

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;
 - 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;
 - generate an identity document, the identity document comprising the identity key for the data item and the verified claim; and
 - send ~~store~~ the identity document for storage 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 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
 - ~~send~~store the first identity document for storage 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. The system of claims 1-5, wherein the data item is a network address.

7. The system of claims 1-5, wherein the data item is a file.

8. A method, comprising:

receiving a verification request for a data item, the verification request comprising an identity key and the data item;

determining that the data item complies with at least one verification rule;

generating a verified claim for the data item, the verified claim indicating that the identity key is associated with the data item and that the data item complies with the at least one verification rule; and

providing the verified claim as a response to the request for authentication of the data item.

9. The method of claim 8, wherein:

the identity key is a second identity key;

the at least one verification rule indicates that the data item originates from an authenticated entity;

the authentication request further comprises a first identity key associated with the authenticated entity;

determining that the data item complies with the at least one verification rule further comprises verifying, based at least in part on the first identity key, that the authentication request originates from the authenticated entity; and

generating the verified claim occurs in response to verifying that the authentication request originates from the authenticated entity.

10. The method of claim 9, wherein verifying, based at least in part on the first identity key, that the authentication request originates from the authenticated entity further comprises:

retrieving an identity document associated with the first identity key, the identity document containing a public encryption key of a respective asymmetric key-pair;

encrypting a token with the public encryption key to create an encrypted token;

sending the encrypted token to an originating entity that sent the authentication request;

receiving the token and a digital signature created with a private key of the respective asymmetric key-pair; and

validating the digital signature with the public encryption key.

11. The method of claims 8-10, wherein:

the at least one verification rule indicates that the data item complies with a specified security policy; and

determining that the data item complies with the at least one verification rule further comprises performing a security analysis of the data item.

12. The method of claims 8-11, further comprising:
 - creating an identity document that comprises the identity key and the verified claim; and
 - registering the identity document with a distributed ledger.
13. The method of claims 8-12, wherein the data item is a network address.
14. The method of claims 8-12, wherein the data item is a file.
15. A non-transitory computer-readable medium comprising machine-readable instructions that, when executed by a processor of a computing device, cause the computing device to at least:
 - send a request to an application for a data item;
 - receive the data item and an identity key from the application, the identity key being linked with the data item;
 - retrieve an identity document identified by the identity key from a distributed ledger, the identity document containing at least one verified claim related to the data item;
 - verify the data item based at least in part on the identity document; and
 - render a user interface based at least in part on a result of a verification of the data item.

16. The non-transitory, computer-readable medium of claim 15, wherein the machine-readable instructions, when executed by the processor, further cause the computing device to at least:

- encrypt a token using a public key included in the identity document to create an encrypted token;

- send the encrypted token to the application;

- receive the token from the application and a cryptographic signature associated with the token; and

- verify the cryptographic signature.

17. The non-transitory, computer-readable medium of claim 15 or 16, wherein the machine-readable instructions that cause the computing device to verify the data item based at least in part on the identity document further cause the computing device to at least evaluate at least one claim in the verified claim, the at least one claim comprising an assertion regarding compliance of the data item with at least one verification rule.

18. The non-transitory, computer-readable medium of claim 17, wherein the machine-readable instructions that cause the computing device to at least evaluate the at least one claim further cause the computing device to determine that the claim is made by a trusted entity.

19. The non-transitory, computer-readable medium of claims 15-18, wherein the data item is a network address.

20. The non-transitory, computer-readable medium of claims 15-18, wherein the data item is a file.