

## WHAT IS CLAIMED IS:

### 1. A method, comprising:

receiving, by an auxiliary device ~~in communication with~~ 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;

~~requesting, by the auxiliary device, a token from a secure server computer;~~

receiving, by the auxiliary device from the secure server computer, the token and ~~a~~ 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 ~~requesting the token from the secure server computer causes the secure server computer to:~~

~~generate a request for the token from a token provider computer, 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 ~~a~~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 ~~a~~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 auxiliary~~ 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 ~~a~~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 ~~in communication with~~ 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;

~~request a token from a secure server computer;~~

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

~~obtain a verification value for the token; 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 ~~provide~~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.

~~20. The auxiliary device of claim 16, wherein the verification value is a transaction authentication verification value.~~

~~21. A method, comprising:  
receiving, by a processing network computer from an access device, an authorization request message;  
comprising data in a first transaction data format;  
converting, by the processing network computer, the data in the first transaction data format to a second transaction data format; and~~

transmitting, by the processing network computer, an authorization request message including data in the second transaction data format to an authorizing entity computer for authorization.

22.—The method of claim 21, wherein the data is converted from the first transaction data format to a second transaction data format in response to identifying an indicator that an auxiliary device in communication with an access device was utilized to generate the authorization request message.

23.—The method of claim 22, wherein the data in the first transaction data format is converted based at least in part on an indicator included in the data.

24.—The method of claim 21, wherein the first transaction data format is a card on file transaction data format and wherein the second transaction data format is a card not present transaction data format.

25.—The method of claim 21, wherein the first transaction data format comprises track 1 and track 2 data of a payment device.

26.—The method of claim 21, wherein converting from the first transaction data format to the second transaction data format comprises deleting data from one data field and storing the data in a different data field.

27.—The method of claim 21, wherein the first transaction data format of the authorization request message is indicated by a first electronic commerce indicator value.

28.—The method of claim 27, wherein the second transaction data format of the authorization request message is indicated by a second electronic commerce indicator value that is different from the first electronic commerce indicator.

29.—The method of claim 21, wherein the first transaction data format is an e-commerce transaction data format and the second transaction data format is a contactless transaction data format.

30.—The method of claim 21, further comprising:  
receiving, by the processing network computer, an authorization response message comprising data in the second transaction data format;

~~converting, the data in the first transaction data format to the second transaction data format; and~~  
~~transmitting the authorization response message including data in the second transaction data format to an access device via a transport computer.~~

31. — ~~A processing network computer, 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 processing network computer to:~~  
~~receive an authorization request message~~  
~~comprise data in a first transaction data format;~~  
~~convert the data in the first transaction data format to a second transaction data format; and~~  
~~transmit an authorization request message including data in the second transaction data format to an authorizing entity computer for authorization.~~

32. — ~~The processing network computer of claim 31, wherein the data is converted from the first transaction data format to a second transaction data format in response to identifying an indicator that an auxiliary device in communication with an access device was utilized to generate the authorization request message.~~

33. — ~~The processing network computer of claim 32, wherein the auxiliary device is different from a user device.~~

34. — ~~The processing network computer of claim 33, wherein the first transaction data format is a card on file transaction data format and wherein the second transaction data format is a card not present transaction data format.~~

35. — ~~The processing network computer of claim 31, wherein the first transaction data format comprises track 1 and track 2 data of a payment device.~~

36. — ~~The processing network computer of claim 31, wherein converting from the first transaction data format to the second transaction data format comprises deleting data from one data field and storing the data in a different data field.~~

37.—~~The processing network computer of claim 31, wherein the first transaction data format of the authorization request message is indicated by a first electronic commerce indicator value.~~

38.—~~The processing network computer of claim 37, wherein the second transaction data format of the authorization request message is indicated by a second electronic commerce indicator value that is different from the first electronic commerce indicator.~~

39.—~~The processing network computer of claim 31, wherein the first transaction data format is an e-commerce transaction data format and the second transaction data format is a contactless transaction data format.~~

40.—~~The processing network computer of claim 31, wherein executing the code further causes the processing network computer to:~~

~~receive an authorization response message comprising data in the second transaction data format;~~

~~convert the data in the first transaction data format to the second transaction data format; and~~

~~transmit the authorization response message including data in the second transaction data format to an access device via a transport computer.~~

41.—A method comprising:

~~generating, by a first computer, a request for a plurality of cryptograms for transactions involving tokens;~~

~~transmitting the request to a second computer;~~

~~receiving, by the first computer from the second computer, the plurality of cryptograms; and~~

~~storing, by the first computer, the plurality of cryptograms for subsequent use.~~

42.—~~The method of claim 41, wherein the first computer is a secure server computer in communication with an auxiliary device, wherein the second computer is a token provider computer, and wherein the request for a plurality of cryptograms is generated based at least in part on receiving, from the auxiliary device, authentication data associated with a user.~~

43.—~~The method of claim 41, wherein the request comprises a number of cryptograms requested, and wherein the second computer verifies that the number of cryptograms requested is less than a maximum number cryptograms allowed for an entity associated with the first computer.~~

44.—~~The method of claim 43, wherein the plurality of cryptograms comprises a quantity equal to the maximum number of cryptograms allowed for the entity, when the request for the plurality of cryptograms requested a number greater than the maximum number of cryptograms.~~

45.—~~The method of claim 41, further comprising:  
receiving, from an auxiliary device, a request for a token; and  
providing, to the auxiliary device, the token requested and one of the plurality of cryptograms.~~

46.—~~The method of claim 41, wherein an association between an entity associated with the first computer and the plurality of cryptograms is maintained by the second computer.~~

47.—~~The method of claim 46, wherein the second computer verifies the entity is authorized to pre-fetch multiple cryptograms in a single request.~~

48.—~~A token provider computer, 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 token provider computer to:~~

~~receive, from a token requestor computer, a request for a token;  
generate the token;  
receive, from the token requestor computer, a cryptogram request for a number of cryptograms associated with the token;  
obtain profile data for a token requestor corresponding to the token requestor computer;  
determine that the token requestor associated with the token requestor computer is authorized to pre-fetch multiple cryptograms in a single request; and~~

transmit a response with a plurality of cryptograms to the token requestor computer.

49.—The token provider computer of claim 48, wherein executing the code further causes the token provider computer to:

determine whether the number of cryptograms requested is less than a maximum number of cryptograms approved for providing to the token requestor;

if the number of cryptograms requested is not less than the maximum number of cryptograms approved for providing to the token requestor, set the number of cryptograms requested to the maximum number of cryptograms; and

if the number of cryptograms requested is less than the maximum number of cryptograms that approved for providing to the token requestor, generate the plurality of cryptograms corresponding to the number of cryptograms requested.

50.—The token provider computer of claim 48, wherein the plurality of cryptograms are stored at the token requestor computer.

51.—The token provider computer of claim 48, wherein executing the code further causes the token provider computer to maintain a record indicating an association between the plurality of cryptograms and the token requestor.

52.—The token provider computer of claim 48, wherein executing the code further causes the token provider computer to:

receive, from a processing network computer, a verification request comprising a cryptogram and a token;

determine that the cryptogram and the token are associated with one another;

retrieve a credential associated with the token; and

provide, to the processing network computer, the credential in response to the verification request.

53.—The token provider computer of claim 52, wherein executing the code further causes the token provider computer to delete the cryptogram after providing the credential in response to the verification request.

54.—The token provider computer of claim 48, wherein the token requestor associated with the token requestor computer is a wallet provider.

55.—~~The token provider computer of claim 48, wherein executing the code further causes the token provider computer to maintain profile data associated with the token requestor, the profile data indicating a maximum number of cryptograms that are allowed to be generated for the token requestor in response to a single cryptogram request.~~

56.—~~The token provider computer of claim 48, wherein executing the code further causes the token provider computer to~~  
~~receive a subsequent cryptogram request for a subsequent number of cryptograms;~~

~~determine that the token requestor is associated with a remaining number of cryptograms previously associated with the token requestor; and~~

~~generate at least one cryptogram in response to the subsequent cryptogram request based at least in part on the subsequent number of cryptograms and a remaining number of cryptograms previously associated with the token requestor.~~

57.—~~The token provider computer of claim 56, wherein the at least one cryptogram is generated based at least in part on determining that the remaining number of cryptograms previously associated with the token requestor is less than a maximum number of cryptograms that are allowed to be generated for the token requestor.~~

58.—~~The token provider computer of claim 48, wherein the token requestor computer generates a number of transactions equal to the number of cryptograms before transmitting a subsequent cryptogram request to the token provider computer.~~

59.—~~The token provider computer of claim 48, wherein the token requestor computer is a secure server computer.~~

60.—~~The token provider computer of claim 48, wherein the token requestor computer is a user device.~~

61.—~~A method comprising:~~  
~~receiving, by a device in communication with an access device, a token and a single use value associated with a credential of a user;~~

receiving, by the device from the access device, access device data comprising at least an unpredictable value;  
generating, by the device, an authorization request cryptogram; and  
transmitting, by the device, the token and the authorization request cryptogram to the access device, wherein the access device generates an authorization request message and transmits the authorization request message to an authorizing computer for authorization, wherein the device is an auxiliary device.

62.—The method of claim 61, wherein the single use value is generated by a token provider computer and stored at a secure server computer, the secure server computer providing the token and the single use value to the device.

63.—The method of claim 61, wherein the authorization request cryptogram is generated based at least in part on the token, the unpredictable value, and the single use value.

64.—The method of claim 61, wherein the authorization request cryptogram is generated based at least in part on generating a combined value comprising a concatenation of the unpredictable value and the single use value.

65.—The method of claim 64, wherein the authorization request cryptogram is generated utilizing a hashing function and the combined value. —

66.—The method of claim 64, wherein the authorization request cryptogram is a portion of a hash value generated based at least in part on a hashing function and the combined value.

67.—The method of claim 61, further comprising deleting, the token and the authorization request cryptogram within a predetermined period of time after transmitting the token and the authorization request cryptogram to the access device.

68.—The method of claim 61, wherein a token authentication verification value and a token expiration date is received with the token and the single use value.

69.—The method of claim 68, wherein the token authentication verification value and token expiration date are included in the authorization request message.

~~70.—The method of claim 61, wherein the token and the authorization request cryptogram are deleted.~~

~~71.—A device in communication with an access 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 device to:  
receive a single use value and a token associated with a credential of a user;  
receive access device data comprising at least an unpredictable value;  
generate an authorization request cryptogram; and  
transmit the token and the authorization request cryptogram to an access device in communication with the device, wherein the access device generates an authorization request message and transmits the authorization request message to an authorizing computer for authorization, wherein the device is an auxiliary device or a secure element device.~~

~~72.—The device of claim 71, wherein the authorization request message is transmitted to an authorizing entity computer via a transport computer and a processing network computer.~~

~~73.—The device of claim 72, wherein the processing network computer verifies the authorization request cryptogram by:  
obtaining the single use value from a source of the single use value;  
retrieving the unpredictable value from the authorization request message;  
generating a hash value based at least in part on a hashing algorithm, the single use value obtained, and the unpredictable value retrieved; and  
comparing at least a portion of the hash value to the authorization request cryptogram.~~

~~74.—The device of claim 73, wherein the authorization request cryptogram is determined to be invalid and authorization is denied when at least the portion of the hash value is different from the authorization request cryptogram.~~

~~75.—The device of claim 74, wherein the authorization request cryptogram comprises the portion of the hash value, the portion of the hash value comprising a right most 8 bits of the hash value as generated.~~

~~76.—The device of claim 71, wherein the authorization request message comprises the authorization request cryptogram and the unpredictable value.~~

~~77.—The device of claim 71, wherein the authorization request cryptogram is formed further based at least in part on a transaction amount and a terminal identifier associated with the access device.~~

~~78.—The device of claim 71, wherein the device is the secure element device comprising a secure memory space that is accessible only to the device.~~

~~79.—The device of claim 71, wherein the secure element device is in wireless communication with the auxiliary device.~~

~~80.—The device of claim 71, wherein the device obtains the token from a secure server computer in communication with the device.~~

~~81.—A method comprising:~~

~~receiving, by a secure element device in communication with an auxiliary device and an access device, a token and a cryptographic key associated with a credential of a user, the token and cryptographic key being received from the auxiliary device;~~

~~receiving, by the secure element device from the access device, access device data comprising at least an unpredictable value;~~

~~generating, by the secure element device, an interaction cryptogram; and~~

~~transmitting, by the secure element device, the token and the interaction cryptogram to the access device, wherein the access device generates an authorization request message and transmits the authorization request message to an authorizing computer for authorization.~~

~~82.—The method of claim 81, wherein the cryptographic key is a limited use key.~~

~~83.—The method of claim 81, wherein the interaction cryptogram is generated based at least in part on the token, the unpredictable value, and the cryptographic key.~~

~~84.—The method of claim 81, wherein the interaction cryptogram is generated based at least in part on encrypting data with the cryptographic key.~~

~~85.—The method of claim 84, wherein the data comprises a terminal identifier and an amount.~~

~~86.—The method of claim 81, wherein the cryptographic key is usable for encrypting data for a threshold number of transactions.~~

~~87.—The method of claim 81, further comprising deleting, the token and the interaction cryptogram after transmitting the token and the interaction cryptogram to the access device.~~

~~88.—The method of claim 81, wherein the secure element device is in wireless communication with the access device.~~

~~89.—The method of claim 81, wherein the secure element device is in wireless communication with the auxiliary device.~~

~~90.—The method of claim 81, wherein the auxiliary device is different from a user device.~~

~~91.—A secure element device in communication with an access device and an auxiliary device, the secure element device comprising:~~

~~a secure memory space,~~

~~a processor; and~~

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

~~receive, from the auxiliary device, a token and cryptographic key associated with a credential of a user;~~

~~store the token and the cryptographic key in the secure memory space;~~

receive access device data comprising at least an unpredictable value;

generate an interaction cryptogram; and

transmit the token and the interaction cryptogram to an access device in communication with the secure element device, wherein the access device generates an authorization request message and transmits the authorization request message to an authorizing computer for authorization.

92. — The secure element device of claim 91, wherein the authorization request message is transmitted to an authorizing entity computer via a transport computer and a processing network computer.

93. — The secure element device of claim 92, wherein the processing network computer verifies the interaction cryptogram by:

obtaining the cryptographic key from a token provider computer;

retrieving data from the authorization request message;

encrypting the data with the cryptographic key to generate encrypted data;

and

comparing the encrypted data to the interaction cryptogram.

94. — The secure element device of claim 93, wherein the authorization request message comprises the encrypted data and the unpredictable value.

95. — The secure element device of claim 93, wherein the interaction cryptogram is determined to be invalid and authorization is denied when the encrypted data is different from the interaction cryptogram.

96. — The secure element device of claim 95, wherein the interaction cryptogram is determined to be valid and authorization is granted when the encrypted data matches the interaction cryptogram.

97. — The secure element device of claim 91, wherein the interaction cryptogram is generated further based at least in part on a transaction amount and a terminal identifier associated with the access device.

98. — The secure element device of claim 91, wherein the secure memory space is accessible only to the secure element device.

99. ~~The secure element device of claim 91, wherein the secure element device is in wireless communication with the auxiliary device.~~

100. ~~The secure element device of claim 91, wherein the auxiliary device obtains the token from a secure server computer in communication with the auxiliary device.~~