

CLAIMS

1. A computer-implemented method, comprising:
 - receiving, by a server system, a client public key being part of a client asymmetric key pair from a client device;
 - sending, by the server system, a server public key being part of a server asymmetric key pair to the client device;
 - generating, by the server system, a random value master key;
 - sending, by the server system, the random value master key encrypted using the client public key being part of the client asymmetric key pair to the client device;
 - generating, by the server system, an initial unique session key, wherein generating the initial unique session key comprises:
 - generating a Base Derived Key (BDK) by a Hardware Security Module (HSM) associated with the server system;
 - receiving a Key Serial Number (KSN) associated with the client device, wherein the KSN at least comprises a session counter set to zero; and
 - generating the initial unique session key from the BDK and the KSN; and
 - sending, by the server system, the initial unique session key encrypted under the random value master key to the client device to derive a set of unique session keys by the client device, wherein a unique session key from the set of the unique session keys is used by the client device to encrypt a session data for transmission to the server system per session.
2. The method as claimed in claim 1, wherein a message authentication code (MAC) encrypted using a unique MAC key is sent to the server system along with the session data encrypted under the unique session key, the unique MAC key selected from a set of unique MAC keys derived by the client device from an initial unique MAC key generated by the server system.
3. The method as claimed in claim 2, wherein the set of unique MAC keys is derived from the initial unique MAC key based on a derived unique key per session.

4. The method as claimed in claim 2, wherein the unique MAC key is validated by the server system and wherein upon successful validation of the unique MAC key, the session data from the unique session key is decrypted.
5. The method as claimed in claim 1, further comprising receiving a public key being part of an asymmetric key pair, the asymmetric key pair belonging to a trusted security model, wherein the trusted security model is configured to:
 - send the public key being part of the asymmetric key pair to the client device,
 - certify the client public key by signing with a private key being part of the asymmetric key pair, and
 - certify the server public key by signing with the private key being part of the asymmetric key pair.
6. The method as claimed in claim 1, wherein the KSN and the initial unique session key are used by the client device to derive the set of the unique session keys, a unique session key from the set of unique session keys generated at least by incrementing the session counter of the KSN per session and wherein the initial unique session key is deleted after derivation of the set of unique session keys.
7. The method as claimed in claim 6, wherein the incremented session counter of the KSN is sent to the server system along with the session data encrypted under the unique session key for decryption of the session data from the unique session key.
8. The method as claimed in claim 1, wherein sending the random value master key encrypted using the client public key being part of the client asymmetric key pair to the client device further comprises:
 - certifying the encrypted random value master key by signing using a server private key being part of the server asymmetric key pair, wherein the encrypted random value master key is verified by the client device using the server public key being part of the server asymmetric key pair and wherein the encrypted random value master key is decrypted by the client device using a client private key being part of the client asymmetric key pair.

9. The method as claimed in claim 1, wherein the server system is one of a payment server, an acquirer server and an issuer server of a payment network and wherein the session data is one of a Personal Identification Number (PIN) of a payment card, a login ID, a password, a Card Verification Value (CVV) and a payment related data.

10. A server system, the server system comprising:

a communication interface configured to:

receive a client public key being part of a client asymmetric key pair from a client device, and

send a server public key being part of a server asymmetric key pair to the client device;

a memory comprising executable instructions;

a hardware security module (HSM) configured to:

generate a random value master key, and

generate an initial unique session key, wherein for generating the initial unique session key, the server system is further caused to:

generate a Base Derived Key (BDK) by the Hardware Security Module (HSM) associated with the server system;

receive a Key Serial Number (KSN) associated with the client device, wherein the KSN at least comprises a session counter set to zero; and

generate the initial unique session key from the BDK and the KSN; and

a processor communicably coupled to the communication interface, the processor

configured to execute the instructions to cause the server system to at least:

send the random value master key encrypted using the client public key being part of the client asymmetric key pair to the client device, and

send the initial unique session key encrypted under the random value master key to the client device to derive a set of unique session keys by the client device, wherein a unique session key from the set of the unique session keys is used by the client device to encrypt a session data for transmission to the server system per session.

11. The server system as claimed in claim 10, wherein a message authentication code (MAC) encrypted using a unique MAC key is sent to the server system along with the session data encrypted under the unique session key, the unique MAC key selected from a set of unique MAC keys derived by the client device from an initial unique MAC key generated by the server system.

12. The server system as claimed in claim 11, wherein the set of unique MAC keys is derived from the initial unique MAC key based on a unique derived key per session.

13. The server system as claimed in claim 11, wherein the unique MAC key is validated by the server system and wherein upon successful validation of the unique MAC key, the session data from the unique session key is decrypted.

14. The server system as claimed in claim 10, the server system is further caused to receive a public key being part of an asymmetric key pair, the asymmetric key pair belonging to a trusted security model, wherein the trusted security model is configured to:

- send the public key being part of the asymmetric key pair to the client device;
- certify the client public key by signing with a private key being part of the asymmetric key pair; and
- certify the server public key by signing with the private key being part of the asymmetric key pair.

15. The server system as claimed in claim 10, wherein the KSN and the initial unique session key are used by the client device to derive the set of the unique session keys, a unique session key from the set of unique session keys generated at least by incrementing the session counter of the KSN per session and wherein the initial unique session key is deleted after derivation of the set of unique session keys.

16. The server system as claimed in claim 10, wherein for sending the random value master key encrypted using a client public key being part of the client asymmetric key pair to the client device, the server system is further caused to:

- certify the encrypted random value master key by signing using a server private key

being part of the server asymmetric key pair wherein the encrypted random value master key is verified by the client device using the server public key being part of the server asymmetric key pair and wherein the encrypted random value master key is decrypted by the client device using a client private key being part of the client asymmetric key pair.

17. A computer-implemented method, comprising:

generating, by a server system, an initial unique MAC key using a Key Serial Number (KSN) of a client device and a Base Derived Key (BDK) generated by a Hardware Security Module (HSM) associated with the server system;

receiving, by the server system, a session data encrypted under a unique session key, a KSN with an incremented session counter and a Message Authentication Code (MAC) encrypted using a unique MAC key valid for a current session, wherein the unique MAC key is selected from a set of unique MAC keys derived by the client device from the initial unique MAC key received from the server system;

validating, by the server system, the unique MAC key using the KSN with the incremented session counter and the BDK; and

upon successful validation of the unique MAC key, decrypting, by the server system, the session data from the unique session key.

18. The method as claimed in claim 17, wherein the initial unique MAC key is generated using the KSN with the session counter set to zero.