Claims

1. A method of encryption key provisioning comprising:

providing, by a quantum computing safe method, a shared secret data to a device and also to a security service;

using the provided shared secret data to provide a root key; and

using the root key as a basis for a sequence of stages, wherein each stage comprises an operation which converts a start key into a different generated key, and the same stages are carried out in parallel at the device and at the security service;

wherein the root key is used as the start key for a first stage of the sequence, and a generated key produced by each stage of the sequence, except for the final stage of the sequence, is used as a start key for a next stage of the sequence; and

wherein the generated keys produced by the last stage of the sequence at the device and at the security service are symmetric keys.

2. The method according to claim 1, and further comprising using the generated keys produced by the last stage of the sequence at the device and at the security service to authenticate the device to the security service.

3. A method of device authentication comprising:

providing, by a quantum computing safe method, a shared secret data to a device and also to a security service;

using the provided shared secret data to provide a root key; and

using the root key as a basis for a sequence of stages, wherein each stage comprises an operation which converts a start key into a different generated key, and the same stages are carried out in parallel at the device and at the security service;

wherein the root key is used as the start key for a first stage of the sequence, and a generated key produced by each stage of the sequence, except for the final stage of the sequence, is used as a start key for a next stage of the sequence;

and further comprising using the generated keys produced by the last stage of the sequence at the device and at the security service to authenticate the device to the security service.

4. The method according to any one of claims 1 to 3, wherein the shared secret data is a symmetric encryption key or data derived from a symmetric encryption key.

5. A method of encryption key provisioning comprising:

providing, by a quantum computing safe method, data derived from a secret data on a device to a security service;

using the provided data derived from the secret data to provide a root key;

using the root key as a basis for a sequence of stages, wherein each stage comprises an operation which converts a start key into a different generated key, and the same stages are carried out in parallel at the device and at the security service;

wherein the root key is used as the start key for a first stage of the sequence, and a generated key produced by each stage of the sequence, except for the final stage of the sequence, is used as a start key for a next stage of the sequence;

wherein the generated keys produced by the last stage of the sequence at the device and at the security service are symmetric keys.

6. The method according to claim 5, and further comprising using the generated keys produced by the last stage of the sequence at the device and at the security service to authenticate the device to the security service.

7. A method of device authentication comprising:

providing, by a quantum computing safe method, data derived from a secret data on a device to a security service;

using the provided data derived from the secret data to provide a root key; and

using the root key as a basis for a sequence of stages, wherein each stage comprises an operation which converts a start key into a different generated key, and the same stages are carried out in parallel at the device and at the security service;

wherein the root key is used as the start key for a first stage of the sequence, and a generated key produced by each stage of the sequence, except for the final stage of the sequence, is used as a start key for a next stage of the sequence;

and further comprising using the generated keys produced by the last stage of the sequence at the device and at the security service to authenticate the device to the security service.

8. The method according to any one of claims 5 to 7, wherein the secret data is a symmetric encryption key or data derived from a symmetric encryption key.

9. The method according to any preceding claim, wherein the start keys for each stage of the sequence of stages at the device and at the security service are used as a symmetric key to authenticate the device to the security service and enable secure communication between the device and the security service.

10. The method according to claim 9, wherein, after the device has been authenticated to the security service, the security service sends data to the device, and further comprising

using this data to convert a start key into a different generated key for the current stage of the sequence of steps.

11. The method according to any preceding claim, wherein each stage comprises a ratchet operation.

12. The method according to claim 11, when dependent from claim 10, wherein the sent data is a ratchet value.

13. The method according to any preceding claim, wherein there are a plurality of stages in the sequence of stages.

14. The method according to claim 13, wherein the sequence of stages generate a corresponding sequence of keys, and different keys of the sequence of keys are associated with different scopes or permissions when used as symmetric keys to authenticate the device to the security service.

15. The method according to claim 4 or claim 8, wherein the provided symmetric encryption key or data derived from a symmetric encryption key is used as the root key.

16. The method according to claim 4 or claim 8, wherein the provided symmetric encryption key or data derived from a symmetric encryption key is further processed to provide the root key.

17. The method according to any one of claims 4, 8, 15, or 16, wherein the symmetric encryption key or data derived from a symmetric encryption key is provided to the device and the security service by a quantum key delivery (QKD) method.

18. The method according to any one of claims 4, 8, 15, or 16, wherein the symmetric encryption key or data derived from a symmetric encryption key is provided to the device and the security service by a classically secured or physical mechanism.

19. The method according to any one of claims 4, 8, 15, or 16, wherein the symmetric encryption key is derived from a key which was provided to the device and the security service by a quantum key delivery (QKD) method.

20. The method according to any one of claims 4, 8, 15, or 16, wherein the symmetric encryption key is derived from a key which was provided to the device and the security service by a classically secured or physical mechanism.

21. The method according to any one of claims 4, 8, 15, or 16, wherein the data derived from a symmetric encryption key is derived from a symmetric encryption key stored on the device.

22. The method according to claim 21, wherein the device is, or comprises, a SIM, and the symmetric encryption key is stored on the SIM.

23. The method according to claim 22, wherein the symmetric encryption key is an OTA key.

24. The method according to claim 21 or claim 22, wherein the data derived from a symmetric encryption key is provided to the security service by a Mobile Network Operator (MNO) associated with the SIM.

25. The method according to any one of claims 4 or 8 to 24, wherein, at least one stage of the sequence of stages requires a user authentication to enable the stage to be completed.

26. The method according to any one of claims 4 or 8 to 25, wherein, at least one stage of the sequence of stages requires an authorisation to enable the stage to be completed.

27. The method according to claim 26, wherein the authorisation is provided by a commissioning officer.

28. The method according to any one of claims 4 or 8 to 27, wherein the sequence of stages is defined by a workflow.

29. The method according to claim 28, wherein the workflow is configurable to require a user authentication for one, some, or all stages of the sequence of stages to be completed.

30. The method according to claim 28 or claim 29, wherein the workflow is configurable to require one or more authorisations for one, some, or all stages of the sequence of stages to be completed.

31. The method according to claim 30, wherein the workflow is configurable to identify who is required to provide each of the one or more authorisations.

32. The method according to any one of claims 4 or 8 to 31, wherein, following authentication of the device to the security service, the security service issues a token to the device with a scope related to the stage of the key used to carry out the authentication.

33. The method according to claim 32, wherein the token is a JSON Web Token (JWT).

34. The method according to any one of claims 4 or 8 to 33, wherein the security service is a cloud service.

35. An encryption key provisioning system comprising:

means arranged to provide, by a quantum computing safe method, a shared secret data to a device and also to a security service;

means arranged to use the provided shared secret data to provide a root key; and

means arranged to use the root key as a basis for a sequence of stages, wherein each stage comprises an operation which converts a start key into a different generated key, and the system is arranged to carry out the same stages in parallel at the device and at the security service;

wherein the root key is used as the start key for a first stage of the sequence, and a generated key produced by each stage of the sequence, except for the final stage of the sequence, is used as a start key for a next stage of the sequence; and

wherein the generated keys produced by the last stage of the sequence at the device and at the security service are symmetric keys.

36. The system according to claim 35, and further comprising means arranged to use the generated keys produced by the last stage of the sequence at the device and at the security service to authenticate the device to the security service.

37. A device authentication system comprising:

means arranged to provide, by a quantum computing safe method, a shared secret data to a device and also to a security service;

means arranged to use the provided shared secret data to provide a root key; and

means arranged to use the root key as a basis for a sequence of stages, wherein each stage comprises an operation which converts a start key into a different generated key, and the same stages are carried out in parallel at the device and at the security service;

wherein the root key is used as the start key for a first stage of the sequence, and a generated key produced by each stage of the sequence, except for the final stage of the sequence, is used as a start key for a next stage of the sequence; and

further comprising means arranged to use the generated keys produced by the last stage of the sequence at the device and at the security service to authenticate the device to the security service.

38. The system according to any one of claims 35 to 37, wherein the shared secret data is a symmetric encryption key or data derived from a symmetric encryption key.

39. An encryption key provisioning system comprising:

means arranged to provide, by a quantum computing safe method, data derived from a secret data on a device to a security service;

means arranged to use the provided data derived from the secret data to provide a root key; and

means arranged to use the root key as a basis for a sequence of stages, wherein each stage comprises an operation which converts a start key into a different generated key, and the same stages are carried out in parallel at the device and at the security service;

wherein the root key is used as the start key for a first stage of the sequence, and a generated key produced by each stage of the sequence, except for the final stage of the sequence, is used as a start key for a next stage of the sequence; and

wherein the generated keys produced by the last stage of the sequence at the device and at the security service are symmetric keys.

40. The system according to claim 39, and further comprising means arranged to use the generated keys produced by the last stage of the sequence at the device and at the security service to authenticate the device to the security service.

41. A device authentication system comprising:

means arranged to provide, by a quantum computing safe method, data derived from a secret data on a device to a security service;

means arranged to use the provided data derived from the secret data to provide a root key; and

means arranged to use the root key as a basis for a sequence of stages, wherein each stage comprises an operation which converts a start key into a different generated key, and the same stages are carried out in parallel at the device and at the security service;

wherein the root key is used as the start key for a first stage of the sequence, and a generated key produced by each stage of the sequence, except for the final stage of the sequence, is used as a start key for a next stage of the sequence;

and further comprising means arranged to use the generated keys produced by the last stage of the sequence at the device and at the security service to authenticate the device to the security service.

42. The system according to any one of claims 39 to 41, wherein the secret data is a symmetric encryption key or data derived from a symmetric encryption key

43. A computer-readable medium comprising code or computer instructions stored thereon, which, when executed by a processor, causes the processor to perform the method according to any one of claims 1 to 34.

44. A computer program comprising instructions, which, when executed by a processor, causes the processor to perform the method according to any one of claims 1 to 34.