

WHAT IS CLAIMED IS:

1 1. A method comprising:
2 broadcasting, by an initiator device, a witness request to ~~one or more a~~
3 plurality of authentication devices, wherein the ~~one or more~~plurality of authentication devices
4 ~~determine an assurance level~~ determines one or more assurance levels with respect to the
5 initiator device, respectively, from a range of assurance levels and ~~determined~~determines a
6 token share corresponding to the one or more assurance level~~levels~~, respectively;
7 receiving, by the initiator device from the ~~one or more~~plurality of
8 authentication devices, ~~at least one a~~ plurality of witness ~~response~~responses comprising ~~the a~~
9 set of token shares corresponding to ~~the an~~ an assurance level among the one or more
10 assurance levels, wherein each of the token shares is a portion of an authentication token or
11 determined using a key share that is a fraction of a cryptographic key;
12 generating, by the initiator device, ~~an the~~ the authentication token using a set of, by
13 combining the token shares of the set; and
14 transmitting, by the initiator device, the authentication token to an
15 authentication server, wherein the authentication server verifies the authentication token.

1 2. The method of claim 1, wherein each of the ~~at least one~~plurality of
2 witness ~~response~~responses further comprises ~~the at least one~~ an assurance level among the one or
3 more assurance levels.

1 3. The method of claim 1, wherein the witness request specifies one or
2 more requested assurance levels, and wherein the one or more requested assurance levels
3 include the assurance level corresponding to the set of token shares~~shares~~.

1 4. The method of claim 1, wherein the set of token shares is associated
2 with a first assurance level of the range of assurance levels, and wherein the method further
3 comprises:
4 determining a first amount of the token shares of the set of token shares; and
5 determining, by the initiator device, the first assurance level ~~of the range of~~
6 ~~assurance levels~~ associated with the set of token shares that include at least a threshold
7 amount of token shares by comparing the first amount to the threshold amount.

1 5. The method of claim 4, wherein the first amount of the token shares is
2 determined by summing weights of the set of token shares, wherein a higher value for a
3 weight indicates the token share is more secure.

1 6. The method of claim 4, further comprising:
2 obtaining, by the initiator device, an initiator token share corresponding to the
3 first assurance level and any other token share(s) when lower assurance levels exist.

1 7. The method of claim 4, wherein the threshold amount of token shares
2 is predetermined for the first assurance level.

1 8. The method of claim 4, wherein the first assurance level is a highest
2 assurance level which the initiator device holds at least the threshold amount of token shares.

1 9. The method of claim 4, wherein the ~~assurance level is one or more~~
2 ~~assurance levels, the token share is one or more~~ shares are included in a plurality of token
3 shares corresponding to the one or more assurance levels, the first assurance level includes
4 one or more first assurance levels respectively associated with one or more sets of token
5 shares, and wherein the authentication token is one or more authentication tokens.

1 10. The method of claim 4 further comprising:
2 transmitting, by the initiator device, the first assurance level to the
3 authentication server.

1 11. The method of claim 1, wherein, prior to broadcasting the witness
2 request, the method further comprises:
3 receiving, by the initiator device, a challenge request from the authentication
4 server.

1 12. The method of claim 11, wherein the authentication server generates
2 the challenge request after receiving authentic credentials from a user device.

1 13. The method of claim 11, wherein the challenge request is received
2 from the authentication server via a user device.

1 14. The method of claim 13, wherein the authentication token is
2 transmitted to the authentication server via the user device.

1 15. The method of claim 1, wherein the ~~one or more~~ plurality of
2 authentication devices are in communication range of the initiator device.

1 16. The method of claim 1, wherein generating the authentication token
2 further comprises:
3 removing, by the initiator device, duplicate token shares from the set of token
4 shares; and

5 XORing, by the initiator device, remaining token shares from the set of token
6 shares to determine the authentication token.

1 17. The method of claim 1, wherein the witness request is broadcast over a
2 Bluetooth communication channel.

1 18. The method of claim 1, wherein, prior to broadcasting the witness
2 request, the method further comprises:

3 determining, by the initiator device, the witness request based on at least one
4 of user input, an internal timer, and a detection of an anomaly.

1 19. A method comprising:

2 receiving, by an authentication device from an initiator device, a witness
3 request;

4 determining, by the authentication device, a first assurance level ~~associated~~
5 with respect to the initiator device based on a trust score, the first assurance level determined
6 from a range of assurance levels;

7 obtaining, by the authentication device, a token share corresponding to the
8 first assurance level, wherein the token share is one of a plurality of token shares associated
9 with a plurality of authentication devices, respectively, wherein each of the plurality of token
10 shares is a portion of an authentication token or determined using a key share that is a
11 fraction of a cryptographic key, and wherein combining the plurality of token shares results
12 in generation of the authentication token; and

13 transmitting, by the authentication device to the initiator device, the token
14 share for the first assurance level.

1 20. The method of claim 19, wherein obtaining the token share further
2 comprises:

3 obtaining, by the authentication device, ~~any~~ other token share(s)
4 corresponding to lower assurance levels when assurance levels lower than the first assurance
5 level exist.

1 21. The method of claim 19, wherein transmitting the token share further
2 comprises:

3 transmitting, by the authentication device, the other token share(s) for each
4 lower assurance level.

1 22. The method of claim 19, wherein the initiator device determines a
2 highest assurance level associated with a threshold amount of token shares received from
3 ~~proximate the plurality of authentication devices including~~that include the authentication
4 device and are proximate the initiator device.

1 23. The method of claim 19 further comprising:
2 determining, by the authentication device, the trust score associated with the
3 initiator device based on at least network data.

1 24. The method of claim 23, wherein the network data includes at least one
2 from among transmission rates, data reception rates, average size of data packets, source
3 addresses, domain name system information, IP addresses, hostnames, signal strength data,
4 and Wi-Fi connection data.

1 25. The method of claim 24, wherein the trust score is determined based
2 on at least one of a difference between historically typical transmission rates and the
3 transmission rates, a difference between historically typical data reception rates and the data
4 reception rates, and a difference between historically typical average size of data packets and
5 the average size of data packets.

1 26. The method of claim 23, wherein the trust score is a local trust score,
2 and wherein determining the trust score further comprises:
3 receiving, by the authentication device, one or more remote trust scores from
4 one or more additional authentication devices; and
5 determining, by the authentication device, the trust score using a weighted
6 average of the local trust score and the one or more remote trust scores.

1 27. The method of claim 21, wherein obtaining the token share
2 corresponding to the first assurance level and ~~any~~the other token share(s) corresponding to
3 the lower assurance levels further comprises:
4 retrieving, by the authentication device, a first key share corresponding to the
5 first assurance level and ~~any~~-other key share(s) corresponding to the~~any~~ other token share(s);
6 deriving, by the authentication device, the token share corresponding to the
7 first assurance level from the first key share; and
8 deriving, by the authentication device, the ~~any~~-other token share(s)
9 corresponding to the lower assurance levels from the~~any~~ other key share(s).

1 28. The method of claim 27, wherein the first key share and the ~~any~~-other
2 key share(s) are fractions of a~~the~~ cryptographic key that is shared among the initiator device
3 and ~~one or more~~the plurality of authentication devices including the authentication device.

1 29. A computer product comprising a computer readable medium storing a
2 plurality of instructions for controlling a computer system to perform ~~operations~~the method
3 of any one of the methods aboveclaims 1-28.

1 30. A system comprising:
2 the computer product of claim 29; and
3 one or more processors for executing the plurality of instructions stored on the
4 computer readable medium.

1 31. A system comprising means for performing the method of any one of
2 ~~the methods above~~claims 1-28.

1 32. A system configured to perform the method of any one of ~~the methods~~
2 ~~above~~claims 1-28.

1 33. A system comprising modules that respectively perform the steps of
2 the method of any one of ~~the methods above~~claims 1-28.