SafeGuard® SecurityServer

Transactions and business processes

Data at Rest

Data in Use

Maximum flexibility with Hardware Security Modules

Business-critical information has to be protected against unauthorized access, manipulation or theft. Utimaco's Hardware Security Modules (HSMs) provide maximum protection against such risks. Utimaco HSMs also help to achieve compliance with internal security requirements and government regulations.

Regardless of the security standard used by your business process, **SafeGuard SecurityServer** is the tamper-resistant Hardware Security Module (HSM) that is ideally suited for all security sensitive applications.

Hardware-based Cryptographic Service Providers (CSPs) for **Microsoft CryptoAPI** have been traditionally used to provide increased security and performance to Windows applications. Protecting private keys in specialized tamper-resistant hardware, **SafeGuard SecurityServer** strongly increases the security of your Microsoft CA (certificate authority) keys, and the trustworthiness of issued certificates.

Besides CryptoAPI, **PKCS#11** has become the most widely used cryptographic standard interface. In Java-based applications, e.g. Application Server, **Java Cryptography Extension** (JCE) is assuming this role. **SafeGuard SecurityServer** provides hardware key storage and cryptographic acceleration when installed in PKCS#11 or JCE environments.

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

Benefits

Support for all major cryptographic standards

- **Microsoft CryptoAPI**
  Cryptographic Service Provider (CSP) for all Microsoft applications (e.g. Microsoft CA)
- **PKCS#11**
  For integration into PKI, Authentication Server, Transaction Processing Systems, Card Management Systems, etc.
- **Java Cryptography Extension**
  Ideal for Application Server and Service Oriented Architecture; Java PKCS#11-Wrapper also available
- **Cryptographic Services Interface**
  For any customized interface, Utimaco's Cryptographic Services Interface (CSI) guarantees easy integration and the best performance

Unmatched Total Cost of Ownership

- **Integrated Key Management**
  Import / export and backup / restore of your cryptographic keys
- **Concurrent Application Access**
  Allocation of several key container respective slots within one HSM. Concurrent access for multiple applications
- **Scalability and high availability**
  Clustering of several HSMs for load-balancing, redundancy and fault-tolerance
- **Field-upgradable**
  Flexible architecture and Secure Messaging connection allows remote key management and firmware updates

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**

utimaco®
safeware

SafeGuard® SecurityServer

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 or printer)
- USB interface
- 5 ¼" floppy disk

System Requirements

- Microsoft Windows™ 2000, XP, 2003 Server
- Linux kernel 2.4.0 and higher
- Solaris 8 and higher

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
- IDEA
- Safer
- 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
- Smartcard protected Master Box Key for backup and restore
- Secure internal storage of more than 2,500 RSA keys (key length 1024 bit) or more than 50,000 Triple-DES keys

Certification

S-Series

- Designed in accordance with FIPS 140-2 Level 3

CS-Series

- 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

Microsoft Crypto API

- Cryptographic Service Provider
- Allocation of multiple key containers
- Concurrent access for several applications

PKCS#11

- Allocation of multiple slots
- Integrated load-balancing and fail-over
- Successfully evaluated by Institute for Applied Information Processing and Communication (IAIK)

Java Cryptography Extension (JCE)

- JCE-Provider of IAIK
- Java PKCS#11 Provider and Wrapper

Cryptographic Services Interface (CSI)

- Easy-to-use cryptographic functions and key management
- Lowest protocol overhead

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 (241) 16 96-20 0
Fax +49 (241) 16 96-19 9
info@utimaco.com

NORTH & SOUTH AMERICA
Utimaco Safeware Inc.
10 Lincoln Road, Suite 102
Foxboro, MA 02035
USA
Phone +1 (508) 543-10 08
Fax +1 (508) 543-10 09
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
Fax +8 52 25 29 26 18
info@utimaco-asia.com

www.utimaco.com

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

Utimaco Safeware Partner: