

WHAT IS CLAIMED IS:

1 1. A communication device comprising:
2 a processor; and
3 a memory coupled to the processor, the memory storing instructions, which when
4 executed by the processor, causes the communication device to perform operations
5 including:
6 during initialization of an application on the communication device:
7 sending a set of device identifiers associated with the communication
8 device to a server;
9 receiving a server-generated dynamic device identifier that is generated
10 by the server based on the set of device identifiers;
11 storing the server-generated dynamic device identifier;
12 receiving a nonce value from the server; and
13 deriving a device derived key based on the nonce value; and
14 during runtime execution of the application:
15 receiving a cryptogram key that is encrypted by the server using the
16 device derived key, wherein the cryptogram key is used as an encryption key by
17 the application to encrypt data to generate a cryptogram for the communication
18 device;
19 receiving, by the application, a request to execute an application specific
20 task including generation of the cryptogram; and
21 in response to receiving the request:
22 generating, by the application, a runtime dynamic device identifier;
23 determining whether the runtime dynamic device identifier matches
24 the server-generated dynamic device identifier;
25 executing the application specific task including generation of the
26 cryptogram using the cryptogram key when the runtime dynamic device
27 identifier matches the server-generated dynamic device identifier; and
28 preventing the application specific task from being executed when
29 the runtime dynamic device identifier does not match the server-generated
30 dynamic device identifier.

1 2. The communication device of claim 1, wherein the server-generated
2 dynamic device identifier from the server is encrypted by the server using the device
3 derived key.

1 3. The communication device of claim 1, wherein the server-generated
2 dynamic device identifier is a hash value computed over at least a portion of the set of
3 device identifiers and a salt value.

1 4. The communication device of claim 3, wherein the operations further
2 include:

3 during the initialization of the application:

4 receiving, by the application, the salt value that the server used for
5 generating the server-generated dynamic device identifier.

1 5. The communication device of claim 1, wherein the set of device identifiers
2 sent to the server is encrypted by the application using a server public key that is
3 embedded in the application.

1 6. The communication device of claim 1, wherein the application is
2 partitioned into a first software layer written in a first programming language and a
3 second software layer written in a second programming language.

1 7. The communication device of claim 6, wherein the server-generated
2 dynamic device identifier is stored in the first software layer of the application, and the
3 runtime dynamic device identifier is generated by the second software layer.

1 8. The communication device of claim 1, wherein the application is a
2 transaction application, and the cryptogram is used for authorizing a transaction being
3 conducted with the communication device.

1 9. A method comprising:

2 during initialization of an application on a communication device:

3 sending, by the application, a set of device identifiers associated with the
4 communication device to a server;

5 receiving, by the application and from the server, a server-generated
6 dynamic device identifier that is generated based on the set of device identifiers;
7 storing, by the application, the server-generated dynamic device identifier;
8 receiving a nonce value from the server; and
9 deriving a device derived key based on the nonce value;
10 during runtime execution of the application:
11 receiving a cryptogram key that is encrypted by the server using the
12 device derived key, wherein the cryptogram key is used as an encryption key by
13 the application to encrypt data to generate a cryptogram for the communication
14 device;
15 receiving, by the application, a request to execute an application specific
16 task including generation of the cryptogram; and
17 in response to receiving the request:
18 generating, by the application, a runtime dynamic device identifier;
19 determining whether the runtime dynamic device identifier matches
20 the server-generated dynamic device identifier;
21 executing the application specific task including generation of the
22 cryptogram using the cryptogram key when the runtime dynamic device
23 identifier matches the server-generated dynamic device identifier; and
24 preventing the application specific task from being executed when
25 the runtime dynamic device identifier does not match the server-generated
26 dynamic device identifier.

1 10. The method of claim 9, wherein the server-generated dynamic device
2 identifier received from the server is encrypted by the server using the device derived
3 key.

1 11. The method of claim 9, wherein the server-generated dynamic device
2 identifier is a hash value computed over at least a portion of the set of device identifiers
3 and a salt value.

1 12. The method of claim 11, further comprising:

2 during the initialization of the application:

3 receiving, by the application, the salt value that the server used for
4 generating the server-generated dynamic device identifier.

1 13. The method of claim 9, wherein the set of device identifiers sent to the
2 server is encrypted by the application using a server public key that is embedded in the
3 application.

1 14. The method of claim 9, wherein the application is partitioned into a first
2 software layer written in a first programming language and a second software layer
3 written in a second programming language.

1 15. The method of claim 14, wherein the server-generated dynamic device
2 identifier is stored in the first software layer of the application, and the runtime dynamic
3 device identifier is generated by the second software layer.

1 16. The method of claim 9, wherein the application is a transaction
2 application, and the cryptogram is used for authorizing a transaction being conducted
3 with the communication device.

1 17. The communication device of claim 1, wherein the cryptogram key is a
2 limited-use key that is associated with a set of one or more limited-use thresholds that
3 limits usage of the limited-use key.

1 18. The communication device of claim 17, wherein the set of one or more
2 limited-use thresholds includes a predetermined number of transactions for which the
3 limited-use key is valid.

1 19. The method of claim 9, wherein the cryptogram key is a limited-use key
2 that is associated with a set of one or more limited-use thresholds that limits usage of
3 the limited-use key.

1 20. The method of claim 19, wherein the set of one or more limited-use
2 thresholds includes a predetermined number of transactions for which the limited-use
3 key is valid.