

CLAIMS

WHAT IS CLAIMED IS:

1. A method comprising:
receiving, by a server computer, a message;
after receiving the message, 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 a second token requestor, the second token being associated with a first token stored in a first token requestor, wherein the first token and the second token are associated with a credential.
2. The method of claim 1, wherein the second token is provided to the second token requestor via the first token requestor.
3. The method of claim 1, wherein the second token is provided to the second token request device without passing through the first token requestor.
4. The method of claim 1, wherein the message is received from the second token requestor.
5. The method of claim 1, wherein the message comprises the first token.
6. The method of claim 1, wherein the message includes a cryptogram request message, and wherein the method further comprises:
transmitting, by the server computer, the first token and a cryptogram associated with the first token to the first token requestor.

7. 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.

8. The method of claim 1, wherein the provisioning request message that is sent to the authorizing entity computer comprises the credential.

9. The method claim 8, wherein the authorizing entity computer programmed to bind a device identifier for the first token requestor to the second token.

10. The method of claim 9, wherein the providing of the second token to the second token requestor is performed after the message is received by the server computer, but is not responsive to the receipt of the message by the server computer.

11. 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.

12. The method of claim 11, wherein the first token requestor is a mobile phone and the second token requestor is an application server that operates an application on the mobile phone.

13. 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 message;

after receiving the message, transmit a provisioning request message to an authorizing entity computer for verification of a credential associated with a first token specific to a 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 a second token requestor, the second token being associated with the first token stored in a first token requestor.

14. The server computer of claim 13, wherein the second token is bound to a device identifier associated with the first token requestor.

15. The server computer of claim 13, wherein the message includes a request for a cryptogram for a transaction conducted using the first token, and wherein the non-transitory computer readable medium further comprises instructions which cause the processor to:

transmit the cryptogram to the first token requestor in response to receiving the message.

16. The server computer of claim 13, 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.

17. A method comprising:

receiving, by a second token requestor, a first token from a first token requestor;

transmitting, by the second token requestor, a provisioning request message requesting a second token from a server computer; and

receiving, by the second token requestor from the server computer, the second token, wherein the second token and the first token are each associated with a credential.

18. The method of claim 17, wherein the second token is received by the second token requestor via an application programming interface (API).

19. The method of claim 17, wherein the second token requestor is an application server.

20. The method of claim 17, wherein the first token requestor is a communication device operated by a user associated with the primary credential.