SONY

# Secure provisioning with Criotive

**Manage connected device credentials securely over-the-air**

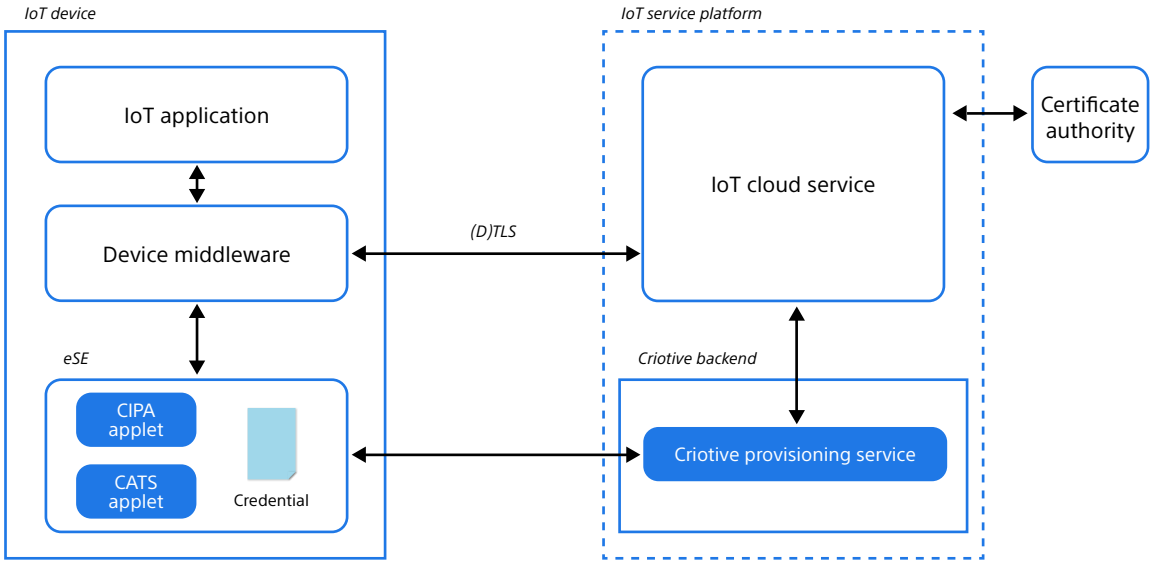
## Challenge

The communication between an IoT device and a backend IoT platform is often secured by a mutual authentication using a combination of certificates and transport layer security (TLS). It must be possible for these certificates to be provisioned over-the-air (OTA) in a way that prevents the data becoming visible to unauthorised people, and to update and revoke them with ease whenever necessary. None of this functionality should be lost or compromised if a customer decides to change to his/her connectivity solution (by adding, for instance, a Wi-Fi-only version of an LTE IoT product).

## Solution

The Criotive IoT provisioning solution addresses these challenges by managing the certificate lifecycle in the secure element embedded in the IoT device. Secret data are either injected during production of the IoT device in a secure environment, or using our special solution for non-secured environments.

CRIOTIVE




## Technology

The Criotive solution includes an identity and provisioning applet (CIPA) and an applet for transport security (CATS).

The CIPA applet is located in its own security domain and is used to load, install and provision other applets in the same domain. Encrypted scripts are sent to the CIPA from the Criotive backend, over a secure session.

The CATS applet, which is located inside the CIPA applet, stores TLS certificates. These are validated against intermediate certificates, all the way to the root certificate.

The cloud-based Criotive backend is creating encrypted scripts, permitting the CIPA to provision other applets and manage its certificates.

Criotive also includes APIs which means IoT platforms can specify the certificate data to be sent to the CIPA on a particular IoT device - regardless of whether the certificate is new or revoked.

## To whom is Criotive secure provisioning relevant?

- **IoT platform providers:** Companies that want to incorporate secure provisioning capabilities into their existing IoT management system and offer their customers a secure certificate update service - perhaps even an automated process. Also, those looking for a complement to the IoT SAFE standard, in order to securely provision devices which don't have a SIM card.
- **Customers:** Any company for whom connected devices and device security are business critical, that want a secure way of managing the certificate lifecycle of their installed base. Criotive's IoT Provisioning solution communicates directly with the secure element, allowing certificates to be updated securely OTA. The certificate update process can also be automated, further reducing the risks of a security breach while reducing manual work.
- **IoT device manufacturers:** Companies that want to increase the relevance of their products, by preparing them for secure TLS sessions and certificate storage and making it possible for customers to take advantage of secure certificate updates in the future.

August/2020

## Facts

(D)TLS version supported TLS 1.2, TLS 1.3
Algorithms PKI & PSK (PSK Plain, PSK ECDHE)
Embedded secure element GP 2.3 or higher

Criotive from Sony is a flexible solution for secure provisioning of connected devices over the air. The platform is end-to-end encrypted, based on open standards, network and vendor-agnostic and fully scalable. Specific solutions based on Criotive secure provisioning are: IoT Provisioning, a mechanism whereby owners of IoT devices can add, update or revoke certificates and keys in a completely secure manner, and Access Management which enables the distribution of time and place-restricted access rights, boosting the security of physical spaces.

*info@criotive.com*