WHAT IS CLAIMED IS:

1. A method, comprising:

receiving, by a server computer, a token request for a token from a token requester, wherein the token is a substitute for an account identifier;

performing, by the server computer, at least one authentication process on the account identifier or a holder of the account identifier;

in response to the performance of the at least one authentication process, generating, by the server computer, the token and a token assurance code based on the at least one authentication process, wherein the token assurance code indicates a level of confidence associated with a binding between the token and the account identifier, wherein the token assurance code represents whether the token was requested by a genuine account holder of the account identifier;

transmitting, by the server computer, the token to the token requester;

receiving, by the server computer, an authorization request message for a transaction, the authorization request message comprising the token;

retrieving, by the server computer and using the token, the token assurance code and the account identifier associated with the token from a token vault;

generating, by the server computer, a modified authorization request message comprising the account identifier and the token assurance code; and

transmitting, by the server computer, the modified authorization request message to an issuer computer for approval, wherein the transaction is approved based at least upon the token assurance code.

2. The method of claim 1 further comprising storing the token assurance code in the token vault.

3. The method of claim 1 wherein the at least one authentication process comprises an authentication process selected from the group consisting of a CVV2 check, an AVS check, and a one time password (OTP) verification check.

4. The method of claim 1, wherein the token request comprises an account identifier associated with a credit or debit card.

5. The method of claim 1, wherein the token assurance code indicates an authentication method associated with the token.

6. The method of claim 5, wherein the authentication method comprises at least one of: no authentication, network authentication, or issuer authentication.

7. The method of claim 1, wherein the token assurance code is based at least in part on a transaction history associated with the account identifier.

8. A server computer comprising a processor, and a computer readable medium coupled to the processor, the computer readable medium comprising code, executable by the processor, for implementing a method comprising:

receiving a token request for a token from a token requester, wherein the token is a substitute for an account identifier;

performing at least one authentication process on the account identifier or a holder of the account identifier;

in response to the performance of the at least one authentication process, generating the token and a token assurance code based on the at least one authentication process, wherein the token assurance code indicates a level of confidence associated with a binding between the token and the account identifier, wherein the token assurance code represents whether the token was requested by a genuine account holder of the account identifier;

transmitting the token to the token requester;

receiving an authorization request message for a transaction, the authorization request message comprising the token;

retrieving, using the token, the token assurance code and the account identifier associated with the token from a token vault;

generating a modified authorization request message comprising the account identifier and the token assurance code; and

transmitting the modified authorization request message to an issuer computer for approval, wherein the transaction is approved based at least upon the token assurance code.

9. The server computer of claim 8, wherein the method further comprises:

storing the token assurance code in the token vault.

10. The server computer of claim 8, wherein the at least one authentication process comprises an authentication process selected from the group consisting of a CVV2 check, an AVS check, and a one time password (OTP) verification check.

11. The server computer of claim 8, wherein the token request comprises an account identifier associated with a credit or debit card.

12. The server computer of claim 8, wherein the token assurance code indicates an authentication method associated with the token.

13. The server computer of claim 12, wherein the authentication method comprises at least one of: no authentication, network authentication, or issuer authentication.

14. The server computer of claim 8, wherein the token assurance code is based at least in part on a transaction history associated with the account identifier.