

WHAT IS CLAIMED IS:

1. A method comprising:

receiving, by a first node in a proxy network of nodes from a user device of a user, an initial authorization request message for an interaction to obtain a resource from a resource provider, the initial authorization request message comprising an interaction identifier, user data, and an authorization capsule, the authorization capsule being associated with an authorizing entity and comprising risk policies, encrypted credentials of the user, a plurality of re-encryption keys respectively associated with the nodes in the proxy network, and a plurality of node identifiers respectively associated with the re-encryption keys;

performing, by the first node, authentication using the user data and the risk policies in the authorization capsule;

determining, by the first node, a re-encryption key of the plurality of re-encryption keys using the interaction identifier and the node identifiers in the authorization capsule, the re-encryption key associated with a second node of the proxy network of nodes;

re-encrypting, by the first node and utilizing the re-encryption key associated with the second node, the encrypted credentials to form re-encrypted credentials; and

transmitting, by the first node to the second node in the proxy network, a routing message comprising the re-encrypted credentials and the interaction identifier, wherein the second node thereafter decrypts the re-encrypted credentials using a secret key of the second node to obtain plaintext credentials, and then generates and transmits a pre-authorization request message to the authorizing entity for approval, wherein the pre-authorization request message requests pre-authorization prior to a subsequent authorization request message to be transmitted by an agent device of an agent of the resource provider upon delivery of the resource,

wherein the proxy network comprises a plurality of communicably connected nodes, the plurality comprising the first node and the second node, wherein each node of the plurality is configured to maintain a blockchain.

2. The method of claim 1, wherein the authorization capsule and the user data are encrypted using a cryptographic key that is shared by each node of the nodes, the authentication comprising:

decrypting, by the first node and utilizing the cryptographic key, the authorization capsule;

decrypting, by the first node and utilizing the cryptographic key, the user data;

verifying, by the first node and based on the decrypting the authorization capsule and the decrypting the user data, that the user data satisfies requirements of the risk policies;

generating, by the first node and based on the verifying, a proof of authentication; and

logging, by the first node, the proof of authentication to the blockchain, wherein the logging comprises transmitting to each node of the nodes the proof of authentication, wherein each node also logs the proof of authentication.

3. The method of claim 1, wherein the interaction identifier is a dynamic data element that is generated by a reception node of the nodes and received by the user device, the dynamic data element corresponding to the interaction and the second node, wherein the resource provider has a pre-existing association with the second node, wherein the reception node transmits the interaction identifier to each node of the plurality to be stored, and wherein the first node transmits the routing message to the second node based on the interaction identifier.

4. The method of claim 1, wherein each node of the nodes comprises a trusted execution environment (TEE), the authentication being performed within the trusted execution environment of the first node.

5. A method comprising:

receiving, by a first node in a proxy network of nodes from a user device of a user, an initial authorization request message for an interaction to obtain a resource from a resource provider, the initial authorization request message comprising an interaction identifier, user data, and an authorization capsule, the

authorization capsule being associated with an authorizing entity and comprising risk policies, encrypted credentials of the user, a plurality of re-encryption keys respectively associated with the nodes in the proxy network, and a plurality of node identifiers respectively associated with the re-encryption keys;

performing, by the first node, authentication using the user data and the risk policies in the authorization capsule;

determining, by the first node, a re-encryption key of the plurality of re-encryption keys using the interaction identifier and the node identifiers in the authorization capsule, the re-encryption key associated with a second node of the proxy network of nodes;

re-encrypting, by the first node and utilizing the re-encryption key associated with the second node, the encrypted credentials to form re-encrypted credentials; and

transmitting, by the first node to the second node in the proxy network, a routing message comprising the re-encrypted credentials and the interaction identifier, wherein the second node thereafter decrypts the re-encrypted credentials using a secret key of the second node to obtain plaintext credentials, and then generates and transmits a pre-authorization request message to the authorizing entity for approval, wherein the pre-authorization request message requests pre-authorization prior to a subsequent authorization request message to be transmitted by an agent device of an agent of the resource provider upon delivery of the resource,

wherein the encrypted credentials are the plaintext credentials that are encrypted using a public key of the authorizing entity, and each re-encryption key of the plurality of re-encryption keys is derived from a secret key of the authorizing entity and a cryptographic key of a respectively associated node of the proxy network, wherein the re-encrypting is performed without first decrypting the encrypted credentials into the plaintext credentials.

6. The method of claim 1, wherein the subsequent authorization request message comprises a pre-authorization approval indicator (PAAI), the pre-authorization approval indicator having been transmitted by the second node to the user device in response to receiving a pre-authorization response from the

authorizing entity, wherein the pre-authorization approval indicator is subsequently stored on the user device.

7. The method of claim 6, wherein a third node of the nodes, upon receiving the subsequent authorization request message from the agent device, authenticates the subsequent authorization request message based in part on the pre-authorization approval indicator.

8. A first node in a proxy network of nodes, the first node comprising:

a processor; and

a computer readable medium, coupled to the processor, the computer readable medium comprising code, executable by the processor, for implementing a method comprising:

receiving, from a user device of a user, an initial authorization request message for an interaction to obtain a resource from a resource provider, the initial authorization request message comprising an interaction identifier, user data, and an authorization capsule, the authorization capsule being associated with an authorizing entity and comprising risk policies, encrypted credentials of the user, a plurality of re-encryption keys respectively associated with the nodes in the proxy network, and a plurality of node identifiers respectively associated with the re-encryption keys;

performing authentication using the user data and the risk policies in the authorization capsule;

determining a re-encryption key of the plurality of re-encryption keys using the interaction identifier and the node identifiers in the authorization capsule, the re-encryption key associated with a second node of the proxy network of nodes;

re-encrypting, utilizing the re-encryption key associated with the second node, the encrypted credentials to form re-encrypted credentials; and

transmitting, to the second node in the proxy network, a routing message comprising the re-encrypted credentials and the interaction identifier, wherein the second node thereafter decrypts the re-encrypted credentials using a secret key of the second node to obtain plaintext credentials, and then generates and transmits a pre-authorization request message to the authorizing entity for approval, wherein the pre-authorization request message requests pre-authorization

prior to a subsequent authorization request message to be transmitted by an agent device of an agent of the resource provider upon delivery of the resource,

wherein the proxy network comprises a plurality of communicably connected nodes, the nodes comprising the first node and the second node, wherein each node of the plurality is configured to maintain a blockchain.

9. The first node of claim 8, wherein the authorization capsule and the user data are encrypted using a cryptographic key that is shared by each node of the nodes, the authentication comprising:

decrypting, utilizing the cryptographic key, the authorization capsule;

decrypting, utilizing the cryptographic key, the user data;

verifying, based on the decrypting the authorization capsule and the decrypting the user data, that the user data satisfies requirements of the risk policies;

generating, based on the verifying, a proof of authentication; and

logging the proof of authentication to the blockchain, wherein the logging comprises transmitting to each node of the nodes the proof of authentication, wherein each node also logs the proof of authentication.

10. The first node of claim 8, wherein the interaction identifier is a dynamic data element that is generated by a reception node of the nodes and received by the user device, the dynamic data element corresponding to the interaction and the second node, wherein the resource provider has a pre-existing association with the second node, and wherein the first node transmits the routing message to the second node based on the interaction identifier.

11. The first node of claim 8, wherein each node of the nodes comprises a trusted execution environment (TEE), the authentication being performed within the trusted execution environment of the first node.

12. A first node in a proxy network of nodes, the first node comprising:

a processor; and

a computer readable medium, coupled to the processor, the computer readable medium comprising code, executable by the processor, for implementing a method comprising:

receiving, from a user device of a user, an initial authorization request message for an interaction to obtain a resource from a resource provider, the initial authorization request message comprising an interaction identifier, user data, and an authorization capsule, the authorization capsule being associated with an authorizing entity and comprising risk policies, encrypted credentials of the user, a plurality of re-encryption keys respectively associated with the nodes in the proxy network, and a plurality of node identifiers respectively associated with the re-encryption keys;

performing authentication using the user data and the risk policies in the authorization capsule;

determining a re-encryption key of the plurality of re-encryption keys using the interaction identifier and the node identifiers in the authorization capsule, the re-encryption key associated with a second node of the proxy network of nodes;

re-encrypting, utilizing the re-encryption key associated with the second node, the encrypted credentials to form re-encrypted credentials; and

transmitting, to the second node in the proxy network, a routing message comprising the re-encrypted credentials and the interaction identifier, wherein the second node thereafter decrypts the re-encrypted credentials using a secret key of the second node to obtain plaintext credentials, and then generates and transmits a pre-authorization request message to the authorizing entity for approval, wherein the pre-authorization request message requests pre-authorization prior to a subsequent authorization request message to be transmitted by an agent device of an agent of the resource provider upon delivery of the resource,

wherein the encrypted credentials are the plaintext credentials that are encrypted using a public key of the authorizing entity, and each re-encryption key of the plurality of re-encryption keys is derived from a secret key of the authorizing entity and a cryptographic key of a respectively associated node of the proxy network, wherein the re-encrypting is performed without first decrypting the encrypted credentials into the plaintext credentials.

13. The first node of claim 8, wherein the subsequent authorization request message comprises a pre-authorization approval indicator (PAAI), the pre-

authorization approval indicator having been previously transmitted by the second node to the user device in response to receiving a pre-authorization response from the authorizing entity, wherein the pre-authorization approval indicator is subsequently stored on the user device.

14. The first node of claim 13, wherein a third node of the nodes, upon receiving the subsequent authorization request message from the agent device, authenticates the subsequent authorization request message based in part on the pre-authorization approval indicator.

15. A method comprising:

- generating, by a second node in a proxy network, a pair of cryptographic keys, the pair comprising a public key and a secret key;
- publishing, by the second node, a cryptographic key of the pair to the proxy network, wherein an authorizing entity fetches the cryptographic key from the proxy network and utilizes a secret key of the authorizing entity and the cryptographic key to generate a re-encryption key;
- receiving, by the second node in the proxy network from a first node in the proxy network, a routing message, the routing message comprising a re-encrypted credentials and an interaction identifier, wherein the re-encrypted credentials are plaintext credentials that are encrypted utilizing the re-encryption key, and the interaction identifier corresponds to an interaction to obtain a resource from a resource provider, the interaction identifier comprising a user device identifier corresponding to a user device;
- decrypting, by the second node, the re-encrypted credentials using the secret key of the second node to obtain the plaintext credentials;
- generating, by the second node and based on the interaction identifier, a pre-authorization request message, the pre-authorization request message comprising the plaintext credentials and interaction data corresponding to the interaction; and
- transmitting, by the second node, the pre-authorization request message to the authorizing entity for approval, wherein the pre-authorization request message requests pre-authorization prior to a subsequent authorization request

message to be transmitted by an agent device of an agent of the resource provider upon delivery of the resource,

wherein the proxy network comprises a plurality of communicably connected nodes, the plurality comprising the first node and the second node, wherein each node of the plurality is configured to maintain a blockchain.

16. The method of claim 15 further comprising:

receiving, by the second node from the authorizing entity, a pre-authorization response comprising a pre-authorization approval indicator (PAAI) from the authorizing entity; and

logging, by the second node, the pre-authorization approval indicator to the blockchain, wherein the logging comprises transmitting to each node of the nodes the pre-authorization approval indicator, wherein each node also logs the pre-authorization approval indicator; and

transmitting, by the second node, the pre-authorization approval indicator to the user device, based on the user device identifier.

17. The method of claim 15 further comprising:

receiving, by the second node from a third node of the nodes, a second routing message, the second routing message being generated based on the subsequent authorization request message that was transmitted by the agent device and received by the third node of the plurality, the second routing message comprising the re-encrypted credentials and a second interaction identifier, the second interaction identifier corresponding to the interaction;

decrypting, by the second node, the re-encrypted credentials using the secret key of the second node to obtain the plaintext credentials;

generating, by the second node and based on the second interaction identifier, an authorization request message comprising the plaintext credentials and the interaction data corresponding to the second interaction identifier; and

transmitting, by the second node to the authorizing entity, the authorization request message to the authorizing entity for authorization;

receiving, by the second node from the authorizing entity, an authorization response;

logging, by the second node, the authorization response to the blockchain, wherein the logging comprises transmitting to each node of the nodes the authorization response, wherein each node also logs the authorization response; and

transmitting, by the second node, the authorization response to the agent device.