CryptoServer Software Development Kit

utimaco®

The Development Environment for the Successful Realization of Your Requirements

The CryptoServer Software Development Kit (SDK) is the professional development environment for all Utimaco Hardware Security Modules. It enables integrators and endusers to create specific applications, e.g. proprietary algorithms, custom key derivation procedures or complex protocols that run in the tamper-proof environment of the CryptoServer. As the SDK provides full access to the underlying Utimaco base firmware, custom firmware modules can be developed in a very short time frame.

- Common development environment for all CryptoServer models.
- Independence from manufacturer
- Full control over functionality of user-created firmware

LOW OPERATIONAL COSTS

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

CONTACT

Utimaco Inc.
Suite 120, 475 Alberto Way
Los Gatos, CA, 95032
USA

phone *+1 844 UTIMACO*
email *hsm@utimaco.com*
web *http://hsm.utimaco.com*

Development environment

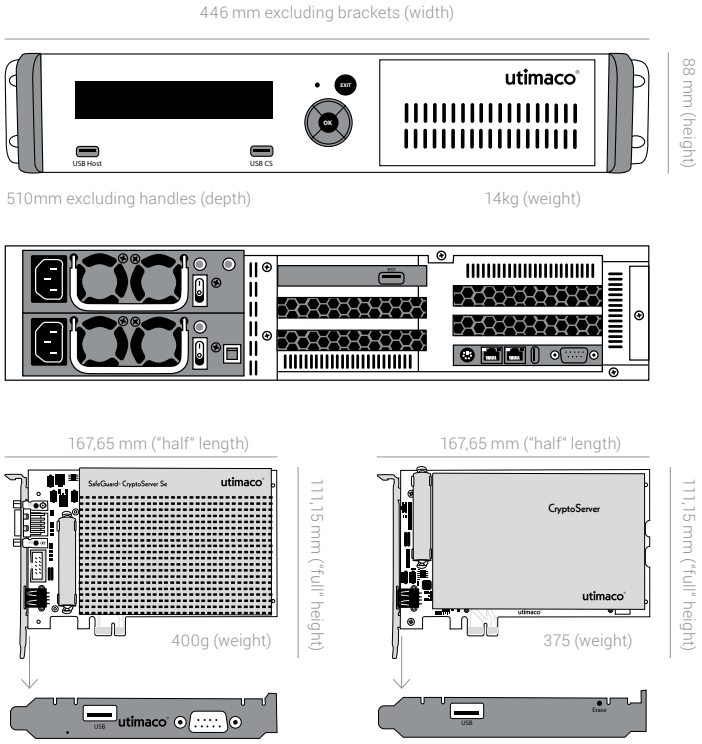
- Include files for Utimaco's underlying base firmware and interface libraries
- Programming examples for firmware modules and applications
- Project files for compilation of programming examples in Microsoft Visual Studio
- Makefiles for compilation of programming examples under Linux gcc
- Tools for final build of CryptoServer firmware modules

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 internal interfaces of Utimaco´s underlying base firmware
- Comprehensive documentation for all tools



Cryptographic Algorithms

- RSA
- DSA, ECDSA
- AES, DES, Triple DES
- AES MAC, Triple DES MAC, Retail MAC
- Hash algorithms SHA-1, SHA-2 family, RIPEMD-160
- Diffie-Hellman
- additional algorithms on request

Programming model

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

Support

- Developer training
- Qualified developer-level support via phone and email

Typical field of application

- Banking Finance
  - Card Personalization
  - PIN Brief generation
  - Acquirer and Processor
- Healthcare
  - Card personalization
  - Health record security
- Automotive
  - Code signing and secure manufacturing
  - Key injection
  - Birth certificate generation
  - Toll Charging System
- Consumer Industry
  - IP protection
  - Content protection

Supported Hardware CryptoServer Hardware

- CryptoServer Se-Series PCIe*
- CryptoServer CSe-Series PCIe*
- CryptoServer Se-Series LAN*
- CryptoServer CSe-Series LAN*

*Full support of hardware acceleration and ECC library

Available models and performance with unlimited client licenses

	Se10		Se50		Se400		Se1000		CSe10		CSe100	
	PCIe	LAN	PCIe	LAN	PCIe	LAN	PCIe	LAN	PCIe	LAN	PCIe	LAN
	RSA Signing Performance (tps: transaction per second)+											
Key length 2048 bit	16	16	80	80	1500	1500	2800	2800	13	13	90	90
Key length 4096 bit	2	2	10	10	290	290	570	570	2	2	14	14
	*Elliptic Curve signature generation (tps: transaction per second)**											
192 bit	180	170	1300	870	1300	870	1300	870	150	140	1500	1150
256 bit	120	120	950	680	950	680	950	680	100	100	1000	850
	*Elliptic Curve key generation (kps: Keys per second)**											
192 bit	40	40	280	250	280	250	280	250	36	35	330	290
256 bit	20	20	190	180	190	180	190	180	21	21	210	190

+ CryptoServer is operated in Bulk signature mode * No ECC activation needed