Product Brochure

SecurityServer – Secure Your Organization's Most Valuable Assets

SecurityServer – The root of trust for business applications

HSM

Utimaco
SecurityServer

Creating Trust in the **Digital Society**

utimaco® 40 YEARS

SecurityServer in a Nutshell

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

In the present world, digital transformation is affecting all companies, institutions and organizations. A broad-scale deployment of digital systems is increasing the amount of data that is being generated. Due to this, all the stakeholders in the market are looking for solutions to secure their confidential data, processes, intellectual property and user and customer data. New-generation digital systems often consist of smart devices and components that require unique digital identities and protection.

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 require the 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 40 years of experience in cryptography and Hardware Security Module (HSM) technology into a unique offering that constitutes the root of trust for the security and compliance of business applications. It adds an extra layer of security to an organization's most valuable assets. Supporting a wide range of hardware platforms, it meets the performance and security requirements of small enterprises up to large crypto infrastructures. It always offers the best price-performance ratio in different deployment scenarios.

Key Features

Hardware

Tamper-protected environment for Secure Key Operations

Easy Licensing Model

No Hidden Costs, Unlimited Client Licenses, Support to algorithms and authentication, Lower TCO

Free Software Simulator

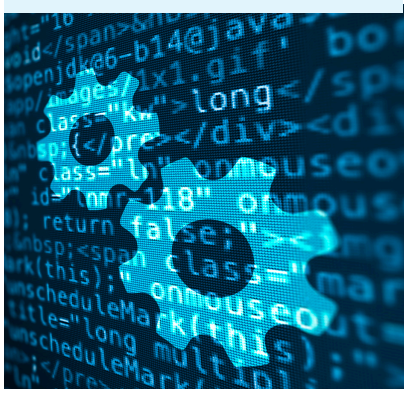
Free virtual experience of SecurityServer before purchase

Internal & External Key Storage

Flexible backup option with internal and external key storage

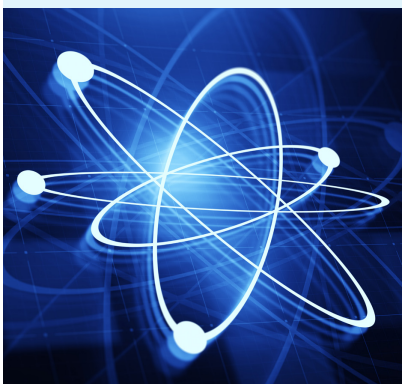
Software Development Kit

Allows the development **of custom firmware** with algorithms and functions of choice



Future-proof Solution

Special firmware extension to support **PQC algorithms** applying quantum resistance to crypto infrastructure



SecurityServer Solution

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

List of all features

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.

Easy Licensing Model

With SecurityServer there is no hidden cost. It provides the unlimited client license, support multiple algorithms and authentication options lowering the TCO.

Free Software Simulator

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

Internal & External Key Storage

Support for internal and external key storage at the location of choice, ensuring a flexible backup option.

Software Development Kit

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 software development kit enables you to finetune and optimize the functionality and performance of your HSMs.

Simulator for SDK

Test and validate the custom firmware with the simulator before actual deployment.

Future-proof Solution

Special firmware extension Q-safe on SecurityServer enables protection against the future risks from quantum computing. It supports PQC algorithms recommended by NIST & BSI. Q-safe Simulator enables testing PQC algorithms before purchase.

Multiple Authentication Options

Authenticate and protect your applications with strong authentication methods like password, key file and smart card authentication.

Seamless Integrations

SecurityServer can be seamlessly integrated with various applications available in the market for secret management to ensure the most robust security.

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.
- **All features included** in product price

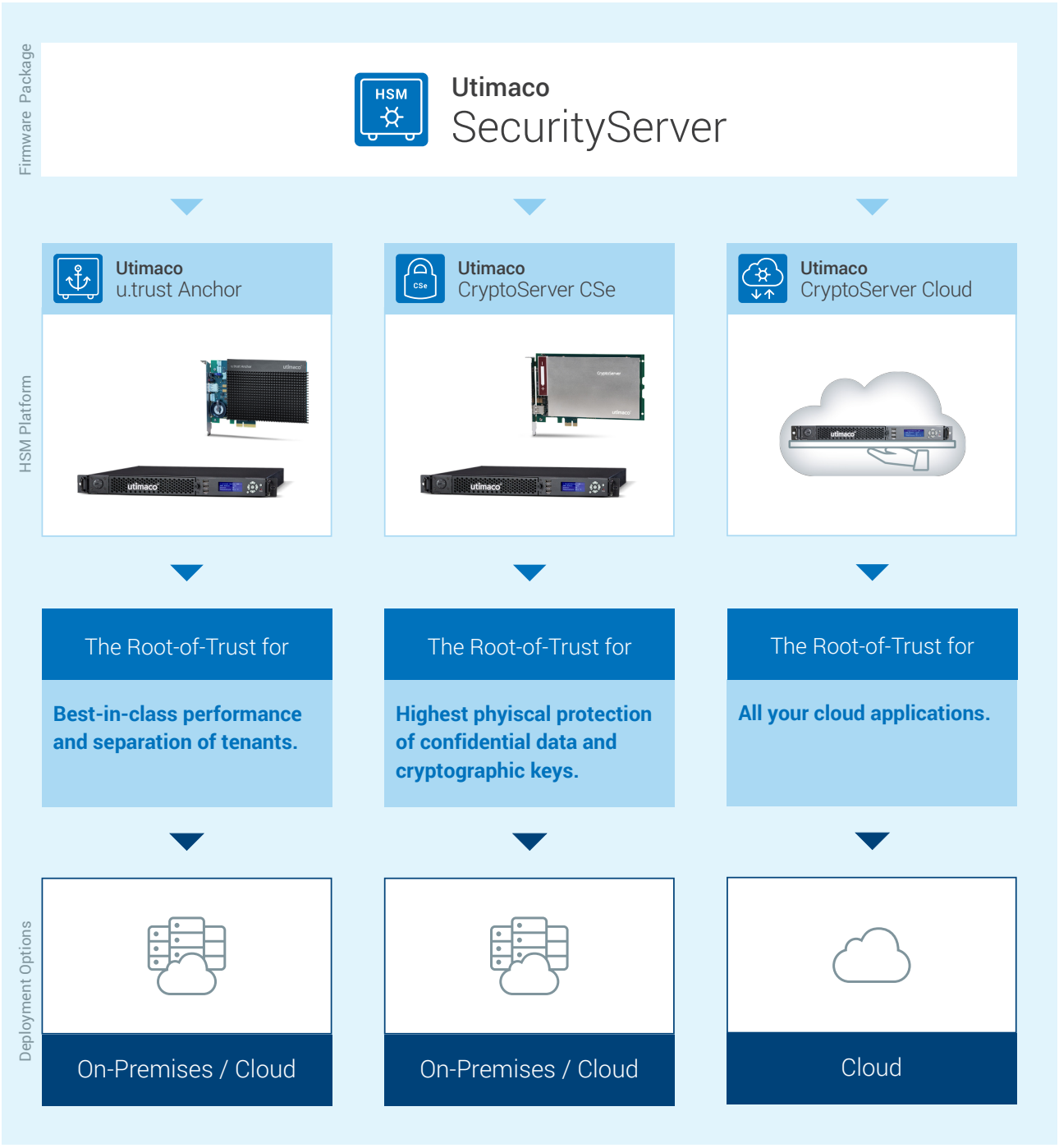
Cryptographic Algorithms

- **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)

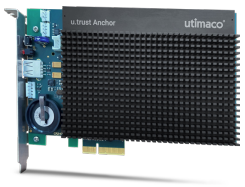
- **PKCS #11**
- **Java Cryptography Extension** (JCE)
- **Microsoft Crypto API** (CSP) and **Cryptography Next Generation** (CNG)
- **Microsoft SQL Extensible Key Management** (SQLEKM)
- **OpenSSL**
- **Cryptographic eXtended services Interface** (CXI) – Utimaco‘s high performance interface ensures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

SecurityServer Platform and Deployment Options



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-condensing
- **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 / Compliance

- **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 CR2477

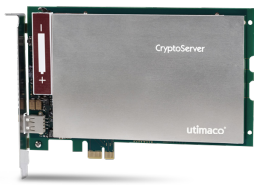
Operating Environment

- **Operating temperature:** +50°F to +113°F (+10°C to +45°C)
- **Operating relative humidity:** 10% to 95%, non-condensing
- **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 / Compliance

- **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 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-condensing
- **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 / Compliance

- **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 CR12600SE-T1 or VARTA CR2NP-T1

Operating Environment

- **Operating temperature:** +50°F to +95°F (+10°C to +35°C)
- **Operating relative humidity:** 10% to 95%, non-condensing
- **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 / Compliance

- **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

Availability

- 99% with one HSM in a single datacenter
- 99.9% with two HSMs in two datacenters each

Certification / Compliance

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

Hosting

- Fully hosted by Utimaco – no efforts from your side

Service

- Monitoring, maintenance, firmware updates of the HSM environment

Management

- Remote management possible

Support

- 24/7 support: included

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 and Public Warning Systems. Utimaco is one of the world's leading manufacturers in its key market segments.

550+ 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

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

6 Temasek Boulevard
#23-04 Suntec Tower Four
Singapore 038986

+65 6993 8918

hsm@utimaco.com

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

utimaco.com

Creating Trust in
the **Digital Society**

utimaco®