Empowering Tomorrow's Automotive Software
www.etas.com

Cryptographic library for embedded systems **ESCRYPT CycurLIB**

Overview

Cryptographic protocols and algorithms provide the fundamental basis for most IT security applications and embedded security solutions. Typical applications include secure software updates, secure boot, encrypted/authenticated communication, and feature activation.

ESCRYPT CycurLIB is a cryptographic libraray that provides efficient implementations of cryptographic algorithms and security standards.

Additionally, it was designed especially for embedded systems where resources such as computational power and memory are particularly limited.

ESCRYPT CycurLIB has no dependencies on specific microcontrollers, operating systems or external libraries. This enables the use on any microcontroller with sufficient RAM/ROM.

ESCRYPT CycurLIB provides a comprehensive set of cryptographic algorithms including post-quantum algorithms together with supporting NIST and Chinese standards.

This enables its' use in many diverse and high-volume applications, especially the automotive industry.

This cryptographic library is geared for new cybersecurity regulations for which the security engineering process has been certified to be compliant to ISO/SAE21434-Road vehicles-Cybersecurity engineering

ESCRYPT CycurLIB is modular and easily integrable and is optimized for code-size while satisfying stringent performance-constraints. It can easily be used to make products secure, e. g., by verifying signatures to determine the authenticity and integrity of data and is highly configurable with an AUTOSAR compliant configuration tool).

Post-quantum algorithms supported

Proven and certified quality

Quality is deeply rooted in the business principles at ETAS and is a fundamental part of every product development. We are committed to offer customers only top-quality products and the quality of our cryptographic library has been proven in multiple ways.

ASPICE

The "Automotive Software Process Improvement and Capability dEtermination" (ASPICE) assessment rating is a widely adapted standard. Major OEMs use it to assess their electronic and software supplier's process quality and capability.

- ESCRYPT CycurLIB is developed by ASPICE compliant processes, capability level 2.

ASIL D

The automotive risk classification ASIL D is part of the larger ISO standard for functional safety ISO 26262 and represents the highest level of risk management. Components designed for ASIL D meet the most stringent safety requirements.

- The development of the cryptographic library follows ISO 26262 compliant processes, up to ASIL D.
- ESCRYPT CycurLIB can be implemented in safety-critical applications.

FIPS and CAVP

The "Federal Information Processing Standard" (FIPS) 140-2 by the National Institute of Standards and Technology (NIST) specifies the security requirements that will be satisfied by a cryptographic module.

The NIST "Cryptographic Algorithm Validation Program" (CAVP) provides validation testing of cryptographic algorithms and their individual components.

- FIPS-certified variant available
- CAVP validation will be available soon

Testing

ESCRYPT CycurLIB is continuously and rigorously tested with about 15.000 unit, integration and qualification tests performed with a passing rate of 100%. The cryptographic librarys' high-quality has further been underscored by its' proven record in the field, in millions of vehicles and applications worldwide.

Comparison freeware vs. ESCRYPT CycurLIB

Freeware cryptographic library	Our cryptographic library
? May be well tested	✓ Rigorously tested
? May be licensed under GPL	✓ No open-source included (GPL-free)
× No product support	✓ Long-term product support and maintenance
× No customer incident handling and support	✓ Customer incident handling and support
× Not qualified for automotive systems and microcontrollers	✓ Qualified for automotive systems and microcontrollers
× Does usually not cover safety use-cases	✓ Qualified for safety critical applications

Available cryptographic algorithms

Category	Algorithms
Symmetric Block Ciphers	AES SM4
Modes of Operation	CBC CCM CTR GCM
Authenticated Encryption	ChaCha20-Poly1305
Symmetric Stream Ciphers	ChaCha20
Digital Signatures	RSASSA-PSS RSASSA-PKCS1-v1_5 ECDSA EdDSA SM2 Digital Signature
Post Quantum Algorithms	CRYSTALS-KYBER CRYSTALS-DILITHIUM
Asymmetric Encryption	SM2 Encryption ECIES ECIES DHAES RSA-OAEP
Hash Functions	SHA-2 SHA-3 SM3
Message Authentication Codes (MACs)	CMAC HMAC Poly1305 SipHash24
Diffie-Hellman Key Exchange	Curve25519 ECDH FFC DH
MQV Key Exchange	SM2 Key Exchange
Key Derivation Functions	KDF2 / ANSI X9.63 KDF Hash-based KDF according to NIST SP800-56C HKDF according to RFC5869 KDF in CTR mode with AES-CMAC according to NIST SP800-108
Key Wrap	NIST AES Key Wrapping
Pseudo-Random Number Generators	HMAC_DRBG Hash_DRBG
Certificates	X.509 parsing and chain validation OCSP response parsing and validation
Password-Authenticated Key Exchange	SPAKE2+

Details

General

- Implemented according to MISRA-C:2012, ANSI-C standard and Cert-C
- HIS Source Code Metrics compliant components
- No external library required, in particular no OSS is included
- No dynamic memory allocation
- Optimized for code size while satisfying stringent performance constraints
- Modular structure to directly adapt the software
- GUI supported configuration
- 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
- FIPS certified variant available
- Well-documented
- Intuitive API
- Easy to integrate in your product
- No dependencies on specific microcontrollers

Supported platforms

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

Outlook

- Components: AUTOSAR CryptoDriver
- Post-quantum algorithms optimization
- EdDSA extension

Your benefits with ESCRYPT CycurLIB

- 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
- High level of customer support
- **Continuous enhancement and adaptation:** Extensions/Modifications – enhancement based on market trends and customer requirements
- **Customization:** Please contact us for questions regarding extensions and modifications.