Embedded devices are ubiquitous in today’s world. They are used heavily in several industries, such as automotive, heavy equipment, medical implants, industrial automation, and home automation. Embedded devices are being connected to the Internet of Things, exposing them to the multitude of attacks that could be launched by malicious hackers causing enormous financial loss and damage to the reputation of these industries.

Cryptographic key management that includes generation, distribution, storage and revocation is a challenging task, and the traditional solutions that focus on users rather than devices are prohibitively expensive to be even considered for low-cost embedded devices. In fact, embedded devices make the situation worse due to being computationally constrained, having very long lifecycles, and being often operated in hostile environments with hackers having full physical access and unlimited time to carry out any attack.

ESCRYPT offers key management solutions targeted specially for embedded devices both as a commercial product named CycurKEYS and as a hosted and managed service on our servers. ESCRYPT combines its competence for embedded security with the reliability, trust and world-wide infrastructure of its multinational parent company.

ESCRYPT’s key management solutions support all commonly used and standardized cryptographic schemes, including RSA, Elliptic Curves, AES, SHA, etc., and are very flexible allowing applications (so-called plug-ins) to be built and run on top of them. ESCRYPT currently offers plug-ins for secure software flashing, secure key injection, secure V2X communication, and secure feature activation. Furthermore, new plug-ins and third-party applications can be easily added due to a powerful and well-defined API of the underlying cryptographic mechanisms.
Secure Flashing (Software / Calibration Data)
The reprogramming and reconfiguration of modern embedded systems have to be protected against misuse of the interfaces by adversaries. Digitally signed software and configurations are state of the art technology to retain authenticity and integrity of the data during transmission and storage. With the signature module of CycurKEYS, ECRYPT has a versatile solution for creating signatures of software and parameterization data with various algorithms and key-lengths to protect the complete life-cycle of embedded software and calibration data.
Secure V2X Communication
Next generation vehicular safety systems will heavily rely on wireless communication. To prevent from tampering and protect the users’ privacy, strong security mechanisms will be required. Participating units, including vehicles and stationary roadside units, would need to be provided necessary digital certificates; and that would in turn require a specialized public key infrastructure (PKI). ECRYPT has the first ready-to-market implementation of V2X PKI and communications software available, which has already been proven in different field operational test. It is constantly adapted to maturing standards and ready for highly available enterprise use.

Secure Feature Activation / Business Model Protection
Digital rights management (DRM) is an established concept for enabling an after-sales market by selling additional features. Additionally, it can serve for configuration management of devices during manufacturing and distribution, and thus reduce cost by reducing hardware variants.

The embedded library CycurLIB together with the powerful security server CycurKEYS form a reliable and scalable basis for adding software activation features to embedded products.
Details

List of Use Cases and Applications
ESCRYPT’s key management solution acts as an enabler for security solutions:
- Secure Authentication
- Secure software flashing
- Protecting wireless, wired, and API interfaces
- Secure internal communication
- Theft protection and access control
- Protecting software and hardware IP
- Remote command and control applications
- Subscription and other fee-based services
- Secure V2X communication

Engineering Services
- Development of customized applications and interfaces
- Setup, integration, customization and service hotline
- Consulting and maintenance

Standard Software Modules / Plug-Ins
- Autonomous key management functions in the embedded device
- Secure firmware flashing using digital signatures
- Secure key injection for cryptographic key/certificate injection at an assembly line
- Feature activation for providing feature activation codes
- Secure V2X software

General
- Key material protected via Hardware Security Module (HSM)
- Support for different commonly used cryptographic primitives, protocols, and certificate formats
- Flexible architecture
- User management
- Tamper-proof log files
- Revocation

ESCRYPT’s Core Competencies

ESCRYPT - Embedded Security is the leading system provider for embedded security world-wide. With locations in Germany, the USA, 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.

With an extensive portfolio of security products and services ESCRYPy offers custom-fit industry solutions for the automotive industry, transport and logistics, public authorities and the financial sector, healthcare, energy suppliers, telecommunications service provider and the processing and engineering industry. The company’s core competency lies in the development and implementation of cost-efficient and flexible security solutions that can easily be integrated into existing IT-landscapes and adapted to keep up with future developments.

ESCRYPT’s service portfolio includes security assessment, security strategy, development, implementation and operation of customized software and hardware, turnkey solutions and managed services, certification support, PKI, key management and trainings.

ESCRYPT is strongly involved in international research. In the context of several regional, national and European research projects the company has continuously contributed decisive impulses to the field of Intelligent Transport Systems (ITS) Security, hardware design and system resistance against side-channel attacks.