

CLAIMS

1. A method comprising:
 - prior to an interaction between a resource provider computer and a user device:
 - receiving, by a gateway computer, a credential from the resource provider computer,
 - transmitting, by the gateway computer, the credential to a token server computer,
 - receiving, by the gateway computer, a data item from the token server computer, the data item having been generated by the token server and comprising a first ciphertext and a second ciphertext,
 - generating, by the gateway computer, a token based on the data item,
 - storing, by the gateway computer, the data item in a database in association with the token, and
 - transmitting, by the gateway computer, the token to the resource provider computer, wherein the resource provider computer stores the token;
 - receiving, by the gateway computer, the token from an edge computer during an interaction between the resource provider computer and the user device, the resource provider computer having transmitted the token to the edge computer;
 - determining, by the gateway computer, the data item comprising the first ciphertext and the second ciphertext associated with the token from the database;
 - transmitting, by the gateway computer, the second ciphertext to the edge computer, wherein the edge computer produces a re-encrypted second ciphertext by re-encrypting the second ciphertext with a re-encryption key corresponding to the gateway computer, the re-encryption key being created by the token server computer based on a gateway computer public key and a token server computer private key;
 - receiving, by the gateway computer, the re-encrypted second ciphertext from the edge computer;
 - decrypting, by the gateway computer, the re-encrypted second ciphertext with a gateway computer private key to obtain a cryptographic key;
 - decrypting, by the gateway computer, the first ciphertext with the cryptographic key to obtain the credential; and

transmitting, by the gateway computer, the credential to an authorizing entity computer, wherein the authorizing entity computer determines whether or not to authorize the interaction.

2. The method of claim 1, wherein the re-encryption key corresponds to a proxy re-encryption scheme.

3. The method of claim 1, further comprising:
receiving, by the gateway computer, from the edge computer, interaction data;
and
before transmitting, by the gateway computer, the credential to the authorizing entity computer, evaluating, by the gateway computer, the interaction based on the interaction data and the credential.

4. The method of claim 1, wherein the database comprises a token vault, wherein the gateway computer stores a plurality of data items in the token vault, the plurality of data items comprising a plurality of first ciphertexts and a plurality of second ciphertexts, the plurality of data items corresponding to a plurality of tokens.

5. The method of claim 1, wherein the authorizing entity computer comprises an issuer computer associated with a user of the user device and the credential.

6. The method of claim 1, wherein the user device transmits the token to the resource provider computer before the resource provider computer transmits the token to the edge computer.

7. The method of claim 1, wherein the edge computer comprises a computer in a cloud computing network.

8. The method of claim 1, wherein the token comprises a hash measurement of the data item.

9. The method of claim 8, further comprising:

transmitting, by the gateway computer, the first ciphertext to the edge computer, wherein the edge computer produces the hash measurement of the data item using a hash function, the first ciphertext, and the second ciphertext, and wherein the edge computer verifies the data item by comparing the hash measurement to the token.

10. The method of claim 1, wherein:

the re-encryption key is one of a plurality of re-encryption keys;

the gateway computer is one of a plurality of gateway computers;

a plurality of gateway identifiers correspond to the plurality of gateway computers;

the plurality of re-encryption keys correspond to the plurality of gateway computers; and

before producing the re-encrypted second ciphertext by re-encrypting the second ciphertext with a re-encryption key, the edge computer identifies the re-encryption key based on a gateway identifier of the plurality of gateway identifiers associated with the gateway computer.

11. The method of claim 1, wherein the token server computer transmits the re-encryption key to the edge computer, or wherein the method further comprises:

transmitting, by the gateway computer, the re-encryption key to the edge computer.

12. The method of claim 1, further comprising generating, by the gateway computer, the token using a hash function and the data item, wherein the token comprises a hash measurement of the data item.

13. The method of claim 1, wherein the token server computer corresponds to an issuing entity associated with a user of the user device.

14. A gateway computer comprising:

a processor; and

a non-transitory computer readable medium coupled to the processor, the non-transitory computer readable medium comprising code, executable by the processor for implementing the method of any of claims 1 to 13.