US 20130301828A1

(19) United States

(12) Patent Application Publication

Gouget et al.

(10) Pub. No.: US 2013/0301828 A1

(43) Pub. Date: Nov. 14, 2013

(54) **METHOD FOR ESTABLISHING A SECURE COMMUNICATION CHANNEL**

(75) Inventors: **Aline Gouget**, Paris (FR); **Mourad Faher**, Meudon (FR)

(73) Assignee: **GEMALTO SA**, Meudon (FR)

(21) Appl. No.: **13/825,814**

(22) PCT Filed: **Sep. 6, 2011**

(86) PCT No.: **PCT/EP11/65382**

§ 371 (c)(1), (2), (4) Date: **Mar. 23, 2013**

(30) **Foreign Application Priority Data**

Sep. 24, 2010 (EP) 10306028.1

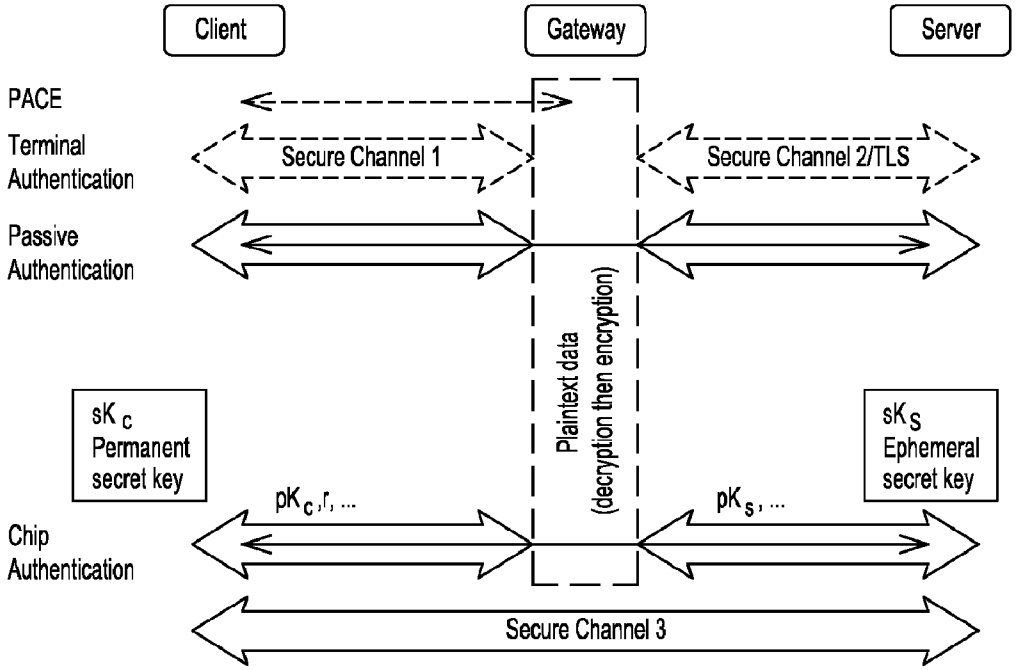
Publication Classification

(51) **Int. Cl.**
H04L 9/08 (2006.01)

(52) **U.S. Cl.**
CPC *H04L 9/0819* (2013.01)
USPC **380/44**

(57) **ABSTRACT**

The present invention provides a method for establishing a secure communication channel between a client (C) and a remote server (S), said client (C) and remote server (S) exchanging data through an intermediate entity (G), said client (C) having a long-term key pair (sk_c,pk_c), said remote server generating an ephemeral key (sk_s,pk_s), the method comprising a mutual authentication step wherein the client (C) sends a public key (pk_c) of said long-term key pair (sk_c, pk_c) and the proof that said public key (pk_c) is valid to the server (S), and wherein the remote server (S) sends the public key (pk_s) of said ephemeral key pair (sk_s,pk_s) to the client (C). The client (C) generates an ephemeral key pair (skC_c,pkC_c) and sends the public key (pK_{cc}) of said ephemeral key pair (sk_{cc},pk_{cc}) to the server (S) so as to generate a secret common to the client (C) and to the remote server (S) for opening the secure communication channel.



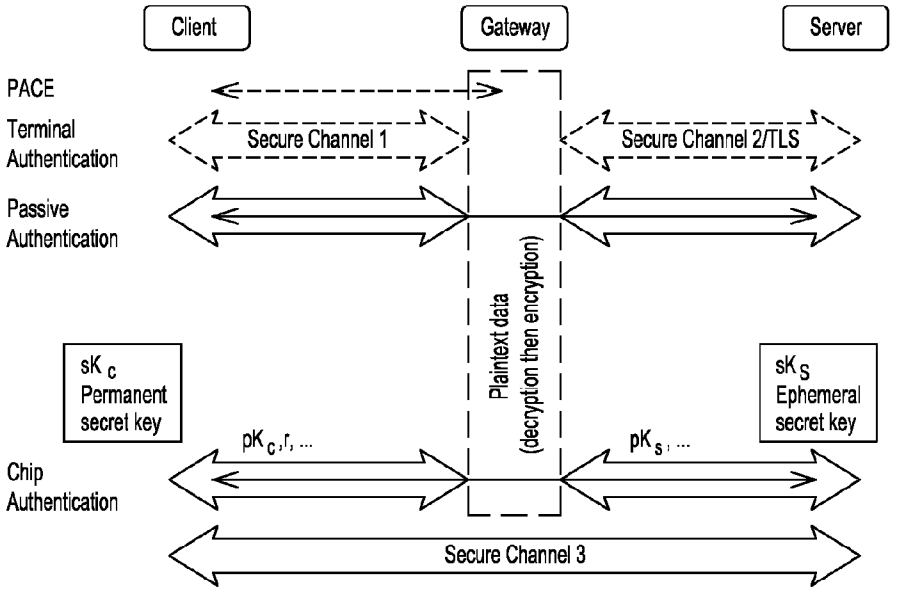

Client
Gateway
Server
PACE
Terminal Authentication
Secure Channel 1
Secure Channel 2/TLS
Passive Authentication
Plaintext data (decryption then encryption)
sK C Permanent secret key
sK S Ephemeral secret key
pK C ,r, ...
pK S , ...
Chip Authentication
Secure Channel 3

Fig. 1

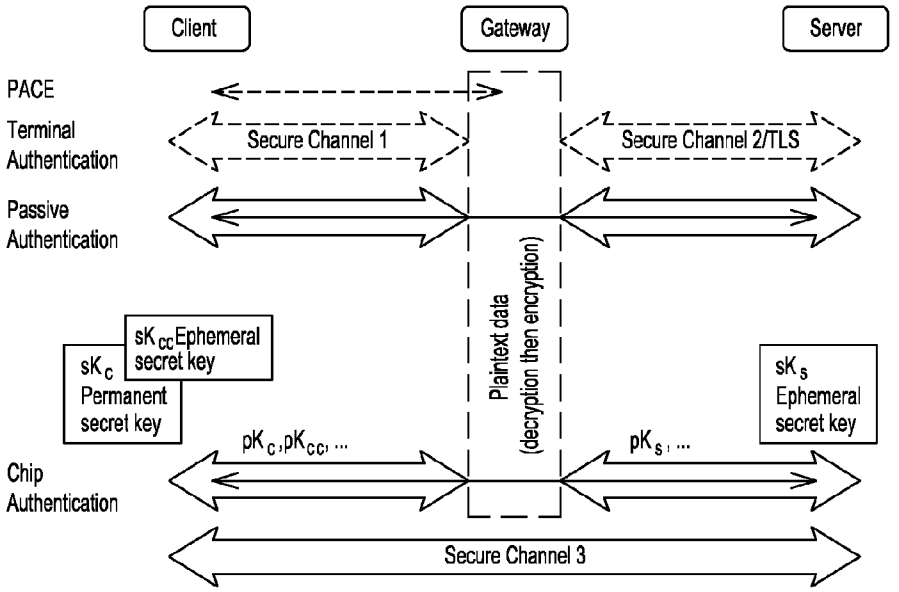

Client
Gateway
Server
PACE
Terminal Authentication
Secure Channel 1
Secure Channel 2/TLS
Passive Authentication
Plaintext data (decryption then encryption)
sK CC Ephemeral secret key
sK C Permanent secret key
sK S Ephemeral secret key
pK C ,pK CC, ...
pK S , ...
Chip Authentication
Secure Channel 3

Fig. 2

METHOD FOR ESTABLISHING A SECURE COMMUNICATION CHANNEL

FIELD OF THE INVENTION

[0001] The invention relates to the field of communication between a client and a remote server.

[0002] The invention especially deals with a method for establishing a secure channel between a client and a remote server, when using an intermediate entity.

BACKGROUND OF THE INVENTION

[0003] When establishing a secure communication channel between a client C and a server S through an intermediate such as a gateway G as shown in FIG. **1**, the client C and the server S don't pre-share a common secret.

[0004] Before establishing the secure communication channel between the client C and the server S, a mutual authentication between the server S and the client C occurred. The mutual authentication may be processed with any cryptographic protocol.

In the case where the mutual authentication comprises three steps: a terminal authentication step, a passive authentication step, and a chip authentication step as shown in FIG. **1**, the server S can be authenticated by the client C through the gateway G, relatively to a certification authority according to a Terminal Authentication protocol, and the client C which has a long-term/permanent secret key sk_c with its related public key pk_c such that pk_c can then be trusted by the remote server S according to a First part of a Passive Authentication/Client Authentication protocol.

[0005] As shown in FIG. **1**, a first secure channel between the client C and the gateway G and a second secure channel between the gateway G and the sever S may have been established. When the client C sends data to the remote server S through the gateway G, the gateway G has to decrypt and then encrypt data from a first protocol, used between the client C and the gateway G, to a second protocol used between the remote server S and the gateway G. The same happens when the remote server S sends data to the client C though the gateway G, which gateway G has to decrypt and then encrypt data from the second protocol used between the remote server S and the gateway G, to the first protocol used between the client C and the gateway G.

[0006] As a consequence, plaintext data are known by the gateway G. The problem of translating a protocol into another protocol through a gateway exposes the exchanged data between two communicating parties to a risk of eavesdropping and secrets re-usability whereby jeopardizing backward and forward secrecy, hence when a secret key is discovered by the attacker. If the gateway is compromised, someone could have access to the exchanged data in clear before the establishment of another secure channel.

[0007] Another problem is added when the client has a permanent secret key shared by a huge number of clients. By sharing the same permanent secret key, the privacy of the user is preserved as it is not possible to determine who's who, and a service provider can grant access to a client without knowing its identity. The service provider only knows that the client is an authorized client. The client can then authenticate to the server without identifying to the server. This authentication permanent secret key sk_c may also be used by the client C to establish a secure channel with the server S, and sk_c could be the only one secret value used by the client C to establish the secure channel. Then, if this permanent secret key sk_c is compromised for a client, all clients from the same lot which share the same permanent secret key may be easily attacked. Once the secret key is compromised, it is possible to open a secure channel and thus to compromise the confidentiality of data transmitted by the clients with the permanent secret key sk_c of the client.

[0008] This problem may occur for example when Web services are accessed with a client-middleware installed on the smartcard host which acts as a gateway G between the smartcard C and the remote server S.

[0009] One solution consists in using a secure IP-enabled reader equipped with a display unit and a PINpad; implementing a Password-Based-Mechanism also called PACE, implementing an interface device IFD-API interface according to ISO 24727 and supporting SOAP-interface for the communication with an application running on the smartcard host as described in the BSI TR-03131 v.1 EAC-Box Architecture and Interfaces Technical Guidelines. However this kind of solution has two main drawbacks: it may require a further mutual authentication between the enhanced reader and the smartcard host thereby raising again the issue of eavesdropping/man-in-the-middle and it represents a costly device.

SUMMARY OF THE INVENTION

[0010] The purpose of the invention is to provide a method for establishing a secure channel between a client C and a remote server S when the client C and the server S exchange data through an intermediate entity G.

[0011] For this purpose, an object of the invention is a method for establishing a secure communication channel between a client (C) and a remote server (S), said client (C) and remote server (S) exchanging data through an intermediate entity (G), said client (C) having a long-term key pair (sk_c,pk_c), said remote server generating an ephemeral key (sk_s,pk_s), the method comprising a mutual authentication step wherein the client (C) sends a public key (pk_c) of said long-term key pair (sk_c,pk_c) and the proof that said public key (pk_c) is valid to the server (S), and wherein the remote server (S) sends the public key (pk_s) of said ephemeral key pair (sk_s,pk_s) to the client (C), characterized in that the client (C) generates an ephemeral key pair (sk_{cc},pk_{cc}) and sends the public key (pk_{cc}) of said ephemeral key pair (sk_{cc},pk_{cc}) to the server (S) so as to generate a secret common to the client (C) and to the remote server (S) for opening the secure communication channel.

[0012] According to other aspects of the invention,

- **[0013]** the method for establishing a secure communication channel between a client (C) and a remote server (S) may comprise generating said common secret by the client (C) and by the server (S), said common secret being based on the ephemeral secret key (sk_{cc}) of said ephemeral key pair (sk_{cc},pk_{cc}) of the client (C);
- **[0014]** the method may comprise generating the common secret according to the Diffie-Hellman protocol;
- **[0015]** the method may comprise using a gateway or a middle-ware as intermediate entity (G);
- **[0016]** the method may comprise using a smartcard as client (C);
- **[0017]** the method may comprise using a middle-ware acting as a gateway (G) hosted on a smartcard host;

[0018] the method may comprise establishing a secure communication channel between the client (C) and the intermediate entity (G);

[0019] the method may comprise establishing a secure communication channel between the intermediate entity (G) and the remote server (S).

[0020] The invention solves the problem of man-in-the-middle attack in case of the exposure of a permanent secret key used to establish a secure channel.

[0021] There is neither need for an additional device nor an additional mutual authentication.

[0022] Thanks to the invention, a secure channel is established between the server S and the client C such that the gateway G cannot access to the plaintext data transmitted into the secure channel, even if the permanent secret key sk_c has been revealed.

[0023] The backward secrecy of the data transmitted into the established secure channel is assured: i.e. if one day the long-term key sk_c is compromised, then the confidentiality of the data that have been exchanged into the secure channel is still assured. It is not possible to open a secure channel even with the knowledge of key sk_c.

[0024] The forward secrecy of the data transmitted into a secure channel is assured, i.e. if one day the long-term key sk_c is compromised, then the confidentiality of the data that will be exchanged into a secure channel is assured.

[0025] Besides a man-in-the-middle attack does not allow to know the plaintext data transmitted into the secure channel.

[0026] The invention is now described, by way of example, with reference to the accompanying drawings. The specific nature of the following description should not be construed as limiting in any way the broad nature of this summary.

BRIEF DESCRIPTION OF THE DRAWINGS

[0027] In order that the manner in which the above recited and other advantages and features of the invention are obtained, a more particular description of the invention briefly described above will be rendered by reference.

[0028] Notwithstanding any other forms that may fall within the scope of the present invention, preferred forms of the invention will now be described, by way of example only, with reference to the accompanying drawing in which:

[0029] FIG. **1** schematically shows a flowchart of a method for establishing a secure channel according to the prior art.

[0030] FIG. **2** schematically shows a flowchart of a method for establishing a secure channel according to an embodiment of the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0031] The present invention may be understood according to the detailed description provided herein.

[0032] Shown in FIG. **2** is a flowchart of an embodiment of the method for establishing a secure channel between a client S, a gateway G and a remote server S.

[0033] In this embodiment, the client C is a smartcard with a middle-ware installed on a smartcard host. The middle-ware acts as a gateway between the smartcard C and a remote service S.

[0034] The method for establishing a secure communication channel between the client C and the remote server S comprises different steps.

[0035] The method comprises a step of mutual authentication between the client C and the server S. The mutual authentication comprises three main steps: a Terminal Authentication TA, a Passive Authentication PA and a Chip Authentication CA.

[0036] In the Terminal Authentication TA step: the server S with a long term authentication secret key $sk_{ServerAuth}$ and a long term certified public key $pk_{ServerAuth}$ is authenticated by the client C for example with a <<challenge-response>> protocol and the server S can compute an ephemeral key pair (sk_s,pk_s) such that the client C can be convicted that the public key $pk_{ServerAuth}$ has been chosen by the server S. Therefore, the server S generates the ephemeral key pair (sk_s,pk_s) and sends the public key pk_s or an element computed from pk_s to the client C.

[0037] The certificate of the public key $pk_{ServerAuth}$ of the server is also checked. The server authenticates the ephemeral public key pk_s to be used later on for the Chip Authentication CA step.

[0038] In the Passive Authentication PA step, data of the client are certified by a certification authority. A <<pseudo-certificate>> is sent by the client C to the remote server S so as to check the validity of the public key pk_c of the client. Therefore, the client C owns a long-term key pair (sk_c,pk_c) such that the public key pk_c of the client C is certified by the certification authority and the server S can be convicted that pk_c is valid. Therefore the client C sends the public key pk_c and the proof that the public key pk_c is valid to the remote server S.

[0039] In the Chip Authentication CA step: the client C is authenticated by the server S by verifying an authentication token computed from an exchanged Diffie-Hellman key so as the public key from client side is the long-term key pk_c certified during the passive authentication step PA and the public key from server side is the ephemeral key pk_s chosen by the server S during the terminal authentication step TA. The Diffie-Hellman key shared between the client C and the server S is used to compute or verify the authentication token and also to establish the secure channel. This Diffie-Hellman key is computed from pk_c and sk_s at the server side and from sk_c and pk_s at the client side.

[0040] Part of the public key pk_s generated by the remote server S is sent during the Terminal Authentication TA step. The complete key pk_s is sent from the server S to the client C in the chip authentication step CA.

[0041] The client C also generates an ephemeral key pair (sk_{cc},pk_{cc}) during the chip Authentication step CA and sends the public key pk_{cc} of said ephemeral key pair (sk_{cc},pk_{cc}) to the server S.

[0042] The client C calculates the common secret key as following:

$$K=\mathrm{KDF}(sk_c,pk_s,sk_{cc},pk_s)$$

[0043] The server is also calculates the common secret key as following:

$$K=\mathrm{KDF}(sk_s,pk_c,sk_s,pk_{cc})$$

[0044] where KDF is a Key Derivation Function.

[0045] According to the invention, the used protocol is the Diffie-Hellman protocol (DH or ECDH) and the used hash function Hash (e.g. SHA-1, SHA-224, or SHA-256) such that:

$$
\begin{aligned}
KDF(sk_c, pk_s, sk_{cc}, pk_s, \ldots) &= \text{Hash}\,(DH(sk_c, pk_s)\|DH(sk_{cc}, pk_s)\| \ldots) \\
&= \text{Hash}\,(pk_s^{skc}\|pk_s^{skcc}\| \ldots) \\
&= \text{Hash}\,(pk_c^{sks}\|pk_{cc}^{sks}\| \ldots) \\
&= \text{Hash}\,(DH(sk_s, pk_c)\|DH(sk_s, pk_{cc})\| \ldots) \\
&= KDF(sk_s, pk_c, sk_s, pk_{cc}, \ldots)
\end{aligned}
$$

[0046] The common secret generated by both the client C and the server S is partly based on the client key pair (sk_c,pk_c).

[0047] The secure channel can then be established with the common secret.

[0048] By doing so, the security impact is reduced significantly when the long-term secret of the client is compromised.

[0049] According to another embodiment, data are securely exchanged between the client and the gateway, and between the gateway and the remote server. Data are exchanged into a secure channel SC1 between the client C and the gateway G. A Password Based Mechanism such as PACE protocol is for example used between the client and the gateway G. This protocol is based on a common password and allows to derivate common session keys between the client C and the gateway G. These keys are then used for establishing a secure channel between the client C and the gateway G, chiefly when the client is a contactless card.

[0050] Data are exchanged into a secure channel SC2 between the remote server S and the gateway G, for example according to a protocol called SSL/TLS protocol.

[0051] It will be well understood that a smartcard with a middle-ware installed on a smartcard host is not a limited example. The invention can be advantageously applied to any web service deployment with a client-middleware installed in the dubious environment of a smartcard host such as a user's PC.

[0052] It also be understood that the middle-ware can be not installed onto the client host and therefore a gateway is provided between the client C and the remote service S.

[0053] This method can be easily incorporated on smart cards by re-using their existing libraries. The changes do not impact kernel cryto functions, only input values to these function may change.

1. A method for establishing a secure communication channel between a client (C) and a remote server (S), said client (C) and remote server (S) exchanging data through an intermediate entity (G), said client (C) having a long-term key pair (sk_c,pk_c), the method comprising: said remote server generating an ephemeral key (sk_s,pk_s), the method comprising a mutual authentication step wherein the client (C) sends a public key (pk_c) of said long-term key pair (sk_c, pk_c) and the proof that said public key (pk_c) is valid to the server (S), and wherein the remote server (S) sends the public key (pks) of said ephemeral key pair (sk_s, pk_s) to the client (C), the client (C) generates an ephemeral key pair (sk_{cc},pk_{cc}) and sends the public key (pk_{cc}) of said ephemeral key pair (sk_{cc},pk_{cc}) to the server (S) so as to generate a secret common to the client (C) and to the remote server (S) for opening the secure communication channel.

2. The method for establishing a secure communication channel between a client (C) and a remote server (S) according to claim **1**, comprising generating said common secret by the client (C) and by the server (S), said common secret being based on the ephemeral secret key (sk_{cc}) of said ephemeral key pair (sk_{cc},pk_{cc}) of the client (C).

3. The method for establishing a secure communication channel between a client (C) and a remote server (S) according to one of the previous claims, comprising generating the common secret according to the Diffie-Hellman protocol.

4. A method for establishing a secure communication channel between a client (C) and a remote server (S) according to claim **1** or **2**, comprising using a gateway or a middle-ware as intermediate entity (G).

5. A method for establishing a secure communication channel between a client (C) and a remote server (S) according to claim **1** or **2**, comprising using a smartcard as client (C).

6. A method for establishing a secure communication channel between a client (C) and a remote server (S) according to claim **5**, comprising using a middle-ware acting as a gateway (G) hosted on a smartcard host.

7. A method for establishing a secure communication channel between a client (C) and a remote server (S) according to claim **1** or **2**, comprising establishing a secure communication channel between the client (C) and the intermediate entity (G).

8. A method for establishing a secure communication channel between a client (C) and a remote server (S) according to claim **4**, comprising establishing a secure communication channel between the intermediate entity (G) and the remote server (S).

9. A method for establishing a secure communication channel between a client (C) and a remote server (S) according to claim **3**, comprising using a gateway or a middle-ware as intermediate entity (G).

10. A method for establishing a secure communication channel between a client (C) and a remote server (S) according to claim **3**, comprising using a smartcard as client (C).

11. A method for establishing a secure communication channel between a client (C) and a remote server (S) according to claim **4**, comprising using a smartcard as client (C).

* * * * *