

CLAIMS

1. A method of provisioning a message authentication protocol in a system of connected devices, the method comprising, by at least one of the connected devices:
generating a private key and a public key;
5 transmitting the public key to each other connected device;
generating, by a sequence of hash operations using the private key, a hash tree,
wherein each leaf node of the hash tree can have two or more values, each of the two or more values being associated with a respective nonce value, and wherein each leaf node has a hash computed from the concatenation of the respective nonce values;
10 signing a root of the hash tree with the private key; and
transmitting the root and the root signature to each other connected device.
2. A method according to claim 1, further comprising each other connected device validating the root signature.
3. A method according to claim 1 or claim 2, wherein each leaf node of the hash tree
15 can have three values, and wherein each of the three values comprises a nonce corresponding to 0, 1, and a break value.
4. A method according to any one of claims 1 to 3, wherein the method is repeated after consumption of a predetermined number of the nonce values, and/or before a predetermined expiry time.
- 20 5. A method of providing authentication information for a message in a system of connected devices, the method comprising:
at one of the connected devices that stores a hash tree in which each leaf node can have two or more values, each of the two or more values being associated with a respective nonce value that is stored in association with the hash tree, each leaf node
25 having a hash computed from the concatenation of the hashes of the respective nonce values:
determining an offset of a leaf node which has not already been used;
determining a symbol sequence of the message, each symbol in the sequence having one of said two or more values;
30 determining a proof by:
for each symbol in the sequence, retrieving a corresponding nonce value of a corresponding leaf node based on the value of the symbol, and hashes of the other respective nonce values for the corresponding leaf node; and
traversing the hash tree to retrieve hashes of siblings of nodes on a path
35 between the leaf node and a root of the hash tree;

- wherein the proof comprises a combination of, for the respective symbols,
the corresponding nonce values, the hashes of the other respective nonce values,
and the hashes of the siblings on the path between the leaf node and the root;
and
- 5 transmitting the proof and the message to at least one of the other
connected devices.
6. A method according to claim 5, wherein each leaf node of the hash tree can have
three values, each of the three values comprising a nonce corresponding to 0, 1, and
a break value, and wherein the message begins and ends with a break symbol.
- 10 7. A method according to claim 5 or claim 6, wherein the hash tree is generated by a
method according to any one of claims 1 to 4.
8. A method of verifying authentication information for a message in a system of
connected devices, the method comprising:
- 15 at a connected device of the connected devices, receiving the message and a
proof from another device of the connected devices, the proof being generated
according to a hash tree;
retrieving a root and a root signature for the another device; and
verifying the proof by:
- 20 determining a sequence of symbols of the message;
determining, based on said sequence of symbols and said proof, a leaf-
level digest;
performing a series of iterative hash operations using said proof and said
leaf-level digest to generate a root value; and
comparing the root value to the retrieved root for the another device.
- 25 9. A method according to claim 8, wherein the proof is generated by a method
according to any one of claims 5 to 7.
10. A connected device comprising: at least one processor; and machine-readable
storage comprising instructions for causing the at least one processor to perform a
method according to any one of claims 1 to 8.
- 30 11. A networked system comprising a plurality of connected devices, wherein each of a
subset of the connected devices is configured to carry out a method according to any
one of claims 1 to 7, and/or is configured to carry out a method according to claim 8
or claim 9.
12. A networked system according to claim 11, wherein the system is an industrial
35 control system.

13. A networked system according to claim 11, wherein the system is a smart grid.