CryptoServer Software Development Kit

utimaco®

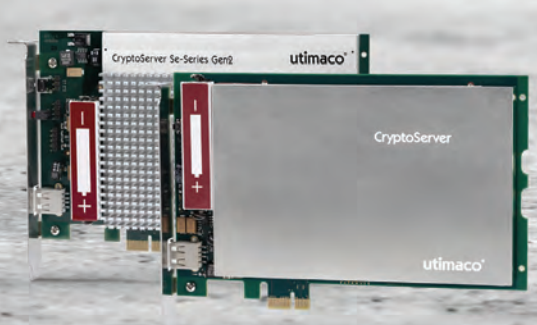
The professional development environment for customized solutions

The Utimaco Software Development Kit (SDK) is the professional development environment for all Utimaco Hardware Security Modules (HSMs). It enables system integrators and users to create their own specific applications, such as proprietary algorithms, custom key derivation procedures or complex protocols. All these run within the tamper-proof environment of a Utimaco HSM.

The development environment enables you to implement your own firmware modules. These can then be executed within the CryptoServer Hardware Security Modules. The Utimaco CryptoServer SDK base firmware allows for the development of security products that require FIPS 140-2 Level 3 or 4.

Cost-effective development

- No additional license fees for runtime environments or for each delivered application
- Minimal training required thanks to the use of standard programming languages and standardized development environments
- Complete description of internal programming interfaces (API) enables maximum utilization of Utimaco base firmware modules
- Efficient testing and debugging using the CryptoServer software simulator
- Reduced price for Hardware Security Modules in development environments



Contact
hsm@utimaco.com
hsm.utimaco.com

EMEA
Utimaco IS GmbH – Headquarters
Germanusstraße 4
52080 Aachen, Germany
Phone +49 241 1696 200

Americas
Utimaco Inc.
910 E Hamilton Ave., Suite 150
Campbell, CA 95008, USA
Phone +1 844 UTIMACO

APAC
Utimaco IS GmbH – Office APAC
One Raffles Quay, North Tower, Level 25
Singapore 048583
Phone +65 6622 5347

Development environment

- Standardized development environment for all CryptoServer models
- Developments are independent from manufacturer
- Full control over functionality of user-created firmware
- Includes files for Utimaco base firmware and interface libraries
- Programming examples for firmware modules and applications
- Project files for compilation of programming examples in Microsoft Visual Studio
- Makefiles for compilation of programming examples (Linux gcc)

Test environment

- Full simulation of CryptoServer Hardware Security Modules in software
- Testing and debugging of new firmware in Windows or Linux development environment

Documentation

- Programming manual
- Full description of Utimaco base firmware internal interfaces
- Comprehensive documentation for all tools

Cryptographic algorithms

- RSA, DSA, ECDSA with NIST and Brainpool curves
- DH, ECDH with NIST and Brainpool curves
- AES, Triple-DES, DES
- MAC, CMAC, HMAC
- SHA-1, SHA2-Family, SHA3, RIPEMD
- Hash-based deterministic random number generator (DRG.4 acc. AIS 31)
- True random number generator (PTG.2 acc. AIS 31)
- All algorithms included in product price

Programming model

- Modular software architecture of the Utimaco base firmware offers maximum design optimization capabilities for applications
- ANSI C/C++, no assembler-level programming knowledge is required

Support

- Developer training
- Qualified developer-level support via phone and e-mail

Fields of application

- Banking and finance
  - Card personalization
  - PIN mailer printing
  - Processing acquirer and processor payment transactions
- Healthcare
  - Card personalization
  - Secure management and storage of health records
- Automotive industry
  - Code signing and secure manufacturing
  - Key injection
  - Birth certificate generation
  - Toll collection systems
- Consumer Industry
  - IP protection
  - Content protection

Supported CryptoServer Hardware

- CryptoServer Se-Series Gen2*
- CryptoServer CSe-Series*
- CryptoServer Se-Series*

**Full support of hardware acceleration and ECC library*