The Hardware Security Module for Securing Cryptographic Key Material

SafeGuard® 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, OpenSSL…) which are used in most application scenarios. Thanks to the modular system architecture of the underlying CryptoServer technology, SafeGuard® SecurityServer operates on all hardware platforms, from plug-in card to network appliance.

**Compliance**

Helps you meet compliance requirements when standard applications such as databases and application servers are used.

Secures your sensitive data in a high-security environment.

**CryptoServer Simulator**


**Low Operational Costs**

- Highest available performance on the market at an attractive price
- Inexpensive starter models for applications with lower performance requirements
- Exhaustive remote administration
- Efficient key management and firmware updates via remote access
- Automation of remote diagnosis through network management system using SNMP protocol

**Secure Investment**

The open and uniquely modular software concept provides the ability to upgrade to new or modified procedures even after several years.
SafeGuard® SecurityServer
The Hardware Security Module for Securing Cryptographic Key Material

Supported Operating Systems

- Microsoft Windows
- Linux
- Solaris
- AIX 5L

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, MD5
- Diffie-Hellman
- additional algorithms on request

Cryptographic Interfaces Included in Delivery

Microsoft Crypto API, Cryptography Next Generation und SQL Extensible Key Management
- Secure key storage and usage for Microsoft applications

PKCS#11
- For integration in public key infrastructures (PKI), authentication servers, transactional processes, card management systems

Java Cryptography Extension (JCE)
- Ideal for application servers and service oriented architectures
- Numerous extensions for key management

OpenSSL
- Integration via CryptoServer ENGINE implementation or by using the OpenSSL engine_pkcs11

Cryptographic eXtended services Interface (CXI)
- Utimaco’s high performance interface guarantees simple integration of cryptographic functionalities for each client-specific application

Performance

Due to its wide range of models, SafeGuard® CryptoServer offers the ideal Hardware Security Module for every performance requirement: Se400 and Se1000, as well as CS10 and CS50

They provide the highest available performance on the market for RSA-Signatures, elliptic curves cryptography and AES encryption.
Se-Series and CS-Series

SafeGuard® SecurityServer is based on the CryptoServer hardware models and is available in two series:

- Se-Series for maximum performance
- CS-Series for highest security requirements

Hardware

Both series are available as a plug-in card (PCI bus for the CS-Series and PCI Express bus for the Se-Series) and as a network appliance (LAN) for use in racks (2 rack units, with 2 ethernet interfaces).

They come equipped with a serial RS232 interface (e.g. for PIN pads or printers). Additionally, the Se-Series appliances feature a USB connection.

Key Management

- Integrated functionality for key generation, export and import, secure backup and restore
- Secure internal storage of thousands of keys

Certification

SafeGuard® CryptoServer Se- and CS-Series meet all current security requirements in financial and commercial environments:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Se-Series</th>
<th>CS-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIPS 140-2 level 3</td>
<td>✔*</td>
<td>✔</td>
</tr>
<tr>
<td>FIPS Level 4 for „physical security“</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Common Criteria EAL4+</td>
<td></td>
<td>✔*</td>
</tr>
</tbody>
</table>

Random Number Generation

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Se-Series</th>
<th>CS-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical random number generation in accordance with AIS 31 (class P2)</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Deterministic random number generation according to FIPS 186-3 or AIS 20 (class K4)</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

Tamper Technology

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Se-Series</th>
<th>CS-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tamper proof</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Tamper responsive</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Zeroization on mechanical / physical / chemical attack</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Zeroization when temperature out of bounds</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Zeroization when power supply out of bounds</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Manual zeroization</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
About Utimaco

Utimaco is a leading global provider of data security solutions, enabling mid-to large-size organizations to safeguard their data assets against intentional or accidental data loss, and to comply with privacy laws. Utimaco’s Hardware Security Module business unit (HSM) is a supplier of innovative, highly flexible and high performance cryptographic hardware.

Learn more at:
http://hsm.utimaco.com

Contact

Utimaco Safeware AG
Germanusstraße 4
D-52080 Aachen
Germany

phone +49.241.1696-200
fax +49.241.1696-199
email hsm@utimaco.com
web http://hsm.utimaco.com

Copyright Information

© 1994-2010 - Utimaco Safeware AG – a member of the Sophos Group
December 2010

SafeGuard® SecurityServer

All SafeGuard products are registered trademarks of Utimaco Safeware AG – a member of the Sophos Group. All other named trademarks are trademarks of the particular copyright holder.