



The next generation Industry Standard Hardware Security Module

The next generation SecurityServer from Utimaco secures cryptographic key material for servers and applications. It includes integration software that supports the industry standards (e.g. PKCS#11, Microsoft CSP/CNG, JCE, ...) which are used in most application scenarios, e.g. Enterprise PKI applications, database encryption, etc.

The next generation SecurityServer Se-Series Gen2 is available as PCIe embedded card or as network attached appliance.



Fully functional CryptoSever Simulator available for evaluation and application integration.

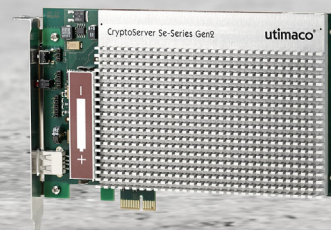
LOW OPERATIONAL COSTS

- Highest performance at an attractive price
- Inexpensive starter models for standard industry applications
- Extensive remote administration based on PinPad and Smartcards
- Efficient key management and firmware updates via remote access
- Automation of remote diagnosis through network management system using SNMP protocol

CONTACT

Utimaco IS GmbH
Germanusstraße 4
52080 Aachen
Germany

phone + 49 241 1696 200
email hsm@utimaco.com
web <http://hsm.utimaco.com>

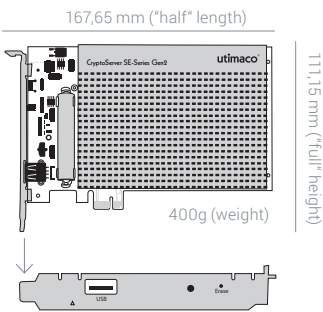


Capabilities

- Secure key storage and processing
- Cryptographic offloading/acceleration
- Extensive key management
- Key storage inside HSM or as encrypted key files
- Multiple options for user authentication and access control
- Smartcard for strong authentication
- “n out of m” authentication
- Separation of duties
- Remote Management
- Supported OS: Windows and Linux
- Multiple integrations with PKI applications, database encryption, etc.

Security, safety, environmental compliance

- FIPS 140-2 Level 3*
- CE, FCC Class B
- UL, IEC/EN 60950-1
- CB certificate
- RoHS II, WEEE



Physical specification PCIe card

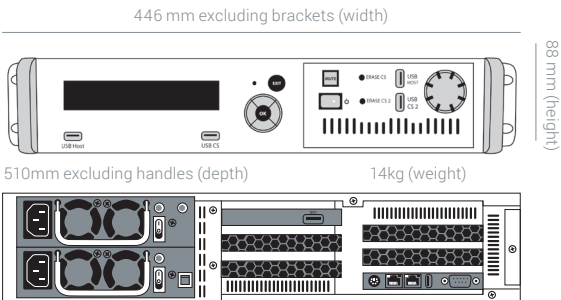
- Half length, full height PCI Express card
- Supports PCIe 1.1, PCIe 2.0 and PCIe 3.0 slots
- Operating voltage 3,3V
- Battery 3 V, Lithium, Ø 12 mm, length 600 mm, FDK CR 12600 SE or VARTA CR2NP
- USB interfaces
- Operating temperature: +10°C to +45°C (+50°F to +113°F)
- Storage temperature: -10°C to +55°C (+14°F to +131°F)
- Relative humidity 10% to 95% non-condensing
- MTBF 360,000 hours at 25°C / 77°F

Cryptography

- RSA
- ECDSA, NIST and Brainpool curves
- DSA
- DH, ECDH
- AES
- DES, Triple DES
- SHA-1, SHA-2, RIPEMD
- MAC, CMAC, HMAC
- Hash-based Deterministic Random Number Generator (DRNG)
- True Random Number Generator (TRNG acc. AIS31 class DRG.4)

Application Programming Interfaces (APIs)

- PKCS#11
 - Java Cryptography Extension (JCE)
 - Microsoft Crypto API (CSP), Cryptography Next Generation (CNG) and SQL Extensible Key Management (SQLEKM)
 - Cryptographic eXtended services Interface (CXI)
- Utimaco's high performance interface guarantees easy integration of cryptographic functionality into client applications



Physical specification network appliance

- 19" 2U form factor
- Redundant field-replaceable power supply 90~264 V, 47~63 Hertz AC 2 x 320 W
- Power consumption typically 70 W / 85 VA, max. 90 W / 100 VA
- Heat dissipation max. 307 BTU/h
- 2 RJ45 1 Gb/s network interfaces
- Operating temperature: +10°C to +50°C (+50°F to +122°F)
- Storage temperature: -10°C to +55°C (+14°F to +131°F)
- Relative humidity 10% to 95% non-condensing
- MTBF 90,000 hours at 25°C / 77°F

Available models and performance with unlimited client licenses

	Se12		Se52		Se500		Se1500	
	PCIe	LAN	PCIe	LAN	PCIe	LAN	PCIe	LAN
RSA signature generation (tps: transactions per second)								
2048 bits	16	16	80	75	690	580	960	780
4096 bits	2	2	11	11	100	90	160	150
RSA bulk signature generation (tps: transactions per second)								
2048 bits	16	16	85	80	2200	2100	3400	3200
4096 bits	2	2	11	11	220	220	360	360
Elliptic Curve signature generation (tps: transactions per second)**								
224 bits	150	140	1000	880	1300	1040	1900	1400
384 bits	50	50	450	390	950	790	1400	1100
Elliptic Curve bulk signature generation (tps: transactions per second)**								
224 bits	160	160	1400	1300	1800	1700	3500	3100
384 bits	54	54	490	490	1300	1200	2400	2200

* FIPS certification in process ** No ECC activation needed