

WHAT IS CLAIMED IS:

1 1. A method for participating in a generation of a cryptogram, the method
2 being performed by a support device and comprising performing at a support device:

3 receiving a request for security assessment, wherein the request is for the
4 support device to participate in a multi-party computation to generate a cryptogram, and
5 wherein the support device stores one or more secret shares generated from one or more
6 secret values, wherein the one or more secret shares are generated using an m -out-of- n secret
7 sharing scheme in which any collection of m secret shares out of a total number n of secret
8 shares are sufficient to generate a shared secret;

9 receiving security data;

10 identifying one or more security properties from the security data, the one or
11 more security properties corresponding to a current state of a device providing the security
12 data;

13 comparing the one or more security properties to reference data accessible to
14 the support device;

15 deciding whether to participate in the multi-party computation based on the
16 comparing of the one or more security properties to the reference data; and

17 in response to when the support device decides the deciding to participate,
18 providing a partial cryptographic value to one or more encryption engines, wherein the partial
19 cryptographic value is configured to be used by the one or more encryption engines to
20 generate the cryptogram via the multi-party computation, and wherein the partial
21 cryptographic value includes the one or more secret shares, at least one partial computation
22 derived using at least one of the one or more secret shares, or a combination thereof.

1 2. The method of claim 1, wherein the security data include one or more
2 of a group consisting of: location of an encryption device, a user authentication risk estimate,
3 whether a user is present at the encryption device, a purpose for generating the cryptogram, a
4 local time at the encryption device, a local time at the support device, and an IP address of the
5 encryption device.

1 3. The method of claim 1, wherein the reference data includes one or
2 more of the following: one or more previous locations of an encryption device, one or more

- 3 previous user authentication risk estimate, whether a user was previously present at the
- 4 encryption device, one or more previous purposes for generating one or more cryptograms,

one or more previous times at which the one or more cryptograms were generated, and one or more previous IP addresses of the encryption device.

4. The method of claim 1, wherein the ~~step of~~ deciding whether to participate in the multi-party computation ~~additionally further~~ comprises:
determining a likelihood that the cryptogram is being generated for a fraudulent purpose; and
comparing the likelihood to a predetermined assurance level, wherein the support device decides to participate in the multi-party computation if the likelihood is less than the predetermined assurance level and decides not to participate if the likelihood is equal to or greater than the predetermined assurance level otherwise.

5. The method of claim 1, ~~additionally further~~ comprising:
transmitting a request for the security data ~~from~~ to one or more other support devices; and
receiving the security data from the one or more other support devices.

6. The method of claim 1, wherein a number of secret shares included in the partial cryptographic value is inversely proportional to a likelihood that the cryptogram is being generated for a fraudulent purpose.

7. The method of claim 1, wherein the cryptogram comprises one or more of the following: an assurance level and user information.

8. The method of claim 1, wherein the one or more security properties include identification data that can be used by the support device to identify a source of the security data, and wherein the ~~step of~~ comparing the one or more security properties to the reference data ~~stored on~~ accessible to the support device comprises identifying a source of the security data to be a peer in a group of devices using the identification data.

9. The method of claim 1, wherein the one or more security properties include one or more signed digital certificates, and wherein the ~~step of~~ comparing the one or more security properties to the reference data ~~stored on~~ accessible to the support device comprises authenticating one or more sources of the security data by verifying the signed digital certificates.

1 10. A method for generating a cryptogram, the method being performed at
2 an encryption device and comprising ~~performing at an encryption device:~~

3 transmitting a request for a security assessment to one or more support
4 devices, wherein the request is for the one or more support devices to participate in a multi-
5 party computation to generate a cryptogram, wherein the one or more support devices store
6 one or more secret shares generated from one or more secret values, wherein the one or more
7 secret shares are generated using an m -out-of- n secret sharing scheme in which any collection
8 of m secret shares out of a total number n of secret shares are sufficient to generate a shared
9 secret;

10 transmitting security data to the one or more support devices;

11 receiving a plurality of partial cryptographic values from a portion of the one
12 or more support devices, wherein the partial cryptographic values include at least one of the
13 one or more secret shares, at least one partial computation derived using at least one of the
14 one or more secret shares, or a combination thereof; and

15 generating the cryptogram using atthe plurality of partial cryptographic values
16 obtained from the portion of the one or more support devices and the encryption device.

1 11. The method of claim 10, wherein the security data include one or more
2 of the following: location of the encryption device, a user authentication risk estimate,
3 whether a user is present at the encryption device, a purpose for generating the cryptogram, a
4 local time at the encryption device, a local time at the one or more support devices, and an IP
5 address of the encryption device.

1 12. The method of claim 10, further comprising transmitting the
2 cryptogram to a decryption device, the decryption device decrypting the cryptogram in order
3 to produce an assurance level, wherein the assurance level is proportional to a likelihood that
4 the cryptogram was generated for a fraudulent purpose.

1 13. The method of claim 10, wherein the cryptogram comprises one or
2 more of the following: an encrypted assurance level and encrypted user information.

1 14. A method of decrypting a cryptogram, the method being performed at
2 a decryption system and comprising performing at a decryption system:

3 storing a plurality of secrets ~~across-on~~ one or more decryption devices of the
4 decryption system, wherein the plurality of secrets are also stored by an encryption system,
5 wherein each of the plurality of secrets are stored by the decryption system in association
6 with a different assurance level, wherein a first assurance level is higher than a second

- 7 assurance level when encryption devices of the encryption system contribute more secret
- 8 shares for the first assurance level than for the second assurance level;
- 9 receiving a cryptogram from the encryption system;

10 selecting a first secret of the plurality of secrets ~~to use~~ to decrypt the
11 cryptogram, wherein the first secret corresponds to the first assurance level;
12 determining that the first secret was used to encrypt the cryptogram;
13 decrypting the cryptogram using the first secret to obtain confidential
14 information; and
15 based on the first assurance level, processing the confidential information
16 according to a first protocol.

1 15. The method of claim 14, further comprising receiving a stated
2 assurance level from the encryption system, and wherein the ~~step of~~ determining that the first
3 secret was used to encrypt the cryptogram comprises comparing the stated assurance level to
4 the first assurance level, wherein the decryption system determines that the first secret was
5 used to encrypt the cryptogram if the stated assurance level matches the first assurance level.

1 16. The method of claim 14, wherein the confidential information
2 comprises a comparison assurance level and user information; and
3 wherein the ~~step of~~ processing the confidential information according to at the
4 first protocol comprises comparing the comparison assurance level to a predetermined
5 threshold assurance level, and comparing the user information against a user record.

1 17. The method of claim 14, further comprising:
2 authenticating an encryption device of the encryption system based on the
3 confidential information and the first protocol.

1 18. A non-transitory computer readable medium storing ~~a plurality of~~
2 ~~instructions for controlling a computer system to perform operations of any of the methods~~
3 ~~above~~ one or more instructions which, when executed by a computer system, cause the
4 computer system to perform the method of any of claims 1-17.

1 19. The A computer system comprising:
2 ~~a processor; and~~
3 ~~the non-transitory computer readable medium of claim 18 coupled to the~~
4 ~~processor, wherein the computer system includes a processor is configured to perform~~ execute
5 ~~the plurality of~~ one or more instructions stored on the non-transitory computer readable
6 medium.

1 20. A system comprising one or more processors configured to perform the
2 method of any of claims 1-17~~any of the above methods.~~