

CLAIMS

1. A security device for provenance verification, the security device comprising:
at least one processor; and
5 machine-readable storage having stored thereon:
a secret key;
a plurality of shared keys derived from the secret key, each shared key
being associated with a pair consisting of the security device and one of a
plurality of other security devices; and
10 instructions for causing the at least one processor to:
generate a message, and/or receive a message from a device with
which the security device is in communication, or from one of the plurality
of other security devices; and
perform at least one cryptographic operation on the message,
15 and/or on data derived from it, using the secret key and/or one of said
shared keys.
2. A security device according to claim 1, wherein each shared key is derived by
generating a hash of the secret key and a salt value that is specific to the pair.
20
3. A security device according to claim 1 or claim 2, wherein the at least one cryptographic
operation comprises generating at least one hash from one or more of: the secret key,
one or more of said shared keys, one or more of said salt values, the message, and a
timestamp.
25
4. A security device according to any one of claims 1 to 3, wherein the at least one
cryptographic operation comprises an initiate operation that comprises:
determining a destination device of said other security devices to which the
message will be sent;
30 generating cryptographic evidence that comprises a hash of: the shared key of
the pair consisting of the security device and the destination device; a timestamp value;
and the message; and
transmitting the cryptographic evidence, the timestamp value, and the message
to the destination device.
35
5. A security device according to any one of claims 1 to 4, wherein the at least one
cryptographic operation comprises a witness operation that comprises:

receiving a cryptographic evidence, a timestamp, and the message from a first device of said other security devices;

determining a second device of said other security devices to which the message will be sent;

5 generating a modified cryptographic evidence comprising a hash of the cryptographic evidence, the shared key of the pair consisting of the security device and the second device, the timestamp, and the message; and

transmitting the modified cryptographic evidence, the timestamp, and the message to the second device.

10

6. A security device according to any one of claims 1 to 5, wherein the at least one cryptographic operation comprises an extend operation that comprises:

receiving a cryptographic evidence, a timestamp, and the message from a first device of said other security devices;

15 determining a second device of said other security devices to which the message will be sent;

generating a modified cryptographic evidence comprising a hash of the cryptographic evidence, the shared key of the pair consisting of the security device and the destination device, the timestamp, the message, and a further message; and

20 transmitting the modified cryptographic evidence, the timestamp, the message, and the further message to the second device.

7. A security device according to any one of claims 1 to 6, wherein the at least one cryptographic operation comprises a verification operation that comprises:

25 receiving a cryptographic evidence, a timestamp, and one or more messages, said one or more messages arriving at the security device through a sequence of said other security devices;

generating a hash for each successive device in the sequence, each successive hash being computed based on: the hash for the previous device in the sequence, the shared key for the pair that consists of the successive device and the previous device, the timestamp, and if applicable, one of the one or more messages; and

30 comparing a last one of said hashes to the cryptographic evidence.

8. A method of provenance verification, comprising:

35 providing a plurality of security devices, each security device being provided with a key set comprising: a secret key, and a plurality of shared keys, each shared key being derived by generating a hash of the secret key and a salt value that is specific to a pair consisting of said security device and another of the plurality of security devices; and

configuring each security device to:

generate and/or receive one or more messages; and

perform at least one cryptographic operation on the message or

messages, and/or on data derived therefrom, using a respective secret key of the
5 security device and/or one of said shared keys.

9. A method according to claim 8, wherein the at least one cryptographic operation
comprises generating at least one hash from one or more of: the respective secret key,
one or more of said shared keys, one or more of said salt values, the message, and a
10 timestamp.

10. A method according to claim 8 or claim 9, wherein the at least one cryptographic
operation comprises an initiate operation that comprises:
determining a destination device to which the message will be sent;
15 generating a cryptographic evidence that comprises a hash of the shared key of
the pair consisting of the security device and the destination device, a timestamp value,
and the message; and
transmitting the cryptographic evidence, the timestamp value, and the message
to the destination device.

20 11. A method according to any one of claims 8 to 10, wherein the at least one cryptographic
operation comprises a witness operation that comprises:
receiving a cryptographic evidence, a timestamp, and the message from a first
device of said other security devices;
25 determining a second device of said other security devices to which the message
will be sent;
generating a modified cryptographic evidence that comprises a hash of the
cryptographic evidence, the shared key of the pair consisting of the security device and
the second device, the timestamp, and the message; and
30 transmitting the modified cryptographic evidence, the timestamp, and the
message to the second device.

12. A method according to any one of claims 8 to 11, wherein the at least one cryptographic
operation comprises an extend operation that comprises:
35 receiving a cryptographic evidence, a timestamp, and the message from a first
device of said other security devices;
determining a second device of said other security devices to which the message
will be sent;

- generating a modified cryptographic evidence that comprises a hash of the cryptographic evidence, the shared key of the pair consisting of the security device and the second device, the timestamp, the message, and a further message; and
transmitting the modified cryptographic evidence, the timestamp, the message,
5 and the further message to the second device.
13. A method according to any one of claims 8 to 12, wherein the at least one cryptographic operation comprises a verification operation that comprises:
receiving a cryptographic evidence, a timestamp, and one or more messages
10 from a first device of said other security devices, said one or more messages arriving through a sequence of said other security devices;
generating a hash for each successive device in the sequence, each successive hash being computed based on the hash for the previous device in the sequence, the shared key for the pair that consists of the successive device and the previous device,
15 the timestamp, and if applicable, one of the one or more messages; and
comparing a last one of said hashes to the cryptographic evidence.
14. A method according to any one of claims 8 to 13, comprising connecting the security devices to a network such that the security devices intercept or otherwise obtain
20 traffic between a plurality of connected devices on the network, wherein the one or more messages comprise data derived from said traffic.
15. A method according to claim 14, wherein the network is a network of an industrial control system or a smart grid.
25
16. A security system for a network of connected devices, the security system comprising:
a plurality of security devices attachable to the connected devices, each security device being provided with a key set comprising: a secret key, and a plurality of shared keys, each shared key being derived by generating a hash of the secret key and a salt
30 value that is specific to a pair consisting of said security device and another of the plurality of security devices;
wherein each security device is a security device according to any one of claims 1 to 7, and/or is configured to perform a method according to any one of claims 8 to 13.
- 35 17. A networked system comprising:
a plurality of connected devices;
wherein a subset of the connected devices is a plurality of security devices, each security device being provided with a key set comprising: a secret key, and a plurality of

shared keys, each shared key being derived by generating a hash of the secret key and a salt value that is specific to a pair consisting of said security device and another of the plurality of security devices;

wherein each security device is a security device according to any one of claims 1
5 to 7, and/or is configured to perform a method according to any one of claims 8 to 13.

18. A networked system according to claim 17, wherein the networked system is an industrial control system or a smart grid.