What is claimed is:

CLAIMS

1. A computer-implemented method for securely performing cryptographic operations, the method comprising:

receiving biometric information associated with a first user and a request to perform one or more cryptographic operations based on one or more cryptographic keys stored in a memory of an identity cryptographic chip (ICC), wherein the request is for performing the one or more cryptographic operations for at least one of a predetermined number of times or in a predetermined time period;

comparing the biometric information associated with the first user with biometric information pre-stored in the memory of the ICC as pre-stored biometric information;

determining that the biometric information associated with the first user matches the pre-stored biometric information;

in response to determining that the biometric information associated with the first user matches the pre-stored biometric information,

generating a token that records the at least one of the predetermined number of times or the predetermined time period,

temporarily storing the token until the token expires, wherein the token expires in response to performance of the one or more cryptographic operations for the predetermined number of times or a lapse of the predetermined time period,

sending the token to a computing device communicably coupled to the ICC, and

authorizing the one or more cryptographic operations to be performed;

receiving new biometric information associated with a second user;

clearing the memory of the ICC; and

subsequent to clearing the memory of the ICC, writing the new biometric information to the memory, wherein the new biometric information cannot be written to the memory before the memory is cleared.

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

performing the one or more cryptographic operations to produce an operational result; and

sending the operational result to a computing device communicably couple to the ICC to be presented to the first user.

3. The computer-implemented method of claim 1, wherein the request is a first request, the operational result is a first operational result, and the method further comprises:

receiving a second request for performing a cryptographic operation;

determining that the token is unexpired; and

performing the cryptographic operation to produce a second operational result.

4. The computer-implemented method of claim 3, wherein the first request is for decrypting a first data, the second operational result is plaintext of the first data, the biometric information associated with the first user is first biometric information, and the computer-implemented method further comprises:

receiving second biometric information and a third request for encrypting a second data associated with the plaintext of the first data;

in response to determining that the second biometric information matches the pre-stored biometric information, encrypting the second data to provide an encrypted second data; and

sending the encrypted second data to the computing device.

5. The computer-implemented method of any one of the preceding claims, wherein:

comparing the biometric information with the pre-stored biometric information is performed based on biometric recognition; and

the biometric recognition includes one or more of fingerprint recognition, voiceprint recognition, iris-scanning, facial recognition, and heartbeat recognition.

6. The computer-implemented method of any one of the preceding claims, wherein the one or more cryptographic operations are performed based on an asymmetric key pair

associated with the first user, and the cryptographic operations include one or more of an encryption operation, a decryption operation, or a digital signature generation operation.

7. The computer-implemented method of any one of the preceding claims, wherein the memory is a programmable read-only memory (PROM), an electrically-erasable PROM (EEPROM) or a flash memory, and wherein the biometric information and the asymmetric key pair are stored in separate storage units of the memory.

8. The computer-implemented method of claim 1, wherein the biometric information associated with the first user is compared with the biometric information pre-stored in the memory of the ICC using an identity verification algorithm stored in the memory of the ICC, and further comprising:

performing the one or more cryptographic operations using a cryptographic operation algorithm stored in the memory of the ICC,

wherein the identity verification algorithm and the cryptographic operation algorithm are stored in encrypted form.

9. A system for securely performing cryptographic operations, comprising:

one or more processors; and

one or more computer-readable memories coupled to the one or more processors and having instructions stored thereon which are executable by the one or more processors to perform the method of any one of claims 1-8.

10. An apparatus for securely performing cryptographic operations, the apparatus comprising a plurality of modules for performing the method of any one of claims 1-8.