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:

selecting an available QD key from the set of QD keys for encrypting a data item;

generating a quantum reference "QREF" locator based on input data associated with the data item for storage and the available QD key selected from the set of QD keys, wherein the generated QREF locator is unique and wherein the QREF locator is a logical address or a physical address for storing and accessing the data item in the repository;

linking the QREF locator to the available QD key of the set of QD keys; and

sending the QREF locator along with the data item encrypted with the available QD key to the repository for storage, wherein the encrypted data item is linked to the QREF locator when stored.

2. The computer-implemented method of claim 1, the method further comprising receiving a set of QD keys using quantum safe key distribution from a quantum key distributor or source; and/or

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

an access control list of users for accessing said data item.

3. The computer-implemented method of as claimed in any of claim 1 or 2, the method further comprising:

generating a QREF access token associated with the data item based on the QREF locator; and

sending the QREF access token to a device of a user associated with the data item.

4. The computer-implemented method of any of claims 1 to 3, the method further comprising:

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 for enabling the user to access said data item.

5. The computer-implemented method of any of claims 1 to 4, the method further 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

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.

6. The computer-implemented method as claimed in any of claims to 1 to 5, further comprising receiving a request for storing the data item by a first user; and/or

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.

7. The computer-implemented method as claimed in claim 1, 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;

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; and/or

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;

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.

8. The computer-implemented method as claimed in claim 1, wherein 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; and/or

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,

preferably 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:

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;

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.

9. The computer-implemented method as claimed in claim 8, 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:

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;

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.

10. The computer-implemented method as claimed in claim 1, the method further comprising:

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;

preferably 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;

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 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:

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 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,

more preferably 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:

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:

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;

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,

even more preferably 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;

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:

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;

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.

11. The computer-implemented method as claimed in claim 1, 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 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; 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; and/or

wherein:

the repository further comprises a shared 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 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) 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,

preferably 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 user; and

accessing the encrypted data item in the distributed or shared ledger using the identified QREF locator based on the access token.

12. The computer-implemented method as claimed in claim 1, wherein:

the repository further comprises a digital storage platform using publish/subscribe, 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 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

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,

preferably 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,

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.

13. The computer-implemented method as claimed in claim 1, wherein each 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

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,

preferably wherein the QS network 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 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

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.

14. The computer-implemented method as claimed in claim 1, 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 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 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,

preferably 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

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 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.

15. The computer-implemented method as claimed in claim 1, 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

the encrypted data item, wherein the data item is encrypted with a QD key associated with the QREF locator,

preferably each record further comprising data representative of:

one or more user identities allowed to access the encrypted data item of said each 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; and/or

preferably each record further comprising data representative of an access control list indicating one or more user identities allowed to access the encrypted data item and corresponding permissions and/or operations in relation to each user identity accessing said encrypted data item.

16. The computer-implemented method as claimed in claim 1, wherein the QREF locator further comprises data representative of:

the user secret;

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,

preferably wherein the QREF locator further comprises data representative of:

a user identifier; and

an access control list to the data item.

17. The computer-implemented method as claimed in any of claim 15 or 16, the method comprising:

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;

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

sending the unique QREF access token to the user for use in accessing, in some manner, the data item,

preferably 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 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 user has permissions to access the data item; or

the method comprising:

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 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;

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;

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,

preferably 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 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

enabling the user access to the data item in response to determining the user has permissions to access the data item; or

the method comprising:

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 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;

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

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,

preferably 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, and/or

preferably wherein the certificate data item is based on data representative of X509 standard and beyond certificates.

18. The computer-implemented method as claimed in any of claims 15 or 16, 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; and/or

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,

preferably 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;

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

19. The computer-implemented method as claimed in claim 15, 16 or 18 , 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 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;

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

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.

20. The computer-implemented method as claimed in claims 18 or 19, 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 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 further between the device and the available QD key in the repository of the QS network,

preferably 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

storing and registering the association between the user and the registered device in the repository of the QS network,

more preferably the method further comprising:

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.

21. The computer-implemented method as claimed in any of claims 18 to 20, the method further comprising:

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;

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;

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; and/or

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,

preferably the method further comprising:

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;

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

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;

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.

22. The computer-implemented method as claimed in claims 18 to 21, 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;

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;

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

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.

23. 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 1 to 22.

24. 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 1 to 22.

25. A QS system comprising:

a QS network comprising at least two QS servers according to the apparatus of claim 23, 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 users with end-point devices; 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.