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 standardized cryptographic functions. Furthermore, CycurLIB is developed by ASPICE (level 2) and ISO 26262 compliant processes (up to ASIL D).

CycurLIB is used in many high-volume products, especially the automotive industry has been using CycurLIB successfully for years in a variety of ECUs.

CycurLIB provides relevant cryptographic algorithms including post-quantum algorithms and Chinese standards and is optimized for code-size while satisfying stringent performance-constraints.

CycurLIB can easily be used to make 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).

Post-quantum algorithms available soon!

ESCRYPT 2021/07

Proven quality of CycurLIB

Quality is deeply rooted in the business principles at ESCRYPT and is part of every product development. ESCRYPT is committed to offer customers only top-quality products and the quality of CycurLIB 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.

- 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 ISO 26262 and represents the highest level of risk management. Componements designed for ASIL D meet the most stringent safety requirements.

- The development of CycurLIB follows ISO 26262 compliant processes, up to ASIL D.

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 componements.

- ESCRYPT offers a FIPS-certified variant of CycurLIB
- CAVP validation will be available soon

Testing of CycurLIB

To ensure a high quality standard, CycurLIB is continuously being tested. ESCRYPT performs about 15.000 unit, integration and qualification tests before CycurLIB reaches our customers – with a passing rate of 100 percent.

Comparison freeware vs. CycurLIB

Freeware cryptographic library	CycurLIB cryptographic library
? May be well tested	✓ Well tested
? May be licensed under GPL	✓ GPL free (no copyleft)
✗ 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

Available cryptographic algorithms

Category	Algorithms
Symmetric Block Ciphers	AES SM4
Modes of Operation	CBC CCM CTR GCM ChaCha20-Poly1305
Symmetric Stream Ciphers	ChaCha20
Digital Signatures	RSASSA-PSS RSASSA-PKCS1-v1_5 ECDSA EdDSA SM2 Digital Signature
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
Key Wrap	NIST AES Key Wrapping
Pseudo-Random Number Generators	HMAC_DRBG
Certificates	X.509 parsing and chain validation

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 CycurLIB variant available
- Well-documented
- Intuitive API
- Easy to integrate in your product

Supported platforms

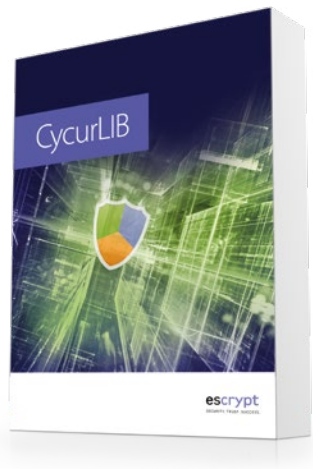
- Any platform providing an ANSI-C conform compiler – from 8 bit to 64 bit

Outlook

- CycurLIB components: AUTOSAR CryptoDriver
- Post-quantum algorithms
- CAVP validation

Your 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
- ✔ 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



Any questions?

Please contact us any time.

info@escrypt.com
Phone: +49 234 43870-200
www.escrypt.com

escrypt
SECURITY. TRUST. SUCCESS.