

WHAT IS CLAIMED IS:

1. A method, comprising:

receiving, by an auxiliary device coupled to an access device, authentication data from a user;

initiating, by the auxiliary device, verifying the authentication data by providing the authentication data to a secure server computer and requesting a token from the secure server computer, wherein the secure server computer determines that the authentication data from the auxiliary device matches previously stored authentication data associated with the user, and requests and receives a token and a transaction authentication verification value from a token provider computer;

receiving, by the auxiliary device from the secure server computer, the token and the transaction authentication verification value; and

providing, by the auxiliary device, the token and the transaction authentication verification value to the access device, wherein the access device generates an authorization request message,

wherein the auxiliary device is an in-store auxiliary device and the access device is an in-store access device.

2. The method of claim 1, wherein the token provider computer generates a one-time password and provides the one-time password to an authorizing entity computer that then provides the one-time password to a client device in response to the request for the token from the secure server computer.

3. The method of claim 2, wherein the token provider computer activates the token in response to receiving, from the authorizing entity computer, an indication the user has been authenticated using the one-time password.

4. The method of claim 2, further comprising:

receiving, by the auxiliary device from the secure server computer, an indication that the user has yet to be authenticated according to a supplementary authentication scheme;

prompting, by the auxiliary device, the user for user input;

receiving, by the auxiliary device, subsequent user input; and

transmitting, by the auxiliary device, the subsequent user input to the secure server computer, that then transmits the subsequent user input to the token

provider computer, wherein the token provider computer activates the token based at least in part on determining that the subsequent user input matches the one-time password.

5. The method of claim 2, wherein the auxiliary device provides the token and the transaction authentication verification value to the access device in response to receiving an indication from the secure server computer that the user has been authenticated using the one-time password.

6. The method of claim 1, wherein requesting the token from the secure server computer causes the secure server computer to:
generate a request for a plurality of cryptograms for transactions involving tokens;
transmit the request to the token provider computer;
receive the plurality of cryptograms; and
store the plurality of cryptograms.

7. The method of claim 1, wherein the authentication data is biometric data of the user, and wherein verifying the authentication data comprises:
transmitting, by the auxiliary device, the biometric data to the secure server computer; and
receiving, by the auxiliary device, an indication that the biometric data was verified by the secure server computer, wherein the access device generates the authorization request message based at least in part on receiving the indication that the biometric data was verified by the secure server computer.

8. The method of claim 1, wherein the authorization request message is generated in a first data format, wherein the access device transmits the authorization request message to a processing network computer, the processing network computer converting the authorization request message from the first data format to a second data format.

9. The method of claim 1, further comprising:
receiving, by the auxiliary device from the secure server computer, a single use value, the secure server computer receiving the single use value from the token provider computer;

receiving, by the auxiliary device, an unpredictable value from the access device,

generating, by the auxiliary device, an authorization request cryptogram using the unpredictable value and the single use value, and

transmitting, by the auxiliary device, the authorization request cryptogram to the access device, wherein the access device generates the authorization request message to comprise the authorization request cryptogram and transmits the authorization request message to a payment processing network through an acquirer computer, wherein the payment processing network obtains the single use value from the token provider computer, computes a new cryptogram using the unpredictable value and the single use value, and processes the authorization request message if the new cryptogram matches the authorization request cryptogram.

10. The method of claim 1, wherein the access device is a POS system.

11. An auxiliary device coupled to an access device, the auxiliary device comprising:

a processor; and

a computer readable medium coupled to the processor, the computer readable medium comprising code executable by the processor to cause the auxiliary device to:

receive authentication data associated with a user;

verify the authentication data by providing the authentication data to a secure server computer and requesting a token from the secure server computer, wherein the secure server computer determines that the authentication data from the auxiliary device matches previously stored authentication data associated with the user, and requests and receives a token and a transaction authentication verification value from a token provider computer;

receive the token and the transaction authentication verification value from the secure server computer; and

provide the token and the transaction authentication verification value to the access device, wherein the access device generates an authorization request message,

wherein the auxiliary device is an in-store auxiliary device and the access device is an in-store access device.

12. The auxiliary device of claim 11, wherein executing the code further causes the auxiliary device to receive, with the token, a cryptogram of a plurality of cryptograms stored at the secure server computer, the plurality of cryptograms being requested and stored at the secure server computer in response to receiving the request for the token.

13. The auxiliary device of claim 11, wherein executing the code further causes the auxiliary device to obtain payment credentials from the secure server computer, wherein the auxiliary device provides the payment credentials to the access device with the token and the transaction authentication verification value.

14. The auxiliary device of claim 11, wherein executing the code further causes the auxiliary device to:

identify that a one-time password authentication process is required;
prompt the user for a one-time password, the one-time password being communicated to the user utilizing a user device associated with the user; and
authenticate the user based at least in part on the one-time password.

15. The auxiliary device of claim 14, wherein the token is limited for use in a threshold number of transactions until the user is authenticated with the one-time password.

16. The auxiliary device of claim 11, wherein executing the code further causes the auxiliary device to:

obtain, from the secure server computer, a cryptographic key;
receive, from the access device, terminal data comprising an amount and an identifier; and
encrypt, by the auxiliary device, the terminal data utilizing the cryptographic key to generate an interaction cryptogram.

17. The auxiliary device of claim 16, wherein the interaction cryptogram is included in the authorization request message.

18. The auxiliary device of claim 16, wherein the cryptographic key is a limited use key.

19. The auxiliary device of claim 16, wherein the authorization request message is authorized based at least in part on verifying, by a remote server, the interaction cryptogram.