the authentication data as received from the merchant terminal;

communicating, by the authentication card, the signed message to the card issuer;

receiving, by the authentication card, authorization data authorizing the sale of the product from the card issuer when information in the signed message fulfils one or more criteria, wherein the authorization data received in the authentication card causes association of the authentication card with the product; and

verifying authenticity of the product based on the authorization data by communicating the authorization data stored in the authentication card to a goods manager after the sale of the product.

2. The method of claim 1, wherein the authentication card is a modified payment card, chip or virtual card provided by an application executed on a computing device.

3. The method of claim 2, wherein the authentication card and the goods manager communicate via at least one element of a transaction infrastructure, and wherein the at least one element of the transaction infrastructure comprises the merchant terminal.

4. The method of claim 1, wherein the merchant terminal is a terminal of a payment system configured to process transactions according to the EMV specification.

5. The method of claim 4, wherein the signed information from the authentication card comprises an application cryptogram.

6. The method of claim 5, wherein the authentication card requests product information as part of the card data object list 1 (CDOL1).

7. The method of claim 1, wherein the authentication card is associated with a card issuer; and

wherein receiving the authorization data from the goods manager includes receiving, by the authentication card, the authorization data from the goods manager via the card issuer in response to receipt, by the goods manager, of a query from the card issuer to verify the product information.

8. The method of claim 7, wherein the product information is stored on the authentication card in one or more data fields used to compute the application cryptogram in a conventional EMV payment device.

9. The method of claim 1, further comprising communicating, by the authentication card, the signed message to a card issuer, whereby the card issuer is permitted to use the information in the message to generate a

unique transaction identifier.

10. The method of claim 9, wherein the transaction identifier comprises an output of a hash function, and wherein the input of the hash function comprises an application cryptogram generated by the authentication card.

11. The method of claim 1, wherein the authentication card is associated with a unique identifier which is comprised in the information of the signed message.

12. The method of claim 1, wherein providing a signed message which comprises information about the authentication card and information about the product received from the merchant terminal comprises providing the signed message to the merchant terminal.

13. The method of claim 1, further comprising storing, by the authentication card, information about the merchant in a personal account number data field.

14. The method of claim 1, wherein receiving by the authentication card the authorization data triggers a start of a warranty associated with the product.

15. An authentication card, comprising:

a communication interface configured to communicate information for the authentication card with another device;

a storage device for storing information on the authentication card; and

a processor coupled to the communication interface and the storage device, the processor configured to:

receive authentication data including information about a product and sale information associated with the product from a merchant terminal associated with a merchant during a sale of the product, wherein the authentication card is associated with a card issuer communicably connected to the merchant terminal and the authentication card is not associated with the product prior to the sale of the product;

once the information about the product has been received, generate, by the authentication card, a signed message at the authentication card, the signed message comprising information about the authentication card and the authentication data as received from the merchant terminal;

communicate the signed message to the card issuer;

receive authorization data authorizing the sale of the product from the card issuer when information in the signed message fulfils one or more criteria, wherein the authorization data received in the authentication card causes association of the authentication card with the product; and

verify authenticity of the product based on the authorization data by communicating the authorization data stored in the authentication card to a goods manager after the sale of the product.

16. The authentication card of claim 15, wherein the authentication card is a modified payment card or a chip card.

17. The authentication card of claim 15, wherein receiving by the processor the authorization data triggers a start of a warranty associated with the product.

18. A method of authenticating products, the method comprising:

obtaining, at a merchant terminal, authentication data during a sale of a product, the authentication data including the product information and sale information for the product;

communicating, by the merchant terminal, the authentication data to an authentication card, wherein the authentication card is not associated with the product prior to the sale of the product;

generating, by the authentication card, a cryptogram which comprises information about the authentication card and the authentication data as received from the merchant terminal;

sending, from the authentication card via the merchant terminal, the cryptogram to a card issuer associated with the merchant terminal;

receiving, by the authentication card via the merchant terminal, authorization data authorizing the sale of the product from the card issuer when information in the cryptogram fulfils one or more criteria, wherein the authorization data received in the authentication card causes association of the authentication card with the product;

storing, at the authentication card, the authentication data and the authorization data; and

verifying authenticity of the product based on the authorization data by retrieving the authorization data from the authentication card and sending the authorization data to a goods manager.

19. The method of claim 18, wherein the authentication card is a modified payment card, chip or virtual card provided by an application executed on a computing device.

5

20. The method of claim 18, wherein receiving the authorization data triggers a start of a warranty associated with the product.