Datasheet

u.trust General Purpose HSM Se-Series

The cloud-inspired, multi-tenant General Purpose Hardware Security Module

The root of trust for business applications

HSM

Utimaco
u.trust General Purpose HSM Se-Series

Creating Trust in the Digital Society

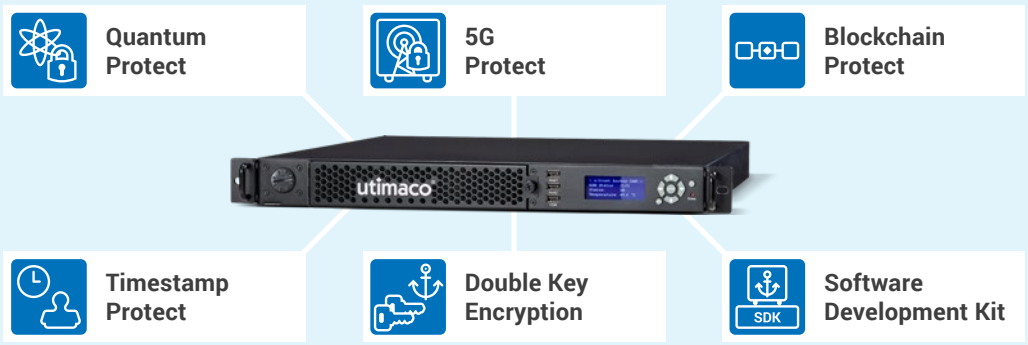
utimaco®

Next-generation General Purpose Hardware Security Module

Superior Performance • Multi-Tenant • PQC-ready • FIPS-certified • Free Simulator

The u.trust General Purpose HSM Se-Series combines superior performance with multi-tenancy.

From entry-level to high-performance use cases, all models are future-proof with post quantum cryptography readiness and are FIPS 140-2 Level 3 certified.



The u.trust General Purpose HSM Se-Series is available with multiple application options to meet your business needs.

Highlights

Performance of up to 40,000 RSA 2K operations per second

Multi-tenancy with up to 31 fully isolated containerized partitions

Designed **crypto-agile** and can be upgraded with **PQC algorithms**

FIPS 140-2 Level 3 certified (FIPS 140-3 Level 3 and Level 4 in progress)

Software Development Kit for custom implementations

u.trust General Purpose HSM Se-Series Models

	Se100	Se2k	Se5k	Se15k	Se40k
Signature Creation (Signatures / s)					
RSA-2048	101	2,050	5,100	15,000	40,000
Key Generation (Key / s)					
RSA-2048	2.53	9.48	10.20	11.10	12.40
ECDSA P-256 bit	267	1,213	2,016	1,168	3,531
Encryption / Decryption (Mbytes / s)					
AES 256 – GCM	37.00	120.90	127.40	125.90	124.60
AES 256 – ECB	67.90	199.10	188.80	193.30	186.40
Containers					
	1	4	8	4	12, 16, or 31

Not sure which model is best for your use case?
Contact us for detailed performance data on our various models and to schedule a consultation.

Key Benefits

Performance of up to 40,000 RSA 2K operations per second

u.trust General Purpose HSM Se-Series are available in various models from entry-level to high-performance use cases.

Multi-tenancy for high availability, scalability, and flexibility

Manage fully isolated, standalone processes in one HSM with the containerization option. Choose between **1, 4, 8, 12, 16, or 31 containers**.

The container approach allows you to run several applications simultaneously within an HSM, ensuring independent operation. You can also use the containers for redundancy purposes.

Key Partitioning System

Multiple PKCS #11 partitions per cHSM available for application separation and key partitioning.

Crypto-agile and PQC-ready

Designed with crypto-agility in mind, the HSMs are in-field upgradable with PQC algorithms such as CRYSTALS-Kyber, CRYSTALS-Dilithium, LMS, HSS, XMSS, and XMSS-MT.

FIPS-certified up to 140-2 Level 3

The u.trust platforms are certified up to FIPS 140-2 Level 3 and can be optionally operated in FIPS mode.

Software Development Kit for custom implementations

Develop custom firmware, implement proprietary algorithms, or establish custom key derivation functions with the SDK.

Flexible Key Storage

The u.trust platforms both support external and internal key storage.

Free, fully functional simulator

Test development and integration capabilities in your environment – no purchase, delivery, or installation needed.

https://utimaco.com/downloads/simulators-and-sdks/securityserver-simulator

Cryptographic Algorithms

All algorithms included in the product price

- RSA, DSA, ECDSA with NIST, Brainpool and FRP256v1 curves, EdDSA
- DH, ECDH with NIST, Brainpool, FRP256v1 and Montgomery curves
- Edwards curves Ed25519 and Ed448
- AES, Triple-DES, DES
- MAC, CMAC, HMAC
- SHA-1, SHA2-Family, SHA3, RIPEMD
- Chinese SM2, SM3 and SM4
- Hash-based deterministic random number generator (DRG.4 acc. AIS 31/ NIST SP800-90B)
- True random number generator (PTG.2 acc. AIS 31)

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

Deployment Options

- On-premise: LAN Appliance, PCIe Card
  Our on-premise options enable you to host the product directly on-site within your own network or data center.
- As a Service
  Our as-a-service options, hosted by Utimaco in certified datacenters, encompass comprehensive support from set-up to deployment to ongoing maintenance.

Centrally monitor and manage your u.trust Se-Series HSMs with **360 HSM Monitoring**

Certifications

- FIPS 140-2 Level 3
- Operation in FIPS Mode is possible
- CC / NITES
- In Progress: FIPS 140-3 Level 3 and Level 4
- In Progress: PCI PTS HSM v3

Hardware

Network Appliance

PCIe Card

Physical Dimensions

Form factor	19" 1U	Half-length, full-height single lane, PCI Express Card
Weight	22.05 lb (10 kg)	0.88 lb (0.4 kg)
Size	W 17.56 in × D 21.79 in × H 1.73 in (W 446 mm × D 533.4 mm × H 44 mm) excluding brackets	W 4.38 in × D 6.60 in × H 0.74 in (W 111.15 mm × D 167.65 mm × H 18.6 mm)

Connectivity

Interfaces	2 RJ45, 1 Gb/s 2 SFP+ 10Gb/s or 2 RJ45 1Gb/s network interfaces as optional extension	PCIe x4 Compatibility: PCIe 1.1, PCIe 2.0 and PCIe 3.0 slots

Electrical Characteristics

Power Supply	Redundant field-replaceable, 2 x 100 ~ 240 V AC, 50 ~ 60 Hertz, 300 W	3.3 V supplied by PCIe connector
Power consumption	22.05 lb (10 kg)	max. 25 W
Heat/battery	Heat dissipation: max. 171 BTU/h	Backup battery: 3 V lithium battery, type CR2477

Operating Environment

Operating temperature	+50°F to +122°F (+10°C to +50°C)	+50°F to +113°F (+10°C to +50°C)
Operating relative humidity	10% to 95%, non-condensing	10% to 95%, non-condensing
Storage temperature	+14°F to +131°F (-10°C to +55°C)	+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	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

	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

Extras

Time Source	DCF-77 or GPS receiver as optional extension	–

The u.trust Application Ecosystem

Extend the capabilities of your u.trust General Purpose HSM Se-Series model with the following extensions.

SDK

Professional Development Kit for u.trust General Purpose HSM Se-Series

Enables custom firmware development based on algorithms and functions of choice

- Create new or proprietary algorithms, key derivation functions, or complex protocols
- Full control for the developers

Quantum Protect

Applying Quantum-resistance to applications and use cases

The extension with Post Quantum Cryptography algorithms recommended by NIST and BSI

- CRYSTALS-KYBER
- CRYSTALS-Dilithium
- XMSS, XMSS-MT
- HSS, LMS

5G Protect

Specially designed for network element providers in mobile networks

The scalable and customizable solution for subscriber authentication and key agreement in mobile networks

- Decryption of concealed subscriber identities in 5G networks
- For subscriber identity de-concealing, authentication, and key agreement (AKA) in mobile networks
- Fulfills 3GPP security requirements

Blockchain Protect

Securing sensitive assets in Blockchain processes

Securing sensitive identities, keys and data in DLT computing platforms.

- Provides certified blockchain-related algorithms such as
  - BIP32/44
  - SLIP-010
- Provides consensus signing and verification using MultiSign & BLS
- Integrated DLT support enables execution of Bitcoin and Ethereum (ETH) use cases

Timestamp Protect

Highly secure, reliable, and accurate timestamps

Reliable proof of existence and status of documents and electronic records at a specific point in time

- Network Time Protocol (NTP) for synchronization with external time server
- Integrated GPS receiver or optional DCF77 receiver
- Compliance with ETSI TS 102 023 “Policy Requirements for Timestamping Authorities” and TS 101 861 “Time stamping profile”

Double Key Encryption

Two-tier security for the most sensitive data in Azure

Double key encryption solution with Microsoft Purview

- Key generation and storage inside a tamper-proof HSM
- Data is encrypted with two keys – one stored in Azure, one in the HSM
- Extra layer of security for cloud-stored data

One hardware, multiple firmware options to fit your personal security need.

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
info@utimaco.com

Americas

Utimaco Inc.

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

+1 844 UTIMACO
info@utimaco.com

APAC

Utimaco IS Pte Limited

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

+65 6993 8918
info@utimaco.com

For more information about Utimaco® products, please visit:

utimaco.com

Creating Trust in
the **Digital Society**

utimaco®