February 2023

M2M Communication Security Enhancement Using Additional Short-lived Certificate

Igor Gariev

M2M Communication Security Enhancement Using Additional Short-lived Certificate

ABSTRACT

Device certificates enable machine-to-machine (M2M) communication. Device certificates can have long lives, e.g., as long as thirty years. The long life of a device certificate can leave a device open to security breaches, e.g., when a future, sophisticated attack makes the device itself vulnerable, rooted, or otherwise insecure. This disclosure describes techniques that enable devices with long-lived certificates to enjoy secure M2M communication for purposes such as digital unlocking of and access to high-value assets, through the use of additional (parallel), short-lived device certificates. The long-lived certificate, issued by the original equipment manufacturer (OEM) of the device, attests to the secure element of the device. The short-lived certificate, issued by the OEM of the device operating system for the same public key as that of the long-lived certificate, attests to the secure status of the device.

KEYWORDS

- Certificate authority (CA)
- Long-lived certificate
- Short-lived certificate
- Trusted element
- Machine-to-machine communication (M2M)
- Chain of trust
- Cross-signing
- Original equipment manufacturer (OEM)
- Car connectivity consortium

BACKGROUND

Certificates associated with devices such as smartphones, automobiles, etc. are referred to as "device certificates." Device certificates enable machine-to-machine (M2M) communication. Device certificates can have long lives, e.g., as long as thirty years. The long life of a device certificate can leave a device open to security breaches, e.g., when a future, sophisticated attack makes the device itself vulnerable, rooted, or otherwise insecure.

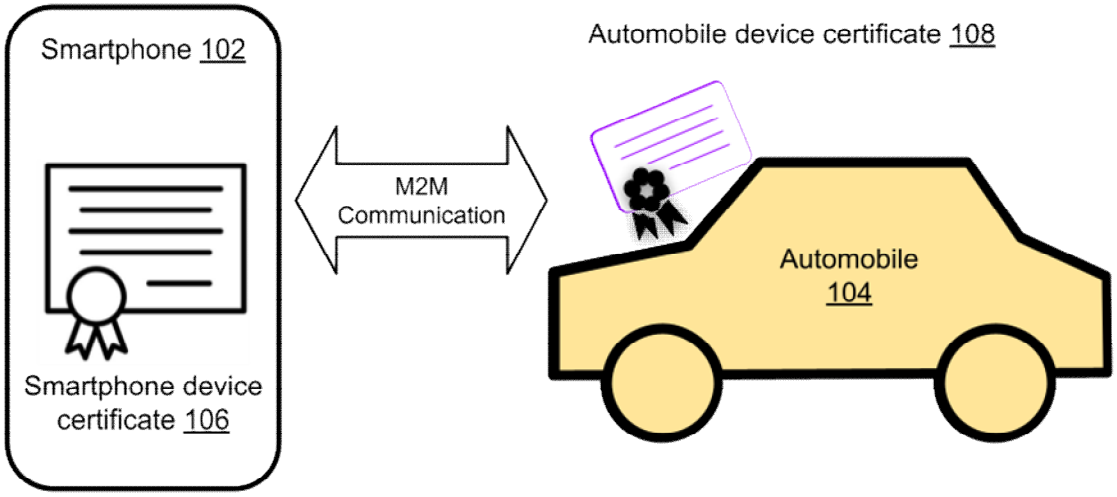

Fig. 1: An example of M2M communications using device certificates for authentication

Fig. 1 illustrates an example of M2M communications that relies on device certificates to authenticate the communicating machines to each other. A smartphone (102) can act, upon user command, as a car key to unlock or start an automobile (104) or another high-value asset. For this purpose, the smartphone and the automobile each have device certificates (104, 106) that are used for mutual authentication. In addition to authentication, each of the communicating machines can use the certificates to verify that the other machine has a secure element (e.g., a chip protected from unauthorized access), that the other machine is not rooted or otherwise tampered with, and that the other machine has a valid version of its operating system. In this

example, if the smartphone device certificate is long-lived, it is possible for the device to be compromised, e.g., rooted, without its certificate showing signs of tampering. This can leave the other device - the automobile - vulnerable to theft or other forms of adverse activity.

DESCRIPTION

This disclosure describes techniques that enable devices with long-lived certificates to enjoy secure M2M communication for purposes such as digital unlocking of and access to high-value assets, through the use of additional (parallel), short-lived device certificates.

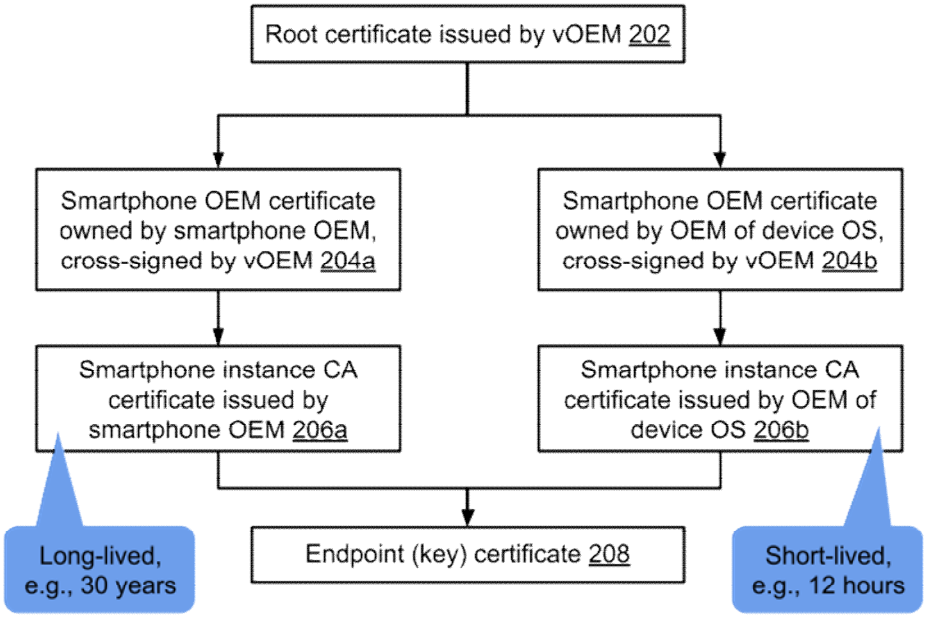

Fig. 2: Security enhancement via the use of an additional, short-lived certificate

Fig. 2 illustrates the generation of an additional short-lived certificate to enhance security, per techniques of this disclosure. The traditional pathway of generating a long-lived certificate, e.g., using a root certificate (202), typically issued by the original equipment manufacturer (OEM) of a high-value asset, e.g., a vehicle OEM (vOEM) to cross-sign a device-OEM certificate (204a, typically issued by the OEM of a device, e.g., a smartphone) to generate a long-

lived, device-instance CA certificate (206a) continues to be in use. A CA certificate is a digital certificate issued by a certificate authority (CA).

In addition, the root certificate issued by the vOEM is used to cross-sign a device-OEM certificate (204b; e.g., owned by the operating system of the device and stored in a keystore within its secure element). A short-lived (e.g., having a lifetime of 12 hours), device-instance CA certificate (206b) is issued by the OEM of the device OS. An endpoint certificate or key (208) is generated based on the short-lived and long-lived certificates. The long-lived certificate issued by the device OEM attests to the secure element of the device, while the short-lived certificate (for the same public key) attests to the status of the device.

The high-value asset (vehicle), which has a copy of the root certificate, validates the endpoint certificate, and, if the validation is successful, unlocks the high-value asset. Validation can be performed either at the vehicle or at a server maintained by the vehicle OEM. The short-lived and long-lived device-instance certificates are both for the same public key but have different durations. The device-OEM and the device-instance certificates can be sent to a vOEM server as necessary, for example to track and audit the number of outstanding digital keys for the vehicle (or another high-value asset). During validation, the vehicle or the vOEM server verifies the device attestation, device-instance certificate, etc.

When the user triggers the regeneration of a key to the high-value asset, the long-lived certificate is validated to attest to the secure element of the device and the short-lived certificate is validated to attest to the status of the device. If either of these validations fail, the request for the new key is denied; if both pass, the key is regenerated. In this manner, key creation on non-secure devices is forestalled.

Some advantages of the described techniques include:

- Reuse of existing application programming interfaces (APIs), for both device-to-server and server-to-server communication; no requirement of investment into the development of new APIs.
- Reuse of the existing framework of device verification, e.g., the issuance of short-lived, device-instance CA certificates to secure devices by checking a recent device attestation.
- Reuse of existing key verification procedures at the vOEM server.

CONCLUSION

This disclosure describes techniques that enable devices with long-lived certificates to enjoy secure M2M communication for purposes such as digital unlocking of and access to high-value assets, through the use of additional (parallel), short-lived device certificates. The long-lived certificate, issued by the original equipment manufacturer (OEM) of the device, attests to the secure element of the device. The short-lived certificate, issued by the OEM of the device operating system for the same public key as that of the long-lived certificate, attests to the secure status of the device.

REFERENCES

[1] Hsu, Yung-Kao, and Stephen Seymour, "Intranet security framework based on short-lived certificates," *Proceedings of IEEE 6th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises*, pp. 228-234. IEEE, 1997.

[2] Topalvic, Emin, Brennan Saeta, Lin-Shung Huang, Collin Jackson, and Dan Boneh, "Towards short-lived certificates," available online at https://cseweb.ucsd.edu/~dstefan/cse127-winter19/papers/topalovic:towards.pdf, accessed Jan. 25, 2023.