

Claims

1. A method for trusted service management, comprising:
obtaining an identification identifier and address information of a computing unit;
obtaining a mapping table for the identification identifier and the address information of the computing unit;
initiating a trusted service request message to a server that provides trusted service management using the identification identifier of the computing unit; and
receiving a corresponding trusted service response message, and transmitting the trusted service response message to the computing unit according to the mapping table.
2. The method for trusted service management of claim 1, wherein the method for trusted service management is performed based on a gateway.
3. The method for trusted service management of claim 1, wherein the gateway is a WIFI gateway.
4. The method for trusted service management of claim 2, wherein the computing unit is a secure element or a secure device embedded with a secure element.
5. The method for trusted service management of claim 4, further comprising:
receiving an execution result returned by the computing unit, and sending the execution result to the server that provides the trusted service management.

6. The method for trusted service management of claim 5, wherein transmitting the trusted service response message to the computing unit comprises: transmitting the trusted service response message to the computing unit in a broadcast mode.

7. The method for trusted service management of claim 6, wherein the identification identifier is a production life cycle (CPLC) of a secure element of the computing unit.

8. The method for trusted service management of claim 4, wherein the address information is a MAC and/or an IP of the secure element or the secure device.

9. The method for trusted service management of claim 8, wherein obtaining the identification identifier and the address information of the computing unit comprises the following processing:

receiving a request from a requesting party, and performing an operation of connection and gateway authentication on the requesting party;

recording address information of the requesting party and querying whether the requesting party is a secure element or a secure device if the authentication is passed;

sending a request for obtaining the identification identifier of the computing unit if affirmative; and

receiving and obtaining the identification identifier of the computing unit.

10. The method for trusted service management of claim 7, wherein: if the address information is a MAC and/or an IP of the secure element or the secure device, the mapping table comprises any one of the following correspondence relationships: a correspondence relationship between CPLC and MAC, a correspondence relationship between CPLC and IP, a correspondence relationship among CPLC, MAC and IP.

11. The method for trusted service management of claim 10, wherein the computing unit is a secure element or a secure device that is able to recognize APDU data specified by a global platform and execute APDU instructions.

12. The method for trusted service management of claim 11, wherein transmitting the response message to the computing unit in the broadcast mode comprises the following processing:

assembling the response message into a broadcast data message according to a packaging protocol; and

broadcasting the broadcast data message according to the mapping table, wherein the packaging protocol includes at least relevant information of the following fields: packet header information and APDU data.

13. The method for trusted service management of claim 12, wherein the packet header information comprises at least the following fields: the identification identifier and a length.

14. The method for trusted service management of claim 12, wherein the packaging protocol comprises any of the following fields: reserved bits and a state.

15. The method for trusted service management of claim 12, wherein the broadcast data message comprises one or more data packets assembled according to the packaging protocol.

16. The method for trusted service management of claim 11, wherein the APDU data comprises at least any of the following content information:

life cycle management information, rights management information, key escrow information, authentication information, secure data transmission and processing information, sensitive personal data, and state report information.

17. The method for trusted service management of claim 12, wherein the server that provides the trusted service management is a SEI-TSM server, and wherein the SEI-TSM is a trusted management end that issues secure elements.

18. The method for trusted service management of claim 17, wherein: when the trusted service request message is a security domain creating request APDU, the trusted service response message is a security domain creating instruction APDU.

19. The method for trusted service management of claim 18, wherein when the execution result returned by the computing unit is a successful creation of a security domain, after receiving the successful creation of the security domain returned by the computing unit, the method further comprises the following processing:

initiating an application download request to a SP-TSM using the identification identifier of the computing unit, wherein the SP-TSM is a server of a service provider of the trusted service management.

20. The method for trusted service management of claim 19, wherein when the trusted service request message is an application download request, the corresponding trusted service response message comprises: an APDU formed by assembling and encrypting an application program requested to be downloaded by the SP-TSM, wherein, the APDU is packaged into a broadcast data packet by a gateway according to the packaging protocol, and is sent out in a broadcast form.

21. The method for trusted service management of claim 20, wherein: when the execution result returned by the computing unit is an application installation state report APDU, after a gateway receives the execution result returned by the computing unit, the method further comprises the following processing: returning the state report APDU to SP-TSM.

22. The method for trusted service management of claim 21, wherein: when the execution result returned by the computing unit is the application installation state report APDU, after the gateway returns the state report APDU to the SP-TSM, the method further comprises the following processing:

 sending a personalized request by the gateway to the SP-TSM using the identification identifier of the computing unit, wherein the SP-TSM obtains personalized data according to the personalized request and sends the personalized data to the gateway in an APDU data format, and the gateway collects data and assembles into a broadcast packet, which is broadcasted to the computing unit according to the mapping table.

23. The method for trusted service management of claim 1, wherein initiating the trusted service request message to the server that provides the trusted service management comprises transparently transmitting the received trusted service request message that is initiated by the computing unit.

24. The method for trusted service management of claim 1, wherein initiating the trusted service request message to the server that provides the trusted service management using the identification identifier of the computing unit comprises initiating the trusted service request message in real-time or in a batch manner.

25. A method for requesting trusted service management, comprising:
reporting address information and identification identifier of a computing unit;
identifying and obtaining a matching data packet according to the identification identifier from a received data message, and parsing out trusted service data from the data packet; and
executing an instruction included in the trusted service data, and returning an execution result.

26. The method for requesting trusted service management of claim 25, wherein the method for requesting trusted service management is performed based on the computing unit, and wherein the computing unit is a secure element or a secure device embedded with a secure element.

27. The method for requesting trusted service management of claim 26, wherein the received data message is a received broadcast data message, and wherein the broadcast data message is a data message broadcasted by a gateway accessed by the computing unit.

28. The method for requesting trusted service management of claim 26, wherein the trusted service data is APDU data specified by a global platform.

29. The method for requesting trusted service management of claim 26, wherein the identification identifier is CPLC information of a secure element.

30. The method for requesting trusted service management of claim 26, wherein the address information is a MAC and/or an IP of the secure element or the secure device.

31. The method for requesting trusted service management of claim 26, wherein: before reporting the identification identifier, the method comprises:

receiving a message that queries whether it is a computing unit; and
reporting the identification of the computing unit if affirmative.

32. The method for requesting trusted service management of claim 27, wherein identifying and obtaining the matching data packet according to the identification identifier from the received data packet comprises the following processing:

recognizing and obtaining, by the secure device, the matching data packet from the received broadcast data message according to the identification identifier thereof.

33. The method for requesting trusted service management of claim 28, wherein executing the instruction included in the trusted service data, and returning the execution result comprise:

communicating, within the secure device, with the secure element embedded in the secure device according to APDU data;

decrypting the APDU data through the secure element, executing an APDU instruction obtained after decryption, and encrypting the execution result to form state report APDU data;
and

reporting the state report APDU data to the gateway through the secure device, and further returning the state report APDU data to a server that provides the trusted service through the gateway.

34. The method for requesting trusted service management of claim 28, wherein executing a corresponding APDU instruction included in the APDU data, and returning the execution result include the following processing:

decrypting the APDU data by the computing unit, executing the APDU instruction obtained after decryption, and encrypting the execution result to form state report APDU data; and

sending the state report APDU data back to the gateway, and then returning the state report APDU data to a server that provides the trusted service through the gateway.

35. The method for requesting trusted service management of claim 28, wherein a corresponding APDU instruction included in the APDU data includes any of the following:

- an instruction for creating a security domain APDU provided by a SEI-TSM server;
- an application program APDU delivered by the SP-TSM; or
- personalized data APDU provided by the SP-TSM.

36. An apparatus for trusted service management, comprising:

- an identification identifier and address acquisition unit configured to obtain an identification identifier and address information of a computing unit;
- a mapping unit configured to obtain a mapping table for the identification identifier and the address information of the computing unit;
- a service-side request unit configured to initiate a trusted service request message to a server that provides trusted service management using the identification identifier of the computing unit; and
- a service-side response processing unit configured to receive a corresponding trusted service response message, and transmit the trusted service response message to the computing unit according to the mapping table.

37. An apparatus for requesting trusted service management, comprising:

- an identification identifier and address reporting unit configured to report address information and an identification identifier of a computing unit;
- a data receiving unit configured to identify and obtain a matching data packet according to the identification identifier from a received data packet, and parse out trusted service data from the data packet; and
- an execution unit configured to execute an instruction included in the trusted service data and return an execution result.

38. A trusted service system, comprising: an apparatus for trusted service management; and an apparatus for requesting trusted service management, wherein:

the apparatus for trusted service management comprises:

an identification identifier and address acquisition unit configured to obtain an identification identifier and address information of a computing unit;

a mapping unit configured to obtain a mapping table for the identification identifier and the address information of the computing unit;

a service-side request unit configured to initiate a trusted service request message to a server that provides trusted service management using the identification identifier of the computing unit; and

a service-side response processing unit configured to receive a corresponding trusted service response message, and transmit the trusted service response message to the computing unit according to the mapping table;

the apparatus for requesting trusted service management comprises:

an identification identifier and address reporting unit configured to report the address information and the identification identifier of the computing unit;

a data receiving unit configured to identify and obtain a matching data packet according to the identification identifier from a received data packet, and parse out trusted service data from the data packet; and

an execution unit configured to execute an instruction included in the trusted service data and return an execution result.

Claims

1. A method implemented by a computing device, the method comprising:
obtaining an identification identifier and address information of a computing unit;
obtaining a mapping table for the identification identifier and the address
information of the computing unit;
initiating a trusted service request message to a server that provides a trusted
service management using the identification identifier of the computing unit; and
receiving a corresponding trusted service response message, and transmitting
the trusted service response message to the computing unit according to the mapping
tables wherein when the trusted service request message is an application download
request, the corresponding trusted service response message comprises: an
Application Protocol Data Unit (APDU) formed by assembling and encrypting an
application program requested to be downloaded by a Service Provider Trusted Service
Management (SP-TSM), and wherein the APDU is packaged into a broadcast data
packet by a gateway according to a packaging protocol, and is sent out in a broadcast
form.
2. The method of claim 1, wherein the computing unit comprises a secure element
or a secure device embedded with the secure element.
3. The method of claim 2, further comprising:
receiving an execution result returned by the computing unit, and
sending the execution result to the server that provides the trusted service
management.

4. The method of claim 3, wherein: when the execution result returned by the computing unit is a successful creation of a security domain, the method further comprises:

initiating an application download request to the SP-TSM using the identification identifier of the computing unit after receiving the successful creation of the security domain returned by the computing unit, wherein the SP-TSM is a server of a service provider of the trusted service management.

5. The method of claim 3, wherein: when the execution result returned by the computing unit is an application installation state report APDU, the method further comprises:

returning a state report APDU to the SP-TSM after receiving the execution result returned by the computing unit.

6. The method of claim 5, further comprising:

sending a personalized request to the SP-TSM using the identification identifier of the computing unit after the state report APDU is returned to the SP-TSM, wherein the SP-TSM obtains personalized data according to the personalized request and sends the personalized data to the computing device in an APDU data format, and the computing device collects and assembles pieces of data into a broadcast packet, which is broadcasted to the computing unit according to the mapping table.

7. The method of claim 1, wherein initiating the trusted service request message to the server that provides the trusted service management comprises transparently transmitting the received trusted service request message that is initiated by the computing unit.

8. The method of claim 1, wherein initiating the trusted service request message to the server that provides the trusted service management using the identification identifier of the computing unit comprises initiating the trusted service request message in real-time or in a batch manner.

9. The method of claim 1, wherein transmitting the trusted service response message to the computing unit in the broadcast mode comprises:

assembling the trusted service response message into a broadcast data message according to the packaging protocol; and

broadcasting the broadcast data message according to the mapping table, wherein the packaging protocol includes at least relevant information of:

packet header information and

APDU data.

10. The method of claim 9, wherein:

if the address information is a Media Access Control (MAC) and/or an Internet Protocol (IP) of a secure element or a secure device, the mapping table comprises one of:

a correspondence relationship between a production life cycle (CPLC) and the MAC,

a correspondence relationship between the CPLC and the IP,

a correspondence relationship among the CPLC, the MAC and the IP.

11. The method of claim 1, wherein the identification identifier comprises a production life cycle (CPLC) of a secure element of the computing unit, and the address information comprises one or more of:

a Media Access Control (MAC) or
an Internet Protocol (IP) of the secure element or a secure device.

12. The method of claim 1, wherein obtaining the identification identifier and the address information of the computing unit comprises:

receiving a request from a requesting party, and performing an operation of connection and gateway authentication on the requesting party;

recording address information of the requesting party and querying whether the requesting party is a secure element or a secure device if the gateway authentication is passed;

sending a request for obtaining the identification identifier of the computing unit if the requesting party is the secure element or the secure device; and

receiving and obtaining the identification identifier of the computing unit.

13. One or more non-transitory computer readable media storing executable instructions that, when executed by one or more processors of a computing unit, cause the one or more processors to perform acts comprising:

reporting address information and identification identifier of the computing unit;

identifying and obtaining a matching data packet according to the identification identifier from a received data message, and parsing out trusted service data from the matching data packet; and

executing an instruction included in the trusted service data, and returning an execution result, wherein executing the instruction included in the trusted service data, and returning the execution result comprise:

communicating with a secure element embedded in a secure device according to Application Protocol Data Unit (APDU) data;

decrypting the APDU data through the secure element, executing an APDU instruction obtained after decryption, and encrypting the execution result to form state report APDU data; and

reporting the state report APDU data to a gateway through the secure device, and returning the state report APDU data to a server that provides a trusted service through the gateway.

14. The one or more non-transitory computer readable media of claim 13, wherein the computing unit further comprises the secure element or the secure device embedded with the secure element.

15. The one or more non-transitory computer readable media of claim 14, wherein the received data message is a received broadcast data message, and wherein the received broadcast data message is a data message broadcasted by the gateway accessed by the computing unit.

16. The one or more non-transitory computer readable media of claim 15 wherein identifying and obtaining the matching data packet according to the identification identifier from the received data message comprises:

recognizing and obtaining the matching data packet from the received broadcast data message according to the identification identifier.

17. An apparatus comprising:

one or more processors;

a memory;

an identification identifier and address acquisition unit stored in the memory and executed by the one or more processors to obtain an identification identifier and address information of a computing unit;

a mapping unit stored in the memory and executed by the one or more processors to obtain a mapping table for the identification identifier and the address information of the computing unit;

a service-side request unit stored in the memory and executed by the one or more processors to initiate a trusted service request message to a server that provides trusted service management using the identification identifier of the computing unit; and

a service-side response processing unit stored in the memory and executed by the one or more processors to receive a corresponding trusted service response message, and transmit the trusted service response message to the computing unit according to the mapping table and

an execution result processing unit stored in the memory and executed by the one or more processors to:

receive an execution result returned by the computing unit,

send the execution result to the server that provides the trusted service management, and

when the execution result returned by the computing unit is an application installation state report Application Protocol Data Unit (APDU), return a state report APDU to a Service Provider Trusted Service Management (SP-TSM) after receiving the execution result returned by the computing unit.