



# SafeGuard<sup>®</sup> SecurityServer

## The Hardware Security Module for Securing Cryptographic Key Material

### Transparent Pricing

Unlimited connections without extra licenses.

Unrestricted use in applications.

### 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

Fully-fledged simulation of CryptoServer Hardware Security Modules for evaluation and application integration, for building test environments and for assessing new functionalities.

SafeGuard<sup>®</sup> 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. Thanks to the modular system architecture of the underlying CryptoServer technology, SafeGuard<sup>®</sup> SecurityServer operates on all hardware platforms, from plug-in card to network appliance.

### Low Operational Costs

- Highest performance 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<sup>®</sup> SecurityServer

The Hardware Security Module for  
Securing Cryptographic Key Material

### Supported Operating Systems

- Microsoft Windows
- Linux

### 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

**Se-Series and CSe-Series  
SafeGuard SecurityServer is  
available on both CryptoServer  
hardware models:**

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

### Cryptographic Interfaces Included in Delivery

#### 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

#### Microsoft Crypto API, Cryptography Next Generation and SQL Extensible Key Management

- Secure key storage and usage for Microsoft applications
- Certificate Services, SQL Server, Rights Management Server

#### Cryptographic eXtended services Interface (CXI)

- Utimaco's high performance interface guarantees simple integration of cryptographic functionalities for each client-specific application



# SafeGuard® CryptoServer Software Development Kit

## The Development Environment for the Successful Realization of Your Requirements

### Transparent Pricing

Common development environment for all CryptoServer models.

No additional license fees for runtime environments or per delivered application.

Independence from Manufacturer

Full control over functionality of user-created firmware.

The SafeGuard® 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 SafeGuard® CryptoServer. As the SDK provides full access to the existing underlying base firmware, custom firmware modules can be developed in a very short time frame. The functionality contained within these custom modules is controlled entirely by you.

### Low Operational Costs

- 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

### Secure Investment

The open and uniquely modular software concept provides the ability to upgrade to new or modified procedures even after several years.



## SafeGuard<sup>®</sup> CryptoServer Software Development Kit

The Development Environment for the  
Successful Realization of Your Requirements

### Supported Operating Systems

- Microsoft Windows
- Linux

### 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

### 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

**CryptoServer SDK provides all the components required for the development of custom firmware modules.**

### Development environment

- Include files for Utimaco's underlying base firmware and interface libraries
- Programming examples for firmware modules and applications
- Project files for compiling 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

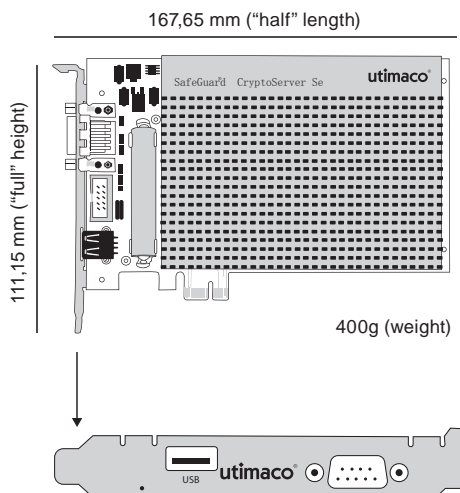
- Programming manual
- Full description of internal interfaces of Utimaco's underlying base firmware
- Comprehensive documentation for all tools

### Support

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



# SafeGuard® CryptoServer Se-Series PCIe Technical Data



<b>Operating power</b>	3,3 volt (PCI Express bus specification)
<b>Battery</b>	3 V, Lithium, Ø 12 mm, length 600 mm, Sanyo CR 12 600 SE or identical type, e.g. VARTA CR2NP
<b>External interfaces</b>	PCI Express V1.1 x1 (1 Lane) 2 serial V.24 interfaces 2 USB 2.0 interfaces (high speed)
<b>Environmental</b>	In operation: +10° C to +45° C (+50° F to +113° F) temperature In warehouse: -10° C to +55° C (+14° F to +131° F)
<b>Humidity</b>	10% to 95% relative humidity, non-condensing
<b>MTBF</b>	360,000 hours (in acc. with MIL-HDBK-217)

## Performance

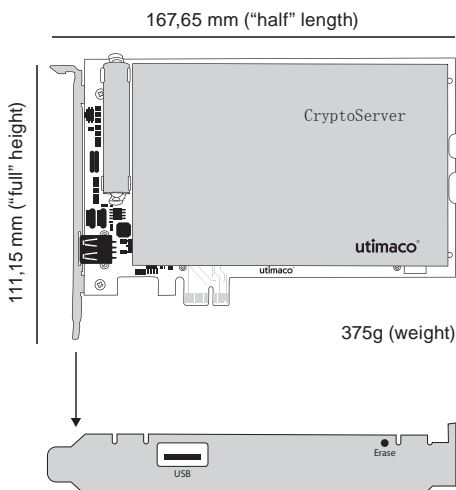
Se-Series is able to generate up to 1300 elliptic curve signatures per second.

## Certification

Certified in accordance with FIPS 140-2 Level 3. Suited for applications and market segments requiring medium to high physical security.



## SafeGuard<sup>®</sup> CryptoServer CSe-Series PCIe Technical Data



<b>Operating power</b>	3,3 volt (PCI Express bus specification)
<b>Battery</b>	3 V, Lithium, Ø 12 mm, length 600 mm, Sanyo CR 12 600 SE or identical type, e.g. VARTA CR2NP
<b>External interfaces</b>	PCI Express V1.1 x1 (1 Lane) 2 USB 1.1 interfaces
<b>Environmental</b>	In operation: +10° C to +35° C / +50° F to +104° F temperature In warehouse: -10° C to +55° C / +14° F to +131° F
<b>Humidity</b>	10% to 95% relative humidity, non-condensing
<b>MTBF</b>	350,000 hours (in acc. with MIL-HDBK-217)

### Performance

CSe-Series is able to generate up to 1500 elliptic curve signatures per second.

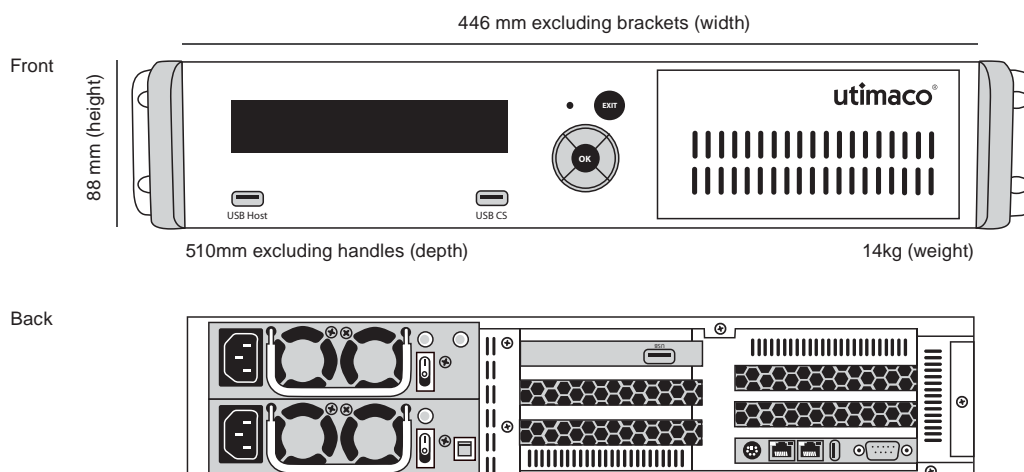
### Certification

Certified in accordance with FIPS 140-2 Level 3 (with Level 4 for "Physical Security"), and DK approved (central committee for german banking applications). Suited for applications and market segments requiring highest physical security.



## SafeGuard<sup>®</sup> CryptoServer LAN

<b>Power supply</b>	90~264 V, 47~63 Hertz AC, 2 x 420 W  Power consumption typically 70 W / 85 VA, maximum 90 W / 100 VA
<b>Environmental temperature</b>	+10° C to +50° C (+50° F to +122° F) (Se-Series) +10° C to +40° C (+50° F to +104° F) (CSe-Series)
<b>Heat dissipation</b>	307 BTU/h
<b>Humidity</b>	10% to 95% relative humidity, non-condensing
<b>MTBF</b>	90,000 hours at 25° C / 77° F (in acc. with MIL-HDBK-217)
<b>RoHS, WEEE</b>	RoHS compliant- Elektro-Altgeräte-Register DE39805015
<b>Compliance</b>	EMC emission: EN 55022 class B EMC immunity: EN 61000-6-2 (industrial environment) Equipment safety: IEC/EN 60950-1 (CB scheme) FCC 47 CFR Ch. 1 Part 15 class B





## Contact

Kuala Lumpur (HQ)  
SecureMetric Technology Sdn. Bhd.  
2-2, Incubator 2, Technology Park Malaysia,  
Lebuhraya Sg Besi - Puchong, Bukit Jalil,  
57000 Kuala Lumpur, Malaysia.

Tel : +603 8996 8225  
Fax : +603 8996 7225  
email : sales@securemetric.com  
web : www.securemetric.com

## Learn more at:

[www.securemetric.com](http://www.securemetric.com)

## About SecureMetric

SecureMetric is South East Asia's market leader in the digital security industry, with more than 16 years experience in serving clients across the world. Combining unparalleled experience, comprehensive R&D capabilities together with clear business and product road map, SecureMetric will continue with our superior achievement by helping more clients to become secure high-performance businesses and governments.

Our "secure high performance business" strategy builds on our expertise in digital security to help clients perform at the highest levels so they can create sustainable value for their customers and shareholders. Using our industry knowledge, service-offering expertise and technology capabilities, we continue to identify new business and technology trends and develop solutions that aim to help clients to defend against latest security threats and risks.

As one of the pioneer player in this region with full capability of producing our own security devices and solution, SecureMetric is proud to be the one of the top rated digital security solution provider origin from South East Asia. SecureMetric's technology expertise comprises of our accumulated more than a decade project and R&D experiences together with our external technology collaboration with selected world leading digital security vendors.

SecureMetric is headquartered in Kuala Lumpur, with subsidiaries in Hanoi, Ho Chi Minh City, Jakarta, Philippine and Singapore. Next, the company is aiming to establish local presence throughout South East Asia region before end of 2015. In addition to South East Asia, SecureMetric has already appointed more than 30 channel partners from around the world as part of our international marketing network.

On top of supporting more than 2,000 software developers worldwide in protecting their software copyright and licensing, SecureMetric also has successfully implemented many high profiles Two Factor Authentication and Cryptography projects to many well-know financial institutions and government agencies across the regions.