Case study

Secure key management for embedded systems

The motivation: Securing the Internet of Things

Across industries, increasing connectivity of devices allows new functions, and new software-based business models generate great opportunities. Embedded devices are used in automotive, the heavy industry, in medical implants, as well as in industrial and home automation. These embedded devices are connected to the Internet of Things (IoT). This makes them a potential target for hackers, potentially resulting in significant financial damages for companies, not to mention the loss of trust and image in the eyes of the customers.

One way of mitigating these risks is the use of encryption. The management of cryptographic keys, i.e. the generation, distribution, storage, and recall of keys for embedded systems is here the most challenging task. Traditional solutions from the PC world cannot be adapted easily, because they require an active user and were designed for high-performance systems. Embedded devices, however, have a relatively low computing power and a long product cycle accompanied by unlimited physical access by the user. All this increase the aforementioned risks of abuse.

A common use case for a key management system is to secure device communication within the IoT. In order to protect the communication between the devices and the backend from unauthorized access, manipulation and espionage, devices need to be accessible only after authentication. For secure this authentication individual certificates are used per device and user; all issued by a Certificate Authority (CA).

The challenge: Secure device communication

The private key of the CA from which all other keys are derived, must be protected under all circumstances, so that only authorized system components and user can produce keys to the secure device communication. To store the private key securely, an HSM needs to be used in the backend of the Key Management System.

The solution: ESCRYPTs CycurKEYS based on Utimaco HSMs

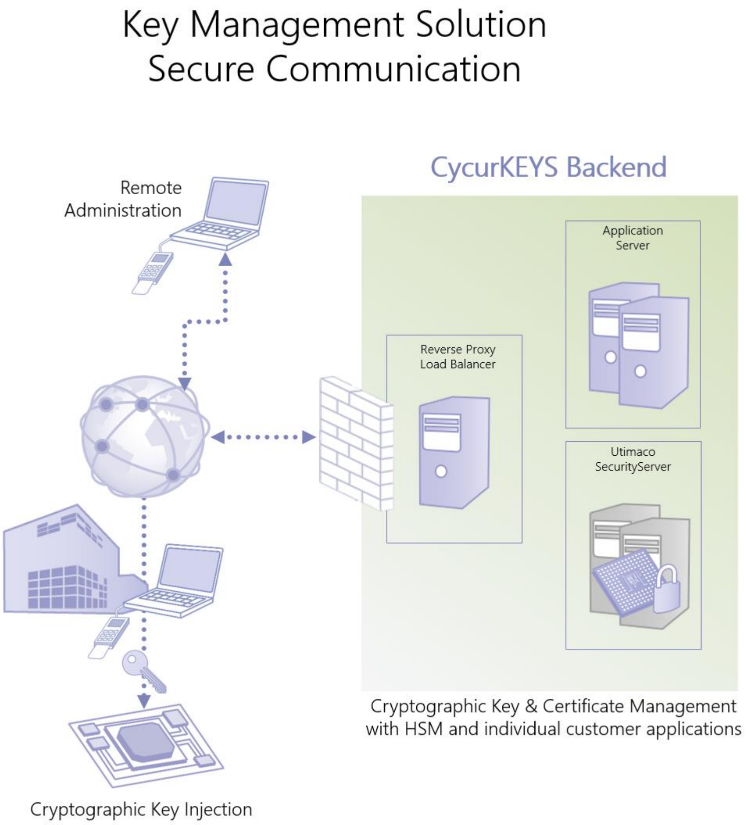
The Key Management Solution from ESCRYPT provides a fully automated process, the devices allows for secure communication with each other, even if they were not previously known to each other. It is based on a cryptographic Key Management system perfectly suited to embedded devices, a dedicated software for Identity Management and communication security. Certificates are automatically injected into the device during production via a secure connection. (They can be renewed during the lifetime of the device). Thanks to these certificates, devices can be authenticated with the help of the appropriate software, and communication channels are encrypted. The backend of this ESCRYPT solution (CycurKEYS) consists of multiple servers for a high level of security ("Defense in depth") and availability.

In addition, hardware security modules are used to ensure the secure storage of all keys and their secured use during the relevant transactions. The key material never leaves the secure environment of the HSM.

The implementation: Securing the Backend

To ensure the highest possible security for the application and storage of cryptographic key material ESCRYPT uses the SecurityServer of UTIMACO.

Also in the context of safety-related device communication, for example in automotive use cases like V2X-communication or in vehicle firmware updates (Over-the-air-updating), the Utimaco SecurityServer is used as the back end of the ESCRYPT Key Management Solution as a safety anchor. Using the comfortable development environment, the CryptoServer SDK, the security experts of ESCRYPT have implemented a customized firmware module to ensure a comprehensive and flexible rights management.


Key Management Solution
Secure Communication
CycurKEYS Backend
Remote Administration
Application Server
Reverse Proxy Load Balancer
Utimaco SecurityServer
Cryptographic Key & Certificate Management with HSM and individual customer applications
Cryptographic Key Injection

About ESCRYPT

Embedded Security is the leading system provider for embedded security world-wide. With locations in Germany, UK, Sweden, USA, Canada, India, China, Korea, and Japan, we have security specialists available to help with current security topics such as secure M2M-communication, IT-security in the Internet of Things, protection of e-business models and automotive security and they develop highly secure, worldwide valued products and solutions which are tailored to the specific requirements of embedded systems and the relevant IT-infrastructure and are tested and proven a million times in automotive series production. ESCRYPT is a subsidiary of ETAS GmbH, a wholly owned subsidiary of the BOSCH Group. For more information, visit www.escrypt.com/home/

About Utimaco

Utimaco is a leading manufacturer of hardware security modules (HSMs) that provide the Root of Trust to the IoT. We keep your cryptographic keys and digital identities safe to protect critical digital infrastructures and high value data assets. Utimaco delivers a general purpose HSM as a customizable platform to easily integrate into existing software solutions or enable the development of new ones. With professional services, we also support our partners in the implementation of their solutions. Put your trust in Utimaco – today and in the future. For more information, visit hsm.utimaco.com