WHAT IS CLAIMED IS:

1. A portable communication device comprising:

one or more processors; and

a memory coupled to the one or more processors and storing computer readable code, which when executed by the one or more processors, implements a software application having a function invoking software layer and a target software layer integrated within the same software application;

wherein the function invoking software layer is configured to:

send a start session request to the target software layer;

receive a session identifier (ID) from the target software layer;

generate a conversation key using the session ID and a key derivation function, wherein the conversation key is further generated based on an authorization key that is shared between the function invoking software layer and the target software layer;

encrypt a payload of a function invocation request using the conversation key, the payload containing a function call of a cryptogram generation function implemented in the target software layer; and

send the function invocation request including the encrypted payload to the target software layer; and

wherein the target software layer is configured to:

execute the cryptogram generation function being called in the function invocation request.

2. The portable communication device of claim 1, wherein the target software layer is further configured to:

generate the session ID in response to receiving the start session request from the function invoking software layer.

3. The portable communication device of claim 2, wherein the target software layer is further configured to:

generate the conversation key using the session ID and the key derivation function; and

decrypt the encrypted payload using the conversation key to retrieve the function call.

4. The portable communication device of claim 1, wherein the function invoking software layer is configured to send the start session request to the target software layer each time the application is launched.

5. The portable communication device of claim 1, wherein the function invoking software layer is configured to send the start session request to the target software layer each time the application is used to initiate a transaction.

6. The portable communication device of claim 1, wherein the target software layer is further configured to execute one of a token request function, or an account parameter replenishment request function.

7. The portable communication device of claim 1, wherein the target software layer is configured to ignore any request from the function invoking software layer that is not either a start session request or a function invocation request.

8. The portable communication device of claim 1, wherein the function invoking software layer is written in a first programming language, and the target software layer is written in a second programming language that is different than the first programming language.

9. A method of controlling access in a software application having a function invoking software layer and a target software layer integrated within the same software application, the method comprising:

sending, by the function invoking software layer of the software application, a start session request to the target software layer of the same software application;

receiving, by the function invoking software layer, a session identifier (ID) from the target software layer;

generating, by the function invoking software layer, a conversation key using the session ID and a key derivation function, wherein the conversation key is further generated based on an authorization key that is shared between the function invoking software layer and the target software layer;

encrypting, by the function invoking software layer, a payload of a function invocation request using the conversation key, the payload containing a function call of a cryptogram generation function implemented in the target software layer;

sending, by the function invoking software layer, the function invocation request including the encrypted payload to the target software layer to invoke the cryptogram generation function.

10. The method of claim 9, wherein the start session request is sent each time the application is launched.

11. The method of claim 9, wherein the start session request is sent each time the application is used to initiate a transaction.

12. The method of claim 9, wherein the target software layer further implements one of a token request function, or an account parameter replenishment request function.

13. A method of controlling access in a software application having a function invoking software layer and a target software layer integrated within the same software application, the method comprising:

receiving, by the target software layer of the software application, a start session request from the function invoking software layer of the same software application;

generating, by the target software layer, a session ID in response to the start session request;

sending, by the target software layer, the session ID to the function invoking software layer;

generating, by the target software layer, a conversation key using the session ID and a key derivation function, wherein the conversation key is further generated based on an authorization key that is shared between the function invoking software layer and the target software layer;

receiving, by the target software layer, a function invocation request including an encrypted payload containing a function call of a cryptogram generation function implemented in the target software layer;

decrypting, by the target software layer, the encrypted payload using the conversation key to retrieve the function call; and

executing, by the target software layer, the cryptogram generation function of the function call.

14. The method of claim 13, wherein the start session request is received each time the application is launched.

15. The method of claim 13, wherein the start session request is received each time the application is used to initiate a transaction.

16. The method of claim 13, wherein the target software layer further implements one of a token request function, or an account parameter replenishment request function.

17. The method of claim 13, wherein the target software layer ignores any request from the function invoking software layer that is not either a start session request or a function invocation request.