

CLAIMS

1. A computer-based method for providing attestations for an identity consumer from an identity provider to a relying party, comprising:
 - providing, by the identity consumer to an identity provider server for the identity provider, identity consumer information;
 - validating, by the identity provider server, the identity consumer information;
 - receiving, by the identity server, the identity consumer information;
 - receiving, by the identity provider server, a root attestation from a system operator that authorizes the identity provider server to issue identity provider attestations;
 - generating, by the identity provider server, an identity provider attestation comprising an attestation about the identity consumer information;
 - generating, by the identity provider server, a nested attestation comprising the identity provider attestation and the root attestation, wherein the nested attestation establishes a chain of trust by building the identity provider attestation on the root attestation in a single attestation;
 - receiving, by an identity consumer computer program executed by an electronic device for the identity consumer and from the identity provider server, a notification that the nested attestation is available;
 - requesting, by the identity consumer computer program, the nested attestation from the identity provider server;
 - downloading, by the identity consumer computer program, the nested attestation to an identity consumer electronic wallet for the identity consumer;

committing, by the identity provider server, the nested attestation to a distributed ledger, wherein the distributed ledger maintains a current status for the root attestation and the identity provider attestation;

receiving, by the identity consumer computer program and from a relying party computer application for the relying party, a request for the nested attestation;

generating, by the identity consumer computer program, a machine-readable code for the nested attestation that is stored in the identity consumer electronic wallet;

communicating, by the identity consumer computer program and to the relying party computer application, the machine-readable code for the nested attestation;

extracting, by the relying party computer application, the nested attestation from the machine-readable code;

identifying, by the relying party computer application, the root attestation and the identity provider attestation from the nested attestation;

verifying, by the relying party computer application and on the distributed ledger, that the root attestation and the identity provider attestation are valid and active; and

executing, by the relying party computer application, an action based on reliance on the verification.

2. The computer-based method of claim 1, wherein the identity provider attestation comprises a license, a certificate, a credential, or an authorization.

3. The computer-based method of claim 1, wherein the identity provider comprises one of a financial institution, a government agency, an employer, and a legal entity.

4. The computer-based method of claim 1, wherein the identity provider attestation comprises an identification of an attestor, an identification of an attestee, a type of attestation, and a date of issuance.

5. The computer-based method of claim 1, wherein the identity consumer electronic wallet comprises a wallet application, a mobile wallet, or a web-based wallet.

6. The computer-based method of claim 1, wherein the current status of the root attestation indicates whether the identity provider attestation comprises valid, expired, or revoked.

7. The computer-based method of claim 1, wherein the relying party computer application periodically verifies the current status of the root attestation or the identity provider attestation using the distributed ledger.

8. The computer-based method of claim 1, wherein the relying party receives a notification that the root attestation or the identity provider attestation is revoked or expired from the distributed ledger.

9. A computer-based method for sending an object using attestations, comprising:

providing, by an identity consumer computer program executed by an identity consumer electronic device to an identity provider server for an identity provider, identity consumer information for an identity consumer;

receiving, by the identity provider server, a root attestation from a system operator that authorizes the identity provider server to issue identity provider attestations;

generating, by the identity provider server, an identity provider attestation comprising an attestation about the identity consumer information;

generating, by the identity provider server, a nested attestation comprising the identity provider attestation and the root attestation, wherein the nested attestation establishes a chain of trust by building the identity provider attestation on the root attestation in a single attestation;

receiving, by the identity consumer computer program, an identity of an object to sign;

requesting, by the identity consumer computer program the nested attestation from the identity provider server;

receiving, by the identity consumer computer program the nested attestation;

storing, by the identity consumer computer program, the nested attestation in an identity consumer electronic wallet for the identity consumer;

retrieving, by the identity consumer computer program, the object;

signing, by the identity consumer computer program, the object with the nested attestation that is stored in the identity consumer electronic wallet by embedding the attestation in the object;

sending, by the identity consumer computer program, the signed object to a receiving party computer program executed by an electronic device for a receiving party;

extracting, by the receiving party computer program, the nested attestation from the object; and

verifying, by the receiving party computer program and on a distributed ledger that maintains a current status for the root attestation and the identity provider attestation, that the root attestation and the identity provider attestation are valid and active.

10. The computer-based method of claim 9, wherein the object comprises a document, and the identity provider attestation attests that the identity consumer is authorized to sign the document.

11. The computer-based method of claim 9, wherein the object is a payment, and the identity provider attestation attests that the identity consumer is authorized to make the payment.

12. The computer-based method of claim 9, wherein the object comprises digital currency.

13. The computer-based method of claim 9, wherein the identity provider attestation comprises a license, a certificate, a credential, or an authorization, and further comprises an identification of an attestor, an identification of an attestee, a type of identity provider attestation, and a date of issuance.

14. The computer-based method of claim 9, further comprising:

generating, by the identity provider server, a receiving party attestation comprising an attestation about the receiving party;

generating, by the identity provider server, a receiving party nested attestation comprising the receiving party attestation and the root attestation, wherein the nested attestation establishes a chain of trust by building the receiving party attestation on the root attestation in a single attestation;

receiving, by the identity consumer computer program and from the receiving party computer program, a request for the object and the receiving party nested attestation; and

verifying, by the identity consumer computer program and on the distributed ledger, that the root attestation and the receiving party attestation are valid and active before sending the object to the receiving party.

15. The computer-based method of claim 14, wherein the receiving party attestation attests to an account for the receiving party.