



Cryptographic library for embedded systems

Overview

Cryptographic protocols and algorithms provide the fundamental basis for most IT security applications. For example, cryptographic algorithms such as digital signature verification are required for secure flash solutions, feature activation, and secure boot. The cryptographic library is used as basis for all embedded security solutions.

CycurLIB includes very efficient implementations of common cryptographic functions. Furthermore, CycurLIB is developed by ASPICE compliant processes and conform to MISRA and ANSI.

CycurLIB is commonly used in many high-volume products, e.g. in the automotive industry, in medical equipment and machine building.

CycurLIB provides relevant cryptographic algorithms optimized for code-size while satisfying stringent performance-constraints.

CycurLIB can easily be used to make your products secure, e.g., by verifying signatures to determine the authenticity and integrity of data. CycurLIB is highly configurable to the customer's needs (with an AUTOSAR compliant configuration tool).

Details

General

- Implemented according to MISRA-C:2012 and ANSI-C standard
- Optimized for code size while satisfying stringent performance constraints
- HIS Source Code Metrics compliant components
- ASPICE compliant development processes
- AUTOSAR compliance
 - AUTOSAR compliant configuration tool
 - AUTOSAR compliant memory mapping
- Easy to integrate in your product
- Intuitive API
- Modular structure to directly adapt the software
- Well-documented

Available Cryptographic Algorithms

- AES
 - Supported key sizes: 128 bit, 192 bit, 256 bit
 - Supported modes of operation: CBC, GCM
- Hash algorithms
 - SHA-224, SHA-256, SHA-384, SHA-512
- MAC
 - HMAC-SHA2
 - CMAC-AES
 - Siphash
- ECC with Curve25519
 - Key agreement with Diffie-Hellman
 - Key pair generation
- RSA
 - Moduli: 1024 bit, 2048 bit, 3072 bit, 4096 bit
 - Supported RSA signature schemes:
PKCS#1 RSASSA-PSS, PKCS#1 RSASSA-V1_5

Supported Platforms

- Any platform providing an ANSI-C conform compiler – from 8 bit to 64 bit

Features & Benefits

- Seamless integration in existing products
- Supports all common cryptographic algorithms and certificate standards
- Implemented to account for highest quality standards
- Low footprint
- Modularity
- Runs on all platforms

Continuous enhancement and adaptation

- Extensions/Modifications: enhancement based on market trends and customer requirements
- Adaptions to HSMS/Secure microcontrollers: adapt implementation to use hardware acceleration

Customization

- Please contact us for questions regarding extensions and modifications

