

Claims

1. A method for securing data communication between a first computer and a second computer, the method performed by the first and second computers and
5 comprising:
- cooperatively executing, by the first and second computers, a first data communication instruction for communicating first data from the first computer to the second computer;
 - generating a first session key by the first computer;
 - 10 encrypting, by the first computer, the first data using the first session key;
 - encrypting, by the first computer, the first session key using a first public key, the first public key paired with a first private key, the first public-private key pair generated for the second computer;
 - 15 sending the encrypted first data and the encrypted first session key from the first computer to the second computer;
 - decrypting, by the second computer, the encrypted first session key using the first private key;
 - decrypting, by the second computer, the encrypted first data using the
20 decrypted first session key; and
 - processing, by the second computer, the decrypted first data based on the first data communication instruction.
2. The method according to claim 1, further comprising cooperatively performing,
25 by the first and second computers, a token generation process before executing the first data communication instruction, the token generation process comprising:
- generating a token session key by the first computer;
 - encrypting, by the first computer, a token request using the token session key;
 - 30 sending the token session key and the encrypted token request from the first computer to the second computer;
 - decrypting, by the second computer, the encrypted token request using the token session key;

- generating the first public-private key pair for and by the second computer;
- encrypting, by the second computer, the first public key using the token session key;
- 5 sending the encrypted first public key from the second computer to the first computer;
- decrypted, by the first computer, the encrypted first public key using the token session key.
- 10 3. The method according to claim 1, further comprising cooperatively performing, by the first and second computers, a token generation process before executing the first data communication instruction, the token generation process comprising:
- generating a token session key by the first computer;
- generating the first public-private key pair by the first computer for the
- 15 second computer;
- encrypting, by the first computer, the first private key using the token session key;
- sending the token session key and the encrypted first private key from the first computer to the second computer;
- 20 decrypting, by the second computer, the encrypted first private key using the token session key.
4. The method according to any one of claims 1 to 3, wherein the first public-private key pair has an expiry condition, such that the first public-private key pair is
- 25 valid for encryption and decryption before the expiry condition is met.
5. The method according to claim 4, wherein the expiry condition is a predefined valid period.
- 30 6. The method according to claim 4 or 5, wherein the expiry condition is a predefined number of uses.

7. The method according to any one of claims 4 to 6, wherein the expiry condition is met after expiry of the token session key.
8. The method according to any one of claims 1 to 7, wherein the first computer
5 is a local client computer and the second computer is a remote computer server.
9. The method according to claim 8, wherein the first data communication instruction relates to storing of the first data on the remote computer server.
- 10 10. The method according to any one of claims 1 to 7, wherein the first computer is a remote computer server and the second computer is a local client computer.
11. The method according to claim 10, wherein the first data communication instruction relates to retrieving of the first data from the remote computer server.
- 15 12. The method according to claim 1, further comprising:
cooperatively executing, by the first and second computers, a second data communication instruction for communicating second data from the second computer to the first computer;
20 generating a second session key by the second computer;
encrypting, by the second computer, the second data using the second session key;
encrypting, by the second computer, the second session key using a second public key, the second public key paired with a second private key,
25 the second public-private key pair generated for the first computer;
sending the encrypted second data and the encrypted second session key from the second computer to the first computer;
decrypting, by the first computer, the encrypted second session key using the second private key;
30 decrypting, by the first computer, the encrypted second data using the decrypted second session key; and
processing, by the first computer, the decrypted second data based on the second data communication instruction.

13. The method according to claim 12, further comprising cooperatively performing, by the first and second computers, a token generation process before executing the first data communication instruction, the token generation process comprising:

5 generating a token session key by the first computer;
 encrypting, by the first computer, a token request using the token session key;
 sending the token session key and the encrypted token request from
10 the first computer to the second computer;
 decrypting, by the second computer, the encrypted token request using the token session key;
 generating the first public-private key pair for and by the second computer;
15 generating the second public-private key pair by the second computer for the first computer;
 encrypting, by the second computer, the first public key and the second private key using the token session key;
 sending the encrypted first public key and the encrypted second private
20 key from the second computer to the first computer;
 decrypting, by the first computer, the encrypted first public key and the encrypted second private key using the token session key.

14. The method according to claim 12, further comprising cooperatively performing, by the first and second computers, a token generation process before executing the first data communication instruction, the token generation process comprising:

25 generating a token session key by the first computer;
 generating the first public-private key pair by the first computer for the
30 second computer;
 generating the second public-private key pair for and by the first computer;

encrypting, by the first computer, the first private key and the second public key using the token session key;

sending the token session key, the encrypted first private key, and the encrypted second public key from the first computer to the second computer;

5 decrypting, by the second computer, the encrypted first private key and the encrypted second public key using the token session key.

15. The method according to any one of claims 12 to 14, wherein each of the first and second public-private key pairs has an expiry condition, such that each of the
10 first and second public-private key pairs is valid for encryption and decryption before the respective expiry condition is met.

16. The method according to claim 15, wherein the expiry condition is a predefined valid period.

15 17. The method according to claim 15 or 16, wherein the expiry condition is a predefined number of uses.

18. The method according to any one of claims 15 to 17, wherein the expiry
20 condition is met after expiry of the token session key.

19. The method according to any one of claims 12 to 18, wherein the first computer is a local client computer and the second computer is a remote computer server.

25 20. The method according to claim 19, wherein the first data communication instruction relates to storing of the first data on the remote computer server, and wherein the second data communication instruction relates to retrieving of the second data from the remote computer server.

30 21. The method according to claim 19, wherein the first data comprises authentication data of a user of the local client computer, and wherein the second data comprises a message authentication code (MAC) generated by the remote

computer server in response to successful authentication of the authentication data by the remote computer server.

22. The method according to any one of claims 1 to 21, wherein the first data
5 comprises measurement data related to medical information.

23. A computer system comprising a first computer and a second computer
communicatively connected to each other, the computer system configured for
securing data communication between the first and second computers, the first and
10 second computers configured for performing steps comprising:

cooperatively executing, by the first and second computers, a first data
communication instruction for communicating first data from the first computer
to the second computer;

generating a first session key by the first computer;

15 encrypting, by the first computer, the first data using the first session
key;

encrypting, by the first computer, the first session key using a first
public key, the first public key paired with a first private key, the first public-
private key pair generated for the second computer;

20 sending the encrypted first data and the encrypted first session key
from the first computer to the second computer;

decrypting, by the second computer, the encrypted first session key
using the first private key;

25 decrypting, by the second computer, the encrypted first data using the
decrypted first session key; and

processing, by the second computer, the decrypted first data based on
the first data communication instruction.

24. The system according to claim 23, further comprising cooperatively
30 performing, by the first and second computers, a token generation process before
executing the first data communication instruction, the token generation process
comprising:

generating a token session key by the first computer;

encrypting, by the first computer, a token request using the token session key;

sending the token session key and the encrypted token request from the first computer to the second computer;

5 decrypting, by the second computer, the encrypted token request using the token session key;

generating the first public-private key pair for and by the second computer;

10 encrypting, by the second computer, the first public key using the token session key;

sending the encrypted first public key from the second computer to the first computer;

decrypting, by the first computer, the encrypted first public key using the token session key.

15

25. The system according to claim 23, further comprising cooperatively performing, by the first and second computers, a token generation process before executing the first data communication instruction, the token generation process comprising:

20 generating a token session key by the first computer;

generating the first public-private key pair by the first computer for the second computer;

encrypting, by the first computer, the first private key using the token session key;

25 sending the token session key and the encrypted first private key from the first computer to the second computer;

decrypting, by the second computer, the encrypted first private key using the token session key.

30 26. The system according to any one of claims 23 to 25, wherein the first computer is a local client computer and the second computer is a remote computer server.

27. The system according to claim 26, wherein the first data communication instruction relates to storing of the first data on the remote computer server.
28. The system according to any one of claims 23 to 26, wherein the first
5 computer is a remote computer server and the second computer is a local client computer.
29. The system according to claim 28, wherein the first data communication instruction relates to retrieving of the first data from the remote computer server.
- 10 30. The system according to claim 23, the steps further comprising:
cooperatively executing, by the first and second computers, a second data communication instruction for communicating second data from the second computer to the first computer;
15 generating a second session key by the second computer;
encrypting, by the second computer, the second data using the second session key;
encrypting, by the second computer, the second session key using a second public key, the second public key paired with a second private key,
20 the second public-private key pair generated for the first computer;
sending the encrypted second data and the encrypted second session key from the second computer to the first computer;
decrypting, by the first computer, the encrypted second session key using the second private key;
25 decrypting, by the first computer, the encrypted second data using the decrypted second session key; and
processing, by the first computer, the decrypted second data based on the second data communication instruction.
- 30 31. The system according to claim 30, further comprising cooperatively performing, by the first and second computers, a token generation process before executing the first data communication instruction, the token generation process comprising:

generating a token session key by the first computer;
encrypting, by the first computer, a token request using the token
session key;
sending the token session key and the encrypted token request from
5 the first computer to the second computer;
decrypting, by the second computer, the encrypted token request using
the token session key;
generating the first public-private key pair for and by the second
computer;
10 generating the second public-private key pair by the second computer
for the first computer;
encrypting, by the second computer, the first public key and the second
private key using the token session key;
sending the encrypted first public key and the encrypted second private
15 key from the second computer to the first computer;
decrypting, by the first computer, the encrypted first public key and the
encrypted second private key using the token session key.

32. The system according to claim 30, further comprising cooperatively
20 performing, by the first and second computers, a token generation process before
executing the first data communication instruction, the token generation process
comprising:

generating a token session key by the first computer;
generating the first public-private key pair by the first computer for the
25 second computer;
generating the second public-private key pair for and by the first
computer;
encrypting, by the first computer, the first private key and the second
public key using the token session key;
30 sending the token session key, the encrypted first private key, and the
encrypted second public key from the first computer to the second computer;
decrypting, by the second computer, the encrypted first private key and
the encrypted second public key using the token session key.

33. The system according to any one of claims 30 to 32, wherein the first computer is a local client computer and the second computer is a remote computer server.

5

34. The system according to claim 33, wherein the first data communication instruction relates to storing of the first data on the remote computer server, and wherein the second data communication instruction relates to retrieving of the second data from the remote computer server.

10

35. The system according to claim 33, wherein the first data comprises authentication data of a user of the local client computer, and wherein the second data comprises a message authentication code (MAC) generated by the remote computer server in response to successful authentication of the authentication data

15 by the remote computer server.