CLAIMS

What is claimed is:

1. A method for establishing a trusted channel between a user and a trusted computing cluster, the trusted computing cluster including a plurality of trusted computing units each maintaining a first cluster key, the method comprising:

at a first trusted computing unit of the trusted computing cluster:

obtaining a first session key through negotiation with a user outside of the trusted computing cluster, and establishing a first trusted channel with the user, the first session key configured to encrypt data to be transmitted through the first trusted channel;

encrypting the first session key using the first cluster key to obtain a first encrypted key; and

sending a first notification to a cluster manager different from the first trusted computing unit, the first notification including the first encrypted key for the cluster manager to transfer the first encrypted key to a second trusted computing unit in the trusted computing cluster.

2. The method according to claim 1, wherein the obtaining the first session key through negotiation with the user includes:

sending a first public key of a first key pair of the first trusted computing unit to the user, the first key pair including the first public key and a first private key, and obtaining a user public key provided by the user; and

generating the first session key based on the first public key, the first private key, and the user public key.

3. The method according to claim 1, further comprising:

before the sending the first notification to the cluster manager:

sending an identifier request message for the first trusted channel to the cluster manager;

obtaining a first session identifier allocated by the cluster manager to the first trusted channel; and

including the first session identifier into the first notification.

4. The method of claim 1, comprising:

at the cluster manager:

receiving the first notification from the first trusted computing unit;

determining the trusted computing cluster to which the first trusted computing unit belongs; and

transferring the first encrypted key to the second trusted computing unit in the trusted computing cluster for the second trusted computing unit to decrypt the first encrypted key based on the first cluster key maintained by the second trusted computing unit to obtain the first session key, and to join the first trusted channel based on the first session key.

5. The method according to claim 4, further comprising:

allocating a first session identifier to the first trusted channel in response to an identifier request message of the first trusted computing unit for the first trusted channel; and

adding the first trusted computing unit to a first trusted computing unit list corresponding to the first session identifier.

6. The method according to claim 5, wherein the first notification further includes the first session identifier, and the method further comprises:

transferring the first session identifier to the second trusted computing unit; and

adding the second trusted computing unit to the first trusted computing unit list.

7. The method according to claim 4, wherein the determining the trusted computing cluster to which the first trusted computing unit belongs includes:

using a maintained cluster information table to determine a first trusted computing cluster to which the first trusted computing unit belongs, and each trusted computing unit included in the first trusted computing cluster.

8. A method for re-establishing a trusted channel between a trusted computing cluster and a user outside of the trusted computing cluster, the trusted computing cluster having established a first trusted channel with the user, the first trusted channel having a first session key to encrypt transmitted data, the trusted computing cluster including a plurality of trusted computing units each maintaining a first cluster key, a first session identifier corresponding to the first trusted channel, the method comprising:

at a first trusted computing unit of the plurality of trusted computing units:

obtaining, through negotiation with the user outside of the trusted computing cluster, a second session key for the first trusted channel, the second session key configured to replace the first session key of the first trusted channel to encrypt transmitted data;

encrypting the second session key using the first cluster key to obtain a second encrypted key; and

sending a notification to a cluster manager first trusted computing unit, the notification including the second encrypted key and the first session identifier for the cluster manager to transfer the second encrypted key to a second trusted computing unit related to the first session identifier.

9. The method of claim 8, comprising:

at the cluster manager:

receiving the notification from the first trusted computing unit;

obtaining, based on the first session identifier, a first trusted computing unit list of trusted computing units that join the first trusted channel, the first trusted computing unit list including the first trusted computing unit and at least one other trusted computing unit belonging to the trusted computing cluster;

removing each of the at least one other trusted computing unit from the first trusted computing unit list; and

transferring the second encrypted key to the second trusted computing unit of the at least one other trusted computing unit for the second trusted computing unit to decrypt the second encrypted key based on the first cluster key maintained by the second trusted

computing unit to obtain the second session key, and to rejoin the first trusted channel based on the second session key.

10. The method according to claim 9, further comprising:

after the transferring the second encrypted key to the second trusted computing unit:

adding the second trusted computing unit to the second trusted computing unit list.

11. A non-transitory computer-readable storage medium, the non-transitory computer-readable storage medium storing computer executable instructions, which when executed by one or more processors, configure the one or more processors to perform acts including:

at a first trusted computing unit of a trusted computing cluster, the trusted computing cluster including a plurality of trusted computing units each maintaining a first cluster key:

obtaining a first session key through negotiation with a user outside of the trusted computing cluster, and establishing a first trusted channel with the user, the first session key configured to encrypt data to be transmitted through the first trusted channel;

encrypting the first session key using the first cluster key to obtain a first encrypted key; and

sending a first notification to a cluster manager different from the first trusted computing unit, the first notification including the first encrypted key for the cluster manager to transfer the first encrypted key to a second trusted computing unit in the trusted computing cluster.

12. The non-transitory computer-readable storage medium according to claim 11, wherein the obtaining the first session key through negotiation with the user includes:

sending a first public key of a first key pair of the first trusted computing unit to the user, the first key pair including the first public key and a first private key, and obtaining a user public key provided by the user; and

generating the first session key based on the first public key, the first private key, and the user public key.

13. The non-transitory computer-readable storage medium according to claim 11, wherein the acts further include:

before the sending the first notification to the cluster manager:

sending an identifier request message for the first trusted channel to the cluster manager;

obtaining a first session identifier allocated by the cluster manager to the first trusted channel; and

including the first session identifier into the first notification.

14. The non-transitory computer-readable storage medium of claim 11, wherein the acts include:

at the cluster manager:

receiving the first notification from the first trusted computing unit;

determining the trusted computing cluster to which the first trusted computing unit belongs; and

transferring the first encrypted key to the second trusted computing unit in the trusted computing cluster for the second trusted computing unit to decrypt the first encrypted key based on the first cluster key maintained by the second trusted computing unit to obtain the first session key, and to join the first trusted channel based on the first session key.

15. The non-transitory computer-readable storage medium according to claim 14, wherein the acts include:

allocating a first session identifier to the first trusted channel in response to an identifier request message of the first trusted computing unit for the first trusted channel; and

adding the first trusted computing unit to a first trusted computing unit list corresponding to the first session identifier.

16. The non-transitory computer-readable storage medium according to claim 15, wherein the first notification further includes the first session identifier, and the acts include:

transferring the first session identifier to the second trusted computing unit; and

adding the second trusted computing unit to the first trusted computing unit list.

17. The non-transitory computer-readable storage medium according to claim 14, wherein the determining the trusted computing cluster to which the first trusted computing unit belongs includes:

using a maintained cluster information table to determine a first trusted computing cluster to which the first trusted computing unit belongs, and each trusted computing unit included in the first trusted computing cluster.

18. A non-transitory computer-readable storage medium, the non-transitory computer-readable storage medium storing computer executable instructions, which when executed by one or more processors, configure the one or more processors to perform acts including:

at a first trusted computing unit of a trusted computing cluster, the trusted computing cluster including a plurality of trusted computing units each maintaining a first cluster key, the trusted computing cluster having established a first trusted channel with a user outside of the trusted computing cluster, the first trusted channel having a first session key to encrypt transmitted data, a first session identifier corresponding to the first trusted channel:

obtaining, through negotiation with the user, a second session key for the first trusted channel, the second session key configured to replace the first session key of the first trusted channel to encrypt transmitted data;

encrypting the second session key using the first cluster key to obtain a second encrypted key; and

sending a notification to a cluster manager different from the first trusted computing unit, the notification including the second encrypted key and the first session identifier for the cluster manager to transfer the second encrypted key to a second trusted computing unit related to the first session identifier.

19. The non-transitory computer-readable storage medium of claim 18, wherein the acts include:

at the cluster manager:

receiving the notification from the first trusted computing unit;

obtaining, based on the first session identifier, a first trusted computing unit list of trusted computing units that join the first trusted channel, the first trusted computing unit list including the first trusted computing unit and at least one other trusted computing unit belonging to the trusted computing cluster;

removing each of the at least one other trusted computing unit from the first trusted computing unit list; and

transferring the second encrypted key to the second trusted computing unit of the at least one other trusted computing unit for the second trusted computing unit to decrypt the second encrypted key based on the first cluster key maintained by the second trusted computing unit to obtain the second session key, and to rejoin the first trusted channel based on the second session key.

20. The non-transitory computer-readable storage medium according to claim 19, wherein the acts include:

after the transferring the second encrypted key to the second trusted computing unit:

adding the second trusted computing unit to the second trusted computing unit list.