Product Brochure

SecurityServer – Secure your organization's most valuable assets

SecurityServer – The root of trust for business applications

UTIMACO
SecurityServer

Creating Trust in
the Digital Society

utimaco®

SecurityServer In A Nutshell

Secure key generation, storage, and usage for numerous business applications

Today, the Digital Transformation affects all companies, institutions and organization from all industries. Broadscale deployment of digital systems is also increasing the amount of data that is being generated. Companies are looking for solutions to secure their confidential data, processes, intellectual property and user and customer data. The introduction of every new smart devices and components additionally also requires protecting their identities.

Data or identity preservation is increasing the demand for applications like authentication, document signing, certificate issuing, key injection, etc. Depending on the use cases some industries need high performance applications while others need highest physical security to protect from virtual and physical attacks.

Security of these applications is only guaranteed if the keys used for performing these applications are secured. In short if the keys are safe then your company is safe.

UTIMACO's **SecurityServer** adds an extra layer of security to your business applications. SecurityServer provides a tamper-protected environment for data encryption, document signing, certificate issuance, and many other critical security requirements.

SecurityServer enables

SECURE
key generation and storage

KEY USAGE
in a tamper-protected environment

HIGH-QUALITY
true random number generation to ensure uniqueness of keys

UTIMACO
SecurityServer

SecurityServer bundles 30 years of experience in cryptography and Hardware Security Module (HSM) technology into a unique offering that constitutes the root of trust for security and compliance of business applications. It adds the extra layer of security to an organization's most valuable assets. Supporting a wide range of hardware platforms, it meets performance and security requirements of small enterprises all the way up to large crypto infrastructures and always offers best price-performance ratio in different deployment scenarios.

Key Features

Hardware

- **Tamper-protected environment** for Secure Key Operations

Administration

- Extensive **Remote Management**

Free Software Simulator

- HSM Simulator **with all SecurityServer functionalities**

Easy Integration

- Easy Integration with **3rd Party Applications**

Software

- **Customizable** Firmware

For applications and market segments with high physical security requirement.

Plug-and-play integration with numerous business applications.

SecurityServer Solution

SecurityServer with its excellent features and functionalities is applicable to various use cases and industries.

Tamper-protected environment for Secure Key Operations

SecurityServer ensures the secure key generation, storage, and usage inside a tamper protected HSM. Based on the market requirements, SecurityServer enables high-volume generation of keys as well as provides high-quality true random number generation to ensure uniqueness of keys.

Extensive Remote Management

SecurityServer enables the efficient key management and firmware updates via remote access. It supports automation of remote diagnosis via SNMP (Simple Network Management Protocol).

Free Software Simulator

SecurityServer simulator makes it straightforward to evaluate SecurityServer and test its integration with business applications before deploying it into production.

Easy Integration with 3rd Party Applications

Supporting all common cryptographic APIs like PKCS #11, JCE, OpenSSL and Microsoft CNG and SQLEKM, a plug-and-play integration with numerous business applications ensures your systems are secured with little effort and time.

Customizable Firmware

Whenever common cryptographic APIs don't satisfy your needs, e.g., they don't support a special government algorithm or a new key derivation method; or are ineffective because multiple commands have to be chained, our HSM firmware development kit enables you to finetune and optimize the functionality and performance of your HSMs.

Use Cases

- **Data Encryption**
- **Document Signing**
- **Code Signing**
- **Certificate Issuing**
- **Public Key Infrastructure**
- **Chip and Device Personalization**
- **User and Device Authentication**
- **Many More**

Industries

- **IoT and Manufacturing**
- **Financial Services**
- **Cloud/Cloud Service Providers**
- **Government**
- **Retail**
- **Telecommunication**
- **Many More**

HSM Functionalities

Features

- **Extensive key management**
- **Secure key storage inside HSM,** as encrypted key blobs in file system or in enterprise-grade database
- **2-factor authentication** with smartcards
- **"m out of n" authentication** (e.g. 3 out of 5)
- Configurable **role-based access control** and separation of functions
- **Multi-tenancy** support
- Supported **operating systems: Windows** and **Linux**
- **Multiple integrations** with PKI applications, database encryption, etc.
- **Up to 10,000 RSA or 6,000 ECDSA*** **/ 35,000 RSA or 32,000 ECDSA**** signing operations in bulk processing modes
- **All features included** in product price

Cryptographic Algorithms

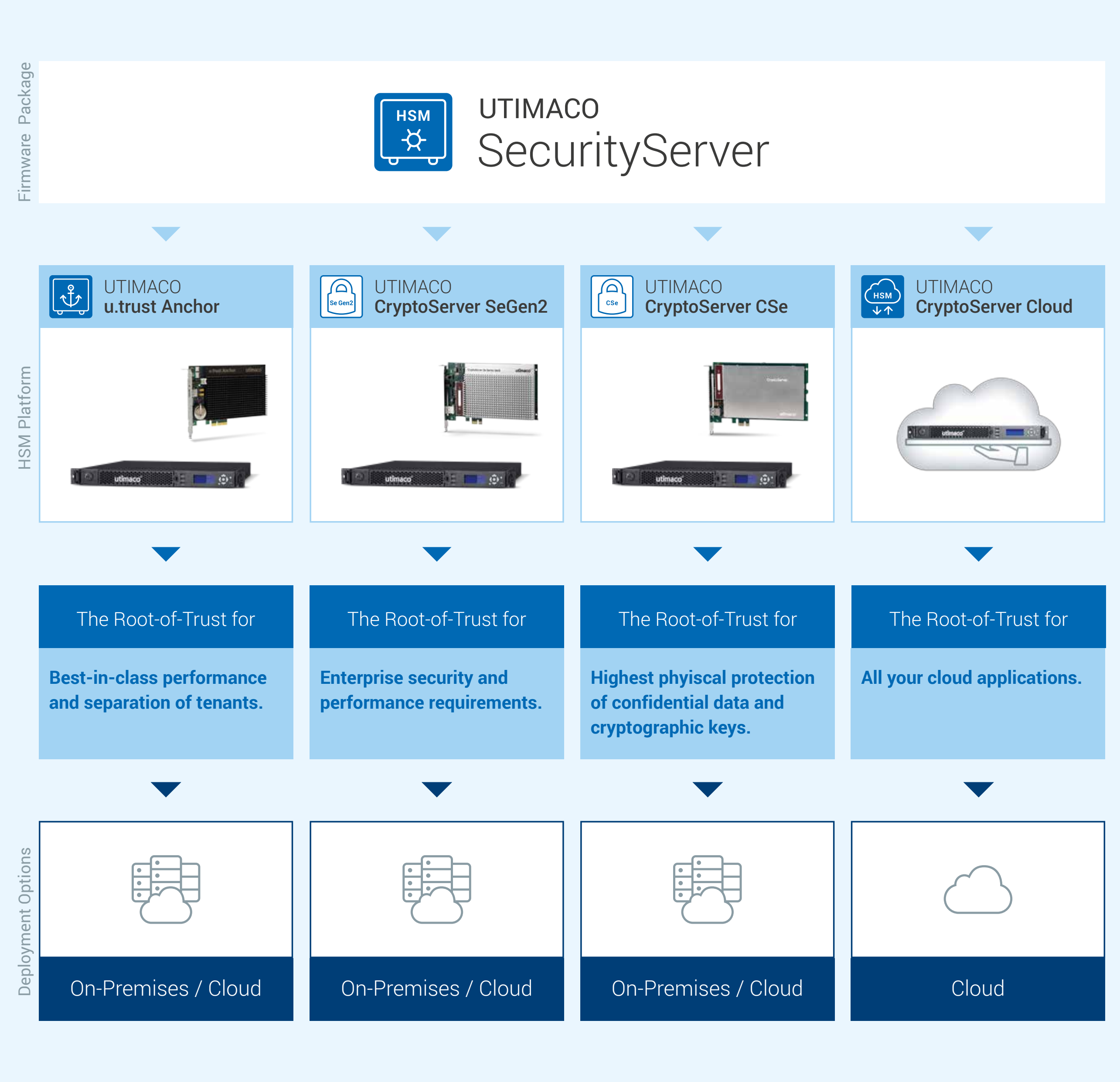
- **RSA, DSA, ECDSA** with NIST, Brainpool and FRP256v1 curves, EdDSA
- **DH, ECDH** with NIST, Brainpool, FRP256v1 and Montgomery curves
- **AES, Triple-DES, DES**
- **MAC, CMAC, HMAC**
- **SHA-1, SHA2-Family, SHA3, RIPEMD**
- **Chinese SM2, SM3 and SM4**
- **5G, Block-chain** and **PQC ready**
- **Hash-based deterministic random number generator** (DRG.4 acc. AIS 31/NIST SP800-90B)
- **True random number generator** (PTG.2 acc. AIS 31)
- **All algorithms included** in product price

Application Programming Interfaces (APIs)

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

* CryptoServer SeGen2 ** u.trust Anchor

SecurityServer Platform and Deployment Options



Firmware Package

UTIMACO SecurityServer

HSM Platform

UTIMACO u.trust Anchor	UTIMACO CryptoServer SeGen2	UTIMACO CryptoServer CSe	UTIMACO CryptoServer Cloud
The Root-of-Trust for	The Root-of-Trust for	The Root-of-Trust for	The Root-of-Trust for
Best-in-class performance and separation of tenants.	**Enterprise security and performance requirements.**	**Highest phyiscal protection of confidential data and cryptographic keys.**	**All your cloud applications.**

Deployment Options

On-Premises / Cloud	On-Premises / Cloud	On-Premises / Cloud	Cloud

Technical Specifications

UTIMACO

u.trust Anchor

Network Appliance

Physical Dimensions

- **Form factor:** 19" 1U
- **Weight**: 22.05 lb (10 kg)
- **Width:** 17.56 in (446 mm) excluding brackets
- **Depth:** 21.79 in (533.4 mm) excluding handles
- **Height:** 1.73 in (44 mm)

Connectivity

- **Interfaces:** 2 RJ45, 1 Gb/s
- 2 SFP+ 10Gb/s or 2 RJ45 1Gb/s network interfaces as optional extension

Electrical Characteristics

- **Power Supply:** Redundant field-replaceable, 2 x 100 ~ 240 V AC, 50 ~ 60 Hertz, 300 W
- **Power Consumption:** typically 55 W / 78 VA, max. 65 W / 90 VA
- **Heat dissipation:** max. 222 BTU/h

Operating Environment

- **Operating temperature:** +50°F to +122°F (+10°C to +50°C)
- **Operating relative humidity:** 10% to 95%, non-considering
- **Storage temperature:** +14°F to +131°F (-10°C to +55°C)
- **MTBF:** 134,250 hours, in acc. With Telcordia Issue 3, temperature 30°C, environment Ground Benign

Certification / Compliancee

- **Safety and Electromagnetic Compliance:** IEC/EN 60950-1, IEC/EN 62368-1, UL, CB Certificate, CE, FCC Class B
- **Environmental:** RoHS II, REACH
- **Security:** FIPS 140-2 Level 3

Time Source

- DCF-77 or GPS receiver as optional extension

PCIe Card

Physical Dimensions

- **Form factor:** Half – length, full-height 4 lane, PCI Express Card
- **Compatibility:** PCIe 1.1, PCIe 2.0 and PCIe 3.0 slots
- **Height:** 0.74 in (18.6 mm)
- **Width:** 4.38 in (111.15 mm)
- **Depth:** 6.60 in (167.65 mm) excluding brackets
- **Weight:** 0.88 lb (0.4 kg)

Connectivity

- **Interface:** PCIe x4

Electrical Characteristics

- **Power Supply:** 3.3 V supplied by PCIe connector
- **Power consumption:** max. 25 W
- **Backup battery:** 3 V lithium battery, type CR2447

Operating Environment

- **Operating temperature:** +50°F to +113°F (+10°C to +50°C)
- **Operating relative humidity:** 10% to 95%, non-considering
- **Storage temperature:** +14°F to +131°F (-10°C to +55°C)
- **MTBF:** 389.797 hours, in acc. with Telcordia Issue 3, temperature 30°C, environment Ground Fixed, temperature 50°C for parts in potting material

Certification / Compliancee

- **Safety and Electromagnetic Compliance:** IEC/EN 60950-1, IEC/EN 62368-1, UL, CB Certificate, CE, FCC Class B
- **Environmental:** RoHS II, REACH
- **Security:** FIPS 140-2 Level 3

UTIMACO

CryptoServer SeGen2

Network Appliance

Physical Dimensions

- **Form factor:** 19" 1U
- **Weight**: 22.05 lb (10 kg)
- **Width:** 17.56 in (446 mm) excluding brackets
- **Depth:** 21.79 in (533.4 mm) excluding handles
- **Height:** 1.73 in (44 mm)

Connectivity

- **Interfaces:** 2 RJ45, 1 Gb/s
- 2 SFP+ 10Gb/s or 2 RJ45 1Gb/s network interfaces as optional extension

Electrical Characteristics

- **Power Supply:** Redundant field-replaceable, 2 x 100 ~ 240 V AC, 50 ~ 60 Hertz, 300 W
- **Power Consumption:** typically 45 W / 66 VA, max. 50 W / 70 VA
- **Heat dissipation:** max. 171 BTU/h

Operating Environment

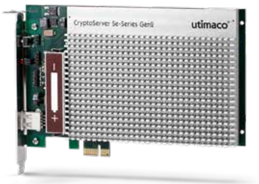
- **Operating temperature:** +50°F to +122°F (+10°C to +50°C)
- **Operating relative humidity:** 10% to 95%, non-considering
- **Storage temperature:** +14°F to +131°F (-10°C to +55°C)
- **MTBF:** 125,322 hours at 25°C / 77°F, environment GB, GC – Ground Benign, Controlled

Certification / Compliancee

- **Safety and Electromagnetic Compliance:** IEC/EN 60950-1, IEC/EN 62368-1, UL, CB Certificate, CE, FCC Class B, BIS, KC
- **Environmental:** RoHS II, WEEE
- **Security:** FIPS 140-2 Level 3

Time Source

- DCF-77 or GPS receiver as optional extension



PCIe Card

Physical Dimensions

- **Form factor:** Half – length, full-height single lane, PCI Express Card
- **Compatibility:** PCIe 1.1, PCIe 2.0 and PCIe 3.0 slots
- **Height:** 4.38 in (111.15 mm) "full" height
- **Weight:** 0.88 lb (0.4 kg)

Connectivity

- **Interface:** PCIe x1

Electrical Characteristics

- **Power Supply:** 3.3 V supplied by PCIe connector
- **Power consumption:** max. 9.9 W
- **Backup battery:** 3 V lithium battery, Ø 12 mm, length 60 mm, FDK CR 12600 SE or VARTA CR2NP

Operating Environment

- **Operating temperature:** +50°F to +113°F (+10°C to +50°C)
- **Operating relative humidity:** 10% to 95%, non-considering
- **Storage temperature:** +14°F to +131°F (-10°C to +55°C)
- **MTBF:** 360,000 hours at 25°C / 77°F, environment GB, GC – Ground Benign, Controlled

Certification / Compliancee

- **Safety and Electromagnetic Compliance:** IEC/EN 60950-1, IEC/EN 62368-1, UL, CB Certificate, CE, FCC Class B
- **Environmental:** RoHS II, WEEE
- **Security:** FIPS 140-2 Level 3

UTIMACO
CryptoServer CSe

Network Appliance

Physical Dimensions

- **Form factor:** 19" 1U
- **Weight**: 22.05 lb (10 kg)
- **Width:** 17.56 in (446 mm) excluding brackets
- **Depth:** 21.79 in (533.4 mm) excluding handles
- **Height:** 1.73 in (44 mm)

Connectivity

- **Interfaces:** 2 RJ45, 1 Gb/s
- 2 SFP+ 10Gb/s or 2 RJ45 1Gb/s network interfaces as optional extension

Electrical Characteristics

- **Power Supply:** Redundant field-replaceable, 2 x 100 ~ 240 V AC, 50 ~ 60 Hertz, 300 W
- **Power Consumption:** typically 45 W / 66 VA, max. 50 W / 70 VA
- **Heat dissipation:** max. 171 BTU/h

Operating Environment

- **Operating temperature:** +50°F to +104°F (+10°C to +40°C)
- **Operating relative humidity:** 10% to 95%, non-considering
- **Storage temperature:** +14°F to +131°F (-10°C to +55°C)
- **MTBF:** 98,244 hours at 25°C / 77°F, environment GB, GC – Ground Benign, Controlled

Certification / Compliancee

- **Safety and Electromagnetic Compliance:** IEC/EN 60950-1, IEC/EN 62368-1, UL, CB Certificate, CE, FCC Class B, BIS, KC
- **Environmental:** RoHS II, WEEE
- **Security:** FIPS 140-2 Level 3, Physical Security FIPS 140-2 Level 4

Time Source

- DCF-77 or GPS receiver as optional extension

PCIe Card

Physical Dimensions

- **Form factor:** Half – length, full-height single lane, PCI Express Card
- **Compatibility:** PCIe 1.1, PCIe 2.0 and PCIe 3.0 slots
- **Height:** 4.38 in (111.15 mm) "full" height
- **Weight:** 0.88 lb (0.4 kg)

Connectivity

- **Interface:** PCIe x1

Electrical Characteristics

- **Power Supply:** 3.3 V supplied by PCIe connector
- **Power consumption:** max. 6 W
- **Backup battery:** 3 V lithium battery, Ø 12 mm, length 60 mm, FDK CR 12600 SE or VARTA CR2NP

Operating Environment

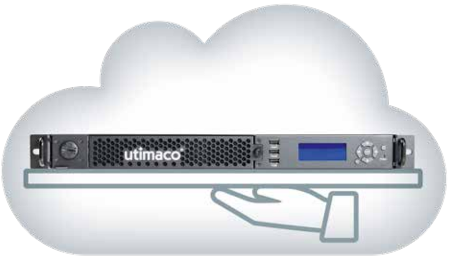
- **Operating temperature:** +50°F to +95°F (+10°C to +35°C)
- **Operating relative humidity:** 10% to 95%, non-considering
- **Storage temperature:** +14°F to +131°F (-10°C to +55°C)
- **MTBF:** 360,000 hours at 25°C / 77°F, environment GB, GC – Ground Benign, Controlled

Certification / Compliancee

- **Safety and Electromagnetic Compliance:** IEC/EN 60950-1, IEC/EN 62368-1, UL, CB Certificate, CE, FCC Class B
- **Environmental:** RoHS II, WEEE
- **Security:** FIPS 140-2 Level 3, Physical Security FIPS Level 4

UTIMACO

CryptoServer Cloud



HSM as a Service

Connectivity

- 99% availability with single connection
- 99.99% availability with redundant connections

Certification / Compliancee

- **Security:** FIPS 140-2 Level 3 Certified HSM
- Hosted in ISO/IEC 27001, PCI and HIPAA (USA only) compliant data center

Support

- **8/5 standard support:** 8 business hours
- **24/7 premium support option:** 4 hours

About UTIMACO

UTIMACO is a global platform provider of trusted Cybersecurity and Compliance solutions and services with headquarters in Aachen (Germany) and Campbell, CA (USA).

UTIMACO develops on-premises and cloud-based hardware security modules, solutions for key management, data protection and identity management as well as data intelligence solutions for regulated critical infrastructures. UTIMACO is one of the world's leading manufacturers in its key market segments.

470+ employees around the globe create innovative solutions and services to protect data, identities and communication networks with responsibility for global customers and citizens. Customers and partners in many different industries value the reliability and long-term investment security of UTIMACO's high-security products and solutions.

Find out more on utimaco.com

Headquarters Aachen, Germany

Headquarters Campbell, USA

People and IDs

People and digital identities against terrorism and cyber crime.

Transactions

Data in motion, IoT devices and financial transactions against theft and sabotage – in the cloud and on premise.

We protect

Data and Ideas

Digital economy and digital transformation processes against theft, abuse and manipulation.

Investments

With proven, future-proof technology, products and solutions that meet regulation and compliance standards.

Contact us

EMEA

UTIMACO IS GmbH

Germanusstrasse 4
52080 Aachen,
Germany

+49 241 1696 200

hsm@utimaco.com

Americas

UTIMACO Inc.

900 E Hamilton Ave., Suite 400
Campbell, CA 95008,
USA

+1 844 UTIMACO

hsm@utimaco.com

APAC

UTIMACO IS Pte Limited

50 Raffles Place,
Level 19, Singapore Land Tower,
Singapore 048623

+65 6631 2758

hsm@utimaco.com

For more information about UTIMACO® HSM products, please visit:

utimaco.com

Creating Trust in
the **Digital Society**

utimaco®