

SafeGuard® CryptoServer

Hardware Security Modules



Hardened Security for your Cryptographic Keys, Critical Applications and Sensitive Data

Electronic transactions and computerized business processes are the lifeblood of organizations today. It is critical to ensure the security of transactions and data. Conventional perimeter security is no longer sufficient because data can be accessed by a wide variety of users on any device from the inside or outside the organization. As a result, organizations rely on cryptography as the surest method to guarantee the confidentiality, authenticity, integrity and non-repudiation of business processes. Encryption and digital signatures ensure that both the data and transactions are safeguarded.

To protect the entire security infrastructure from being compromised, the cryptographic keys have to be stored and managed in a hardened security environment. Purpose-built Hardware Security Modules (HSM) protect the keys, data and applications during storage and use. The use of Hardware Security Modules also helps to ensure regulatory compliance. Utimaco's **SafeGuard CryptoServer** is a tamper-resistant high-performance Hardware Security Module that is certified in accordance with stringent international security standards.

SafeGuard CryptoServer supports a wide range of applications: transaction security in ERP systems, PKI environments, document management and archiving solutions, database security, authentication server, payment applications and electronic invoicing. **SafeGuard CryptoServer** offers a broad range of interfaces to simplify integration with your existing applications and processes. Its flexible development environment enables security specialists to provide customized security solutions for your unique business processes.

SafeGuard CryptoServer offers you the highest levels of security and performance for your transactions and business processes.

About Utimaco – The Data Security Company.

Utimaco is the leading provider for data security solutions. The Data Security Company enables mid-sized to large organizations to safeguard their data assets against attacks and to comply with privacy laws by protecting their confidentiality and integrity. Utimaco's complete range of solutions provides full 360° protection unlike free, end-point or built into encryption solutions which only cover specific security needs. Its advanced SafeGuard Solutions help to manage and secure data in what ever conditions: during storage (data at rest), during transmission (data in motion) and during processing (data in use). Utimaco offers its customers comprehensive on site support via a worldwide network of partners and subsidiaries in Europe, the USA and Asia. For more information, visit www.utimaco.com

Benefits

SafeGuard CryptoServer models

- **S-Series**
For most commercial security requirements, designed in accordance with FIPS 140-2 Level 3
- **CS-Series**
For highest security requirements, certified in accordance with FIPS 140-2 Level 3, with Level 4 for "Physical Security"



TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments.

- Approved by the German Central Banking Committee (ZKA)

Flexible security solutions

- **Security Server**
Supports all major standard interfaces including PKCS#11, Microsoft Crypto API and CNG, JCE, OpenSSL
- **Timestamp Server**
Timestamp your data and documents in accordance with RFC3161
- **Payment Server**
Data preparation for debit and credit cards (EMV), and processing of electronic fund transfers
- **Challenge Response Server**
Securely store administrator passwords for emergency procedures in SafeGuard environments
- **Securing Custom Applications**
Software Development Kit (SDK) enables your proprietary algorithms and complex protocols to be easily implemented in the HSM

Available form factors

- SafeGuard CryptoServer is available as **PCI card** and as **19" network appliance**

utimaco[®]
s a f e w a r e

Hardware

SafeGuard CryptoServer PCI

- PCI card, PCI local bus interface
- Two serial RS232 interfaces
(e.g. for connecting a PIN pad or printer)

SafeGuard CryptoServer LAN

- 19" network appliance, 2 height units
- 10/100/1000 MBit/s Ethernet
- 10/100 MBit/s Ethernet
(e.g. for separate administration network)
- Two serial RS232 interfaces
(e.g. for connecting a PIN pad or printer)
- Two USB interfaces
- 3,5" floppy disk

System Requirements

- Microsoft Windows XP, Vista, Server 2003, Server 2008
- Linux kernel 2.4.0 and higher
- Solaris 8 and higher
- AIX 5L version 5.3

Cryptography and Security

Cryptographic algorithms

- RSA up to a key length of 16,384 bits
- DSA, ECDSA
- AES
- DES, Triple DES
- Triple DES MAC, Retail MAC, AES MAC
- Hash algorithms SHA-1, SHA-2 family, RIPEMD-160, MD5
- Diffie-Hellman
- Additional algorithms on request

Random Number Generation

- Physical random number generation in accordance with AIS 31 (highest possible class P2)
- Deterministic random number generation in accordance with FIPS 186-2 or AIS 20 (highest possible class K4)

Key management

- Key generation, import / export, backup / restore
- Secure internal storage of more than 2,500 RSA keys (key length 1024 bit) or more than 50,000 Triple-DES keys

HSM models and Certification

S-Series

- For most commercial security requirements
- Designed in accordance with FIPS 140-2 Level 3

CS-Series

- For highest security requirements
- Certified in accordance with FIPS 140-2 Level 3, with Level 4 for "Physical Security"
- Approved by ZKA (German Central Banking Committee)

Both S-Series and CS-Series are available as PCI card and as network appliance (LAN version).

Interfaces and Protocols

Security Server

- Microsoft Crypto API and Cryptography Next Generation (CNG)
- PKCS#11
- Java Cryptography Extension (JCE)
- OpenSSL
- Utimaco's Cryptographic Services Interface (CSI)

Timestamp Server

- Timestamp Requests and Responses according to RFC 3161
- CryptoServer Timestamp API (CTS)

Payment Server

- EMV (CVV, PVV, PIN generation and check, etc.)
- ISO 8583 message processing
- ISO PIN block formats
- PAC / MAC calculation and verification
- ZKA formats

Software Development Kit (SDK)

- Implementation of proprietary algorithms, protocols and interfaces

Performance

Model S10 / CS10

- 100 RSA signatures (1024 bit) per second
- 250 ECDSA signatures (160 bit) per second
- Triple DES encryption 2 MByte/s
- AES encryption 6 MByte/s (256 bit)
- 1,000 PIN operations per second

Model S50 / CS50

- 500 RSA signatures (1024 bit) per second
- 2,500 ECDSA signatures (160 bit) per second
- Triple DES encryption 8 MByte/s
- AES encryption 40 MByte/s (256 bit)
- 10,000 PIN operations per second

Contact

EMEA

Utimaco Safeware AG
Germanusstraße 4
DE-52080 Aachen
Germany
Phone +49 (2 41) 16 96-20 0
hsm@aachen.utimaco.com

NORTH & SOUTH AMERICA

Utimaco Safeware Inc.
10 Lincoln Road
Foxboro, MA 02035
USA
Phone +1 (508) 543-10 08
sales.us@utimaco.com

ASIA PACIFIC

Utimaco Safeware Asia Ltd.
Unit 602, Stanhope House
734 King's Road, Quarry Bay
Hong Kong
Phone +8 52 25 20 26 08
info@utimaco-asia.com

JAPAN

Utimaco Safeware K.K.
Nisso 16 Building, 3F
3-8-8 Shin Yokohama, Kohoku-ku
Yokohama 222-0033
Japan
Phone +81 (0) 45 470-1430
info.jp@utimaco.jp

Additional information about SafeGuard CryptoServer:
www.utimaco.com/hsm

Utimaco Safeware Partner: