

CLAIMS

What is claimed is:

- 1 1. A method, comprising:
 - 2 receiving, by a field server, a notification that a software update is sent to a
 - 3 device, the field server for authenticating that software of the device is secure;
 - 4 setting, by the field server, a flag that indicates an association between the
 - 5 device and the software update in a memory based at least in part on receiving the
 - 6 notification;
 - 7 receiving, from the device, a connection request that comprises a certificate
 - 8 associated with a first key for authenticating the device;
 - 9 determining that the first key received from the device is invalid based at least
 - 10 in part on receiving the connection request;
 - 11 determining the first key as valid based at least in part on the flag indicating
 - 12 the association; and
 - 13 establishing a connection between the device and a service based at least in
 - 14 part on determining the first key as valid.
- 1 2. The method of claim 1, further comprising:
 - 2 storing the first key in a list in the memory based at least in part on
 - 3 determining the first key as valid based at least in part on the flag.
- 1 3. The method of claim 2, further comprising:
 - 2 receiving an updated certificate associated with the device after the software
 - 3 of the device is updated; and
 - 4 updating a certificate associated with the device stored by the field server
 - 5 based at least in part on receiving the updated certificate.
- 1 4. The method of claim 3, further comprising:
 - 2 processing an additional connection request from the device based at least in
 - 3 part on determining the first key as valid.

1 5. The method of claim 1, further comprising:
2 identifying a discrepancy between the certificate associated with the first key
3 and a certificate associated with the device based at least in part on receiving the connection
4 request; and
5 validating the connection request regardless of the discrepancy based at least
6 in part on the flag, wherein determining the first key is valid is based at least in part on
7 validating the connection request.

1 6. The method of claim 1, further comprising:
2 comparing the certificate associated with the first key to a certificate stored by
3 the field server; and
4 authenticating the device for access to an application platform based at least in
5 part on comparing the certificate associated with the first key and the certificate.

1 7. The method of claim 6, further comprising:
2 validating a subscription to the service based at least in part on authenticating
3 the device.

1 8. The method of claim 6, wherein the authenticating allows the device to
2 communicate with the application platform and subscribe to the service.

1 9. The method of claim 1, wherein the certificate associated with the first
2 key received from the device is based at least in part on a hash of the software of the device.

1 10. The method of claim 1, further comprising:
2 transmitting, to the device, an acknowledgement message or a negative
3 acknowledgement message indicating whether the first key is valid based at least in part on
4 receiving the connection request.

1 11. A method, comprising:
2 identifying, by a first server, a software update for a device;
3 transmitting, to a second server for authenticating that software of the device
4 is secure, a notification that the software update is sent to the device based at least in part on
5 identifying the software update; and

6 transmitting, to the device, the software update based at least in part on
7 identifying the software update for the device.

1 12. The method of claim 11, further comprising:
2 receiving, from the device, a completion message indicating that the device
3 performed the software update; and
4 transmitting an updated certificate associated with the device based at least in
5 part on receiving the completion message.

1 13. The method of claim 11, wherein the notification is for identifying that
2 a certificate associated with a key received from the device is altered based at least in part on
3 the software update.

1 14. The method of claim 11, further comprising:
2 configuring a portion of the device to operate in an append write mode based
3 at least in part on transmitting the software update.

1 15. The method of claim 14, further comprising:
2 appending additional information to the software based at least in part on
3 configuring the portion of the device to operate in the append write mode;
4 preventing access to a version of the software available prior to the software
5 update based at least in part on appending the additional information; and
6 updating a key received from the device based at least in part on appending the
7 additional information.

1 16. A system, comprising:
2 a first server configured to;
3 identify a software update for a device;
4 transmit a notification that the software update is sent to the device
5 based at least in part on identifying the software update; and
6 a second server in electronic communication with the first server and
7 configured to;
8 receive the notification that the software update is sent to the device;
9 set a flag that indicates an association between the device and the
10 software update in a memory based on least in part on receiving the notification;

11 receive a connection request that comprises a certificate associated
12 with a first key for authenticating the device; and
13 accept the first key as valid based at least in part on the flag indicating
14 the association.

1 17. The system of claim 16, further comprising:
2 the device in electronic communication with the first server and the second
3 server, the device is configured to;
4 receive the software update; and
5 perform the software update based at least in part receiving the software
6 update.

1 18. The system of claim 17, wherein the device is further configured to:
2 hash software of the device; and
3 generate the first key based at least in part on the hash of the software and a
4 device-specific secret.

1 19. The system of claim 17, wherein the device is further configured to:
2 determine the connection request that comprises the certificate associated with
3 the first key for authenticating the device based at least in part on performing the software
4 update.

1 20. The system of claim 16, wherein the second server is further
2 configured to:
3 identify that the first key received from the device is invalid based at least in
4 part on receiving the connection request.

1 21. The system of claim 16, wherein the second server is further
2 configured to:
3 compare the certificate associated with the first key to a certificate associated
4 with the device; and
5 perform an authentication procedure for the device to access an application
6 service based at least in part on comparing certificate associated with the first key to the
7 certificate.

- 1 22. The system of claim 16, wherein the first server is further configured
2 to:
3 transmit an updated certificate associated with the device after the software
4 update of the device is completed.