

Claims

1. A computer-implemented method of storing one or more data item(s) in a quantum-safe "QS" network, the QS network comprising one or more QS server(s) and a repository for storing and accessing said data item(s), each QS server comprising a hardware security module "HSM" for storing an identical set of quantum distributed "QD" keys, said identical set of QD keys having been distributed to each of said QS server(s) in a quantum-safe manner, and said QS server(s) configured to communicate securely with each other and the repository using one or more available QD keys from the identical set of QD keys, the method performed by a QS server comprising:
- 5 generating a quantum reference "QREF" locator based on input data associated with a data item for storage and an available QD key selected from the set of QD keys; and sending the QREF locator along with the data item encrypted with the available QD key to the repository.
- 10
- 15 2. The computer-implemented method of claim 1, the method further comprising: selecting an available QD key from the set of QD keys for encrypting a data item; generating the QREF locator for storing and accessing the data item based on input data associated with the data item and the selected available QD key, wherein the generated QREF locator is unique;
- 20 linking the QREF locator to the available QD key of the set of QD keys; and sending the QREF locator and encrypted data item to the repository for storage, wherein the encrypted data item is linked to the QREF locator when stored.
- 25 3. The computer-implemented method of claims 1 or 2, the method further comprising receiving a set of QD keys using quantum safe key distribution from a quantum key distributor or source.
- 30 4. The computer-implemented method of any of claims 1 to 3, wherein the input data associated with the data item further comprises one or more input data from the group of:
- a device identifier;
- a manufacturer identifier;
- a user identifier;
- a user secret;
- a customer number; and
- 35 an access control list of users for accessing said data item.

5. The computer-implemented method of as claimed in any of claims 1 to 4, the method further comprising:
generating a QREF access token associated with the data item based on the QREF locator; and
5 sending the QREF access token to a device of a user associated with the data item.
6. The computer-implemented method of any of claims 1 to 5, the method further comprising:
generating a QREF access token for accessing the data item based on the QREF
10 locator using an irreversible function, process or operation, wherein the QREF access token is unique; and
sending the QREF access token to a device of a user for enabling the user to access said data item.
7. The computer-implemented method of any of claims 1 to 6, the method further
15 comprising:
receiving, from a device of a user, a QREF access token requesting access to a data item stored in the repository;
identifying a QREF locator based on the QREF access token and input data from the user; and
20 in response to identifying the QREF locator, performing the steps of:
retrieving the data item from the repository, wherein the data item is decrypted using the QD key corresponding to the QREF locator; and
providing access operations to the user in relation to the decrypted data item.
8. A computer-implemented method of quantum safe "QS" storage in a QS network, the
25 QS network comprising at least two QS servers and a repository for storing and accessing data items in relation to a plurality of users, wherein each QS server comprises a hardware security module "HSM" with an identical set of quantum distributed "QD" keys stored thereon and the QS servers communicate securely with each other and the repository using quantum encryption based on one or more available QD keys from the set of QD keys, the method
30 comprising:
generating a quantum reference "QREF" locator associated with a data item based on input data associated with a first user of the plurality of users and an available QD key selected from the set of QD keys; and
storing the data item encrypted with the available QD key in the repository indexed
35 with the QREF locator.

9. The computer-implemented method as claimed in claim 8, further comprising:
generating an QREF access token based on the QREF locator, wherein the QREF
access token enables access operations to be performed on the data item stored in the
repository;
5 sending the QREF access token to at least said first user of the plurality of users;
and
in response to receiving an QREF access token from a second user of the plurality of
users in relation to a data item stored in the repository performing the steps of:
identifying a QREF locator in relation to the access token, and said second
10 user; and
providing access operations in relation to the encrypted data item in the
repository based on the identified QREF locator and the identified said second user.
10. A computer-implemented method of quantum safe "QS" storage and retrieval in a QS
network, the QS network comprising one or more QS server(s) and a repository for storing
15 and retrieving one or more data item(s) by a plurality of users, wherein each QS server
comprises a hardware security module "HSM" with an identical set of quantum distributed
"QD" keys stored thereon and the QS servers communicate securely with each other and the
repository using quantum encryption based on one or more available QD keys from the set of
QD keys, the method performed by a QS server comprising:
20 in response to receiving a data item for storage
generating a quantum reference "QREF" locator based on a user secret of
the first user and an available QD key selected from the set of QD keys, wherein the
QREF locator indicates the location for storing the data item encrypted with the
selected QD key in the repository and an identity of the first user;
25 generating an QREF access token based on the QREF locator, wherein the
QREF access token enables access operations to be performed on the data item
when stored in the repository;
storing the data item in the repository indexed by the QREF locator; and
sending the QREF access token to the first user; and
30 in response to receiving an QREF access token for a data item stored in the
repository;
identifying a QREF locator based on the QREF access token and the identity
of the second user; and
providing access operations to the second user in relation to the encrypted
35 data item in the repository based on the identified QREF locator.
11. The computer-implemented method as claimed in any of claims to 1 to 10, further
comprising receiving a request for storing the data item by a first user.

12. The computer-implemented method as claimed in claims 10 or 11, wherein the first user and the second user are the same.
13. The computer-implemented method as claimed in claims 10 or 11, wherein the first user and the second user are different.
- 5 14. The computer-implemented method as claimed in any of claims 1 to 13, wherein the QS network further comprises one or more user devices, each user device comprising a hardware security module for storing a set of QD keys, wherein the one or more user devices and one or more of the QS servers communicate using quantum key encryption based on the set(s) of QD keys.
- 10 15. The computer-implemented method as claimed in any preceding claim, wherein the repository comprises a repository or storage system based on at least one from the group of:
- distributed ledger technology or network;
shared ledger technology or network;
blockchain technology or network;
15 publish/subscribe, response/request and/or real-time based digital storage cloud/repository technology;
any other secure cloud storage system or platform;
any other secure storage system or platform; and
any other secure database management system.
- 20 16. The computer-implemented method as claimed in any preceding claim, wherein each set of QD keys are distributed to each of the QS devices based on at least one from the group of:
- satellite quantum key distribution;
fibre optic quantum key distribution;
25 terrestrial quantum key distribution
optical quantum key distribution; and
any other quantum key distribution system capable of distributing an identical set of QD keys to each of the QS server(s) of the QS network.
17. The computer-implemented method as claimed in any preceding claim, wherein
30 generating the QREF locator further comprising:
- receiving a user secret from a device of a first user;
receiving an available QD key selected from the set of QD keys from one of the QS server(s); and

generating the QREF locator based on a first set of cryptographic or mathematical operations in relation to data representative of the user secret and the received QD key, wherein the QREF locator is unique.

5 18. The computer-implemented method as claimed in any preceding claim, wherein generating the QREF access token further comprising generating the QREF access token based on a second set of cryptographic or mathematical operations in relation to data representative of the QREF locator, wherein the QREF access token is unique.

10 19. The computer-implemented method as claimed in any of claims 17 or 18, wherein generating the QREF locator based on the first set of cryptographic or mathematical operations further comprises generating the QREF locator from data representative of the user secret and the received QD key based on any one or more cryptographic or mathematical operations from the group of:

15 one or more one-way functions;
one or more hash functions;
one or more hash-based message authentication code functions;
one or more key derivation functions;
one or more of multiplication, subtraction, addition, division, factorisation and/or any other mathematical operation;
20 any other combination of one or more cryptographic functions, mathematical operations, operable to generate data representative of a QREF locator that is unique, obfuscates the received QD key and user secret and capable of providing an address for locating the associated data item for storing in a repository.

25 20. The computer-implemented method as claimed in any of claims 17 to 19, wherein generating the QREF access token based on the second set of cryptographic or mathematical operations further comprises generating the QREF access token from data representative of the QREF locator based on any one or more cryptographic or mathematical operations from the group of:

30 one or more one-way functions;
one or more hash functions;
one or more hash-based message authentication code functions;
one or more key derivation functions;
one or more of multiplication, subtraction, addition, division, factorisation and/or any other mathematical operation;
35 any other combination of one or more cryptographic functions, mathematical operations, operable to generate data representative of an QREF access token that is unique, obfuscates the data representative of the QREF locator, and capable of being used

by a QS server to identify the QREF locator for providing an address for locating the associated data item stored in a repository.

21. The computer-implemented method as claimed in any preceding claim, the method further comprising:

- 5 receiving an QREF access token from a user;
identifying the QREF locator associated with the QREF access token; and
in response to identifying the QREF locator, performing one or more access operations in relation to the data item corresponding to the QREF locator stored in the repository and the QREF access token.

10 22. The computer-implemented method as claimed in claim 21, the method further comprising:

- storing a registration record of each user storing a data item in the repository,
wherein each registration record includes data representative of:
a user identity of said each user;
15 a user secret of said each user;
authentication challenges and responses;
the QREF locator associated with the data item;
a data item reference identifier associated with the data item;
a quantum key identifier associated with the QD key used to encrypt the data
20 item; and
an access control list associated with the data item;
receiving an QREF access token associated with a data item from a second user;
retrieving one or more registration records associated with the second user;
identifying the QREF locator associated with the QREF access token by:
25 generating, for each retrieved registration record, an QREF access token
based on said each retrieved registration record; and
matching the generated QREF access token with the received QREF access
token; and
identifying the QREF locator from the registration record associated with the
30 generated QREF access token matching the received QREF access token;
in response to identifying the QREF locator, performing one or more access operations in relation to the data item corresponding to the QREF locator stored in the repository and the QREF access token.

35 23. The computer-implemented method as claimed in claim 22, the QS network comprising one or more QS registration server(s) and a plurality of registration nodes, wherein a QS registration server connects to a set of registration nodes of the plurality of

registration nodes, and one or more QS server(s) distribute one or more groups of QD keys from the set of QD keys to the QS registration servers, each QS registration server distributing one or more QD keys from a group of QD keys to the corresponding set of registration nodes, the method further comprising:

- 5 receiving, from a QS registration server generating a registration record associated with a user, the registration record of the user, wherein a device of the user is in communication with a registration node coupled to the QS registration server, the registration record including one or more user data representative of:
- 10 a user identity of said each user;
 - one or more device identifiers associated with the user;
 - user credentials associated with logging into the QS system;
 - a user secret of said each user;
 - authentication challenges and responses;
 - 15 a QREF locator associated with a data item in relation to the user;
 - a data item reference identifier associated with the data item;
 - a QD key identifier associated with the QD key used to encrypt the data item;
- and
- an access control list associated with the data item; and
 - storing the registration record of said user in the repository.

- 20 24. The computer-implemented method as claimed in claim 23, the method further comprising:
- receiving user credentials from a QS registration server associated with a user, wherein a device of the user is in communication with a registration node coupled to the QS registration server;
 - 25 retrieving the registration record associated with the user based on the user credentials;
 - receiving a QREF access token associated with a data item from the user;
 - identifying the QREF locator associated with the QREF access token by:
 - 30 generating, for each retrieved registration record, an QREF access token based on said each retrieved registration record; and
 - matching the generated QREF access token with the received QREF access token; and
 - identifying the QREF locator from the retrieved registration record associated with the generated QREF access token matching the received QREF access token;
 - 35 in response to identifying the QREF locator, performing one or more access operations in relation to the data item corresponding to the QREF locator stored in the repository and the QREF access token.

25. The computer-implemented method as claimed in any preceding claim, wherein:
the repository further comprises a distributed ledger;
the QS network further comprising a plurality of QS servers, each QS server
comprises a HSM with an identical set of QD keys stored thereon and each QS server of the
5 plurality of QS servers comprising a node for operating the distributed ledger, wherein the
nodes of the plurality of QS servers form a QS distributed ledger network configured for
providing storage and access to one or more data item(s) stored on the distributed ledger,
wherein the method further comprising:
receiving a QREF locator for storing an encrypted data item in the distributed ledger;
10 and
storing the encrypted data item in the distributed ledger using the QREF locator as
an address for the location of the encrypted data item in the distributed ledger.
26. The computer-implemented method as claimed in any preceding claim, wherein:
the repository further comprises a shared ledger;
15 the QS network further comprising a plurality of QS servers, each QS server
comprises a HSM with an identical set of QD keys stored thereon and each QS server of the
plurality of QS servers comprising a node for operating the shared ledger between
corresponding nodes, wherein the nodes of the plurality of QS servers form a QS shared
ledger network configured for providing storage and access to one or more data item(s)
20 stored on the shared ledger, wherein the method further comprising:
receiving a QREF locator for storing the encrypted data item in the shared ledger;
and
storing the encrypted data item in the shared ledger using the QREF locator as an
address for the location of the encrypted data item in the shared ledger.
27. The computer-implemented method as claimed in claims 25 or 26, the method
further comprising:
receiving an QREF access token from the second user for accessing an encrypted
data item stored in the distributed or shared ledger;
identifying a QREF locator corresponding to the QREF access token and second
30 user; and
accessing the encrypted data item in the distributed or shared ledger using the
identified QREF locator based on the access token.
28. The computer-implemented method as claimed in any preceding claim, wherein:
the repository further comprises a digital storage platform using publish/subscribe,
35 request/response and/or real-time based messaging for storing and accessing data items,
the QS network further comprising a plurality of QS servers, each QS server comprises a

- HSM with an identical set of QD keys stored thereon and each QS server of the plurality of QS servers comprising a node for operating digital storage platform messaging between corresponding nodes, wherein the nodes of the plurality of QS servers form the digital storage platform as a QS distributed storage network configured for providing storage and
5 access to one or more data item(s) based on the digital storage platform messaging, wherein the method further comprising:
- receiving a QREF locator for storing the encrypted data item in the distributed storage platform; and
 - 10 storing the encrypted data item in the shared ledger using the QREF locator as an address for the location of the encrypted data item in the distributed storage platform.
29. The computer-implemented method as claimed in claim 28, the method further comprising:
- receiving an QREF access token from the second user for accessing an encrypted data item stored in the distributed storage platform,
 - 15 identifying a QREF locator corresponding to the QREF access token and second user; and
 - accessing the encrypted data item in the distributed storage platform using the identified QREF locator based on the access token.
30. The computer-implemented method as claimed in any preceding claim, wherein each
20 QS server comprises a satellite receiver, the method further comprising:
- receiving, at each of the one or more QS servers of the QS network, one or more sets of QD keys from a satellite quantum key distribution system, the satellite quantum key distribution system comprising at least one satellite configured for generating and distributing a set of QD keys; and
 - 25 storing, on each of the one or more QS servers of the QS network, the received set(s) of QD keys on the corresponding hardware security module, wherein after distribution of a set of QD keys to each of the QS servers, each of the QS servers has stored thereon an identical set of QD keys.
31. The computer-implemented method as claimed in claim 30, wherein the QS network
30 further comprises one or more user devices, each user device comprising a HSM for storing a set of QD keys, wherein the one or more user devices and one or more of the QS servers communicate using quantum key encryption based on the set(s) of QD keys, wherein each QS user device comprises a satellite receiver, the method further comprising:
- receiving, at one or more of the user devices, one or more sets of QD keys from the
35 satellite quantum key distribution system, the satellite quantum key distribution system

comprising at least one satellite configured for generating and distributing the one or more sets of QD keys; and

5 storing, on each of the one or more QS user devices of the QS network, the received set(s) of QD keys on the corresponding HSM, wherein after distribution of said one or more sets of QD keys to each of the QS user devices, each of the QS user devices has stored thereon an identical set of QD keys.

32. The computer-implemented method as claimed in any preceding claim, wherein each QS server of the QS network includes a hardware security module "HSM" for storing a set of QD keys, wherein each of the QD keys in the set of QD keys is mapped to a corresponding
10 QD key identifier and stored in the HSM based on data representative of:
the QD key identifier for identifying said each QD key; and
said each QD key;
wherein each set of QD keys stored on each of the QS servers of the QS network have identical mappings between the QD key identifier and each said QD key from the set of
15 QD keys, the method further comprising:
receiving a set of QD keys from a quantum key distribution system, each QD key of the set of QD keys mapped to a corresponding QD key identifier; and
storing data representative of the set of QD keys and corresponding QD key identifiers.

20 33. The computer-implemented method as claimed in claim 32, wherein data representative of a mapping of a QREF locator associated with a QD key is stored in the HSM, based on data representative of:
the QREF locator;
the QD key associated with the QREF locator; and
25 the QD key identifier identifying said selected QD key;
wherein each set of QD keys stored on an HSM of each of the QS servers of the QS network are updated based on the data representative of the mapping between the QD key identifier, the QREF locator and corresponding QD key, the method further comprising:
receiving a QREF locator and a QD key identifier associated with a QD key, the QD
30 key selected from the set of QD keys for use in generating the QREF locator and encrypting an associated data item; and
storing data representative of the mapping between the QREF locator, QD key identifier and QD key in the HSM of a QS server.

34. The computer-implemented method as claimed in any preceding claim, wherein the repository further comprises a plurality of records for storing one or more encrypted data item(s), each record comprising data representative of:
- a QREF locator associated with an encrypted data item; and
 - 5 the encrypted data item, wherein the data item is encrypted with a QD key associated with the QREF locator.
35. The computer-implemented method as claimed in claim 34, each record further comprising data representative of:
- one or more user identities allowed to access the encrypted data item of said each
 - 10 record; and
 - one or more permissions or operations associated with each of the one or more user identities in relation to accessing said encrypted data item.
36. The computer-implemented method as claimed in claim 34 or 35, each record further comprising data representative of an access control list indicating one or more user identities
- 15 allowed to access the encrypted data item and corresponding permissions and/or operations in relation to each user identity accessing said encrypted data item.
37. The computer-implemented method as claimed in any preceding claim, wherein the QREF locator further comprises data representative of:
- the user secret;
 - 20 a customer number allocated to the user;
 - a data item reference identifier allocated to the data item; and
 - a QD key identifier of the available QD key of the set of QD keys used to encrypt the data item.
38. The computer-implemented method as claimed in claim 37, wherein the QREF
- 25 locator further comprises data representative of:
- a user identifier; and
 - an access control list to the data item.
39. The computer-implemented method as claimed in any of claims 34 to 38, the method comprising:
- 30 receiving a request to register a user;
 - authenticating the user;
 - receiving user details for registering the user with the QS network in response to positive authentication of the user;
 - receiving a data item from the user for storing in a QS repository of the QS network;

- generating a unique QREF locator based data representative of the received user details and the data item;
associating the generated QREF locator with the registered user details and also the data item;
- 5 generating a unique QREF access token based on data representative of the QREF locator associated with the data item;
storing the QREF locator and the data item in the QS repository of the QS network;
and
10 sending the unique QREF access token to the user for use in accessing, in some manner, the data item.
40. The computer-implemented method as claimed in claim 39, further comprising:
receiving an QREF access token associated with a data item from a user;
authenticating the user;
identifying the QREF locator based on the user registration details and the access
15 token in relation to the user;
retrieving the data item associated with the QREF locator from the QS repository;
checking the user has permissions to access the data item based on an access control list associated with the data item; and
enabling the user access operations to the data item in response to determining the
20 user has permissions to access the data item.
41. The computer-implemented method as claimed in any of claims 34 to 38, the method comprising:
receiving a request to register a user;
authenticating the user;
- 25 receiving user details for registering the user with the QS network in response to positive authentication of the user;
receiving a know your own client "KYC" data item from the user for storing in a QS repository of the QS network, the KYC data item including data representative of know your own client details of the user;
- 30 generating a unique QREF locator based data representative of the received user details and the KYC data item;
associating the generated QREF locator with the registered user details and also the KYC data item;
- 35 generating a unique QREF access token based on data representative of the QREF locator corresponding to the KYC data item and the KYC data item;
storing the QREF locator and the KYC data item in the QS repository of the QS network; and

sending the unique KYC QREF access token to the user for use in providing KYC data of the user to one or more service providers.

42. The computer-implemented method as claimed in claim 41, further comprising:
- 5 receiving an QREF access token associated with a data item from a user;
authenticating the user;
identifying the QREF locator based on the user registration details and the access token;
retrieving the data item associated with the QREF locator from the QS repository;
checking the user has permissions to access the data item based on an access control list associated with the data item; and
10 enabling the user access to the data item in response to determining the user has permissions to access the data item.
43. The computer-implemented method as claimed in any of claims 34 to 38, the method comprising:
- 15 receiving a request to register a user;
authenticating the user;
receiving user details for registering the user with the QS network in response to positive authentication of the user;
receiving a certificate data item from the user for storing in a QS repository of the QS network, the certificate data item including data representative of a web certificate for
20 certifying the trustworthiness of a website operated by the user;
generating a unique QREF locator based data representative of the received user details and the certificate data item;
associating the generated QREF locator with the registered user details and also the certificate data item;
25 generating a unique QREF access token based on data representative of the QREF locator corresponding to the certificate data item and the certificate data item;
storing the QREF locator and the certificate data item in the QS repository of the QS network; and
30 sending the unique certificate QREF access token to the user for use by the website in providing the certificate QREF access token to web browsers of users visiting the website.
44. The computer-implemented method as claimed in claim 43, further comprising:
receiving an certificate QREF access token associated with a certificate data item from a web browser of a user;

- identifying the QREF locator associated with the certificate data item based on certificate data within the certificate QREF access token and the user registration data associated with the certificate access token;
- retrieving the certificate data item associated with the QREF locator from the QS repository;
- checking the certificate data item matches the received certificate details of the received certificate access token; and
- confirming to the web browser of the user that the certificate QREF access token is valid in response to the received certificate details matching the corresponding details of the certificate data item.
45. The computer-implemented method as claimed in claims 43 or 44, wherein the certificate data item is based on data representative of X509 standard and beyond certificates.
46. The computer-implemented method as claimed in any of claims 34 to 38, the method comprising:
- establishing QS communication channel with a first device of a first user;
- receiving, from the first device, a QREF access token associated with a QD key selected from the set of QD keys, the QD key for use in QS communications with a second device of a second user;
- retrieving the QD key selected from the set of QD keys from the repository based on the received QREF access token;
- sending the retrieved QD key to the first device and a second device for use in QS communications therebetween.
47. The computer-implemented method as claimed in any of claims 34 to 38, the method comprising:
- establishing a first communication channel with a first device of a first user;
- receiving, from the first device, a request for communicating with a second device of a second user via the QS network;
- establishing a second communication channel with the second device of the second user;
- receiving a response from the second device of the second user to connect with the first device of the first user;
- establishing a QS communication channel through the QS network based on an available QD Key selected from the set of QD keys;

connecting the first device of the first user with the second device of the second user via a communication path comprising the first communication channel, the QS communication channel and the second communication channel.

48. The computer-implemented method as claimed in claim 47, wherein the first device
5 has a first QD key from the set of QD keys stored thereon for QS communications with the QS network, and the second device has a second QD key stored thereon for QS communications with the QS network, and wherein:

the first communication channel is a first QS communication channel connecting the QS network with the first device using the first QD key;
10 the second communication channel is a second QS communication channel connecting the QS network with the second device using the second QD key.

49. The computer-implemented method as claimed in claim 34 to 38 or 46, wherein a first device has a first QD key from the set of QD keys stored thereon for QS communications with the QS network, and a second device has a second QD key stored thereon for QS
15 communications with the QS network, the method further comprising:

establishing a first QS communication channel with the first device using the first QD key;

receiving, from the first device, the request for QS communications with the second device;

20 establishing a second QS communication channel with the second device using the second QD key;

receiving, from the second device, a response to establish QS communications with the first device;

allocating a QD key from the set of QD keys for QS communications between the
25 first and second device; and

sending via the established first and second QS channels the third QD key to the first and second device, respectively, for use in QS communications therebetween.

50. The computer-implemented method as claimed in claims 46 or 49, the method further comprising registering a device for use with the QS network, wherein registering the
30 device further comprising:

connecting with the device over a direct wired connection with a QS server of the QS network;

selecting an available QD key from the set of QD keys for use by the device;

uploading the selected QD key to secure storage of the device via the direct wired
35 connection; and

storing and registering an association between the device and the available QD key in the repository of the QS network.

51. The computer-implemented method as claimed in claim 50, the method further comprising registering a user with the QS network, wherein registering the user further comprising:
- 5 associating the user with a device registered for use with the QS network; and storing and registering the association between the user and the registered device in the repository of the QS network.
52. The computer-implemented method as claimed in claim 51, the method further comprising:
- 10 registering the first user with the QS network and associating the first user with the first device; and registering the second user with the QS network and associating the second user with the second device.
53. The computer-implemented method as claimed in any of claims 46 to 52, the method further comprising:
- 15 assigning a further QD key from the set of QD keys for use in QS communications between the first device and the second device, wherein the further QD key is to be stored as a QD key data item in the QS repository;
- 20 generating a QREF locator associated with the QD key data item and an available QD key for encrypting the QD key data item;
- generating a QREF access token associated with the QD key data item based on the QREF locator;
- linking the QREF locator with the available QD key;
- 25 associating the QREF locator with the registrations of the first user and the second user to form a communication pair;
- storing the QD key data item encrypted with the available QD key in the QS repository with the QREF locator; and
- 30 sending the QREF access token to the first device and the second device for use in QS communications therebetween.
54. The computer-implemented method as claims in any of claims 46 to 53, the method further comprising:
- selecting an available QD key for forming a communication pair between the first and second device; and

storing the available QD key as a QD key data item for use when the first and second device request QS communication therebetween.

55. The computer-implemented method as claimed in claim 54, the method further comprising:

- 5 in response to storing a QK key data item associated with a communication pair between a first device and a second device;
- generating a quantum reference "QREF" locator based on a user secret of the first and second users and an available QD key selected from the set of QD keys for encrypting the QD key data item, wherein the QREF locator indicates the location of the QD Key data item encrypted with the selected QD key in the repository;
- 10 generating an QREF access token based on the QREF locator, wherein the QREF access token enables access operations to be performed on the QD key data item stored in the repository;
- providing the QREF locator to the repository for storing the encrypted QD key data item in the repository; and
- 15 sending the QREF access token to the first device of the first user and the second device of the second user; and
- in response to receiving a request for accessing the QD Key data item from the repository by the first or the second user;
- 20 receiving an QREF access token from the first user or the second user;
- identifying a QREF locator based on the QREF access token and the identity of the first user or the second user; and
- providing access to the encrypted QD key data item in the repository to the first user or the second user in response to identifying the QREF locator.

25 56. The computer-implemented method as claimed in claims 46 to 55, the method further comprising:

- establishing a first QS communication channel with the first device using the first QD key;
- receiving, from the first device, a QREF access token corresponding to a QD key data item associated with a communication pair between the first user and the second user;
- 30 identifying the QREF locator associated with the QREF access token based on the communication pair between the first and second users;
- providing access to a decrypted QD key data item in the repository via the first QS communication channel with the first device of the first user in response to identifying the
- 35 QREF locator;
- establishing a second QS communication channel with the second device of the second user using the second QD key;

receiving, from the second device, a QREF access token corresponding to a QD key data item associated with a communication pair between the first user and the second user;
 identifying the QREF locator associated with the QREF access token based on the communication pair between the first and second users; and
 5 providing access to a decrypted QD key data item in the repository via the second QS communication channel with the second device of the second user in response to identifying the QREF locator.

57. A computer-implemented method of quantum safe "QS" storage and retrieval in a QS network, the QS network comprising one or more QS server(s) and a repository for storing
 10 and retrieving one or more data item(s) by a plurality of users, wherein each QS server comprises a hardware security module "HSM" with an identical set of quantum distributed "QD" keys stored thereon and the QS servers communicate securely with each other and the repository using quantum encryption based on one or more available QD keys from the set of QD keys, the method performed by an end-point device of a user comprising:
 15 sending a data item for storage in a repository of the QS network, wherein a QS server is configured, in response to receiving the data item, to:
 generate a quantum reference "QREF" locator based on a user secret of the user and an available QD key selected from the set of QD keys, wherein the QREF locator indicates the location for storing the data item encrypted with the selected QD
 20 key in the repository and an identity of the user;
 generate a QREF access token based on the QREF locator, wherein the QREF access token enables access operations to be performed on the data item when stored in the repository;
 store the data item in the repository indexed by the QREF locator; and
 25 send the QREF access token to the end-point device of the user; and
 receiving a QREF access token corresponding to the data item stored in the repository;
 storing the QREF access token for use in accessing the data item stored in the QS system.

30 58. A computer-implemented method of quantum safe "QS" storage and retrieval in a QS network, the QS network comprising one or more QS server(s) and a repository for storing and retrieving one or more data item(s) by a plurality of users, wherein each QS server comprises a hardware security module "HSM" with an identical set of quantum distributed "QD" keys stored thereon and the QS servers communicate securely with each other and the
 35 repository using quantum encryption based on one or more available QD keys from the set of QD keys, the method performed by an end-point device of a user comprising:

receiving a QREF access token corresponding to a data item stored in the repository of the QS system, wherein a QS server is configured, in response to receiving the data item, to:

- 5 generate a quantum reference "QREF" locator based on a user secret of a user submitting the data item and an available QD key selected from the set of QD keys, wherein the QREF locator indicates the location for storing the data item encrypted with the selected QD key in the repository and an identity of the user submitting the data item;
- 10 generate a QREF access token based on the QREF locator, wherein the QREF access token enables access operations to be performed on the data item when stored in the repository;
- sending the QREF access token corresponding to the data item stored in the repository and user credentials to the QS system, wherein a QS server is configured, in response to receiving the QREF access token, to:
- 15 identify a QREF locator based on the QREF access token and the identity of the user; and
- receiving access in relation to the data item stored in the QS system when the QS server identifies the QREF locator.

59. An apparatus comprising a processor unit, a memory unit and a communication
20 interface, the processor unit connected to the memory unit and the communication unit, wherein the apparatus is configured to implement the computer-implemented method according to any of claims 1 to 58.

60. A computer-readable medium comprising code or computer instructions stored
25 thereon, which when executed by a processor unit, causes the processor unit to perform the computer-implemented method according to any one of claims 1 to 58.

61. An end-point device comprising a processor unit, a memory unit and a
communication interface, the processor unit connected to the memory unit and the
communication unit, wherein the apparatus is configured to implement the computer-
implemented method according to any of claims 57 or 58.

30 62. A computer-readable medium comprising code or computer instructions stored thereon, which when executed by a processor unit, causes the processor unit to perform the computer-implemented method according to any one of claims 57 or 58.

63. A QS system comprising:
a QS network comprising at least two QS servers according to the apparatus of claim 59, each of the QS servers comprising a hardware security module "HSM" with an identical set of quantum distributed "QD" keys stored thereon;
5 a plurality of users with end-point devices according to claim 61; and
a repository for storing and accessing data items associated with users of the end-point devices;
wherein the QS servers communicate securely with each other and the repository using quantum encryption based on one or more available QD keys from the set of QD keys.
- 10 64. A computer-implemented method of quantum safe "QS" communication between a first device and a second device using a QS network, the QS network comprising at least two QS servers and a repository for storing and accessing data items associated with users of the first and second devices, wherein each QS server comprises a hardware security module "HSM" with an identical set of quantum distributed "QD" keys stored thereon and the QS
15 servers communicate securely with each other and the repository using quantum encryption based on one or more available QD keys from the set of QD keys, the method comprising:
establishing QS communication channel with the first device of a first user;
receiving, from the first device, a QREF access token associated with a QD key selected from the set of QD keys, the QD key for use in QS communications with a second
20 device of a second user;
retrieving the QD key selected from the set of QD keys from the repository based on the received QREF access token;
sending the retrieved QD key to the first and second devices for use in QS communications therebetween.
- 25 65. A computer-implemented method of quantum safe "QS" communication between a first device and a second device using a QS network, the QS network comprising at least two QS servers and a repository for storing and accessing data items associated with users of the first and second devices, wherein each QS server comprises a hardware security module "HSM" with an identical set of quantum distributed "QD" keys stored thereon and the QS
30 servers communicate securely with each other and the repository using quantum encryption based on one or more available QD keys from the set of QD keys, the method comprising:
establishing a first communication channel with a first device of a first user;
receiving, from the first device, a request for communicating with a second device of a second user via the QS network;
35 establishing a second communication channel with the second device of the second user;

receiving a response from the second device of the second user to connect with the first device of the first user;

establishing a QS communication channel through the QS network based on an available QD Key selected from the set of QD keys;

5 connecting the first device of the first user with the second device of the second user via a communication path comprising the first communication channel, the QS communication channel and the second communication channel.

66. The computer-implemented method as claimed in claims 64 or 65, wherein the first device has a first QD key from the set of QD keys stored thereon for QS communications with the QS network, and the second device has a second QD key stored thereon for QS communications with the QS network, and wherein:

the first communication channel is a first QS communication channel connecting the QS network with the first device using the first QD key;

15 the second communication channel is a second QS communication channel connecting the QS network with the second device using the second QD key.

67. The computer-implemented method as claimed in any of claims 64 to 66, wherein the first device has a first QD key from the set of QD keys stored thereon for QS communications with the QS network, and the second device has a second QD key stored thereon for QS communications with the QS network, the method further comprising:

20 establishing a first QS communication channel with the first device using the first QD key;

receiving, from the first device, the request for QS communications with the second device;

25 establishing a second QS communication channel with the second device using the second QD key;

receiving, from the second device, a response to establish QS communications with the first device;

allocating a QD key from the set of QD keys for QS communications between the first and second device; and

30 sending via the established first and second QS channels the third QD key to the first and second device, respectively, for use in QS communications therebetween.

68. The computer-implemented method as claimed in any of claims 64 to 67, the method further comprising registering a device for use with the QS network, wherein registering the device further comprising:

35 connecting with the device over a direct wired connection with a QS server of the QS network;

selecting an available QD key from the set of QD keys for use by the device;
uploading the selected QD key to secure storage of the device via the direct wired
connection; and
storing and registering an association between the device and the available QD key
5 in the repository of the QS network.

69. The computer-implemented method as claimed in claim 68, the method further
comprising registering a user with the QS network, wherein registering the user further
comprising:
associating the user with a device registered for use with the QS network; and
10 storing and registering the association between the user and the registered device in
the repository of the QS network.

70. The computer-implemented method as claimed in claim 69, the method further
comprising:
registering the first user with the QS network and associating the first user with the
15 first device; and
registering the second user with the QS network and associating the second user
with the second device.

71. The computer-implemented method as claimed in any of claims 64 to 69, the method
further comprising:
20 assigning a further QD key from the set of QD keys for use in QS communications
between the first device and the second device, wherein the further QD key is to be stored as
a QD key data item in the QS repository;
generating a QREF locator associated with the QD key data item and an available
QD key for encrypting the QD key data item;
25 generating a QREF access token associated with the QD key data item based on the
QREF locator;
linking the QREF locator with the available QD key;
associating the QREF locator with the registrations of the first user and the second
user to form a communication pair;
30 storing the QD key data item encrypted with the available QD key in the QS
repository with the QREF locator; and
sending the QREF access token to the first device and the second device for use in
QS communications therebetween.

72. The computer-implemented method as claims in any of claims 64 to 70, the method further comprising:

selecting an available QD key for forming a communication pair between the first and second device; and

5 storing the available QD key as a QD key data item for use when the first and second device request QS communication therebetween.

73. The computer-implemented method as claimed in claim 72, the method further comprising:

10 in response to storing a QK key data item associated with a communication pair between a first device and a second device;

generating a quantum reference "QREF" locator based on a user secret of the first and second users and an available QD key selected from the set of QD keys for encrypting the QD key data item, wherein the QREF locator indicates the location of the QD Key data item encrypted with the selected QD key in the repository;

15 generating an QREF access token based on the QREF locator, wherein the QREF access token enables access operations to be performed on the QD key data item stored in the repository;

providing the QREF locator to the repository for storing the encrypted QD key data item in the repository; and

20 sending the QREF access token to the first device of the first user and the second device of the second user; and

in response to receiving a request for accessing the QD Key data item from the repository by the first or the second user;

receiving an QREF access token from the first user or the second user;

25 identifying a QREF locator based on the QREF access token and the identity of the first user or the second user; and

providing access to the encrypted QD key data item in the repository to the first user or the second user in response to identifying the QREF locator.

74. The computer-implemented method as claimed in claim 73, the method further comprising:

30 establishing a first QS communication channel with the first device using the first QD key;

receiving, from the first device, a QREF access token corresponding to a QD key data item associated with a communication pair between the first user and the second user;

35 identifying the QREF locator associated with the QREF access token based on the communication pair between the first and second users;

providing access to a decrypted QD key data item in the repository via the first QS communication channel with the first device of the first user in response to identifying the QREF locator;

- 5 establishing a second QS communication channel with the second device of the second user using the second QD key;
- receiving, from the second device, a QREF access token corresponding to a QD key data item associated with a communication pair between the first user and the second user;
- identifying the QREF locator associated with the QREF access token based on the communication pair between the first and second users; and
- 10 providing access to a decrypted QD key data item in the repository via the second QS communication channel with the second device of the second user in response to identifying the QREF locator.

75. A computer-implemented method of quantum safe "QS" communication between a first device and a second device using a QS network, the QS network comprising at least two
- 15 QS servers and a repository for storing and accessing data items associated with users of the first and second devices, wherein each QS server comprises a hardware security module "HSM" with an identical set of quantum distributed "QD" keys stored thereon and the QS servers communicate securely with each other and the repository using quantum encryption based on one or more available QD keys from the set of QD keys, the method performed by
- 20 the first device comprising:

- establishing a first QS communication channel with a first QS server of the QS network;
- transmitting a QREF access token associated with a QD key selected from the set of QD keys for use in QS communications with a second device of a second user;
- 25 receiving the retrieved QD key from the QS server for use in QS communications with the second device therebetween;
- establishing a third QS communication channel with the second device of the second user based on the received QD key, wherein, prior to establishing the third QS communication channel, the second device receives the retrieved QD key by establishing a
- 30 second QS communication channel with a second QS server of the QS network and transmitting the QREF access token corresponding to the QD key.

76. A computer-implemented method of quantum safe "QS" communication between a first device and a second device using a QS network, the QS network comprising at least two
- 35 QS servers and a repository for storing and accessing data items associated with users of the first and second devices, wherein each QS server comprises a hardware security module "HSM" with an identical set of quantum distributed "QD" keys stored thereon and the QS servers communicate securely with each other and the repository using quantum encryption

based on one or more available QD keys from the set of QD keys, the method performed by the first device comprising:

- 5 establishing a first communication channel with a first QS server of the QS network;
 transmitting, to the first QS server, a request for communicating with a second device
 of a second user;
 establishing a second communication channel with the second device of the second
 user;
 receiving a response from the second device of the second user to connect with the
 first device of the first user;
- 10 establishing a QS communication channel through the QS network based on an
 available QD Key selected from the set of QD keys;
 communicating with the second device of the second user based on a
 communication path comprising the first communication channel, a QS communication
 channel through the QS network and a second communication channel between the second
 15 device and the QS network.

77. A computer-implemented method of quantum safe "QS" communication between a first device and a second device using a QS network, the QS network comprising at least two QS servers and a repository for storing and accessing data items associated with users of the first and second devices, wherein each QS server comprises a hardware security module "HSM" with an identical set of quantum distributed "QD" keys stored thereon and the QS servers communicate securely with each other and the repository using quantum encryption based on one or more available QD keys from the set of QD keys, the method performed by the first device comprising:
- 20 establishing a first communication channel with the first QS server of the QS
 25 network;
 receiving, from the first QS server, a connection request from the second device of
 the second user;
 in response to accepting the connection request, communicating with the second
 device of the second user based on a communication path comprising the first
 30 communication channel, a QS communication channel through the QS network and a second
 communication channel between the second device and the QS network.

78. The computer-implemented method as claimed in claims 76 or 77, wherein the first device has a first QD key from the set of QD keys stored thereon for QS communications

with the QS network, and the second device has a second QD key stored thereon for QS communications with the QS network, and wherein:

the first communication channel is a first QS communication channel connecting the QS network with the first device using the first QD key;

5 the second communication channel is a second QS communication channel connecting the QS network with the second device using the second QD key.

79. The computer-implemented method as claimed in any of claims 75 to 78, wherein the first device has a first QD key from the set of QD keys stored thereon for QS communications with the QS network, and the second device has a second QD key stored thereon for QS communications with the QS network, the method further comprising:

10 establishing a first QS communication channel with the first QS server using the first QD key;

transmitting, to the first QS server, a request for QS communications with the second device;

15 receiving via the established first QS channel the third QD key from the first QS server for use in QS communications with the second device, wherein the second device receives via an established second QS channel the third QD key from a second QS server in response to the request.

80. The computer-implemented method as claimed in any of claims 75 to 79, the method further comprising registering a device of a user for use with the QS network, wherein registering the device further comprising:

connecting the device over a direct wired connection with a QS server of the QS network;

25 downloading an available QD key from the set of QD keys to secure storage on the device for use by the device in QS communications with the QS network;

registering the association between the device and the user for storage in the repository of the QS network.

81. The computer-implemented method as claimed in claim 80, the method further comprising registering the user with the QS network, wherein registering the user further comprising providing user credentials and the device identifier of the device for registering the user and associated device for use with the QS network.

82. The computer-implemented method as claimed in any of claims 75 to 81, the method further comprising:

receiving a QREF access token corresponding to a further QD key for use in QS communications between the first device and the second device, wherein the QS server is configured to perform the steps of:

- 5 assigning a further QD key from the set of QD keys for use in QS communications between the first device and the second device, wherein the further QD key is to be stored as a QD key data item in the QS repository;
- generating a QREF locator associated with the QD key data item and an available QD key for encrypting the QD key data item;
- 10 generating a QREF access token associated with the QD key data item based on the QREF locator;
- linking the QREF locator with the available QD key;
- associating the QREF locator with the registrations of the first user and the second user to form a communication pair;
- 15 storing the QD key data item encrypted with the available QD key in the QS repository with the QREF locator; and
- sending the QREF access token to the first device and the second device for use in QS communications therebetween.

20 83. The computer-implemented method as claims in any of claims 75 to 82, wherein the QS network is configured to select an available QD key for forming a communication pair between the first and second device, and store the available QD key as a QD key data item for use when the first and second device request QS communication therebetween, the method further comprising:

- 25 sending a request for QS communications with a second device of a second user;
- receiving a QD key for use in QS communications with the second device; and
- establishing QS communications with the second device based on the received QD key.

30 84. The computer-implemented method as claimed in claim 83, the method further comprising:

- transmitting a QREF access token for accessing a QD Key data item from the repository for use in QS communications between the first device of the first user and second device of a second user;
- receiving access to the QD Key data item, wherein the QD Key data item comprises data representative of a QD Key selected from a set of QD Keys for use by the first and second devices in QS communications therebetween;
- 35

establishing QS communications with the second device using the QD Key, wherein the second device receives access to the QD Key data item by transmitting the QREF access token for accessing the QD Key data item.

85. The computer-implemented method as claimed in claim 84, the method further comprising:
- 5 establishing a first QS communication channel with the first QS server using the first QD key;
- transmitting, to the first QS server, a QREF access token corresponding to a QD key data item associated with a communication pair between the first user and the second user;
- 10 receiving access to a decrypted QD key data item in the repository via the first QS communication channel with the first QS server in response to the first QS server identifying the QREF locator associated with the QREF access token;
- establishing a QS communication channel with the second device of the second user using the decrypted QD key, wherein the second device of the second user receives
- 15 receiving access to a decrypted QD key data item in the repository via a second QS communication channel with a second QS server in response to the first QS server identifying the QREF locator associated with the QREF access token.

86. An apparatus comprising a processor unit, a memory unit and a communication interface, the processor unit connected to the memory unit and the communication unit,
- 20 wherein the apparatus is configured to implement the computer-implemented method according to any of claims 64 to 74.

87. A computer-readable medium comprising code or computer instructions stored thereon, which when executed by a processor unit, causes the processor unit to perform the computer-implemented method according to any one of claims 64 to 74.

- 25 88. An end-point device comprising a processor unit, a memory unit and a communication interface, the processor unit connected to the memory unit and the communication unit, wherein the apparatus is configured to implement the computer-implemented method according to any of claims 75 to 85.

89. A computer-readable medium comprising code or computer instructions stored
- 30 thereon, which when executed by a processor unit, causes the processor unit to perform the computer-implemented method according to any one of claims 75 to 85.

90. A QS system comprising:
a QS network comprising at least two QS servers according to the apparatus of claim 86, each of the QS servers comprising a hardware security module "HSM" with an identical set of quantum distributed "QD" keys stored thereon;
5 a plurality of end-point devices according to claim 88;
a repository for storing and accessing data items associated with users of the end-point devices;
wherein the QS servers communicate securely with each other and the repository using quantum encryption based on one or more available QD keys from the set of QD keys.
- 10 91. A computer-implemented method of quantum safe "QS" communication between a first device and a second device using a QS network, the QS network comprising at least two QS servers and a repository for storing and accessing data items associated with users of the first and second devices, wherein each QS server comprises a hardware security module "HSM" with an identical set of quantum distributed "QD" keys stored thereon and the QS
15 servers communicate securely with each other and the repository using quantum encryption based on one or more available QD keys from the set of QD keys, wherein the first device has a first QD key from the set of QD keys stored thereon and the second device has a second QD key from the set of QD keys stored thereon, the method comprising:
establishing a first QS communication channel with the first device using the first QD
20 key;
receiving, from the first device, a request for QS communications with the second device;
establishing a second QS communication channel with the second device using the second QD key;
25 receiving, from the second device, a response to establish QS communications with the first device;
allocating a third QD key from the set of QD keys for QS communications between the first and second device; and
sending via the established first and second QS channels the third QD key to the first
30 and second device, respectively, for use in QS communications therebetween.
92. The computer-implemented method as claimed in claim 91, the method further comprising registering a device for use with the QS network, wherein registering the device further comprising:
connecting with the device over a direct wired connection with a QS server of the QS
35 network;
selecting an available QD key from the set of QD keys for use by the device;

uploading the selected QD key to secure storage of the device via the direct wired connection; and

storing and registering an association between the device and the selected available QD key in the repository of the QS network.

- 5 93. The computer-implemented method as claimed in claims 91 or 92, the method further comprising registering a user with the QS network, wherein registering the user further comprising:

associating the user with a device registered for use with the QS network; and

- 10 storing and registering the association between the user and the registered device in the repository of the QS network.

94. The computer-implemented method as claimed in any one of claims 91 to 93, the method further comprising:

registering the first user with the QS network and associating the first user with the first device; and

- 15 registering the second user with the QS network and associating the second user with the second device.

95. A computer-implemented method of quantum-safe "QS" transaction or message signing using a QS network, the QS network comprising at least two QS servers and a repository for storing and accessing data items associated with users of one or more end-point devices, wherein each QS server comprises a hardware security module "HSM" with an identical set of quantum distributed "QD" keys stored thereon and the QS servers communicate securely with each other and the repository using quantum encryption based on one or more available QD keys from the set of QD keys, the method comprising:

- 20 receiving, from a device of a user, a transaction or message requiring a digital signature associated with the user to be applied thereto;

receiving, from a device of a user, a QREF access token associated with a data item stored in the repository, the data item is associated with a signing key for use in digitally signing the received transaction or message;

- 25 identifying a QREF locator based on the QREF access token and input data from the user; and

in response to identifying the QREF locator, performing the steps of:

retrieving the data item from the repository, wherein the data item is decrypted using the QD key corresponding to the QREF locator; and

- 30 digitally signing the received transaction or message using a digital signature algorithm based on the retrieved data item; and

35 sending the digitally signed transaction or digitally signed message.

96. The computer-implemented method of claim 95, the method further comprising:
generating a quantum reference "QREF" locator based on input data associated with
a data item for storage and an available QD key selected from the set of QD keys, wherein
the data item is associated with a signing key from a set of signing keys and the generated
5 QREF locator is unique; and
sending the QREF locator along with the data item encrypted with the available QD
key to the repository.
97. The computer-implemented method of any of claims 95 or 96, the method further
comprising:
10 generating a QREF access token for accessing the data item based on the QREF
locator using an irreversible function, process or operation, wherein the QREF access token
is unique; and
sending the QREF access token to a device of a user.
98. The computer-implemented method of claims 95 to 98, the method further
15 comprising:
receiving a set of signing keys associated with a user of an end-point device;
generating, for each key in the set of signing keys, a QREF locator based on user
data of the user and an available QD key from the set of QD keys, wherein a set of QREF
locators is generated corresponding to the set of signing keys;
20 linking each QREF locator in the set of QREF locators to the corresponding available
QD key of the set of QD keys;
generating, for each QREF locator in the set of QREF locators, a QREF access
token based on said each QREF locator, wherein a set of QREF access tokens are
generated corresponding to the set of signing keys;
25 sending, for each QREF locator in the set of QREF locators, said each QREF locator
and an encrypted data item, the encrypted data item comprising a data item representative of
a key from the set of signing keys corresponding to said each QREF locator and encrypted
with a QD key corresponding to said each QREF locator, to the repository for storage,
wherein the encrypted data item is linked to the QREF locator when stored;
30 sending the set of QREF access tokens to a device of the user associated with the
set of signing keys.
99. The computer-implemented method as claimed in claim 98, wherein receiving a set
of signing keys associated with a user of an end-point device further comprises generating a
35 set of signing keys associated with a user based on one or more available QD keys from the
set of QD keys.

100. The computer-implemented method as claimed in any of claims 95 to 99, the method further comprising sending the digitally signed transaction or digitally signed message to the device of the user.
- 5 101. The computer-implemented method as claimed in any of claims 95 to 100, the method further comprising sending the digitally signed transaction or digitally signed message to another device of another user that is a counter-party to the transaction or is addressed for receiving the digitally signed message, wherein the request for signing the transaction .
- 10 102. The computer-implemented method as claimed in any of claims 95 to 101, the method further comprising sending the digitally signed transaction or digitally signed message to a system configured for processing and/or storing the digitally signed transaction or digitally signed message on behalf of the device of the user.
- 15 103. The computer-implemented method of any of claims 95 to 102, the method further comprising sending the digitally signed transaction or digitally signed message to a DLT system configured for processing and/or storing the digitally signed transaction or digitally signed message on behalf of the device of the user.
- 20 104. The computer-implemented method as claimed in any of claims 102 or 103, wherein the system comprises a system or service based on at least one from the group of:
distributed ledger technology;
shared ledger technology; and
blockchain technology.
- 25 105. The computer-implemented method as claimed in claim 104, wherein the system comprises a system or service using a consensus method or process for verifying whether one or more digitally signed transactions are stored in the distributed ledger, shared ledger and/or blockchain associated with said system or service.
- 30 106. The computer-implemented method as claimed in any of claims 95 to 105, the method performed by a QS server of the QS network further comprising performing the QS storage and/or access of data items based on the computer-implemented method according to any of claims 1 to 58, wherein the data items corresponding to one or more signing keys.
107. The computer-implemented method as claimed in any of claims 95 to 106, further comprising registering permissions for one or more users to access data items based on one or more QREF access token(s) corresponding to one or more data item(s) representing one or more signing key(s) stored in the repository.

108. The computer-implemented method as claimed in claim 107, further comprising sending the one or more QREF access token(s) to the devices associated with the one or more users.
109. The computer-implemented method as claimed in any of claims 107 or 108, further comprising:
- 5 transmitting the set of signing keys over the QS network to one or more load-balanced geographically located HSMS, wherein the set of signing keys are stored in the repository accessible by the HSMS via the QS network;
- 10 sending the corresponding QREF access tokens associated with the set of signing keys to one or more devices of users with permissions to use the QREF access tokens.
110. The computer-implemented method as claimed in any of claims 95 to 106, wherein the set of signing keys are a set of master keys or secrets associated with two or more systems requiring interoperability, further comprising registering permissions for one or more devices or apparatus of the two or more systems to access data items based on one or more
- 15 QREF access token(s) corresponding to one or more data item(s) representing said one or more master key(s) or secrets stored in the repository.
111. The computer-implemented method as claimed in claim 107, further comprising sending the one or more QREF access token(s) to the devices.
112. The computer-implemented method as claimed in any of claims 95 to 111, wherein
- 20 the set of signing keys are a set of master keys, the method further comprising registering permissions for one or more users to access data items based on one or more QREF access token(s) corresponding to one or more data item(s) representing one or more signing key(s) stored in the repository.
113. The computer-implemented method as claimed in claim 112, further comprising
- 25 sending the one or more QREF access token(s) to the devices associated with the one or more users.

114. The computer-implemented method as claimed in any of claims 112 or 113, further comprising:

- transmitting the set of master keys over the QS network to one or more load-balanced geographically located HSMS, wherein the set of master keys are stored in the repository accessible by the HSMS via the QS network;
- 5 sending the corresponding QREF access tokens associated with the set of master keys to one or more devices of users with permissions to use the QREF access tokens.

115. A computer-implemented method of quantum-safe "QS" transaction or message signing using a QS network, the QS network comprising at least two QS servers and a repository for storing and accessing data items associated with users of one or more end-point devices, wherein each QS server comprises a hardware security module "HSM" with an identical set of quantum distributed "QD" keys stored thereon and the QS servers communicate securely with each other and the repository using quantum encryption based on one or more available QD keys from the set of QD keys, the method performed by a device of a user comprising:

- receiving a transaction or message requiring a digital signature associated with the user to be applied thereto;
- 15 sending data representative of the received transaction or message and a QREF access token associated with a data item stored in the repository, the data item comprising a signing key for use in digitally signing the transaction or message;
- receiving a digitally signed transaction or digitally signed message comprising the transaction or message digitally signed using a digital signature algorithm based on the data item;
- 20 sending the digitally signed transaction for further processing or storage; and
- 25 indicating to the user of the device that the QREF access token has been used.

116. The computer-implemented method of claim 115, wherein the digitally signed transaction or digitally signed message corresponds to the transaction or message having been processed by a QS server of the QS network configured to:

- identify a QREF locator based on the QREF access token and input data from the user; and
- 30 in response to identifying the QREF locator, the QS server is configured to:
 - retrieve the data item from the repository, wherein the data item is decrypted using the QD key corresponding to the QREF locator; and
 - digitally sign the received transaction or message using a digital signature algorithm based on the retrieved data item; and
 - 35 send the digitally signed transaction or digitally signed message.

117. The computer-implemented method as claimed in claims 115 or 116, the method further comprising:

transmitting a set of signing keys associated with the user of the end-point device;

and

5 receiving a set of QREF access tokens associated with the set of signing keys.

118. The computer-implemented method as claimed in any of claims 115 to 117, the method further comprising:

10 transmitting a request for a set of signing keys associated with the user of the end-point device; and

receiving a set of QREF access tokens associated with a generated set of signing keys, wherein the generated set of signing keys are stored in encrypted form in the repository and each key in the set of signing keys is linked to a QREF locator corresponding to a QREF access token of the set of QREF access tokens, wherein a QREF access token is generated
15 by an irreversible operation or function based on the QREF locator.

119. The computer-implemented method as claimed in claim 118, wherein the generated set of signing keys are generated by an HSM based on one or more available QD keys from the set of QD keys.

120. The computer-implemented method as claimed in claim 118, wherein a QS server is
20 configured to generate the set of QREF access tokens, the QS server configured to:

generate, for each key in the set of signing keys, a QREF locator based on user data of the user and an available QD key from the set of QD keys, wherein a set of QREF locators is generated corresponding to the set of signing keys;

link each QREF locator in the set of QREF locators to the corresponding available
25 QD key of the set of QD keys;

generate, for each QREF locator in the set of QREF locators, a QREF access token based on said each QREF locator, wherein a set of QREF access tokens are generated corresponding to the set of signing keys;

send, for each QREF locator in the set of QREF locators, said each QREF locator
30 and an encrypted data item, the encrypted data item comprising a data item representative of a key from the set of signing keys corresponding to said each QREF locator and encrypted with a QD key corresponding to said each QREF locator, to the repository for storage, wherein the encrypted data item is linked to the QREF locator when stored; and

send the set of QREF access tokens associated with the set of signing keys to a
35 device associated with the user.

121. The computer-implemented method as claimed in any of claims 115 to 120, the method further comprising receiving the digitally signed transaction or digitally signed message at the device of the user.
- 5 122. The computer-implemented method as claimed in any of claims 115 to 121, the method further comprising sending the digitally signed transaction or digitally signed message to another device of another user that is a counter-party to the transaction or is addressed for receiving the digitally signed message, wherein the request for signing the transaction .
- 10 123. The computer-implemented method as claimed in any of claims 115 to 122, the method further comprising sending the digitally signed transaction or digitally signed message to a system configured for processing and/or storing the digitally signed transaction or digitally signed message on behalf of the device of the user.
- 15 124. The computer-implemented method of any of claims 115 to 123, the method further comprising sending the digitally signed transaction or digitally signed message to a DLT system configured for processing and/or storing the digitally signed transaction or digitally signed message on behalf of the device of the user.
- 20 125. The computer-implemented method as claimed in any of claims 123 or 124, wherein the system comprises a system or service based on at least one from the group of:
distributed ledger technology;
shared ledger technology; and
blockchain technology.
- 25 126. The computer-implemented method as claimed in any of claims 115 to 125, the method comprising performing the quantum-safe communications with a QS server or another device or system based on the computer-implemented method according to any of claims 75 to 85.
127. The computer-implemented method as claimed in any of claims 115 to 126, the method performed by a client DLT application executing on the device of the user, the client application configured for signing DLT transactions and sending signed DLT to a DLT system.
- 30 128. An apparatus comprising a processor unit, a memory unit and a communication interface, the processor unit connected to the memory unit and the communication unit, wherein the apparatus is configured to implement the computer-implemented method according to any of claims 95 to 114.

129. A computer-readable medium comprising code or computer instructions stored thereon, which when executed by a processor unit, causes the processor unit to perform the computer-implemented method according to any one of claims 95 to 114.
- 5 130. An end-point device comprising a processor unit, a memory unit and a communication interface, the processor unit connected to the memory unit and the communication unit, wherein the apparatus is configured to implement the computer-implemented method according to any of claims 115 to 127.
131. The end-point device of claim 130 further comprising a secure enclave for implementing the computer-implemented method according to any of claims 115 to 127
- 10 132. A computer-readable medium comprising code or computer instructions stored thereon, which when executed by a processor unit, causes the processor unit to perform the computer-implemented method according to any one of claims 115 to 127.
133. A QS system comprising:
a QS network comprising at least two QS servers according to the apparatus of claim
15 128, each of the QS servers comprising a hardware security module "HSM" with an identical set of quantum distributed "QD" keys stored thereon;
a plurality of end-point devices according to claim 130 or 131;
a repository for storing and accessing data items associated with users of the end-point devices;
20 wherein the QS servers communicate securely with each other and the repository using quantum encryption based on one or more available QD keys from the set of QD keys.
134. A computer-implemented method of quantum-safe "QS" cryptographic processing of a data item, transaction or message using a QS network, the QS network comprising at least two QS servers and a repository for storing and accessing data items associated with users
25 of one or more end-point devices, wherein each QS server comprises a hardware security module "HSM" with an identical set of quantum distributed "QD" keys stored thereon and the QS servers communicate securely with each other and the repository using quantum encryption based on one or more available QD keys from the set of QD keys, the method comprising:
30 receiving a data item, transaction or message requiring a cryptographic processing associated with a user or system;
receiving a QREF access token associated with a data item stored in the repository, the data item is associated with a cryptographic key for use in cryptographically processing the received data item, transaction or message;

- identifying a QREF locator based on the QREF access token and input data from the user or system; and
- in response to identifying the QREF locator, performing the steps of:
- retrieving the data item from the repository, wherein the data item is
- 5 decrypted using the QD key corresponding to the QREF locator; and
- processing the received data item, transaction or message using one or more cryptographic operations based on the retrieved data item; and
- sending the cryptographically processed data item, cryptographically processed transaction or cryptographically processed message.
- 10 135. The computer-implemented method of claim 134, the method further comprising:
- generating a quantum reference "QREF" locator based on input data associated with a data item for storage and an available QD key selected from the set of QD keys, wherein the data item is associated with a cryptographic key from a set of cryptographic keys and the generated QREF locator is unique; and
- 15 sending the QREF locator along with the data item encrypted with the available QD key to the repository.
136. The computer-implemented method of any of claims 134 or 135, the method further comprising:
- generating a QREF access token for accessing the data item based on the QREF
- 20 locator using an irreversible function, process or operation, wherein the QREF access token is unique; and
- sending the QREF access token to a device of a user.
137. The computer-implemented method of claims 134 to 136, the method further comprising:
- 25 receiving a set of cryptographic keys associated with the system or the user of an end-point device;
- generating, for each key in the set of signing keys, a QREF locator based on system data of the system or user data of the user and an available QD key from the set of QD keys, wherein a set of QREF locators is generated corresponding to the set of cryptographic keys;
- 30 linking each QREF locator in the set of QREF locators to the corresponding available QD key of the set of QD keys;
- generating, for each QREF locator in the set of QREF locators, a QREF access token based on said each QREF locator, wherein a set of QREF access tokens are generated corresponding to the set of cryptographic keys;
- 35 sending, for each QREF locator in the set of QREF locators, said each QREF locator and an encrypted data item, the encrypted data item comprising a data item representative of

a key from the set of cryptographic keys corresponding to said each QREF locator and encrypted with a QD key corresponding to said each QREF locator, to the repository for storage, wherein the encrypted data item is linked to the QREF locator when stored;

- 5 sending the set of QREF access tokens to the system or a device of the user associated with the set of cryptographic keys.

138. The computer-implemented method as claimed in claim 137, wherein receiving a set of cryptographic keys associated with a system or a user of an end-point device further comprises generating a set of cryptographic keys associated with the system or the user
10 based on one or more available QD keys from the set of QD keys.

139. The computer-implemented method as claimed in any of claims 134 to 138, the method further comprising sending the cryptographically processed transaction or cryptographically processed signed message to the system or a device of the user.

140. The computer-implemented method as claimed in any of claims 134 to 139, the
15 method further comprising sending the cryptographically processed data item, cryptographically processed transaction or cryptographically processed message to another system or another device of another user that is a counter-party to the transaction or is addressed for receiving the cryptographically processed message.

141. The computer-implemented method as claimed in any of claims 134 to 140, the
20 method further comprising sending the cryptographically processed data item, cryptographically processed transaction or cryptographically processed message to the system or another system configured for using, processing and/or storing the cryptographically processed data item, cryptographically processed transaction or cryptographically processed message.

142. The computer-implemented method of any of claims 134 to 141, the method further comprising sending the cryptographically processed data item, cryptographically processed transaction or cryptographically processed message to a DLT system configured for using, processing and/or storing the cryptographically processed data item, cryptographically processed transaction or cryptographically processed message on behalf of the device of the
25 user.
30

143. The computer-implemented method as claimed in any of claims 141 or 142, wherein the system comprises a system or service based on at least one from the group of:

- 5 distributed ledger technology;
shared ledger technology; and
blockchain technology.

144. The computer-implemented method as claimed in claim 142 or 143, wherein the system or said another system is configured to use a consensus method or process for verifying whether one or more cryptographically processed data item(s), cryptographically processed transaction(s) or cryptographically processed message(s) are stored in a distributed ledger, shared ledger and/or blockchain associated with said system or said another system.

10

145. The computer-implemented method as claimed in any of claims 134 to 144, the method performed by a QS server of the QS network further comprising performing the QS storage and/or access of data items based on the computer-implemented method according to any of claims 1 to 58, wherein the data items corresponding to one or more cryptographic keys.

15

146. The computer-implemented method as claimed in any of claims 134 to 145, wherein the cryptographic operations comprise one or more cryptographic operations based on the group of: encryption, digital signing, decryption, authentication, hashing, authenticated encryption.

20

147. The computer-implemented method as claimed in any of claims 134 to 147, wherein the cryptographic keys comprise one or more cryptographic keys for use with said one or more cryptographic operations.

148. The computer-implemented method as claimed in any of claims 134 to 147, wherein the set of cryptographic keys are a set of cryptographic signing keys associated with the system or the user for use with said one or more cryptographic operations, said one or more cryptographic operations corresponding to one or more digital signature cryptographic operation(s) or algorithm(s) associated with digitally signing one or more data item(s), transaction(s), or message(s) using a signing key associated with a QREF access token, and the set of cryptographic key(s) are a set of signing key(s).

25
30

149. The computer-implemented method as claimed in claim 148, further comprising registering permissions for one or more systems or one or more users to access data items

based on one or more QREF access token(s) corresponding to one or more data item(s) representing one or more signing key(s) of the set of signing key(s) stored in the repository.

5 150. The computer-implemented method as claimed in claim 149, further comprising sending the one or more QREF access token(s) to the one or more systems, or one or more devices associated with the one or more users.

151. The computer-implemented method as claimed in any of claims 107 or 108, further comprising:

10 transmitting the set of signing keys over the QS network to one or more load-balanced geographically located HSMs, wherein the set of signing keys are stored in the repository accessible by the HSMs via the QS network;
sending the corresponding QREF access tokens associated with the set of signing keys to one or more systems, or one or more devices of users located in relation to the geographically located HSMs, with permissions to use the QREF access tokens.

15 152. The computer-implemented method as claimed in any of claims 95 to 106, wherein the set of cryptographic keys are a set of master keys or secrets associated with two or more systems requiring interoperability, further comprising registering permissions for the two or more systems to access data items based on one or more QREF access token(s) corresponding to one or more data item(s) representing said one or more master key(s) or secrets stored in the repository for use in cryptographic operations on one or more received
20 data items, received transactions or messages that enable interoperability between the two or more systems.

153. The computer-implemented method as claimed in claim 107, further comprising sending the one or more QREF access token(s) to the two or more system and/or devices of users associated with the two or more systems.

25 154. The computer-implemented method as claimed in any of claims 95 to 111, wherein the set of cryptographic keys are a set of master keys, the method further comprising registering permissions for one or more users to access data items based on one or more QREF access token(s) corresponding to one or more data item(s) representing one or more master key(s) stored in the repository for use in cryptographic operations on one or more
30 received data items, received transactions or messages using one or more master keys corresponding to the one or more QREF access token(s).

155. The computer-implemented method as claimed in claim 154, further comprising sending the one or more QREF access token(s) to the devices or systems associated with the one or more users.

156. The computer-implemented method as claimed in claims 154 or 155, wherein the set of master keys are a set of master hierarchical deterministic "HD" keys further comprising sending the one or more QREF access token(s) to the devices or systems associated with the one or more users.

5 157. The computer-implemented method as claimed in any of claims 134 to 156, wherein the set of cryptographic keys comprise a set of cryptographic encryption keys associated with the system or the user for use with said one or more cryptographic operations, said one or more cryptographic operations corresponding to one or more encryption cryptographic operation(s) or algorithm(s) associated with encrypting one or more data item(s),
10 transaction(s), or message(s) using the cryptographic encryption key corresponding to a QREF access token.

158. The computer-implemented method as claimed in any of claims 134 to 157, wherein the set of cryptographic keys comprise a set of cryptographic decryption keys associated with the system or the user for use with said one or more cryptographic operations, said one or
15 more cryptographic operations corresponding to one or more decryption cryptographic operation(s) or algorithm(s) associated with decrypting one or more encrypted data item(s), encrypted transaction(s), or encrypted message(s) using the cryptographic decryption key corresponding to a QREF access token.

159. The computer-implemented method as claimed in any of claims 134 to 158, wherein
20 the one or more data items comprise data representative of a set of data required to be backed-up and/or archived, and the set of cryptographic keys comprise a set of cryptographic encryption keys associated with the system or the user for use with said one or more cryptographic operations for encrypting the one or more data items.

160. A computer-implemented method of quantum-safe "QS" cryptographic processing of
25 a data item, transaction or message using a QS network, the QS network comprising at least two QS servers and a repository for storing and accessing data items associated with users of one or more end-point devices, wherein each QS server comprises a hardware security module "HSM" with an identical set of quantum distributed "QD" keys stored thereon and the QS servers communicate securely with each other and the repository using quantum
30 encryption based on one or more available QD keys from the set of QD keys, the method comprising:

receiving a data item, transaction or message requiring cryptographic processing associated with a user or system;

35 sending data representative of the received data item, transaction or message and a QREF access token associated with another data item stored in the repository, the other data

item comprising a cryptographic key for use in cryptographically processing the received data item, transaction or message; and

- 5 receiving a cryptographically processed data item, transaction or message comprising the received data item, transaction or message cryptographically processed using one or more cryptographic operations based on the other data item.

161. The computer-implemented method of claim 160, further comprising sending the cryptographically processed data item, transaction or message to a system or user with a device for further processing or storage.

- 10 162. The computer-implemented method of claims 160 or 161, wherein the cryptographically processed data item, transaction or message corresponds to the transaction or message having been cryptographically processed by a QS server of the QS network, the QS server configured to:

identify a QREF locator based on the QREF access token and input data from the user; and

- 15 in response to identifying the QREF locator, the QS server is configured to:
retrieve the other data item from the repository, wherein the retrieved data item is decrypted using the QD key corresponding to the QREF locator; and
process the received data item, transaction or message using one or more cryptographic operations based on the retrieved data item; and
20 send the cryptographically processed data item, cryptographically processed transaction or cryptographically processed message.

163. The computer-implemented method as claimed in claims 160 to 162, the method further comprising:

- 25 transmitting a set of cryptographic keys associated with the system or user of the end-point device; and
receiving a set of QREF access tokens associated with the set of cryptographic keys.

164. The computer-implemented method as claimed in any of claims 160 to 163, the method further comprising:

- 30 transmitting a request for a set of cryptographic keys associated with the system or user of the end-point device; and
receiving a set of QREF access tokens associated with a generated set of cryptographic keys, wherein the generated set of cryptographic keys are stored in encrypted form in the repository and each key in the set of cryptographic keys is linked to a QREF
35 locator corresponding to a QREF access token of the set of QREF access tokens, wherein a

QREF access token is generated by an irreversible operation or function based on the QREF locator.

165. The computer-implemented method as claimed in claim 164, wherein the generated set of cryptographic keys are generated by an HSM based on one or more available QD keys from the set of QD keys.

166. The computer-implemented method as claimed in claims 164 or 165, wherein a QS server is configured to generate the set of QREF access tokens, the QS server configured to:

generate, for each key in the set of cryptographic keys, a QREF locator based on user data of the user and an available QD key from the set of QD keys, wherein a set of QREF locators is generated corresponding to the set of cryptographic keys;

link each QREF locator in the set of QREF locators to the corresponding available QD key of the set of QD keys;

generate, for each QREF locator in the set of QREF locators, a QREF access token based on said each QREF locator, wherein a set of QREF access tokens are generated corresponding to the set of cryptographic keys;

send, for each QREF locator in the set of QREF locators, said each QREF locator and an encrypted data item, the encrypted data item comprising a data item representative of a key from the set of cryptographic keys corresponding to said each QREF locator and encrypted with a QD key corresponding to said each QREF locator, to the repository for storage, wherein the encrypted data item is linked to the QREF locator when stored; and

send the set of QREF access tokens associated with the set of cryptographic keys to the system, or device associated with the user.

167. The computer-implemented method as claimed in any of claims 160 to 166, the method further comprising receiving the cryptographically processed data item, transaction or message at the device of the user.

168. The computer-implemented method as claimed in any of claims 160 to 167, the method further comprising sending the cryptographically processed data item, transaction or message to one or more from the group of:

another system for processing or storage;

a device of another user that is a counter-party to the transaction;

a device of another user or system addressed for receiving the cryptographically processed data item, transaction or message.

169. The computer-implemented method as claimed in any of claims 160 to 168, the method further comprising sending the cryptographically processed data item, transaction or

message to a system configured for processing and/or storing the cryptographically processed data item, transaction or message.

170. The computer-implemented method of any of claims 160 to 169, the method further comprising sending the cryptographically processed data item, transaction or message to a DLT system configured for processing and/or storing the cryptographically processed data item, transaction or message.

171. The computer-implemented method as claimed in any of claims 169 or 170, wherein the system or the another system comprises a system or service based on at least one from the group of:

distributed ledger technology;
shared ledger technology; and
blockchain technology.

172. The computer-implemented method as claimed in any of claims 160 to 171, the method comprising performing the quantum-safe communications with a QS server or another device or system based on the computer-implemented method according to any of claims 75 to 85.

173. The computer-implemented method as claimed in any of claims 160 to 172, the method performed by a client DLT application executing on the device of the user, the client application configured for signing DLT transactions and sending signed DLT to a DLT system.

174. The computer-implemented method as claimed in any of claims 160 to 174, wherein the set of cryptographic keys are a set of cryptographic signing keys associated with the system or the user for use with said one or more cryptographic operations, said one or more cryptographic operations corresponding to one or more digital signature cryptographic operation(s) or algorithm(s) associated with digitally signing one or more data item(s), transaction(s), or message(s) using a signing key associated with a QREF access token.

175. The computer-implemented method as claimed in claim 174, further comprising registering permissions for one or more systems or one or more users to access data items based on one or more QREF access token(s) corresponding to one or more data item(s) representing one or more signing key(s) of the set of signing key(s) stored in the repository.

176. The computer-implemented method as claimed in claim 175, further comprising sending the one or more QREF access token(s) to the one or more systems, or one or more devices associated with the one or more users.

177. The computer-implemented method as claimed in any of claims 175 or 176, wherein the QS server is configured to transmit the set of signing keys over the QS network to one or more load-balanced geographically located HSMs, wherein the set of signing keys are stored in the repository accessible by the HSMs via the QS network, the method
5 comprising receiving the corresponding QREF access tokens associated with the set of signing keys of one or more systems, or one or more devices of users located in relation to the geographically located HSMs, with permissions to use the QREF access tokens.

178. The computer-implemented method as claimed in any of claims 160 to 173, wherein the set of cryptographic keys are a set of master keys or secrets associated with two or more
10 systems requiring interoperability, further comprising registering permissions for the two or more systems to access data items based on one or more QREF access token(s) corresponding to one or more data item(s) representing said one or more master key(s) or secrets stored in the repository for use in cryptographic operations on one or more received data items, received transactions or messages that enable interoperability between the two
15 or more systems.

179. The computer-implemented method as claimed in claim 178, further comprising receiving the one or more QREF access token(s) at the two or more system and/or devices of users associated with the two or more systems.

180. The computer-implemented method as claimed in any of claims 160 to 173, wherein the set of cryptographic keys are a set of master keys, the method further comprising
20 registering permissions for a system or one or more users to access data items based on one or more QREF access token(s) corresponding to one or more data item(s) representing one or more master key(s) stored in the repository for use in cryptographic operations on one or more received data items, received transactions or messages using one or more master keys
25 corresponding to the one or more QREF access token(s).

181. The computer-implemented method as claimed in claim 154, further comprising receiving the one or more QREF access token(s) at the systems, or devices or systems associated with the one or more users.

182. The computer-implemented method as claimed in claims 180 or 181, wherein the set
30 of master keys are a set of master hierarchical deterministic "HD" keys further comprising sending the one or more QREF access token(s) to the devices or systems associated with the one or more users.

183. The computer-implemented method as claimed in any of claims 160 to 173, wherein the set of cryptographic keys comprise a set of cryptographic encryption keys associated with

the system or the user for use with said one or more cryptographic operations, said one or more cryptographic operations corresponding to one or more encryption cryptographic operation(s) or algorithm(s) associated with encrypting one or more data item(s), transaction(s), or message(s) using the cryptographic encryption key corresponding to a
5 QREF access token.

184. The computer-implemented method as claimed in any of claims 160 to 173 or 183, wherein the set of cryptographic keys comprise a set of cryptographic decryption keys associated with the system or the user for use with said one or more cryptographic operations, said one or more cryptographic operations corresponding to one or more
10 decryption cryptographic operation(s) or algorithm(s) associated with decrypting one or more encrypted data item(s), encrypted transaction(s), or encrypted message(s) using the cryptographic decryption key corresponding to a QREF access token.

185. The computer-implemented method as claimed in any of claims 183 to 184, further comprising sending one or more data items comprising data representative of a set of data
15 required to be backed-up and/or archived, wherein the set of cryptographic keys comprise a set of cryptographic encryption keys associated with the system or the user for use with said one or more cryptographic operations for encrypting said one or more data items.

186. An apparatus comprising a processor unit, a memory unit and a communication interface, the processor unit connected to the memory unit and the communication unit,
20 wherein the apparatus is configured to implement the computer-implemented method according to any of claims 134 to 159.

187. A computer-readable medium comprising code or computer instructions stored thereon, which when executed by a processor unit, causes the processor unit to perform the computer-implemented method according to any one of claims 134 to 159.

25 188. An end-point device comprising a processor unit, a memory unit and a communication interface, the processor unit connected to the memory unit and the communication unit, wherein the apparatus is configured to implement the computer-implemented method according to any of claims 160 to 185.

189. The end-point device of claim 188 further comprising a secure enclave for
30 implementing the computer-implemented method according to any of claims 160 to 185

190. A computer-readable medium comprising code or computer instructions stored thereon, which when executed by a processor unit, causes the processor unit to perform the computer-implemented method according to any one of claims 160 to 185.

191. A QS system comprising:
- a QS network comprising at least two QS servers according to the apparatus of claim 186, each of the QS servers comprising a hardware security module "HSM" with an identical set of quantum distributed "QD" keys stored thereon;
 - 5 a plurality of end-point devices according to claims 188 or 189;
 - a repository for storing and accessing data items associated with users of the end-point devices;
 - wherein the QS servers communicate securely with each other and the repository using quantum encryption based on one or more available QD keys from the set of QD keys.