

WHAT IS CLAIMED

- 1 1. A method comprising:
2 generating, by a processor computer, a first master key for a token
3 requestor, the first master key being generated based on (a) a second master key
4 managed by the processor computer and (b) an identifier of the token requestor;
5 transmitting, by the processor computer to a token requestor computer
6 corresponding to the token requestor, the first master key;
7 receiving, by the processor computer from the token requestor
8 computer, a request for a token;
9 responsive to receiving the request for the token, transmitting, by the
10 processor computer, the token to the token requestor computer; and
11 receiving, by the processor computer from the token requestor
12 computer, an authorization request message comprising the token and a cryptogram
13 generated by the token requestor computer using the first master key and the token.
- 1 2. The method of claim 1, wherein the token requestor computer
2 generates a cryptogram generation key using the first master key, and the
3 cryptogram is generated using the cryptogram generation key and the token.
- 1 3. The method of claim 1, further comprising:
2 validating, by the processor computer, the cryptogram.
- 3 4. The method of claim 3, further comprising:
4 identifying, by the processor computer, a primary account identifier
5 corresponding to the token;
6 generating, by the processor computer, a modified authorization
7 request message comprising an indication of the validation of the cryptogram and
8 the primary account identifier; and
9 transmitting, by the processor computer to an authorization computer,
10 the modified authorization request message.

1 5. The method of claim 4, further comprising receiving, by the
2 processor computer, an authorization response message from the authorization
3 computer, the authorization response message comprising an authorization result
4 generated by the authorization computer based on the modified authorization
5 request message.

1 6. The method of claim 1, wherein the token is domain restricted.

1 7. The method of claim 1, wherein the second master key is stored
2 in a hardware secure module (HSM) in the processor computer.

1 8. The method of claim 1, wherein the first master key has a limited
2 use.

1 9. A processor computer comprising:
2 a memory;
3 a processor;
4 a non-transitory computer-readable medium comprising instructions,
5 which, when executed by the processor, perform the steps of:
6 generating a first master key for a token requestor, the first master key
7 being generated based on (a) a second master key managed by the processor
8 computer and (b) an identifier of the token requestor;
9 transmitting, to a token requestor computer corresponding to the token
10 requestor, the first master key;
11 receiving, from the token requestor computer, a request for a token;
12 responsive to receiving the request for the token, transmitting the token
13 to the token requestor computer; and
14 receiving, from the token requestor computer, an authorization request
15 message comprising the token and a cryptogram generated by the token requestor
16 computer using the first master key and the token.

1 10. The processor computer of claim 9, wherein generating the
2 cryptogram by the token requestor comprises generating a cryptogram generation
3 key using the first master key, and the cryptogram is generated using the cryptogram
4 generation key and the token.

1 11. The processor computer of claim 9, the steps further comprising:
2 validating the cryptogram.

1 12. The processor computer of claim 11, the steps further
2 comprising:
3 identifying a primary account identifier corresponding to the token;
4 generating a modified authorization request message comprising an
5 indication of the validation of the cryptogram and the primary account identifier; and
6 transmitting, to an authorization computer, the modified authorization
7 request message.

1 13. The processor computer of claim 12, the steps further
2 comprising receiving an authorization response message from the authorization
3 computer, the authorization response message comprising an authorization result
4 generated by the authorization computer based on the modified authorization
5 request message.

1 14. The processor computer of claim 9, further comprising a
2 hardware secure module (HSM) storing the second master key.

1 15. The processor computer of claim 9, wherein the token is domain
2 restricted.

1 16. The processor computer of claim 9, wherein the first master key
2 has a limited use.

1 17. A method comprising:
2 receiving, by a token requestor computer from a processor computer in
3 a processing network, a first master key and a token, wherein the first master key
4 was generated by the processor computer using a second master key;
5 generating, by the token requestor computer, a cryptogram generation
6 key using the first master key; and
7 generating, by the token requestor computer, a cryptogram using the
8 cryptogram generation key and the token.

1 18. The method of claim 17, further comprising:

2 after receiving the first master key, transmitting, by the token requestor
3 computer to the processor computer, a request for the token, wherein the token is
4 received responsive to transmitting the request for the token.

1 19. The method of claim 17, further comprising:
2 generating, by the token requestor computer, an authorization request
3 message comprising the token and the cryptogram; and
4 transmitting, by the token requestor computer to the processor
5 computer, the authorization request message, thereby causing the processor
6 computer to validate the cryptogram.

1 20. The method of claim 17, wherein the token is domain restricted.

1 21. The method of claim 17, wherein the first master key has a
2 limited use.

1 22. A token requestor computer comprising:
2 a memory;
3 a processor;
4 a non-transitory computer-readable medium comprising instructions,
5 which, when executed by the processor, perform the steps of:
6 receiving, from a processor computer, a first master key and a token,
7 wherein the first master key was generated by the processor computer using a
8 second master key;
9 generating a cryptogram generation key using the first master key; and
10 generating a cryptogram using the cryptogram generation key and the
11 token.

1 23. The token requestor computer of claim 22, the steps further
2 comprising:
3 after receiving the first master key, transmitting, by the token requestor
4 computer to the processor computer, a request for the token, wherein the token is
5 received responsive to transmitting the request for the token.

1 24. The token requestor computer of claim 22, the steps further
2 comprising:

3 generating an authorization request message comprising the token and
4 the cryptogram; and
5 transmitting, to the processor computer, the authorization request
6 message, thereby causing the processor computer to validate the cryptogram.

1 25. The token requestor computer of claim 22, wherein the token is
2 domain restricted.

1 26. The token requestor computer of claim 22, wherein the
2 cryptogram generation key has a limited use.