

CLAIMS

What is claimed is:

1. A system for providing a hardware security module extension having support for custom cryptographic operations, the system comprising:
 - an application execution server providing an application execution environment, the application execution server configured to
 - receive a cryptographic request associated with a custom cryptographic operation,
 - access key data from a hardware security module in response to receiving the cryptographic request,
 - execute, within the application execution environment, the custom cryptographic operation against the key data from the hardware security module, and
 - transmit a response to the cryptographic request.
2. The system of claim 1, wherein the application execution server is configured to receive the cryptographic request from a private network.
3. The system of claim 1, wherein the custom cryptographic operation includes at least one selected from a group consisting of padding plaintext data, encrypting data, splitting encrypted data, padding split encrypted data, further encrypting encrypted data, and joining data structures.
4. The system of claim 1, further comprising:
 - an event stream server providing an event stream, the event stream server configured to
 - receive an event associated with the cryptographic request,
 - store the event in a secure event storage, and
 - trigger a notification associated with the event to an event queue.
5. The system of claim 1, further comprising:

a data process execution server providing a data process execution environment, the data process execution server configured to

- access an event associated with the cryptographic request from an event queue,
- perform an action based on the cryptographic request, and
- output a result from performing the action.

6. The system of claim 5, wherein the action includes at least one selected from a group consisting of creation of key data, rotation of key data, deletion of key data, and specification of a key permission.

7. The system of claim 5, wherein the data process execution server is configured to output the result to the hardware security module, the result including an update to the key data of the hardware security module.

8. The system of claim 5, wherein the data process execution server is configured to output the result to a secure data storage, the result including an update to a cryptographic request log.

9. The system of claim 5, wherein the data process execution server does not have access to the key data of the hardware security module.

10. The system of claim 1, wherein the application execution server is configured to receive the cryptographic request from a customer server through an application programming interface gateway.

11. The system of claim 1, further comprising:
an application programming interface gateway configured to
receive the cryptographic request,
validate the cryptographic request, and
route the cryptographic request to the application execution server.
12. The system of claim 1, wherein the custom cryptographic operation is not a supported operation of the hardware security module.
13. A method for providing a hardware security module extension having support for custom cryptographic operations, the method comprising:
receiving, at an application execution environment, a cryptographic request associated with a custom cryptographic operation;
accessing key data from a hardware security module;
executing, within the application execution environment, the custom cryptographic operation against the key data from the hardware security module, wherein the custom cryptographic operation is not a supported operation of the hardware security module; and
transmitting a response to the cryptographic request.
14. The method of claim 13, wherein receiving the cryptographic request includes receiving the cryptographic request at an application programming interface gateway and routing, with the application programming interface gateway, the cryptographic request to an application execution server.
15. The method of claim 14, further comprising:
validating, with the application programming interface gateway, the cryptographic request prior to routing the cryptographic request to the application execution server.

16. The method of claim 13, further comprising:
enabling access to a secure data storage based on the execution of the custom cryptographic operation against the key data from the hardware security module,
wherein enabling access to the secure data storage includes at least one selected from a group consisting of reading data from the secure data storage and writing data to the secure data storage.
17. The method of claim 13, further comprising:
restricting access to a secure data storage based on the execution of the custom cryptographic operation against the key data from the hardware security module.
18. A non-transitory, computer-readable medium storing instructions that, when executed by an electronic processor, perform a set of functions, the set of functions comprising:
receiving, at an application execution environment, a plurality of cryptographic requests;
accessing key data from a hardware security module;
executing, within the application execution environment, at least one custom cryptographic operation against the key data from the hardware security module,
wherein that at least one custom cryptographic operation is associated with one or more of the plurality of cryptographic requests; and
transmitting a response based on the execution of the at least one custom cryptographic operation.

19. The computer-readable medium of claim 18, wherein the set of functions further comprises:

writing a plurality of events to a secure event storage of an event stream, wherein each of the plurality of events is associated with one of the plurality of cryptographic requests;

accessing, from the event stream, two or more events included in the plurality of events;

for each of the two or more events, performing, within a data process execution environment, an action associated with each of the two or more events using the hardware security module; and

outputting a result from performing the action for each of the two or more events.

20. The computer-readable medium of claim 18, wherein receiving the plurality of cryptographic requests includes receiving the plurality of cryptographic requests from different private networks.