WHAT IS CLAIMED IS:

1. A message transmitting system, comprising:

a message exchange center;

at least a first user device and a second user device, which are both in communication with the message exchange center via a network for message exchange; and

a hardware security module, which is adapted to be inserted into the first user device,

wherein after the hardware security module is inserted into the first user device, the hardware security module generates a first key establishment combination including at least a first public-private key pair according to a key establishment algorithm, wherein a first private key of the first public-private key pair is only stored in the hardware security module, and a first public key of the first public-private key pair is sent to the message exchange center; and

wherein for transmitting a first message from the second user device to the first user device, the second user device obtains the first public key from the message exchange center for establishing or encrypting a shared key, uses the shared key to encrypt a plaintext of the first message into a ciphertext of the first message, and transmits the ciphertext of the first message to the first user device via the message exchange center, and the first user device performs key establishment or decryption with a specific information, which includes the first private key stored in the hardware security module, to derive the shared key, and uses the shared key to decrypt the ciphertext of the first message to recover the plaintext of the first message.

2. The system according to claim 1, wherein the second user device generates a second key establishment combination including at least a second public-private key pair according to the key establishment algorithm, wherein a second private key of the second public-private key pair is only stored in the second user device, and a second public key of the second public-private key pair is sent to the message exchange center, and the shared key is established by the second user device according to at least the first public key and the second private key.

3. The system according to claim 2, wherein the specific information further includes the second public key obtained from the message exchange center, and the hardware security module uses the second public key and the first private key to perform key establishment, thereby deriving the shared key.

4. The system according to claim 2, wherein the message exchange center includes an identity register center, which receives the first public key and the second public key for identity verification of the first user device and the second user device, respectively, and the hardware security module executes identity verification of the first user device and does not generate the first key establishment combination and/or recover the shared key until the first user device is successfully verified.

5. The system according to claim 4, wherein after being successfully verified, the first user device generates a digital signature with the first private key or another private key of the first user device, and the second user device receives the digital signature via the message exchange center, verifies the first user device by verifying the digital signature based on the first public

key or another public key of the first user device, and derives the shared key from a shared secret, which is generated according to at least the first public key and the second private key, after successfully verifying the digital signature.

6. The system according to claim 5, wherein the first user device further includes an action sensor disposed in the hardware security module for detecting vibration of the first user device, and the identity verification is determined to fail if no vibration is detected by the action sensor.

7. The system according to claim 1, wherein the shared key is established in a way that:

the shared key is generated by the second user device randomly;

the shared key is implemented with a constant that is stored in the second user device; or

the shared key is derived from a key derivation function with a character string that is inputted to the second user device by a user.

8. The system according to claim 1, wherein the first user device uses the first private key to decrypt the shared key, which is encrypted with the first public key by the second user device, so as to derive the shared key.

9. The system according to claim 1, wherein the hardware security module includes a secure element generating and exclusively storing a main key, which is used to encrypt and recover the first private key, wherein the main key is randomly generated, is a constant value or is derived with a key derivation function in response to a character string inputted by a user.

10. A message transmitting system, comprising:

a first user device in communication with an Internet,

a hardware security module adapted to be inserted into the first user device, and generating a first key establishment combination including at least a first public-private key pair according to a key establishment algorithm after the hardware security module is inserted into the first user device, wherein a first private key of the first public-private key pair is only stored in the hardware security module; and

a second user device in communication with the Internet,

wherein for transmitting a first message from the second user device to the first user device, the second user device provides an IP address for the first user device via the Internet to conduct an end-to-end connection between the first user device and the second user device, obtains the first public key from the first user device for establishing or encrypting a shared key, uses the shared key to encrypt a plaintext of the first message into a ciphertext of the first message, and transmits the ciphertext of the first message to the first user device via the end-to-end connection, and the first user device performs key establishment or decryption with a specific information, which includes the first private key stored in the hardware security module, to derive the shared key, and uses the shared key to decrypt the ciphertext of the first message to recover the plaintext of the first message.

11. The system according to claim 10, wherein the second user device generates a second key establishment combination including at least a second public-private key pair according to the key establishment algorithm,

wherein a second private key of the second public-private key pair is only stored in the second user device, and the shared key is established according to at least the first public key and the second private key.

12. The system according to claim 11, wherein the specific information further includes the second public key obtained from the second user device by way of the end-to-end connection, and the hardware security module uses the second public key and the first private key to perform key establishment, thereby deriving the shared key.

13. The system according to claim 10, wherein the shared key is established in a way that:

the shared key is generated by the second user device randomly;

the shared key is implemented with a constant that is stored in the second user device; or

the shared key is derived from a key derivation function with a character string that is inputted to the second user device by a user.

14. The system according to claim 10, wherein the shared key is encrypted by the second user device according to the first public key obtained from the first user device and then transmitted to the first user device by way of the end-to-end connection.

15. The system according to claim 10, wherein the first user device uses the first private key to decrypt the shared key, which is encrypted with the first public key by the second user device, so as to derive the shared key.

16. A hardware security module, comprising a secure element and adapted to be inserted into a housing of a user device, wherein the hardware security module generates a key establishment combination according to a key establishment algorithm after the hardware security module is inserted into the user device and when the user device is in communication with another user device via a message exchange center or via an end-to-end connection, wherein the key establishment combination includes at least a first public-private key pair, and a first private key of the first public-private key pair is exclusively stored in the hardware security module, and wherein the hardware security module uses a specific information, which includes the first private key stored therein, to derive a shared key received from the another user device via the message exchange center or the end-to-end connection, and uses the shared key to process a message transmitted from the another user device to the user device by way of a specific application program.