Summary

According to a first aspect of the present invention there is provided an authentication system which is configured, in response to receiving a request to authenticate a transaction, to send a first challenge to a secure element comprised in a mobile terminal via a first channel and, in response to receiving a first response to the first challenge from the secure element via the first channel, to determine whether the first response is correct, to send a second challenge to a processor-based controller comprised in the mobile terminal via a second, different channel and, in response to receiving a second response to the second challenge from the processor-based controller via the second channel, to determine whether the second response is correct, and, in dependence upon the first and second responses being correct, to signal that the transaction is authenticated.

The first challenge may be sent to an applet (or "SIM applet") on a secure element (such as a SIM, a USIM, a UICC embedded SIM, embedded UICC or virtual SIM) in the mobile terminal. The first channel may comprise a mobile phone network operator channel used to communicate securely with a secure element. The first channel preferably comprises an over-the-air (OTA) channel. The OTA channel may be an SMS-based OTA channel. The OTA channel may be a TCP/IP-based OTA channel. The second channel may comprise the Internet. The second channel may be provided via a short-range communications network link (such as WiFi) or mobile data link.

The authentication system may be configured, in relation to the first challenge, to retrieve a secure element identifier uniquely identifying a secure element in the mobile terminal (for example, an IMSI) and a hardware identifier uniquely identifying the hardware of the mobile terminal (for example, an IMEI), and to transmit the first challenge to the secure element via the first channel. The first reply may include a terminal fingerprint and/or a password (such as a one-time password), wherein the terminal fingerprint includes the secure element identifier and the hardware identifier or is generated in dependence on the secure element identifier and the hardware identifier. The authentication system is configured to determine whether the received terminal fingerprint is correct in dependence upon the retrieved secure element identifier and hardware identifier and/or to determine whether the received password is correct in dependence upon a locally-generated or locally-held password.

The authentication system may be configured, in relation to the second challenge, to transmit information relating to the transaction. The second response may include a password generated in dependence on a terminal fingerprint generated by the terminal

and at least some of the information relating to the transaction. The authentication system may be configured to determine whether the received password is correct in dependence upon a locally-generated or locally-held password.

The second response may be signed or encrypted with a key (key K1). The first and second responses may be signed or encrypted with first and second different keys (K2, K1) respectively.

The authentication system may be configured, in an enrolment phase, to exchange data with the mobile terminal via the second channel so as to receive a terminal fingerprint of the mobile terminal via the second channel and to exchange data with the mobile terminal via the first channel so as to determine the secure element identifier and the hardware identifier of the terminal via the first channel.

The authentication system may be configured, in an enrolment phase, to send a key (key K2) to the mobile terminal via the first channel.

According to a second aspect of the present invention there is provided and authentication system configured, in an enrolment phase, to exchange data with a processor-based controller comprised in a mobile terminal via a second channel so as to receive a terminal fingerprint of the mobile terminal via the second channel and to exchange data with a secure element comprised in the mobile terminal via a first, different channel so as to determine, via the first channel, a secure element identifier and a hardware identifier of the mobile terminal.

The terminal fingerprint may comprise a set of data about the mobile terminal hardware and/or software running on the mobile terminal, such as the operating system, for uniquely characterising the mobile terminal.

The authentication system may be configured, in response to receiving, from a source, a request to enrol a user comprising a user identifier and a mobile terminal identifier, to transmit a password to the source for presentation to the user and/or to a mobile terminal, in response to receiving, from an application running on the mobile terminal, a first key, a first terminal fingerprint and a copy of the first password via a second channel, to link the user identifier, the mobile terminal identifier, the application and the mobile terminal, to transmit a random number to secure element in the mobile terminal via a first, different channel, to send a second key to the secure element via the

first channel, in response to receiving, from the secure element via the first channel, an encrypted message comprising a second terminal fingerprint encrypted with the second key, to transmit a second password, to the secure element via the first channel and, in response to receiving, from the application via the second channel, a copy of the second password and in dependence upon the copy of the second password matching the second password, to link the user identifier and the second terminal fingerprint or data included the second terminal fingerprint.

According to a third aspect of the present invention there is provided a mobile terminal for use in authenticating a transaction comprising a secure element and a processor-based controller, the secure element configured, in response to receiving a first challenge from an authentication system via a first channel, to generate and transmit a first response to the authentication system via the first channel, and, the processor-based controller configured in response to receiving a second challenge from the authentication system via a second, different channel, to generate and transmit a second response to the authentication system via the second channel.

An application on the secure element may generate the first response.

The mobile terminal may be configured, in an enrolment phase, to exchange data with the authentication system via the second channel so as to provide a terminal fingerprint of the mobile terminal to the authentication system via the second channel and to exchange data with the authentication system via the first channel so as to provide the secure element identifier and the hardware identifier of the mobile terminal to the authentication system via the first channel.

According to a fourth aspect of the present invention there is provided a mobile terminal for use in authenticating a transaction comprising a secure element and a processor-based controller, the secure element configured, in an enrolment phase, to exchange data with an authentication system via a second channel so as to provide a terminal fingerprint of the mobile terminal to the authentication system via the second channel and the processor-based controller configured, in an enrolment phase, to exchange data with the authentication system via a first, different channel so as to provide a secure element identifier and a hardware identifier of the mobile terminal to the authentication system via the first channel.

Claims

1. An authentication system (21) configured, in response to receiving a request to authenticate a transaction:

to send a first challenge (313) to a secure element (5) comprised in a mobile terminal (4) via a first channel (78) and, in response to receiving a first response (316) to the first challenge from the secure element via the first channel, to determine whether the first response is correct;

to send a second challenge to a processor-based controller (61) comprised in the mobile terminal (4) via a second, different channel (79) and, in response to receiving a second response (338) to the second challenge from the processor-based controller via the second channel, to determine whether the second response is correct; and

in dependence upon the first and second responses being correct, to signal that the transaction is authenticated.

2. An authentication system according to claim 1, wherein the first channel (78) comprises a mobile phone network operator channel used to communicate securely with the secure element (5) in the mobile terminal.

3. An authentication system according to claim 1 or 2, wherein the second channel (79) comprises the Internet.

4. An authentication system according to any preceding claim which is configured, in relation to the first challenge:

to retrieve a secure element identifier (58) uniquely identifying the secure element (5) in the mobile terminal (4) and a hardware identifier (59) uniquely identifying the hardware of the mobile terminal; and

to transmit the first challenge to the secure element via the first channel (78); wherein the first reply (316) includes a terminal fingerprint (314) and/or a password (315), wherein the terminal fingerprint includes the secure element identifier (58) and the hardware identifier (59) or is generated in dependence on the secure element identifier (58) and the hardware identifier (59), wherein the authentication system is configured:

to determine whether the received terminal fingerprint is correct in dependence upon the retrieved secure element identifier and hardware identifier and/or to

determine whether the received password is correct in dependence upon a locally-generated or locally-held password.

5. An authentication system according to any preceding claim, which is configured, in relation to the second challenge:

to transmit information (319) relating to the transaction;

wherein the second response (338) includes a password generated in dependence on a terminal fingerprint and at least some of the information (319) relating to the transaction, and wherein the authentication system is configured:

to determine whether the received password is correct in dependence upon a locally-generated or locally-held password.

6. An authentication system according to any preceding claim, wherein the second response (338) is signed or encrypted with a key (K1).

7. An authentication system according to any preceding claim configured, in an enrolment phase:

to exchange data with the mobile terminal (4) via the second channel (79) so as to receive a terminal fingerprint of the mobile terminal via the second channel; and

to exchange data with the mobile terminal via the first channel (78) so as to determine the secure element identifier (58) and the hardware identifier (59) of the mobile terminal via the first channel.

8. An authentication system (21) configured, in an enrolment phase:

to exchange data with a processor-based controller (61) comprised in a mobile terminal (4) via a second channel (79) so as to receive a terminal fingerprint of the mobile terminal via the second channel; and

to exchange data with a secure element (5) comprised in the mobile terminal via a first, different channel (78) so as to determine, via the first channel, a secure element identifier (58) and a hardware identifier (59) of the mobile terminal via the first channel.

9. An authentication system according to claim 7 or 8, configured to sending a key (K2) to the mobile terminal (4) via the first channel (78).

10. An authentication system according to any one of claims 7 to 9, configured to transmit a password (186) via the first channel (78) and to receive a copy of the password via the second channel (78).

11. An authentication system according to any preceding claim configured, in an enrolment phase:

in response to receiving, from a source (37), a request (133) to enrol a user comprising a user identifier (26) and a mobile terminal identifier (27, 57), to transmit a password to the source for presentation to the user and/or to the mobile terminal;

in response to receiving, from an application (3) running on the mobile terminal, a first key (K1), a first terminal fingerprint and a copy of the first password via a second channel (79), to link the user identifier, the mobile terminal identifier, the application and the mobile terminal, to transmit a random number (153) to a secure element (5) in the mobile terminal via a first, different channel (78);

to send a second key (K2) to the secure element (5) via the first channel;

in response to receiving, from the secure element (5) via the first channel, an encrypted message (185) comprising a second terminal fingerprint encrypted with the second key, to transmit a second password, to the secure element via the first channel; and

in response to receiving, from the application via the second channel, a copy of the second password and in dependence upon the copy of the second password matching the second password, to link the user identifier and the second terminal fingerprint or data included the second terminal fingerprint.

12. A mobile terminal (4) for use in authenticating a transaction comprising a secure element (5) and a processor-based controller (61), the secure element configured:

in response to receiving a first challenge (313) from an authentication system (21) via a first channel (78), to generate and transmit a first response (316) to the authentication system via the first channel; and

the processor-based controller configured:

in response to receiving a second challenge from the authentication system (21) via a second, different channel (79), to generate and transmit a second response (338) to the authentication system via the second channel.

13. A mobile terminal according to claim 12, configured, in an enrolment phase:

to exchange data with the authentication system (21) via the second channel (79) so as to provide a terminal fingerprint of the mobile terminal to the authentication system via the second channel; and

to exchange data with the authentication system via the first channel (78) so as to provide the secure element identifier (58) and the hardware identifier (59) of the mobile terminal to the authentication system via the first channel.

14. A mobile terminal for use in authenticating a transaction comprising a secure element (5) and a processor-based controller (61), the secure element configured, in an enrolment phase:

to exchange data with an authentication system (21) via a second channel (79) so as to provide a terminal fingerprint of the mobile terminal to the authentication system via the second channel; and

the processor-based controller configured, in an enrolment phase:

to exchange data with the authentication system via a first, different channel (8) so as to provide a secure element identifier (58) and a hardware identifier (59) of the mobile terminal to the authentication system via the first channel.