WHAT IS CLAIMED IS:

1. A computer-implemented method, comprising:

receiving, at a registration authority computer, a certificate signing request from a token requestor computer associated with a merchant, wherein the registration authority computer is operated by or on behalf of a financial institution that manages a financial account associated with the token requestor;

in response to receiving the certificate signing request, authenticating, by the registration authority computer, the token requestor based on data associated with the financial account;

transmitting, by the registration authority computer to a certificate authority computer, a modified version of the certificate signing request comprising an identifier associated with the registration authority computer, the certificate authority computer being operated by an entity different from the financial institution;

receiving, by the registration authority computer from the certificate authority computer, a token requestor ID for the token requestor; and

transmitting, by the registration authority computer, the token requestor ID to the token requestor computer, wherein receipt of the token requestor ID by the token requestor computer configures the token requestor computer to obtain a token from a token provider computer for a subsequent token-based transaction in which payment data is replaced by the token in an authorization request message.

2. The computer-implemented method of claim 1, wherein authenticating the token requestor by the registration authority computer comprises executing a know-your-customer process to authenticate the token requestor.

3. The computer-implemented method of claim 1, wherein transmitting the modified certificate signing request to the certificate authority computer causes the certificate authority computer to:

verify the registration authority computer authenticated the token requestor based at least in part on determining that the identifier associated with the registration authority computer is included in the modified certificate signing request;

in response to verifying the registration authority computer authenticated the token requestor, generate a token requestor identifier (ID) for the token requestor; and

store a mapping between a token requestor ID and a public key generated by and received from the token requestor computer.

4. The computer-implemented method of claim 1, further comprising:

receiving, by the registration authority computer, a token provisioning request message, the token provisioning request message comprising a digital signature generated by the token requestor computer using the token requestor ID generated by the certificate authority computer;

transmitting the token provisioning request message to the token provider computer, wherein transmitting the token provisioning request messages causes the token provider computer to retrieve a public key associated with the token requestor ID and verify the digital signature using the public key;

in response to transmitting the token provisioning request message, receiving, by the registration authority computer from the token provider computer, a token provisioned to the token requestor from the token provider computer; and

transmitting the token to the token requestor computer, wherein transmitting the token to the token requestor computer causes the token requestor computer to transmit an authorization request message including the token.

5. The computer-implemented method of claim 4, wherein the token provisioning request message comprises a digital signature, the digital signature being generated based on the token requestor ID, an identifier associated with registration authority computer, an identifier associated with the token requestor, a terminal identifier, a time stamp, and a message counter.

6. The computer-implemented method of claim 4, further comprising notifying an authorization computer related to the token provisioning request message that the token has been provisioned to the token requestor, the authorization computer being associated with an issuer corresponding to the token-based transaction.

7. The computer-implemented method of claim 4, wherein transmitting the token provisioning request message to the token provider computer causes the token provider computer to decrypt the digital signature to generate decrypted information and compare the decrypted information against one or more data fields of the token provisioning request message.

8. The computer-implemented method of claim 1, further comprising:

receiving, by the registration authority computer from the token requestor computer, an authorization request message associated with a token-based transaction, the authorization request message comprising a token and a digital signature generated by the token requestor computer;

transmitting, by the registration authority computer to the token provider computer, the authorization request message, wherein receipt of the authorization request message by the token provider computer causes the token provider computer to modify the authorization request message prior to sending the authorization request message to an authorization computer;

receiving, by the registration authority computer, an authorization response message corresponding to the authorization request message; and

transmitting, by the registration authority computer to the token requestor computer, the authorization response message.

9. A registration authority computer, comprising:

a processor; and

a computer readable medium, the computer readable medium comprising code, executable by the processor, for implementing a method comprising:

receiving a certificate signing request from a token requestor computer associated with a merchant, wherein the registration authority computer is operated by or on behalf of a financial institution that manages a financial account associated with the token requestor;

in response to receiving the certificate signing request, authenticating the token requestor based on data associated with the financial account;

transmitting, to a certificate authority computer, a modified version of the certificate signing request comprising an identifier associated with the registration

authority computer, the certificate authority computer being operated by an entity different from the financial institution;

receiving, by the registration authority computer from the certificate authority computer, a token requestor ID for the token requestor; and

transmitting, by the registration authority computer, the token requestor ID to the token requestor computer, wherein receipt of the token requestor ID by the token requestor computer configures the token requestor computer to obtain a token from a token provider computer for a subsequent token-based transaction in which payment data is replaced by the token in an authorization request message.

10. The registration authority computer of claim 9, wherein the token requestor ID is generated by the certificate authority computer in response to receiving the modified version of the certificate signing request from the registration authority computer.

11. The registration authority computer of claim 9, wherein the certificate signing request is received and the modified certificate signing request is transmitted within an authorization request message conforming to an ISO 8583 transaction message format.

12. The registration authority computer of claim 9, wherein the method further comprises notifying the authorization computer that the token has been provisioned to the token requestor, the authorization computer being associated with an issuer corresponding to the payment data.

13. The registration authority computer of claim 9, wherein the method further comprises:

receiving a token provisioning request message comprising a digital signature generated by the token requestor computer utilizing the token requestor ID generated by the certificate authority computer; and

transmitting the token provisioning request message to the token provider computer, wherein transmitting the token provisioning request messages causes the token provider computer to obtain a public key associated with the token requestor ID and verify the digital signature using the public key.

14. The registration authority computer of claim 9, wherein the token is a first token associated with a first token domain and the method further comprises:

transmitting a token provisioning request message to the certificate authority computer using the first token, wherein the token provider computer generates a second token in response to receiving the token provisioning request message, the second token being associated with a second token domain that is different than the first token domain;

receiving the second token from the token provider computer; and

transmitting the second token to the token requestor computer.

15. The registration authority computer of claim 14, wherein the token provisioning request message is routed through a transport computer prior to being received by the token provider computer, and wherein the transport computer authenticates an identity of a token requestor associated with the token provisioning request message.

16. The registration authority computer of claim 14, wherein the first token domain is associated with a lesser security restriction than the second token domain.

17. The registration authority computer of claim 9, wherein the identifier associated with the registration authority computer is added to the modified certificate signing request as an indication to the certificate signing authority that the registration authority computer has authenticated the token requestor.

18. The registration authority computer of claim 9, where receiving the token requestor ID is in response to transmitting the modified version of the certificate signing request.

19. The registration authority computer of claim 9, wherein the modified certificate signing request comprises a public key associated with the token requestor, and wherein the certificate authority computer is configured to maintain a mapping the

token requestor ID generated for the token requestor and the public key of the token requestor.