escrypt
SECURITY. TRUST. SUCCESS.

CycurLIB

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 (level 2) and ISO 26262 compliant processes (up to ASIL D).

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).

ESCRYPT 2020/01

escrypt
SECURITY. TRUST. SUCCESS.

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 (level 2) compliant development processes
- ISO 26262 compliant development processes, up to ASIL D
- 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-2 (SHA-224, SHA-256, SHA-384, SHA-512)
  - SM3
- Message Authentification Code
  - HMAC-SHA2, HMAC-SM3
  - CMAC-AES
  - Siphash
- Eliptic Curve
  - Signature generation and verification
    - ECDSA (deterministic and non-deterministic) with NIST P-224, P-256, P-384
    - Ed 25519
    - SM2 Digital Signature Algorithm
  - Key Exchange and Generation
    - ECDH with NIST P-224, P384
    - Curve 25519
    - SM2 Key Exchange
  - Asymmetric Encryption
    - ECIES
    - SM2 Encryption
- RSA
  - Moduli: 1024 bit, 2048 bit, 3072 bit, 4096 bit
  - Supported RSA signature schemes: PKCS#1 RSAS-SA-PSS, PKCS#1 RSASSA-V1_
- Certificates
  - X.509 parser and chain validation
- RNG and KDF
  - Random Number Generation: HMAC-DRBG
  - Key Derivation Functions: KDF2, KDF according to NIST SP800-56A rev1
- Chinese algorithms
  - SM2, SM3, SM4 (Elliptic Curve Cryptography, Hash Function and Block Cipher accord to Chinese National Standard)

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

Customization

- Please contact us for questions regarding extensions and modifications

Outlook

- CycurLIB components: AUTOSAR CryptoDriver

New in 2020:
Compliant to ISO 26262 up to ASIL D