

CLAIMS

Therefore, the following is claimed:

1. A system, comprising:
 - a computing device comprising a processor and a memory; and
 - machine-readable instructions stored in the memory that, when executed by the processor, cause the computing device to at least:
 - generate an identity key for a data item, the identity key representing a unique address that specifies a location where an identity document can be found;
 - send a request for authentication of the data item to a security service, the request comprising the identity key and the data item;
 - receive a verified claim for the data item from the security service, the verified claim representing one or more verified assertions about the data item described by the identity document;
 - generate the identity document, the identity document comprising the identity key for the data item and the verified claim; and
 - send the identity document in a distributed ledger.
2. The system of claim 1, wherein the machine-readable instructions, when executed by the computing device, further cause the computing device to at least:
 - receive a request for the data item; and

send a response to the request, the response comprising the data item and the identity key.

3. The system of claim 1 or 2, wherein:

the identity key is a second identity key;

the identity document is a second identity document;

the request for authentication of the data item is a second request for authentication; and

the machine-readable instructions further cause the computing device to at least:

send the request for authentication of the identity of an operator of the machine-readable instructions to the authentication service;

receive a first identity key and a verified claim from the authentication service;

create a first identity document, the identity document comprising the identity key and the verified claim; and

store the first identity document in a distributed ledger; and

the second request for authentication of the data item is sent subsequent to the first identity document being stored in the distributed ledger.

4. The system of claims 1-3, wherein the machine-readable instructions, when executed by the processor, further cause the computing device to at least:

generate an asymmetric key-pair uniquely associated with the data item; and

wherein the identity document further comprises a public key of the asymmetric key-pair.

5. The system of claim 4, wherein the machine-readable instructions, when executed by the processor, further cause the computing device to at least:

receive a validation request that comprises an encrypted token encrypted with the public key;

decrypt the encrypted token using a private key of the asymmetric key-pair to generate an unencrypted token;

create a cryptographic signature of the unencrypted token using the private key; and

provide a validation response that comprises the unencrypted token and the cryptographic signature.

6. A computer-readable medium comprising machine-readable instructions that, when executed by a processor of a computing device, cause the computing device to at least:

generate an identity key for a data item, the identity key representing a unique address that specifies a location where an identity document can be found;

send a request for authentication of the data item to a security service, the request comprising the identity key and the data item;

receive a verified claim for the data item from the security service, the verified claim representing one or more verified assertions about the data item described by the identity document;

generate an identity document, the identity document comprising the identity key for the data item and the verified claim; and

store the identity document in a distributed ledger.

7. The computer-readable medium of claim 6, wherein the machine-readable instructions, when executed by the computing device, further cause the computing device to at least:

receive a request for the data item; and

send a response to the request, the response comprising the data item and the identity key.

8. The computer-readable medium of claim 6 or 7, wherein:

the identity key is a second identity key;

the identity document is a second identity document;

the request for authentication of the data item is a second request for authentication; and

the machine-readable instructions further cause the computing device to at least:

send the request for authentication of the identity of an operator of the machine-readable instructions to the authentication service;

receive a first identity key and a verified claim from the authentication service;

create a first identity document, the identity document comprising the identity key and the verified claim; and

store the first identity document in a distributed ledger; and

the second request for authentication of the data item is sent subsequent to the first identity document being stored in the distributed ledger.

9. The computer-readable medium of claims 6-8, wherein the machine-readable instructions, when executed by the processor, further cause the computing device to at least:

generate an asymmetric key-pair uniquely associated with the data item; and

wherein the identity document further comprises a public key of the asymmetric key-pair.

10. The computer-readable medium of claim 9, wherein the machine-readable instructions, when executed by the processor, further cause the computing device to at least:

receive a validation request that comprises an encrypted token encrypted with the public key;

decrypt the encrypted token using a private key of the asymmetric key-pair to generate an unencrypted token;

create a cryptographic signature of the unencrypted token using the private key; and

provide a validation response that comprises the unencrypted token and the cryptographic signature.

11. A method, comprising

generating an identity key for a data item, the identity key representing a unique address that specifies a location where an identity document can be found;

sending a request for authentication of the data item to a security service, the request comprising the identity key and the data item;

receiving a verified claim for the data item from the security service, the verified claim representing one or more verified assertions about the data item described by the identity document;

generating the identity document, the identity document comprising the identity key for the data item and the verified claim; and

storing the identity document in a distributed ledger.

12. The method of claim 11, further comprising

receiving a request for the data item; and

sending a response to the request, the response comprising the data item and the identity key.

13. The method of claim 11 or 12, wherein:
- the identity key is a second identity key;
 - the identity document is a second identity document;
 - the request for authentication of the data item is a second request for authentication; and
- the method further comprises:
- sending the request for authentication of the identity of an operator of the machine-readable instructions to the authentication service;
 - receiving a first identity key and a verified claim from the authentication service;
 - creating a first identity document, the identity document comprising the identity key and the verified claim; and
 - storing the first identity document in a distributed ledger; and
- the second request for authentication of the data item is sent subsequent to the first identity document being stored in the distributed ledger.
14. The method of claims 11-13 further comprising:
- generating an asymmetric key-pair uniquely associated with the data item; and
 - wherein the identity document further comprises a public key of the asymmetric key-pair.

15. The method of claim 14, further comprising
 - receiving a validation request that comprises an encrypted token encrypted with the public key;
 - decrypting the encrypted token using a private key of the asymmetric key-pair to generate an unencrypted token;
 - creating a cryptographic signature of the unencrypted token using the private key; and
 - providing a validation response that comprises the unencrypted token and the cryptographic signature.