WHAT IS CLAIMED IS:

1. A method for a secure transaction with a network resource, the method comprising:

receiving, at a computing device corresponding to the network resource from a first client device, a request for a security token to authenticate a transaction session corresponding to a user account administered by the network resource, wherein the first client device is associated with the user account;

in response to the request:

generating, by the computing device, a particular security token, and

sending, to the first client device, the particular security token, wherein the first client device communicates the particular security token to a second client device;

receiving, at the computing device from the second client device, a modified security token,

wherein the modified security token includes the particular security token and a signature on the particular security token that is signed using a first key stored in a trusted hardware component coupled to the second client device, and

wherein a second key corresponding to the first key is registered with the network resource by:

receiving, prior to receiving the request from the first client device, a registration message from the second client device, the registration message including the second key, information associating the second client device with the user account, and information authenticating the second client device; and

upon successfully verifying the information, authenticating the second client device, recording the second client device as associated with the user account and storing the second key as associated with the second client device and the user account;

verifying, by the computing device, the modified security token using the second key, wherein the first key is an asymmetric private key and the second key is a public key corresponding to the private key; and

upon successfully verifying the modified security token, enabling, by the computing device, the transaction session corresponding to the user account.

2. The method of claim 1, wherein the request includes information identifying the first client device, and wherein generating the particular security token comprises:

examining the information identifying the first client device;

determining, based on the examining, whether the first client device is authorized to host the transaction session; and

generating the particular security token conditioned on determining that the first client device is authorized to host the transaction session.

3. The method of claim 2, wherein the information identifying the first client device includes one or more of a network address of the first client device, a location of the first client device, or a time of the request, and wherein determining whether the first client device is authorized to host the transaction session comprises at least one of:

determining that an association of the network address with the user account is registered with the network resource,

determining that the transaction session is permitted at the location of the first client device, or

determining that the transaction session is permitted at the time of the request.

4. The method of claim 2, further comprising:

conditioned on determining that the first client device is not authorized to host the transaction session, generating an error condition.

5. The method of claim 1, wherein the first key is an asymmetric private key and the second key is a public key corresponding to the private key, wherein the registration message further includes information associating the second client device with the user account, and wherein registering the second key further comprises:

upon successfully verifying the information authenticating the second client device:

recording the second client device as associated with the user account.

6. The method of claim 1, ~~wherein the first key is a symmetric key and the second key is generated based on the symmetric key, wherein the registration message further includes information associating the second client device with the user account, and~~ wherein registering the second key further comprises:

upon successfully verifying the information authenticating the second client device:

~~recording the second client device as associated with the user account, and~~

initiating a secure key exchange communication with the second client device; and

receiving, from the second client device, the second key as part of the secure key exchange communication.

~~7. The method of claim 6, wherein the second key is a hash value resulting from hashing the first key.~~

~~8~~7. The method of claim 1, wherein sending the particular security token to the first client device comprises sending, along with the particular security token, information indicating a validity time period for the particular security token, and wherein verifying the modified security token comprises:

determining whether the validity time period has expired; and

conditioned on determining that the validity time period has not expired, verifying the signature using the second key.

~~9~~8. The method of claim 1, wherein sending the particular security token to the first client device comprises sending, along with the particular security token, information uniquely identifying the particular security token, and wherein verifying the modified security token comprises:

determining, using the information uniquely identifying the particular security token, whether the modified security token has been used before; and

conditioned on determining that the modified security token has not been used before, verifying the signature using the second key.

~~10~~9. The method of claim 1, wherein enabling the transaction session corresponding to the user account comprises:

sending information to the first client device to provide a portal for the transaction session; and

enabling transactions corresponding to the user account through the portal provided on the first client device.

~~11~~10. The method of claim 1, further comprising:

obtaining, by the second client device using an application executed by the second client device, a representation of the security token presented on the first client device;

upon obtaining the representation of the security token, requesting, by the second client device, confirmation to sign the security token;

in response to the request, receiving an input confirming proceeding with signing the security token;

authenticating the input;

upon successfully authenticating the input, controlling a trusted hardware component coupled to the second client device to generate the modified security token by signing the security token using the first key stored in the trusted hardware component; and

sending, by the second client device to the computing device, the modified security token.

~~12~~11. The method of claim 1, wherein the network resource is a cryptoasset custodial system, and the user account is a custodial account administered by the cryptoasset custodial system.

~~13~~12. A system comprising:

one or more processors; and

storage media storing instructions that are operable to cause the one or more processors to perform operations comprising:

receiving, at a computing device corresponding to a network resource from a first client device, a request for a security token to authenticate a transaction session corresponding to a user account administered by the

network resource, wherein the first client device is associated with the user account;

in response to the request:

generating, by the computing device, a particular security token, and

sending, to the first client device, the particular security token, wherein the first client device communicates the particular security token to a second client device;

receiving, at the computing device from the second client device, a modified security token,

wherein the modified security token includes the particular security token and a signature on the particular security token that is signed using a first key stored in a trusted hardware component coupled to the second client device, and

wherein a second key corresponding to the first key is registered with the network resource by:

receiving, prior to receiving the request from the first client device, a registration message from the second client device, the registration message including the second key, information associating the second client device with the user account, and information authenticating the second client device; and

upon successfully verifying the information authenticating the second client device, recording the second client device as associated with the user account and storing the second key as associated with the second client device and the user account, wherein the first key is an asymmetric private key and the second key is a public key corresponding to the private key; and

~~verifying, by the computing device, the modified security token using the second key; and~~

upon successfully verifying the modified security token, enabling, by the computing device, the transaction session corresponding to the user account.

~~14~~13. The system of claim ~~13~~12, wherein the request includes information identifying the first client device, and wherein generating the particular security token comprises:

examining the information identifying the first client device;

determining, based on the examining, whether the first client device is authorized to host the transaction session; and

generating the particular security token conditioned on determining that the first client device is authorized to host the transaction session.

~~15~~14. The system of claim ~~14~~13, wherein the information identifying the first client device includes one or more of a network address of the first client device, a location of the first client device, or a time of the request, and wherein determining whether the first client device is authorized to host the transaction session comprises at least one of:

determining that an association of the network address with the user account is registered with the network resource,

determining that the transaction session is permitted at the location of the first client device, or

determining that the transaction session is permitted at the time of the request.

~~16~~15. The system of claim ~~14~~13, wherein the operations further comprise:

conditioned on determining that the first client device is not authorized to host the transaction session, generating an error condition.

~~17~~16. The system of claim ~~13~~12, wherein sending the particular security token to the first client device comprises sending, along with the particular security token, information indicating a validity time period for the particular security token, and wherein verifying the modified security token comprises:

determining whether the validity time period has expired; and

conditioned on determining that the validity time period has not expired, verifying the signature using the second key.

~~18~~17. The system of claim ~~13~~12, wherein sending the particular security token to the first client device comprises sending, along with the particular security token, information uniquely identifying the particular security token, and wherein verifying the modified security token comprises:

determining, using the information uniquely identifying the particular security token, whether the modified security token has been used before; and

conditioned on determining that the modified security token has not been used before, verifying the signature using the second key.

~~19~~18. The system of claim ~~13~~12, wherein enabling the transaction session corresponding to the user account comprises:

sending information to the first client device to provide a portal for the transaction session; and

enabling transactions corresponding to the user account through the portal provided on the first client device.

~~20~~19. A non-transitory storage medium storing instructions that are operable to cause one or more processors to perform operations comprising:

receiving, at a computing device corresponding to a network resource from a first client device, a request for a security token to authenticate a transaction session corresponding to a user account administered by the network resource, wherein the first client device is associated with the user account;

in response to the request:

generating, by the computing device, a particular security token, and

sending, to the first client device, the particular security token, wherein the first client device communicates the particular security token to a second client device;

receiving, at the computing device from the second client device, a modified security token,

wherein the modified security token includes the particular security token and a signature on the particular security token that is signed using a first key stored in a trusted hardware component coupled to the second client device, and

wherein a second key corresponding to the first key is registered with the network resource by:

receiving, prior to receiving the request from the first client device, a registration message from the second client device, the registration message including the second key, information associating the second client device with the user account, and information authenticating the second client device; and

upon successfully verifying the information authenticating the second client device, recording the second client device as associated with the user account and storing the second key as associated with the second client device and the user account;

verifying, by the computing device, the modified security token using the second key, wherein the first key is an asymmetric private key and the second key is an public key corresponding to the private key; and

upon successfully verifying the modified security token, enabling, by the computing device, the transaction session corresponding to the user account.