

WHAT IS CLAIMED IS:

1 1. A method for obtaining an access token by a client, the method comprising:
2 receiving a credential for gaining access to a computer resource;
3 hashing the credential to obtain a first hash;
4 sending request messages to a plurality of servers, each request message including a
5 blinded hash of the first hash and a user identifier;
6 receiving response messages from the plurality of servers, wherein each response
7 message is received from a corresponding server and includes:
8 a partial hash response generated using the blinded hash sent to the
9 corresponding server and a secret share stored in the corresponding server, and
10 an encrypted token share generated by encrypting a token share of the
11 corresponding server using a hash portion that was previously generated by the client
12 using the first hash and the secret share and sent to the corresponding server;
13 deblinding each of the partial hash responses of the plurality of servers, to obtain hash
14 portions corresponding to the plurality of servers, respectively;
15 decrypting the encrypted token shares using the hash portions to obtain token shares
16 of the plurality of servers, respectively; and
17 combining the obtained token shares to acquire the access token.

1 2. The method of claim 1, further comprising:
2 prior to the receiving the credential, performing a registration with the plurality of
3 servers, the performing the registration comprising:
4 sending registration requests to the plurality of servers, respectively,
5 each request including a blinded hash of a registration credential provided for
6 the registration by a user;
7 receiving registration responses from the plurality of servers,
8 respectively, wherein each of the registration responses is received from the
9 corresponding server and includes a corresponding partial hash response
10 generated by applying the secret share to the blinded hash of the registration
11 credential that is sent to the corresponding server in a corresponding
12 registration request;

13 deblinding the corresponding partial hash responses received from the
14 plurality of servers, to obtain registration hash portions for the registration
15 with the plurality of servers, respectively; and
16 sending the registration hash portions to the plurality of servers,
17 respectively, to be stored,
18 wherein the hash portion used to encrypt the token share of the corresponding server
19 is one of the registration hash portions sent to the plurality of servers.

1 3. The method of claim 2, further comprising:
2 generating a plurality of secret shares; and
3 sending the plurality of secret shares to the plurality of servers, respectively,
4 wherein the secret share is one of the plurality of secret shares.

1 4. The method of claim 3, wherein the plurality of secret shares differ from each
2 other.

1 5. The method of claim 2, wherein the performing the registration includes
2 sending one or more additional registration hash portions to one or more additional servers,
3 and wherein only a portion of all servers are required to provide the response message to
4 obtain the access token.

1 6. The method of claim 1, wherein the blinded hash is the same for each of the
2 plurality of servers.

1 7. The method of claim 1, wherein the blinded hash is different for each of the
2 plurality of servers.

1 8. The method of claim 1, wherein the token shares and the access token are
2 generated using a non-interactive threshold token generation scheme.

1 9. The method of claim 8, wherein the non-interactive threshold token generation
2 scheme comprises one from among symmetric key based message authentication code
3 (MAC), public key based MAC, secret sharing (Shamir) RSA based digital signature, and
4 pairing based digital signature.

1 10. The method of claim 8, wherein the response messages from the plurality of
2 servers are received without any further interaction after sending the request messages to the
3 plurality of servers.

1 11. The method of claim 1, wherein the request messages to the plurality of
2 servers are sent in parallel.

1 12. A method performed by a plurality of server computers, the method
2 comprising:

3 receiving, by two or more server computers of the plurality of server computers,
4 request messages from a client, respectively, each of the request messages including a
5 blinded hash of a first hash of a credential and a user identifier;

6 performing, by a corresponding server computer among the two or more server
7 computers, operations comprising:

8 generating a partial hash response using the blinded hash sent to the
9 corresponding server computer and a secret share stored in the corresponding
10 server computer;

11 identifying a hash portion corresponding to the user identifier, wherein
12 the hash portion was previously received by the corresponding server
13 computer from the client and was generated by the client using the first hash
14 and the secret share;

15 generating, by the corresponding server computer, a token share of the
16 corresponding server computer based on the user identifier and the secret
17 share;

18 encrypting the token share using the hash portion identified as
19 corresponding to the user identifier; and

20 sending a response message to the client, the response message
21 including the partial hash response and the encrypted token share,

22 wherein the client is adapted to deblind the blinded partial hash responses received
23 from the two or more server computers to obtain respective hash portions corresponding to
24 the two or more server computers, decrypt the encrypted token shares received from the two
25 or more server computers using the respective hash portions to obtain respective token shares
26 of the two or more server computers, and combine the respective token shares to obtain an
27 access token.

1 13. The method of claim 12, further comprising:
2 prior to the receiving the request messages, performing a registration with the client,
3 wherein the performing the registration comprises:
4 receiving, by each of the two or more server computers, respective registration
5 requests from the client, each of the respective registration requests including the user
6 identifier and a blinded hash of a registration credential provided for the registration by a
7 user;
8 sending, by each of the two or more server computers, respective registration
9 responses to the client, each of the respective registration responses including a first
10 respective partial hash response generated by applying the secret share of the corresponding
11 server computer to the blinded hash of the registration credential that is received in the
12 respective registration request;
13 receiving, by the two or more server computers, respective registration hash portions
14 from the client, wherein the respective registration hash portions are generated by the client
15 by deblinding the first respective partial hash responses received from the two or more server
16 computers; and
17 storing the respective registration hash portions, by the two or more server computers,
18 in association with the user identifier,
19 wherein the hash portion used to encrypt the token share of the corresponding server
20 computer is one of the respective registration hash portions.

1 14. The method of claim 12, wherein the secret share is received from the client.

1 15. The method of claim 12, wherein the token share is generated using a non-
2 interactive threshold token generation scheme.

1 16. The method of claim 15, wherein the non-interactive threshold token generation
2 scheme comprises one from among symmetric key based message authentication code
3 (MAC), public key based MAC, secret sharing (Shamir) RSA based digital signature, and
4 pairing based digital signature.

1 17. The method of claim 15, wherein the response message is sent to the client by the
2 corresponding server computer without any further interaction from the client after receiving
3 a corresponding request message among the request messages from the client.

1 18. A computer product comprising a computer readable medium storing a
2 plurality of instructions for controlling a computer system to perform the method of any one
3 of claims 1-17.

1 19. A system comprising:
2 one or more processors; and
3 a non-transitory computer readable memory storing instructions that, when executed
4 by the one or more processors, cause the one or more processors to perform the method of
5 any of claims 1-17.