

WHAT IS CLAIMED IS:

- 1 1. A method comprising:
2 receiving, by a gateway computer, a token from an edge computer
3 during an interaction between a resource provider computer and a user device,
4 wherein the resource provider computer transmits the token to the edge computer;
5 determining, by the gateway computer, a data item comprising a first
6 ciphertext and a second ciphertext associated with the token in a database;
7 transmitting, by the gateway computer, the second ciphertext to the
8 edge computer, wherein the edge computer produces a re-encrypted second
9 ciphertext by re-encrypting the second ciphertext;
10 receiving, by the gateway computer, the re-encrypted second
11 ciphertext from the edge computer;
12 decrypting, by the gateway computer, the re-encrypted second
13 ciphertext with a gateway computer private key to obtain a cryptographic key;
14 decrypting, by the gateway computer, the first ciphertext with the
15 cryptographic key to obtain a credential; and
16 transmitting, by the gateway computer, the credential to an authorizing
17 entity computer, wherein the authorizing entity computer determines whether or not
18 to authorize the interaction.
- 1 2. The method of claim 1, wherein the edge computer produces
2 the re-encrypted second ciphertext using a re-encryption key, and wherein the re-
3 encryption key corresponds to a proxy re-encryption scheme.
- 1 3. The method of claim 1, further comprising:
2 receiving, by the gateway computer, from the edge computer,
3 interaction data; and
4 before transmitting, by the gateway computer, the credential to the
5 authorizing entity computer, evaluating, by the gateway computer, the interaction
6 based on the interaction data and the credential.
- 1 4. The method of claim 1, wherein the database comprises a token
2 vault, wherein the gateway computer stores a plurality of data items in the token
3 vault, the plurality of data items comprising a plurality of first ciphertexts and a

4 plurality of second ciphertexts, the plurality of data items corresponding to a plurality
5 of tokens.

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

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

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

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

1 9. The method of claim 8, further comprising:
2 transmitting, by the gateway computer, the first ciphertext to the edge
3 computer, wherein the edge computer produces the hash measurement of the data
4 item using a hash function, the first ciphertext, and the second ciphertext, and
5 wherein the edge computer verifies the data item by comparing the hash
6 measurement to the token.

1 10. The method of claim 1, wherein:
2 the edge computer produces the re-encrypted second ciphertext by re-
3 encrypting the second ciphertext with a re-encryption key;
4 the re-encryption key is created by a token server computer and
5 corresponds to the gateway computer; and
6 the re-encryption key is based on a gateway computer public key and a
7 token server computer private key.

1 11. The method of claim 10, wherein:
2 the re-encryption key is one of a plurality of re-encryption keys;
3 the gateway computer is one of a plurality of gateway computers;

4 a plurality of gateway identifiers correspond to the plurality of gateway
5 computers;
6 the plurality of re-encryption keys correspond to the plurality of gateway
7 computers; and
8 before producing the re-encrypted second ciphertext by re-encrypting
9 the second ciphertext with a re-encryption key, the edge computer identifies the re-
10 encryption key based on a gateway identifier of the plurality of gateway identifiers
11 associated with the gateway computer.

1 12. The method of claim 10, wherein the token server computer
2 transmits the re-encryption key to the edge computer, or wherein the method further
3 comprises:
4 transmitting, by the gateway computer, the re-encryption key to the
5 edge computer.

1 13. The method of claim 1, further comprising:
2 prior to the interaction between the resource provider computer and the
3 user device, receiving, by the gateway computer, the credential from the resource
4 provider computer;
5 transmitting, by the gateway computer the credential to a token server
6 computer, wherein the token server computer generates the data item comprising
7 the first ciphertext and the second ciphertext, and wherein the token server computer
8 transmits the data item to the gateway computer;
9 receiving, by the gateway computer, the data item from the token
10 server computer;
11 generating, by the gateway computer, a token using a hash function
12 and the data item, wherein the token comprises a hash measurement of the data
13 item;
14 storing, by the gateway computer, the data item in the database in
15 association with the token; and
16 transmitting, by the gateway computer, the token to the resource
17 provider computer, wherein the resource provider computer stores the token.

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

1 15. A gateway computer comprising: a processor; and
2 a non-transitory computer readable medium coupled to the processor,
3 the non-transitory computer readable medium comprising code, executable by the
4 processor for implementing the method of any of claims 1-14.

1 16. A method comprising:
2 receiving, by an edge computer, from a resource provider computer, a
3 token as part of an interaction between the resource provider computer and a user
4 device;
5 identifying, by the edge computer, based on the token, a gateway
6 computer;
7 transmitting, by the edge computer, to the gateway computer, the
8 token, wherein the gateway computer identifies a data item comprising a first
9 ciphertext and a second ciphertext corresponding to the token in a database;
10 receiving, by the edge computer, from the gateway computer, the
11 second ciphertext;
12 producing, by the edge computer, a re-encrypted second ciphertext by
13 re-encrypting the second ciphertext using a re-encryption key; and
14 transmitting, by the edge computer, to the gateway computer, the re-
15 encrypted second ciphertext, wherein the gateway computer produces a
16 cryptographic key by decrypting the re-encrypted second ciphertext using a gateway
17 computer private key, produces a credential by decrypting the first ciphertext using
18 the cryptographic key, and transmits the credential to an authorizing entity computer,
19 wherein the authorizing entity computer determines whether or not to authorize the
20 interaction.

1 17. The method of claim 16, further comprising:
2 receiving, by the edge computer, from the gateway computer, the first
3 ciphertext;
4 generating, by the edge computer, a hash measurement of the first
5 ciphertext and the second ciphertext; and
6 verifying, by the edge computer, the token by comparing the token to
7 the hash measurement.

1 18. The method of claim 16, further comprising:
2 receiving, by the edge computer, from a token server computer, the re-
3 encryption key, wherein the re-encryption key is generated by the token server
4 computer, and wherein the re-encryption key is based on a token server computer
5 private key and a gateway computer public key.

1 19. The method of claim 16, wherein:
2 the re-encryption key is one of a plurality of re-encryption keys;
3 the plurality of re-encryption keys correspond to a plurality of gateway
4 computers;
5 the plurality of gateway computers correspond to a plurality of gateway
6 identifiers; and
7 the method further comprises identifying, by the edge computer, the re-
8 encryption key based on a gateway identifier of the plurality of gateway identifiers
9 associated with the gateway computer.

1 20. The method of claim 19, further comprising:
2 receiving, by the edge computer, from the gateway computer or a
3 token server computer, a server-less function, wherein the edge computer uses the
4 server-less function to identify the re-encryption key based on the gateway identifier
5 and produces the re-encrypted second ciphertext.

1 21. An edge computer comprising:
2 a processor; and a non-transitory computer readable medium
3 coupled to the processor, the non-transitory computer readable medium comprising
4 code, executable by the processor, for implementing a method comprising:
5 receiving, from a resource provider computer, a token as part of an
6 interaction between the resource provider computer and a user device;
7 identifying, based on the token, a gateway computer;
8 transmitting, to the gateway computer, the token, wherein the gateway
9 computer identifies a data item comprising a first ciphertext and a second ciphertext
10 corresponding to the token in a database;
11 receiving, from the gateway computer, the second ciphertext;

12 producing a re-encrypted second ciphertext by re-encrypting the
13 second ciphertext using a re-encryption key; and
14 transmitting, to the gateway computer, the re-encrypted second
15 ciphertext, wherein the gateway computer produces a cryptographic key by
16 decrypting the re-encrypted second ciphertext using a gateway computer private
17 key, produces a credential by decrypting the first ciphertext using the cryptographic
18 key, and transmits the credential to an authorizing entity computer, wherein the
19 authorizing entity computer determines whether or not to authorize the interaction

1

1