

CLAIMS

1. A computer-implemented method, comprising:

receiving, by a server system, a cryptographic service request from at least one application of a plurality of applications over a network communication channel, the cryptographic service request comprising a cryptographic operation to be performed, a Hardware Security Module Local Master Key (HSM LMK) identifier, and a cryptographic keys index, wherein the cryptographic keys index is an identifier of the at least one application and the HSM LMK identifier is an identifier of an HSM dedicated to the at least one application for performing the cryptographic operation;

generating, by the server system, a cryptographic operation command to perform the cryptographic operation;

sending, by the server system, the cryptographic operation command to the HSM identified by the HSM LMK identifier, the HSM configured to perform the cryptographic operation;

receiving, by the server system, a response from the HSM, the response indicative of a result of the performed cryptographic operation; and

sending, by the server system, the response to the at least one application over the network communication channel.

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

maintaining one or more cryptographic keys of the at least one application of the plurality of applications in a database, the one or more cryptographic keys identified using the cryptographic keys index received in the cryptographic service request;

fetching the one or more cryptographic keys based on the cryptographic operation to be performed;

sending the fetched one or more cryptographic keys along with the cryptographic operation command to the HSM; and

receiving the response from the HSM for the performed cryptographic operation, the cryptographic operation performed by the HSM the using the one or more

cryptographic keys.

3. The method as claimed in claim 2, wherein for the cryptographic operation being a translation of the one or more cryptographic keys from encrypted under an old Local Master Key (LMK) to be encrypted under a new Local Master Key (LMK), further comprising:

fetching the one or more cryptographic keys from the database;
sending the one or more cryptographic keys to the HSM for encrypting under the new LMK; and
sending the one or more cryptographic keys encrypted under the new LMK to the at least one application.

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

receiving one or more cryptographic keys of the at least one application of the plurality of applications along with the cryptographic service request;
sending the one or more cryptographic keys along with the cryptographic operation command to the HSM; and
receiving the response from the HSM for the performed cryptographic operation, the cryptographic operation performed by the HSM the using the one or more cryptographic keys.

5. The method as claimed in claim 4, wherein for the cryptographic operation being a translation of the one or more cryptographic keys from encrypted under an old Local Master Key (LMK) to be encrypted under a new Local Master Key (LMK), further comprising:

receiving the one or more cryptographic keys encrypted under the old LMK along with the cryptographic service request;
sending the one or more cryptographic keys encrypted under the old LMK to the HSM for encrypting under the new LMK; and
sending the one or more cryptographic keys encrypted under the new LMK to the at least one application.

6. The method as claimed in claim 1, wherein the cryptographic operation is one of a Personal Identification Number (PIN) verification, a Card Verification Value (CVV) verification, an Authorization Response Code (ARC) verification, an Authorization Response Cryptogram (ARPC) generation, an Authorization Request Cryptogram (ARQC) validation and a PIN translation.

7. The method as claimed in claim 1, wherein the cryptographic operation comprises testing one or more complex cryptographic functionalities of the HSM as a tester tool and wherein the one or more complex cryptographic functionalities of the HSM are one of an AKDS, an HSM Key block, an EMV issuing script, a Payment Card Industry (PCI) Mandate, a Terminal Line Encryption (TLE), a Secure Sockets Layer (SSL) protocol, and a Derived Unique Key per Transaction (DUKPT).

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

authenticating the at least one application prior to processing the cryptographic service request.

9. The method as claimed in claim 1, wherein the HSM LMK identifier is initially shared by the server system with the at least one application of the plurality of applications.

10. A server system, the server system comprising:

a communication interface;

a memory comprising executable instructions;

a hardware security module (HSM) identified by a Hardware Security Module Local Master Key (HSM LMK) identifier, the HSM configured to:

receive a cryptographic operation command generated to perform a cryptographic operation,

perform the cryptographic operation in response to receiving the cryptographic

operation command,
generate a response indicative of a result of the performed cryptographic operation;
and
a processor communicably coupled to the communication interface, the memory, and
the HSM, the processor configured to execute the instructions to cause the processor
to at least:
receive, via the communication interface, a cryptographic service request from at
least one application of a plurality of applications over a network communication
channel, the cryptographic service request comprising the cryptographic
operation to be performed, the HSM LMK identifier, and a cryptographic keys
index, wherein the cryptographic keys index is an identifier of the at least one
application, wherein the HSM is dedicated to the at least one application for
performing the cryptographic operation,
generate the cryptographic operation command to perform the cryptographic
operation,
transmit, via the communication interface, the cryptographic operation command to
the HSM,
receive, via the communication interface, the response from the HSM for the
performed cryptographic operation, and
send, via the communication interface, the response to the at least one application
over the network communication channel.

11. The server system as claimed in claim 10, wherein the processor is further caused
to:

maintain one or more cryptographic keys of the at least one application of the plurality
of applications in a database, the one or more cryptographic keys identified using
the cryptographic keys index received in the cryptographic service request;
fetch the one or more cryptographic keys based on the cryptographic operation to be
performed;
send the fetched one or more cryptographic keys along with the cryptographic operation
command to the HSM; and
receive the response from the HSM, the cryptographic operation performed by the HSM

the using the one or more cryptographic keys.

12. The server system as claimed in claim 11, wherein for the cryptographic operation being a translation of the one or more cryptographic keys from encrypted under an old Local Master Key (LMK) to be encrypted under a new Local Master Key (LMK), the processor is further caused to:

fetch the one or more cryptographic keys from the database;
send the one or more cryptographic keys to the HSM for encrypting under the new LMK; and
send the one or more cryptographic keys encrypted under the new LMK to the at least one application.

13. The server system as claimed in claim 10, wherein the processor is further caused to:

receive one or more cryptographic keys of the at least one application of the plurality of applications along with the cryptographic service request;
send the one or more cryptographic keys along with the cryptographic operation command to the HSM; and
receive the response from the HSM for the performed cryptographic operation, the cryptographic operation performed by the HSM the using the one or more cryptographic keys.

14. The server system as claimed in claim 13, wherein for the cryptographic operation being a translation of the one or more cryptographic keys from encrypted under an old Local Master Key (LMK) to be encrypted under a new Local Master Key (LMK), the processor is further caused to:

receive the one or more cryptographic keys encrypted under the old LMK along with the cryptographic service request;
send the one or more cryptographic keys encrypted under the old LMK to the HSM for encrypting under the new LMK; and
send the one or more cryptographic keys encrypted under the new LMK to the at least

one application.

15. The server system as claimed in claim 10, wherein the cryptographic operation comprises one of: a Personal Identification Number (PIN) verification; a Card Verification Value (CVV) verification; an Authorization Response Code (ARC) verification; an Authorization Response Cryptogram (ARPC) generation; an Authorization Request Cryptogram (ARQC) validation; and a PIN translation.

16. The server system as claimed in claim 10, wherein the cryptographic operation comprises testing one or more complex cryptographic functionalities of the HSM as a tester tool and wherein the one or more complex cryptographic functionalities of the HSM are one of: an AKDS; an HSM Key block; an EMV issuing script; a Payment Card Industry (PCI) Mandate; a Terminal Line Encryption (TLE); a Secure Sockets Layer (SSL) protocol; and a Derived Unique Key per Transaction (DUKPT).

17. The server system as claimed in claim 10, wherein processor is further caused to: authenticate the at least one application prior to processing the cryptographic service request.

18. The server system as claimed in claim 10, wherein the HSM LMK identifier is initially shared by the processor, via the communications interface, with the at least one application of the plurality of applications.

19. A computer-implemented method, comprising:

receiving, from an application by a payment server associated with a payment network, a cryptographic operation to be performed, a Hardware Security Module Local Master Key (HSM LMK) identifier, and cryptographic keys index over a network communication channel, the payment server comprising a microservice core engine and one or more Hardware Security Modules (HSMs), wherein the HSM LMK

identifier is an identifier of a selected HSM of the one or more HSMs that is dedicated to the application for performing the cryptographic operation;
generating, by the microservice core engine, a cryptographic operation command to perform the cryptographic operation,
sending, by the microservice core engine, the cryptographic operation command to the HSM identified by the HSM LMK identifier;
performing, by the identified HSM, the cryptographic operation,
sending, by the identified HSM, a response to the microservice core engine, the response being indicative of a result of the performed cryptographic operation; and
sending, by the payment server, the response to the application over the network communication channel.

20. The method as claimed in claim 19, wherein the network communication channel established between the payment server and the application is through a web service call using a Hyper Text Transfer Protocol Secure (HTTPS).