

CLAIMS

What is claimed is:

1. A computer-implemented method for performing cryptographic operations subject to identity verification, the method comprising:

receiving, by a cryptography chip, a request to perform a requested cryptographic operation from a client, wherein the request includes client identity information associated with the client, wherein the request includes first data to be processed, and wherein the cryptography chip is a hardware component including

a processing resource that performs cryptographic operations, and

a storage resource, distinct from the processing resource, that stores a first key, encrypted identity information associated with clients that are permitted to request cryptographic operations, and program logic executable by the processing resource to perform the requested cryptographic operation;

decrypting, by the cryptography chip, the encrypted identity information using the first key;

retrieving, by the cryptography chip, a second key, wherein the second key is hardcoded into software instructions stored in a firmware of the processing resource;

determining, by the cryptography chip, that the client identity information is associated with one of the clients that are permitted to request cryptographic operations based on comparing the client identity information to the decrypted identity information; and

in response to determining that the client identity information is associated with one of the clients that are permitted to request cryptographic operations, performing, by the cryptography chip, the requested cryptographic operation on the first data by executing the program logic stored in the storage resource using the second key hardcoded into the software instructions stored in the firmware of the processing resource, to generate a cryptographic result.

2. The computer-implemented method of claim 1, wherein the requested cryptographic operation is an encryption operation, a decryption operation, a digital signature verification operation, or a digital signature generation operation.

3. The computer-implemented method of any preceding claim, wherein the cryptography chip is a field-programmable gate array (FPGA), an application specific integrated circuit (ASIC), or a microprocessor.

4. The computer-implemented method of any preceding claim, wherein the cryptography chip includes an operating system executed by the processing resource to operate a computer system in which the cryptography chip is included.

5. The computer-implemented method of any preceding claim, wherein the request is a first request, the requested cryptographic operation is a first requested cryptographic operation, the client identity information is first client identity information, the method further comprising:

receiving, by the cryptography chip, a second request to perform a second requested cryptographic operation from a second client, wherein the request includes second client identity information associated with the second client; and

determining, by the cryptography chip, that the second client identity information is not associated with any of the clients that are permitted to request cryptographic operations based on comparing the second client identity information to the decrypted identity information,

wherein, in response to determining that the second client identity information is not associated with any of the clients that are permitted to request cryptographic operations, the cryptography chip does not perform the second requested cryptographic operation.

6. The computer-implemented method of any preceding claim, further comprising:

determining, by the cryptography chip, that one or more requests to perform cryptographic operations are malicious based on the one or more requests not including client

identity information associated with any of the clients that are permitted to request cryptographic operations; and

in response to determining that the one or more requests to perform cryptographic operations are malicious, clearing, by the cryptography chip, the encrypted identity information and the first key from the storage resource.

7. The computer-implemented method of any preceding claim, wherein the cryptography chip is a field-programmable gate array (FPGA), and the method further comprising:

receiving, by the cryptography chip, a request to reprogram the cryptography chip including reprogramming information; and

in response to receiving the request, replacing, by the cryptography chip, information stored in the storage resource with the reprogramming information.

8. A system for performing cryptographic operations subject to identity verification, comprising:

one or more processors; and

one or more computer-readable memories coupled to the one or more processors and having instructions stored thereon that are executable by the one or more processors to perform the method of any of claims 1 to 7, and 10 to 12.

9. An apparatus for performing cryptographic operations subject to identity verification, the apparatus comprising a plurality of modules for performing the method of any of claims 1 to 7, and 10 to 12.

10. The computer-implemented method of claim 1, wherein the client identity information comprises biometric information associated with the client.

11. The computer-implemented method of claim 1, wherein the program logic is stored unencrypted.

12. The computer-implemented method of claim 1, wherein the cryptography chip includes a physical interface, and wherein receiving the request to perform the requested cryptographic operation comprises:

receiving a selection of a desired cryptographic operation through the physical interface.