

WHAT IS CLAIMED IS:

1. A method comprising:

receiving, by a first token gateway, a first request message requesting a token from a token requestor computer;

determining, by the first token gateway, a plurality of token service computers from a cluster of token service computers based on a service configuration information of the token requestor computer, each token service computer in the plurality of token service computers operating independently of each other;

transmitting, by the first token gateway, a plurality of second request messages to the plurality of token service computers, each second request message of the plurality of second request messages requesting the token;

receiving, by the first token gateway, at least one first response message comprising the token from the plurality of token service computers, wherein each token service computer of the plurality of token service computers is communicatively coupled, via a second token gateway to an authorizing computer that is configured to validate the token requestor computer; and

transmitting, by the first token gateway, a second response message to the token requestor computer, the second response message comprising the token, wherein the first token gateway is different than the second token gateway.

2. The method of claim 1, wherein the at least one first response message comprises supplemental data associated with the token, the supplemental data comprising a cryptogram that limits an interaction channel for a corresponding token.

3. The method of claim 1, wherein determining the plurality of token service computers comprises accessing a routing table that maps, token requestor data elements in the first request message to the plurality of token service computers.

4. The method of claim 3, wherein the token requestor data elements include token requestor identifiers.

5. The method of claim 3, wherein the token requestor data elements include a real credential.

6. The method of claim 1, wherein the second response message comprises the token and supplemental data associated with the token.

7. The method of claim 1, wherein the first request message is a provisioning request message.

8. The method of claim 1, wherein the first request message is a cryptogram request message.

9. A first token gateway computer comprising:
a processor; and

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

receiving a first request message requesting a token from a token requestor computer;

determining a plurality of token service computers from a cluster of token service computers based on a service configuration information of the token requestor computer, each token service computer in the plurality of token service computers operating independently of each other;

transmitting a plurality of second request messages to the plurality of token service computers, each second request message of the plurality of second request messages requesting the token;

receiving at least one first response message comprising the token from the plurality of token service computers, wherein each token service computer of the plurality of token service computers is communicatively coupled, via a second token gateway computer to an authorizing computer that is configured to validate the token requestor computer; and

transmitting, a second response message to the token requestor computer, the second response message comprising the token, wherein the first token gateway computer is different than the second token gateway computer.

10. The first token gateway computer of claim 9, wherein the at least one first response message comprises supplemental data associated with the token, the supplemental data comprising a cryptogram that limits an interaction channel for a corresponding token.

11. The first token gateway computer of claim 9, wherein determining the plurality of token service computers comprises accessing a routing table that maps, token requestor data elements in the first request message to the plurality of token service computers.

12. The first token gateway computer of claim 11, wherein the token requestor data elements include token requestor identifiers.

13. The first token gateway computer of claim 11, wherein the token requestor data elements include a real credential.

14. The first token gateway computer of claim 13, wherein the real credential is one of a primary account number and identity data of a user.

15. The first token gateway computer of claim 11, wherein the first request message is a cryptogram request message.

16. A method comprising:
receiving, from a first token gateway, a first request message for a token, the first request message being sent to the first token gateway from a token requestor computer;

transmitting, via a second token gateway, to an authorizing computer, a second request message to verify a user associated with the token requestor computer;

generating, in response to receiving a successful verification message from the authorizing computer via the second token gateway, at least one token and/or supplemental data associated with the at least one token; and

transmitting the at least one token and/or supplemental data associated with the at least one token to the first token gateway, wherein the first token gateway is different than the second token gateway.

17. The method of claim 16, wherein the supplemental data comprises a cryptogram that limits an interaction channel for a corresponding token.

18. The method of claim 17, further comprising:
receiving, from the authorizing computer and via the second token gateway, a third request message for verifying an earlier generated cryptogram.