CLAIMS

1. A method, comprising:

receiving, by a field server, a notification that a software update is sent to a device, the field server for authenticating that software of the device is secure;

setting, by the field server, a flag that indicates an association between the device and the software update in a memory based at least in part on receiving the notification;

receiving, from the device, a connection request that comprises a certificate associated with a first key for authenticating the device;

determining that the first key received from the device is invalid based at least in part on receiving the connection request;

determining the first key as valid based at least in part on the flag indicating the association; and

establishing a connection between the device and a service based at least in part on determining the first key as valid.

2. The method of claim 1, further comprising:

storing the first key in a list in the memory based at least in part on determining the first key as valid based at least in part on the flag.

3. The method of claim 2, further comprising:

receiving an updated certificate associated with the device after the software of the device is updated; and

updating a second certificate associated with the device stored by the field server based at least in part on receiving the updated certificate.

4. The method of claim 3, further comprising:

processing an additional connection request from the device based at least in part on determining the first key as valid.

5. The method of claim 1, further comprising:

identifying a discrepancy between the certificate associated with the first key and a second certificate associated with the device based at least in part on receiving the connection request; and

validating the connection request regardless of the discrepancy based at least in part on the flag, wherein determining the first key is valid is based at least in part on validating the connection request.

6. The method of claim 1, further comprising:

comparing the certificate associated with the first key to a second certificate stored by the field server; and

authenticating the device for access to an application platform based at least in part on comparing the certificate associated with the first key and the second certificate.

7. The method of claim 6, further comprising:

validating a subscription to the service based at least in part on authenticating the device.

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

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

10. The method of claim 1, further comprising:

transmitting, to the device, an acknowledgement message or a negative acknowledgement message indicating whether the first key is valid based at least in part on receiving the connection request.

11. A system, comprising:

a first server device configured to:

identify a software update for a device; and

transmit a notification that the software update is sent to the device based at least in part on identifying the software update; and

a second server device in electronic communication with the first server device and configured to:

receive the notification that the software update is sent to the device;

set a flag that indicates an association between the device and the software update in a memory based on least in part on receiving the notification;

receive a connection request that comprises a certificate associated with a first key for authenticating the device;

determine that the first key received from the device is invalid based at least in part on receiving the connection request; and

determine the first key as valid based at least in part on the flag indicating the association.

12. The system of claim 11, further comprising:

the device in electronic communication with the first server device and the second server device, wherein the device is configured to:

receive the software update; and

perform the software update based at least in part on receiving the software update.

13. The system of claim 12, wherein the device is further configured to:

hash software of the device; and

generate the first key based at least in part on the hash of the software and a device-specific secret.

14. The system of claim 12, wherein the device is further configured to:

determine the connection request that comprises the certificate associated with the first key for authenticating the device based at least in part on performing the software update.

15. The system of claim 11, wherein the second server device is further configured to:

compare the certificate associated with the first key to a second certificate associated with the device; and

perform an authentication procedure for the device to access an application service based at least in part on comparing the certificate associated with the first key to the second certificate.

16. The system of claim 11, wherein the first server device is further configured to:

transmit an updated certificate associated with the device after the software update of the device is completed.