

CLAIMS

1. A service communication method executed by an electronic device, the method including:
 - receiving an authentication request sent by a service access process;
 - performing synchronous verification processing on the service access process, and performing asynchronous verification processing on the service access process;
 - determining service key information allocated for the service access process according to a synchronous verification processing result of the service access process;
 - sending the service key information to the service access process for encrypted service communication with the service access process based on the service key information; and
 - controlling a communication connection used for bearing the encrypted service communication with the service access process according to an asynchronous verification processing result of the service access process.
2. The method according to claim 1, wherein the performing synchronous verification processing on the service access process comprises:
 - taking a matching result between a process path of the service access process and a set security directory as a first verification processing result;
 - verifying signature information about the service access process to obtain a second verification processing result; and
 - determining the synchronous verification processing result of the service access process according to the first verification processing result and the second verification processing result.
3. The method according to claim 2, wherein the verifying signature information about the service access process to obtain a second verification processing result comprises:
 - determining the second verification processing result according to at least one of a result of whether the signature information comprises a digital signature, a validity verification processing result of the digital signature, a matching result between a signer and a signer blacklist of the digital signature, and a matching result between certificate information in the signature information and a certificate information blacklist.
4. The method according to claim 3, wherein the method further comprises:
 - determining a digital signature in the signature information, and a decryption key corresponding to the digital signature;

decrypting the digital signature according to the decryption key to obtain a first hash result of a process file of the service access process;

performing hash processing on the process file of the service access process to obtain a second hash result; and

taking a matching result between the first hash result and the second hash result as the validity verification processing result of the digital signature.

5. The method according to claim 1, wherein the authentication request comprises a public key of an asymmetric key pair generated by the service access process; wherein the asymmetric key pair comprises the public key and a private key corresponding to the public key;

the sending the service key information to the service access process comprises:

encrypting the service key information according to the public key; and

sending the encrypted service key information to the service access process, so that the service access process decrypts the encrypted service key information according to the private key.

6. The method according to claim 5, wherein the service key information comprises a key identifier and a symmetric key;

upon sending the encrypted service key information to the service access process, the method further comprises:

receiving a service request sent by the service access process; wherein the service request comprises the key identifier and request data encrypted using the symmetric key;

querying a symmetric key corresponding to the key identifier in the service request in the distributed symmetric key;

decrypting the encrypted request data in the service request according to the queried symmetric key;

performing response processing on the request data obtained by the decryption to obtain response data; and

encrypting the response data according to the public key, and sending the encrypted response data to the service access process, so that the service access process decrypts the encrypted response data according to the private key.

7. The method according to claim 6, wherein the service request further comprises a time stamp and first checking information; wherein the first checking information is obtained by the

service access process performing hash processing on the key identifier, the symmetric key, the time stamp, and request data encrypted using the symmetric key;

the performing response processing on the request data obtained by the decryption comprises:

performing hash processing on the key identifier, the queried symmetric key, the time stamp, and the encrypted request data to obtain second checking information; and

performing response processing on the request data obtained by the decryption in a case that a matching result between the first checking information and the second checking information is matching success.

8. The method according to claim 6, wherein upon the querying a symmetric key corresponding to the key identifier in the service request in the distributed symmetric key, the method further comprises:

sending expired information to the service access process in a case that a usage parameter of the queried symmetric key satisfies an expired parameter condition, so that the service access process resends an authentication request in response to receiving the expired information;

wherein the usage parameter comprises at least one of a usage number and a usage duration.

9. The method according to claim 1, wherein the authentication request comprises an authentication request address;

the determining service key information allocated for the service access process comprises:

executing any of the following processing:

allocating different service key information with respect to authentication request addresses sent by the different service access processes, and allocating different service key information with respect to different authentication request addresses sent by the same service access process;

allocating different service key information with respect to authentication request addresses sent by the different service access processes, and allocating same service key information with respect to different authentication request addresses sent by the same service access process; and

allocating same service key information with respect to authentication request addresses sent by the different service access processes, and allocating same service key information with respect to different authentication request addresses sent by the same service access process.

10. The method according to claim 1, wherein the determining service key information allocated for the service access process according to a synchronous verification processing result of

the service access process comprises:

determining service key information allocated for the service access process in a case that a synchronous verification processing result of the service access process is verification success;

the method further comprises:

executing any of the following processing in a case that the synchronous verification processing result of the service access process is verification failure:

notifying the service access process to resend an authentication request;

disconnecting a communication connection used for transmitting the authentication request with the service access process; and

interrupting the asynchronous verification processing on the service access process.

11. The method according to claim 1, wherein the controlling a communication connection used for bearing the encrypted service communication with the service access process according to an asynchronous verification processing result of the service access process comprises:

maintaining the communication connection for bearing the encrypted service communication with the service access process in a case that the asynchronous verification processing result of the service access process is verification success; and

disconnecting the communication connection for bearing the encrypted service communication with the service access process in a case that the asynchronous verification processing result of the service access process is verification failure.

12. The method of any one of claims 1 to 11, wherein the method further comprises:

executing the following processing in the process of the encrypted service communication:

receiving a credential request sent by the service access process; wherein the credential request is sent by the service access process in response to intercepting a service request of an application process, and a destination address of the service request is an address of a service server;

performing synchronous verification processing on the application process;

determining a service credential and a gateway address allocated for the application process, and sending the service credential and the gateway address to the service access process according to a synchronous verification processing result of the application process, so that

the service access process sends the service credential and the service request to a service gateway corresponding to the gateway address;

wherein the service gateway is configured to perform verification processing on the received service credential, and send the received service request to the service server in a case that a verification processing result of the service credential is verification success; and the service server is configured to perform response processing on request data in the received service request.

13. The method according to claim 12, wherein the performing synchronous verification processing on the application process comprises:

determining a user account in a login state in a device where the application process is located, and acquiring process information about a trusted application process corresponding to the user account and an address of an accessible service server corresponding to the user account;

taking a matching result between process information about the application process and the process information about the trusted application process as a third verification processing result;

taking a matching result between the address of the service server requested by the service request and the address of the accessible service server as a fourth verification processing result;

acquiring device information about the device where the application process is located, and taking a matching result between the device information and device security conditions as a fifth verification processing result; and

determining a synchronous verification processing result of the application process according to the third verification processing result, the fourth verification processing result and the fifth verification processing result.

14. The method according to claim 12, wherein upon receiving a credential request sent by the service access process, the method further comprises:

periodically matching process information about the application process with a process information blacklist, and taking the obtained matching result as an asynchronous verification processing result of the application process; and

controlling a communication connection used for bearing the encrypted service communication with the service access process according to the asynchronous verification processing result of the application process.

15. The method of any one of claims 1 to 11, wherein the performing asynchronous verification processing on the service access process comprises:

periodically matching process information about the service access process with a process information blacklist, and taking the obtained matching result as an asynchronous verification

processing result of the service access process.

16. A service communication system, comprising a service access client, a security client, and a security server; wherein the service access client runs a service access process;

the security client is configured to:

receive an authentication request sent by the service access process;

perform synchronous verification processing on the service access process, and notify the security server to perform asynchronous verification processing on the service access process;

determine service key information allocated for the service access process according to a synchronous verification processing result of the service access process;

send the service key information to the service access process for encrypted service communication with the service access process based on the service key information; and

control a communication connection used for bearing the encrypted service communication with the service access process according to an asynchronous verification processing result of the security server on the service access process.

17. The system according to claim 16, wherein

the security client is further configured to:

receive a credential request sent by the service access process; wherein the credential request is sent by the service access process in response to intercepting a service request of an application process, and a destination address of the service request is an address of a service server;

notify the security server to perform synchronous verification processing on the application process;

the security server is configured to determine a service credential and a gateway address allocated for the application process according to a synchronous verification processing result of the application process, and send the service credential and the gateway address to the service access process via the security client;

the service access client is also configured to send the service credential and the service request to a service gateway corresponding to the gateway address via the service access process;

wherein the service gateway is configured to perform verification processing on the received service credential, and send the received service request to the service server in a case that a verification processing result of the service credential is verification success; and the service server

is configured to perform response processing on request data in the received service request.

18. A service communication apparatus, the apparatus comprising:

a receiving module configured to receive an authentication request sent by a service access process;

a verification module configured to perform synchronous verification processing on the service access process, and perform asynchronous verification processing on the service access process;

a determination module configured to determine service key information allocated for the service access process according to a synchronous verification processing result of the service access process;

a sending module configured to send the service key information to the service access process for encrypted service communication with the service access process based on the service key information; and

a connection control module configured to control a communication connection used for bearing the encrypted service communication with the service access process according to an asynchronous verification processing result of the service access process.

19. An electronic device, comprising:

a memory, configured to store executable instructions; and

a processor, configured to perform the service communication method according to any one of claims 1 to 15 when executing the executable instructions stored in the memory.

20. A computer-readable storage medium, storing executable instructions, the executable instructions, when executed by a processor, performing the service communication method according to any one of claims 1 to 15.