

CLAIMS

WHAT IS CLAIMED IS:

1. A method comprising:
 - receiving, by a server computer, a cryptogram request message from a first token requestor, wherein the first token requestor is a mobile phone operated by a user;
 - responsive to receiving the cryptogram request message, transmitting, by the server computer, to the first token requestor, a cryptogram, wherein the first token requestor uses a first token and the cryptogram to conduct a transaction with a point of sale terminal;
 - after the transaction is conducted and automatically without intervention of the user, transmitting, by the server computer, a provisioning request message to an authorizing entity computer;
 - receiving, by the server computer, a provisioning response message from the authorizing entity computer; and
 - providing, by the server computer, a second token to an application on the first token requestor, wherein the application provides the second token to a second token requestor so that the second token requestor stores the second token to conduct future transactions, and then performs another transaction using the second token, the second token being associated with the first token stored in the first token requestor, wherein the second token requestor is an application server associated with the application, and the first token and the second token are associated with a credential.
2. The method of claim 1, wherein the cryptogram request message comprises the first token.
3. The method of claim 1, wherein the second token is provided to the second token requestor via an application programming interface (API) in an API response message.
4. The method of claim 1, wherein the provisioning request message that is sent to the authorizing entity computer comprises the credential.

5. The method claim 4, wherein a device identifier for the first token requestor is bound to the second token.

6. The method of claim 5, wherein the providing of the second token to the second token requestor is performed after the cryptogram request message is received by the server computer, but is not responsive to the receipt of the cryptogram request message by the server computer.

7. The method of claim 1, further comprising:
updating, by the server computer, a token store to include the second token as mapping to the credential, an identifier identifying the first token requestor, and the first token, wherein the credential comprises a primary account number.

8. A server computer comprising:
a processor; and
a non-transitory computer readable medium, the non-transitory computer readable medium comprising instructions, executable by the processor, to cause the processor to:
receive a cryptogram request message from a first token requestor, wherein the first token requestor is a mobile phone operated by a user,
responsive to receiving the cryptogram request message, transmitting, to the first token requestor, a cryptogram, wherein the first token requestor uses a first token and the cryptogram to conduct a transaction with a point of sale terminal,
after the transaction is conducted and automatically without intervention of the user, transmit a provisioning request message to an authorizing entity computer for verification of a credential associated with the first token specific to the first token requestor,
receive a provisioning response message from the authorizing entity computer indicating whether the credential is verified,
obtain a second token, the first token and the second token both associated with the credential, and
provide the second token to an application on the first token requestor; and

the application on the first token requestor programmed to provide the second token to a second token requestor, so that the second token requestor stores the second token to conduct future transactions, and then performs another transaction using the second token, the second token being associated with the first token stored in the first token requestor, wherein the second token requestor is an application server associated with the application, and the first token and the second token are associated with the credential.

9. The server computer of claim 8, wherein the second token is bound to a device identifier associated with the first token requestor.

10. The server computer of claim 8, wherein the credential is an account number.

11. The server computer of claim 8, wherein the non-transitory computer readable medium further comprises instructions, which cause the processor to:
update a token store to include the second token as mapping to the credential, a device identifier uniquely identifying the first token requestor, and the first token.