CLAIMS

1. A computer-implemented method, comprising:

generating, by a server system, a cryptographic certificate, the cryptographic certificate comprising an asymmetric key pair;

generating, by the server system, a random value key, the random value key forming at least a part of a Content Encryption Key (CEK) to be generated by a web application;

sending, by the server system, the random value key to a client device running the web application over a secure network communication channel for generating the CEK, wherein the CEK is to be utilized for encrypting a content entered by a user of the web application on the client device and wherein the CEK is encrypted using a public key being part of the asymmetric key pair for transmission over the secure network communication channel; and

translating, by the server system, the CEK encrypted under the public key to CEK encrypted under a Local Master Key (LMK) using a private key, the private key being part of the asymmetric key pair.

2. The method as claimed in claim 1, wherein the private key is encrypted under the LMK of a Hardware Security Module (HSM).

3. The method as claimed in claim 1, wherein the random value key is a sixteen byte long key.

4. The method as claimed in claim 1, wherein the secure network communication channel is established according to at least one of: a Secure Socket Layer (SSL) protocol; and a Transport Layer Security (TLS) protocol.

5. The method as claimed in claim 1, further comprising:

sending the cryptographic certificate to the client device for retrieval of the public key being part of the asymmetric key pair; and

validating the cryptographic certificate prior to retrieving the public key.

6. The method as claimed in claim 5, wherein the cryptographic certificate is validated based on one or more parameters, the one or more parameters comprising:

validity of a start date and an end date of the cryptographic certificate;

validity of a certificate chain up to a subordinate certificate authority;

validity of certificate extension, a certificate revocation list (CRL), an Online Certificate Status Protocol (OCP), and a key usage frequency; and

validity of a distributed name.

7. The method as claimed in claim 1, wherein the CEK is generated by the web application at the client device by randomly selecting a predefined length key from a hash value of an intermediate key, wherein the hash value is generated using a hashing algorithm and wherein the predefined length key is 16 byte long.

8. The method as claimed in claim 7, wherein the intermediate key is generated by concatenating a self-generated key with the random value key, the self-generated key formed by the web application at the client device.

9. The method as claimed in claim 8, wherein the self-generated key is 16 byte long.

10. The method as claimed in claim 1, further comprising:

generating a content offset using the CEK encrypted under the LMK and content encrypted under the LMK.

11. The method as claimed in claim 10, wherein the content offset is matched with an original content entered by the user of the web application for validation.

12. The method as claimed in claim 1, wherein the content is a Personal Identification Number (PIN) of a payment card.

13. The method as claimed in claim 1, wherein the server system is a payment server of a payment network, and wherein the content includes at least one of a login ID, a

password, a Card Verification Value (CVV) and a payment related data.

14. A server system, the server system comprising:

a communication interface configured to establish a secure network communication channel with a client device running a web application;

a memory comprising executable instructions;

a hardware security module (HSM) configured to

generate a cryptographic certificate, the cryptographic certificate comprising an asymmetric key pair comprising a public key and a private key,

generate a random value key forming at least a part of a Content Encryption Key (CEK) to be generated by the web application, and

translate the CEK encrypted under the public key to CEK encrypted under a Local Master Key (LMK) using the private key; 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 key to the client device running the web application over the secure network communication channel for generating the CEK, wherein the CEK is to be utilized for encrypting a content entered by a user of the web application on the client device and wherein the CEK is encrypted using the public key of the asymmetric key pair for transmission over the secure network communication channel.

15. The server system as claimed in claim 14, wherein the private key is encrypted under the LMK of the HSM.

16. The server system as claimed in claim 14, wherein the secure network communication channel is established according to at least one of: a Secure Socket Layer (SSL) protocol; and a Transport Layer Security (TLS) protocol.

17. The server system as claimed in claim 14, wherein the server system is further caused to:

send the cryptographic certificate to the client device for retrieval of the public key being part of the asymmetric key pair; and

validate the cryptographic certificate prior to retrieving the public key.

18. The server system as claimed in claim 17, wherein the cryptographic certificate is validated based on one or more parameters, the one or more parameters comprising:

validity of a start date and an end date of the cryptographic certificate;

validity of a certificate chain up to a subordinate certificate authority;

validity of certificate extension, a certificate revocation list (CRL), an Online Certificate Status Protocol (OCP), and a key usage frequency; and

validity of a distributed name.

19. The server system as claimed in claim 14, wherein the CEK is generated by the web application at the client device by randomly selecting a predefined length key from a hash value of an intermediate key, wherein the hash value is generated using a hashing algorithm and wherein the predefined length key is a 16 byte long key.

20. A computer-implemented method, comprising:

generating, by a web application running on a client device, a self-generated key;

concatenating the self-generated key with a random value key to generate an intermediate key, the random value key received from a server system;

creating a hash value of the intermediate key using a hashing algorithm;

generating a CEK by randomly selecting a predefined length key from the hash value of the intermediate key;

encrypting a content under the CEK; and

encrypting the CEK using a public key being part of an asymmetric key pair for transmission over a secure network communication channel to the server system, wherein the public key is retrieved from a cryptographic certificate sent by the server system which generates the asymmetric key pair using a Hardware Security Module (HSM), and the server system translates the CEK encrypted under the public key to CEK encrypted under a Local Master Key (LMK) using a private key of the asymmetric key pair.