



Leading Payment Hardware Security Module in the Industry

Superior Performance • Remote Management • Multi-Tenant • Native Support • EMV Processing • Compliance Driven

The Atalla AT1000 Payment HSM secures the payment ecosystem and plays a crucial role in securing inter-banking communication, user- and card authentication, as well as user data protection for both in-person and remote payments transactions.

Key use cases



Highlights

Superior performance
of up to 10,000 transactions per second.

Remote Management
via the PCI PTS KLD certified Utimaco C3, and Secure Configuration Assistant – Windows (SCA-W).

Multi-Tenant Architecture – less to administer and operate thanks to the power of partitions

Native support – payment applications natively support the Atalla AT1000 Payment HSM's APIs.

EMV Card Processing – supports all the major Payment Cards.

Compliance Driven – FIPS 140-3 Level 3 and FIPS 140-2 Level 4 (physical design) compliant, and PCI PTS v3 certified.

Most secure hardware formfactor with double-locking pick-resistant locks and NIC Bonding.

Available as Payment HSM-as-a-Service. Choose between an on-premises or cloud deployment.

Key Benefits

Superior performance

With the unrivaled speed of 10,000 transactions per second, the Atalla AT1000 Payment HSM is the fastest multi-core HSM on the market. It has been specifically designed for retail use cases and cardholder authentication, providing unique speed for processes in the cashless payment transaction lifecycle.

Remote Management

Unlike with any other HSM on the market, key custodians can be geographically dispersed, working independently of one another. However, with the Atalla AT1000 Payment HSM, loading Master File Keys (MFK) and lower-level keys does not need to be done at the same time at the same location. This not only saves travel costs, but also ensures workflows are not impeded. Configure commands, define parameters, calculate cryptograms, and inject cryptographic keys – all remote.

Multi-Tenant Architecture

The Atalla AT1000 Payment HSM comes with 10 partitions. Our unique partitioning capability allows vendors to consolidate applications into fewer HSMs. Since each domain has its own MFK, you can isolate access, security policies and separate administrative access independent from other partitions.

Native Support Payment App Ecosystem

Payment applications natively support the Atalla AT1000 Payment HSM's APIs. Provides superior hardware security to deliver maximum privacy, integrity, and performance for host applications.

EMV Card Processing

Supports MasterCard CVC, Visa CVV, American Express CSC, MasterCard CVC3, Visa DCVV, Discover DCVV, American Express, Expresspay, and Visa cloud based payments.

Compliance Driven

The Atalla AT1000 is PCI PTS HSM v3 certified for the most demanding application profile, as well as compliant with: FIPS 140-3 Level 3 • FIPS 140-2 Level 4 (physical design) • TR-31 Key Block for AES and TDES key management

Most Secure Hardware Formfactor

Tamper-responsive with the ability to act in response to side-channel attacks. Provides the highest hardware security to deliver maximum privacy, integrity, and performance for host applications. Offers: Double redundant power supplies • Dual-locking bezel and Medeco pick-resistant locks • Isolated domain access due to unique partitioning capability • Redundancy & Failover. Teaming/NIC Bonding – no single point of failure

Available as Payment HSM as-a-Service

Connect seamlessly to a group of Atalla AT1000 Payment HSMs with Utimaco's Payment HSM as-a-Service. As a fully managed, subscription-based PCI PIN compliant service, the Payment HSM-as-a-Service can be accessed globally, without having to invest in any on-premises devices.

Upgradable performance
in increments of 500 TPS, up to 10,000 TPS!

Payment Standards

NIST security standards SP800-90 (RBG), SP800-38A, SP800-67

Supported algorithms

- Asymmetric algorithms: RSA 1024 to 4096
- Hashing algorithms: SHA-1 to SHA512

Performance

- Up to 10,000 TPS

API and Communication Protocol

- TCP/IP sockets, TLS sockets, REST API

Using open API there is no host side software from Utimaco that resides on the server; this has a number of advantages, such as:

- Easy replacement of the HSM in case of failure or new product
- Possible to use off the shelf load balancers
- Easy to extend capacity with more HSMs
- Upgrading the operating system or the payment application has no impact on the HSM version (no need to upgrade an API)
- No dependencies on operating system

Logical Security

- **Symmetric Key management**
TR-31, X9.24
(incl. AES and TDES DUKPT), X9.17, APACS 40/70, GICC/ZKA
- **Asymmetric Key management**
TR-34, legacy RSA keying protocols
including those for Diebold and NCR ATMs
- **Data Encryption**
AES, RSA OAEP, DES/TDES (X3.92, ISO 10126-2, X9.52)
- **Message authentication**
CMAC (AES and TDES), HMAC (SHA1 and SHA256),
CBC MAC (ANSI X9.9, ANSI X9.19, ISO 9797-1, ISO 16609, ISO 9807)
- **Digital signatures**
RSA PKCS#1 v1.5, PSS, ISO 9796-2, and ECDSA
- **PIN management and security**
ANSI X9.8/ISO 9564 PIN blocks 0 to 4, plus legacy techniques
- **PIN verification**
IBM 3624, PVV, Atalla Bi-Level DES, Diebold, NCR
- **Payment Card Processing**
MasterCard CVC, Visa CVV, American Express CSC, MasterCard CVC3,
Visa CVV, Discover DCVV, American Express, Expresspay, and Visa Cloud
based payments
- **EMV-based smart card support**

Deployment Options

- **On-premise:** Physical 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 Atalla
AT1000 Payment HSM
with 360 HSM
Monitoring

Hardware

Physical Security and Specifications

Appliance Security	Rack-mountable (1U), physically fortified, double-locking bezel, Medeco pick-resistant locks
Electrical Security	Dual redundant power supplies, out-of-range temperature and voltage detection, low-battery voltage detection
Controls	Power on/off switch, unit ID switch, LCD control panel
Weight	27.8 lb (12.6 kg)
Size	W 19.0 in x D 26.0 in x H 1.75 in (W 482.6 mm x D 660.4 mm x H 44.5 mm) excluding brackets

Connectivity

Communications Ethernet	TCP/IP, TLS 1.2 (only) with TLS Client Certificate Validation and CN Whitelisting 2 x 10Gbps Copper and 2 x 10Gbps equipped with a 10G SFP + optical transceiver
Support for DHCP	Yes
Connection	10/100/1000BASE-T (RJ45) auto-sensing Supports Static Routes
Communication Protocols	TCP: host and management commands UDP: host commands
Networking Standard	IEEE 802.1Q

Electrical and thermal characteristics

Rated input voltage	100 to 127 VAC 200 to 240 VAC
Rated input current	5.0 A to 3.0 A 2.4 A at 200 VAC
Rated input frequency	50 Hz to 60 Hz
BTUs per hour	1195 at 100 VAC 1195 at 200 VAC
Power Consumption	Rated steady-state power: 90 W Maximum peak power: 100 W

Operating Environment

Operating temperature	0° C to 40° C (32° F to 104° F)
Operating relative humidity	5% to 95%, non-condensing

Certification / Compliance

Industry standards	FIPS 140-3 Level 3 certified HSM PCI PTS HSM V3 PCI DSS PCI PIN TR-31 Key Block Support
---------------------------	---

EMEA

Utimaco IS GmbH

📍 Krefelder Str. 220,
52070 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



Reliable VS-NfD Approved Encryption of Hard Drives

Approved for VS-NfD / NATO-RESTRICTED / UE/EU-RESTRICTED • Sector-based, full disk encryption • No impact on performance

Utimaco DiskEncrypt is a software for reliable, sector-based hard drive encryption approved for VS-NfD, RESTREINT UE/ EU RESTRICTED and NATO RESTRICTED data.

DiskEncrypt is the VS-NfD approved solution for all government customers and the classified security industry who want to use conventional laptops in the VS-NfD environment.

Developed specifically to meet the requirements of the German BSI, it is a sector-based, full disk encryption solution for laptops that effectively prevents unauthorized access to (personal) data on the hard drive if the laptop is stolen or lost and the Windows password is bypassed.



Highlights

Approved for VS-NfD RESTREINT UE / EU-RESTRICTED and NATO-RESTRICTED

Sector-based, complete hard disk encryption

Reliable data security without loss of performance

Secure sharing of laptops

Convenient and user-friendly login process

Key Benefits

Approved by the BSI for data with the classification RESTREINT UE / EU RESTRICTED, NATO RESTRICTED and VS-NfD

Designed in accordance with the requirements of the BSI and specially developed for German public authority customers and the secret-protection industry.

Sector-based, complete hard disk encryption

Reliable data security through user-transparent partition encryption with reliable encryption algorithms.

No impact on device performance

DiskEncrypt uses proven encryption algorithms and maximizes data security by encryption of all system files, including swap and temporary files, without affecting device performance.

Highest security even with shared use of laptops

Offer the possibility of several people using the laptop without the shared use of passwords or smart cards.

Convenient login process

Based on the unchanged Windows operating system login process after the pre-boot authentication DiskEncrypt provides secure and convenient device usage for the users.

Functionalities

Secure and convenient pre-boot authentication

- Authentication before hard-disk boot using username and password or smart card
- Effective protection against unauthorized access to data in the event of theft or loss of the laptop
- Effective protection against bypassing the Windows password
- Allows sharing of laptops with the same data security
- Simple user guidance through unchanged Windows operating system login process after pre-boot authentication

User-transparent partition scrambling

- Use of the encryption algorithm AES-256-XTS
- Encryption using either full partition encryption or fast initial encryption

Secure entropy generation

- Using Utimaco's CryptoServer General Purpose HSM with VS-NfD Protect (BSI approved)
- By means of a BSI-approved true random number generator and smart card integration

Microsoft upgrade mechanism support

- Support of the respective Windows 10 Semi-Annual Channel (SAC) from version 1809
- Support of the integrated Microsoft In-Place Upgrade mechanism
- Allows Windows 10 SAC to be upgraded to a successor version while retaining encrypted partitions / disks

Support for various smartcards

- Atos CardOS 5.0 and 5.3 (BSI approved)
- Telekom TCOS 3
- Telekom TCOS 4 (BSI approved)



Technical Requirements

Client

- Support for Windows 10 and 11
- CCID compatible and supported smart card reader

DiskEncrypt Server

- Windows Server 2016 Standard 64-bit and later

DiskEncrypt Management Center

- Windows 11 from version 22H2
- Windows 10 64-bit Pro and Enterprise from version 1809 onwards
- Windows Server 2016 Standard 64-bit and later

DiskEncrypt Database Server

- Microsoft SQL Server 2017 Express, Standard or Enterprise 64-bit and later

EMEA

Utimaco IS GmbH

📍 Krefelder Str. 220,
52070 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



The most interoperable and integrated Key Manager in the Market

Scalable to thousands of nodes and millions of keys • Competitive APIs • Highest Level of Security on the Hardware Level

Utimaco's ESKM provides a single pane of glass for all cryptographic keys.



Highlights

Scalable to thousands of nodes, and millions of keys

Competitive APIs

Highest Level of Security on the Hardware Level

Cloud and on-prem workloads

Simplified Key Lifecycle Management

Secure Audit Logging

Supported Cryptographic Algorithms

Custom Integrations

Pre-Installed Software

Key Benefits

Scalable to thousands of nodes, and millions of keys

Unprecedented capacity for >2 million keys, >25,000 clients, and thousands of ESKM nodes per distributed cluster

Competitive Application Programming Interfaces (APIs)

OASIS KMIP (Key Management Interoperability Protocol) • RESTful interface API • KMS

Highest Level of Security on the Hardware Level

Security hardened Linux-based server appliance with encrypted redundant storage • FIPS-compliant architecture*, certificate-based authentication, and built-in CA • Embedded Utimaco GP HSM for highest local key protection** • Integration with CC and VS-NfD certified Utimaco GP HSM for key protection compliant to specific compliance requirements***

Cloud and on-prem workloads

Enterprise Secure Key Manager offers organizations of all sizes a superior solution for key storage and management capabilities, delivering high security and compliance; whether on premises or in the cloud.

Simplified Key Lifecycle Management

Enables unified enterprise key management with reliable policy controls, centralized administration, and comprehensive audit trails.

Secure Audit Logging

Complete with digitally signed logs and key lifecycle activities, reducing audit costs, enhancing visibility, and accelerating operational efficiency.

Supported Cryptographic Algorithms

Such as AES, 3-Key Triple DES, HMAC, RSA, and ECDSA key types • TLS and on-demand backups with SSH key authentication, for secure administrator remote access

Custom Integrations

- Simplified RESTful API interface for key CRUD (Create, Read, Update, Delete) operations and crypto
- Supports open client libraries such as KMIP, OpenKMIP and PyKMIP
- Conforms with KMIP 1.0 through 2.1 specifications
- Implements auto-registration with native XML-based KMS protocol
- NIC Teaming Support

Pre-Installed Software

- Comprehensive monitoring, recovery, scheduled backups, log rotations, and restore functionality
- Web browser GUI and Command Line Interface supported
- SNMP alerts and SIEM log monitoring
- TLS and on-demand backups with SSH key authentication, for secure administrator remote access

* FIPS 140-3 Level 2 appliance (pending), FIPS 140-2 L3 and L4 (embedded HSM) , ** For ESKM L3 and ESKM L4 (physical), *** for vESKM

Deployment Options

Enterprise Secure Key Manager (ESKM) provides easy deployment and licensing processes. It can be effortlessly installed and configured; simply drop in as hardware or virtual appliance. Access transparent client licensing, with **no hidden costs attached to key volume or scalability.**

ESKM Product	Deployment Type	FIPS Security	Embedded HSM
ESKM L1	Virtual appliance	FIPS 140-2 Level 1	n/a
ESKM L2	1U appliance	FIPS 140-3 Level 2 (certification pending)	No
ESKM L3	1U appliance	FIPS 140-2 Level 3 (via FIPS-certified embedded HSM)	Utimaco GP HSM
ESKM L4	1U appliance	FIPS 140-2 Level 4 (via FIPS-certified embedded HSM)	Utimaco GP HSM

Virtual Enterprise Secure Key Manager (vESKM)

Easy Implementation of a virtual key management strategy with vESKM.

- Pre-configured and hardened security virtual appliance
- Enables continuous local and remote access to your encryption keys
- Fully integrable with Utimaco’s CC and VS-NfD certified HSM to protect keys at rest

Get a fully functional 60 day trial of vESKM*



Network Appliance



Physical Dimensions

Form factor	19" 1U
Weight	
– ESKM L2	24.9 lbs (11.3 kg)
– ESKM L3/L4	27.8 lbs (12.6 kg)
Size	W 19 in x D 26 in x H 1,75 in (W 482.6 mm x D 660.4 mm x H 44.5 mm)

Connectivity

Communications ethernet	TCP/IP, TLS 1.2 (only)
Connection	10/100/1000BASE-T (RJ45) auto-sensing

Electrical and Thermal Characteristics

Rated input voltage	100 to 127 VAC / 200 to 240 VAC
Rated input current	5 A – 3 A at 200 VAC
Rated input frequency	50 Hz to 60 Hz
Rated input power	350 W at 200 VAC
BTUs per hour	1195 at 100 VAC/ 1195 at 200 VAC
Rated steady-state power	250 W at 100 VAC / 250 W at 200 VAC
Maximum peak power	400 W at 100 VAC (3 sec.)

Operating Environment

Operating temperature	32°F to 104°F (0°C to 40°C)
Operating relative humidity	5% to 95%, non-condensing

Physical Security

Appliance security	Rack-mountable (1U), physically fortified, double-locking bezel, Medeco pick-resistant locks
Electrical security	Dual redundant power supplies, out-of-range temperature, and voltage detection
Controls	Power on/off switch, unit ID switch, LCD control panel

Certification / Compliance

Certifications	FIPS 140-2 Levels 1, 2, 3 and 4 (physical)**
Compliance	Meets NIST SP 800-131A Standards Compliant to CC EAL2+ Controls for PCI-DSS, HIPAA, EU data privacy laws, and other regional privacy mandates
Safety	UL/CUL, CE, TUV, BIS, BSMI, SII
Emissions	FCC Class B, VCCI, BSMI, C-Tick, IC, KCC
Environmental	RoHS, REACH

* Registration required., ** depending on the ESKM Deployment Option

EMEA

Utimaco IS GmbH

Krefelder Str. 220,
52070 Aachen,
Germany

+49 241 1696 200
info@utimaco.com

Americas

Utimaco Inc.

900 E Hamilton Ave,
Suite 400
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



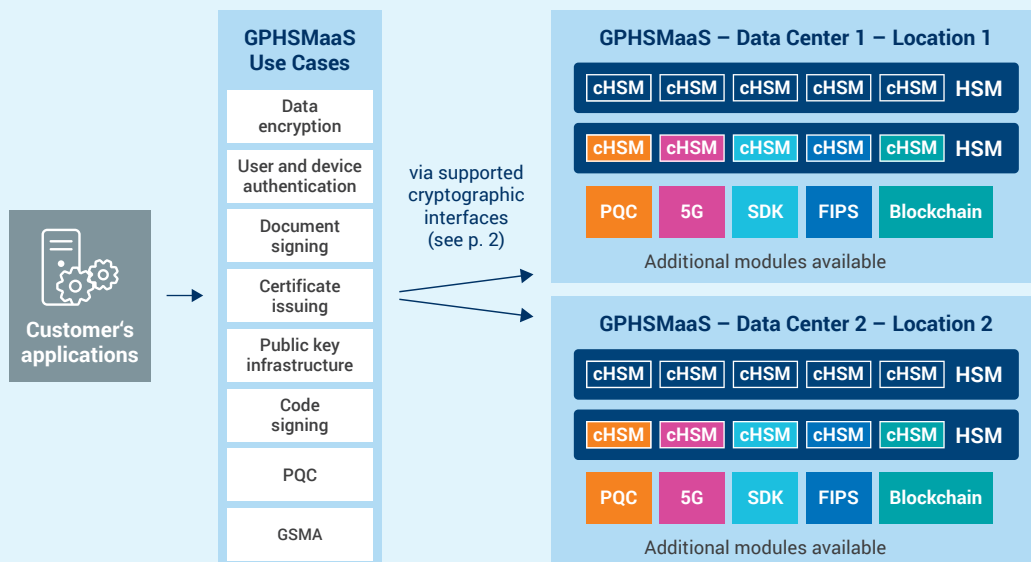
Protect Data with Flexible and Scalable General Purpose HSM as a Service

Lower Operational Costs • FIPS-Certified • No CSP vendor lock-in • Fully Hosted • Zero Maintenance

General Purpose HSM-as-a-Service protects sensitive data through secure key generation, storage and management.

Delivered from resilient data centers, it enables flexible deployment across multi-cloud and hybrid environments.

As a fully managed service, it reduces total cost of ownership while providing high scalability and built-in readiness for post-quantum cryptography.



Highlights

Lower Operational Costs

Reduce your costs by adopting a flexible and scalable solution.

FIPS 140-3 Level 3 Certified

Protect your data with a highly secure service based on FIPS-certified GP HSMs.

No CSP Vendor Lock-in

Gain full flexibility in choosing a cloud strategy that fits your needs.

Fully Hosted

Switch to a fully hosted service that can be deployed instantly.

Zero Maintenance

No operational overhead or maintenance costs with fully managed service provided.

Key Benefits

Lower Operational Costs

Reduce total ownership costs with a predictable and flexible OPEX model. Eliminate upfront hardware investments, reduce staffing costs, and benefit from transparent subscription pricing with predictable costs and seamless scalability.

FIPS 140-3 Level 3 Certified

Built on an HSM-grade root of trust, the service meets the highest security standards. GP HSMs are FIPS 140-3 Level 3 certified, ensuring secure and compliant operations.

No CSP Vendor Lock-in

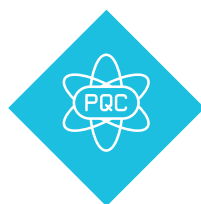
GP HSM as a Service is multi-cloud and cloud-agnostic and integrates seamlessly with major cloud providers, including Amazon Web Services, Microsoft Azure, and Google Cloud, giving you the flexibility to choose the right cloud strategy for your business.

Fully Hosted

Gain operational efficiency by offloading complexity to a fully hosted, instantly deployable service. Delivered from resilient, high-availability data centers, it enables global access and seamless scaling to meet your security needs.

Zero Maintenance

Utimaco provides a fully managed service covering maintenance, updates, and HSM lifecycle replacement. This reduces operational overhead, maintenance costs, and infrastructure management effort.



Service Benefits and Capabilities

- Predictable OPEX subscription, no physical footprint.
- Fully managed service, including firmware updates, operations, and maintenance.
- Scale as you grow.
- Rapid deployment.
- Access to trial and Shared Test Service.
- Based on Utimaco's market-leading GP HSMs.

Certifications and Compliance

Fulfilling relevant security and regulatory certifications, as well as various data security requirements:

- ISO 27001, ISO 9001, ISO 14001, SOC 2 (US data centers)
- GDPR
- PCI DSS
- GSMA

Supported Cryptographic Interfaces

- PKCS #11
- Java Cryptography Extension (JCE)
- Microsoft Crypto API (CSP), Cryptography Next Generation (CNG), and SQL
- Extensible Key Management (SQLEKM)
- OpenSSL
- Utimaco's comprehensive Cryptographic eXtended services Interface (CXI)

Service Setup

- Fully redundant setup per data center, with geo-redundancy per availability zone.
- State-of-the-art IT design enabling local disaster recovery and high availability.
- Highly fault-tolerant service and infrastructure setup.
- Secure server rooms with shared or dedicated HSM.
- Key security remains under your control with your master key.

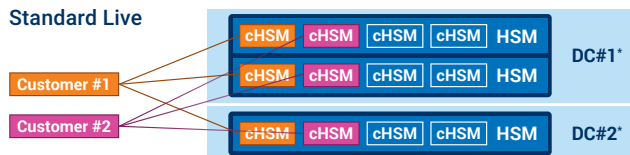
Deployment Models

- Utimaco's data centers
- Hybrid cloud: private and public
- Multi-cloud
- IBM Cloud co-located data centers

Service Options

Shared or dedicated GPHSMaaS accessible in containerized HSMs (cHSMs). Test environments are available.

Standard Live



*Geographically separated data centers

Global and Regional Availability

Our services operate across multiple geographically separated data centers ensuring continuity even during major incidents or regional disruptions.



Service Management: GP HSM as a Service

Manage and configure GP HSM service from one central location. Perform tasks such as:

- Report collection
- Consumption view
- Service administration
- User management



EMEA

Utimaco IS GmbH

Krefelder Str. 220,
52070 Aachen,
Germany

+49 241 1696-0
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



Protection for Business-Critical Data – Convenient. Reliable. Secure.

Transparent Encryption ♦ Data Protection ♦ Compliance Fulfillment ♦ Access Management ♦ Secure Sharing

Utimaco's LAN Crypt File and Folder Encryption offers a software-based data encryption solution for securing files and folders. It is based on a role-split approach ensuring separation between system administration and security management. LAN Crypt 2Go is the logical extension highly relevant for secure file sharing, both internally and externally, with user-managed keys.

Highlights

Transparent Encryption of the organization's data without affecting the established/familiar workflows

Data Protection at rest and in motion, preventing unauthorized access and interception

Compliance Fulfillment – Worldwide

Role-based Access Management for assigning specific permissions based on user roles

Secure file sharing solution that works with on-demand encryption and user-managed keys

30-day Free Trial – Explore the solution with a free 30-day trial before you buy.

Utimaco's Data Encryption Solution



Securing Data privacy



Securing Collaboration and File Sharing



Preventing Unauthorized Access



Securing Intellectual Property



Securing Remote Workforce



Securing Financial Records



Data Backup and Recovery



Securing Email and Communication

Key Benefits

Transparent Encryption

Transparent encryption ensures that users are unaware of the encryption process, seamlessly integrating it into their workflow without necessitating changes to established organization procedures.* Encryption rules are defined and managed by the security officer, allowing for secure data handling without disrupting daily operations.

Data Protection at Rest and in Motion

All files are encrypted and decrypted directly on the users' endpoint (e.g., PC/Laptop, Tablet, Smartphone, Terminal Client) regardless of the storage location (e.g. remote share, Cloud Storage, Data Center, local drive, removable device). This ensures that data remains encrypted throughout the transfer, safeguarding against unauthorized access and interception.*

Compliance Fulfillment

LAN Crypt File and Folder Encryption solution helps to fulfill various regulations worldwide. This includes VS-NfD, TISAX, and KHZG in Germany. GDPR, NIS2, and DORA on the EU level. CCPA, HIPAA, and Executive Order on Improving the Nation's Cybersecurity in the USA. Philippines Data Privacy Act of 2012, PDPA, and the company's individual security policies can also be fulfilled.

Role-based Access Management

Organization data is fully encrypted and can only be accessed and decrypted by users with corresponding access privileges. Organizations can flexibly decide which users or groups can access which kinds of data. With a role split, the organization ensures that the system admin can access the files but not read them, and the security officers can manage keys to files but not the files themselves.

Secure Sharing

LAN Crypt 2Go, as a logical extension, allows the secure external sharing of documents with encryption keys managed by the users. They can simply set a password for a specific file and share it with people inside and outside their organization, e.g., external consultants. The recipients can then decrypt it with the corresponding password. Only one party needs to have LAN Crypt File and Folder Encryption installed. LAN Crypt 2Go web portal allows encrypting or decrypting data from within the browser – no installation needed. A detailed comparison is on the next page.

30-day Free Trial

Experience the power of data encryption solution with a 30-day free trial. To gain a handful of experience of LAN Crypt File and Folder Encryption and LAN Crypt 2Go (Business-level), please contact our sales team.

* Also applicable to LAN Crypt 2Go

	LAN Crypt File and Folder Encryption	LAN Crypt 2Go
Key Management	Centrally managed	User managed
Key Custody	Organization or 3 rd party via integration with Utimaco Enterprise Secure Key Manager	User or 3 rd party
Encryption	Policy-driven and transparent	User managed and on-demand
Data Sharing	Internally	Internally and externally
Key Sharing	Not supported	Supported
Transparent Encryption	Supported	Supported
Platform Support	Windows/macOS/Mobile	Windows/macOS/Mobile/Linux/Browser
OEM-Rebranding	Not applicable	Supported
Scope of Use	Business	Business and personal use
Installation	Deployment and central management	Instant installation and use, and zero-install (browser app)
Cloud Integration	Supported	Supported
Outlook Integration	Not applicable	Supported
Role-based Administration	Supported	Not applicable
30-day Trial Period	Based upon agreement	Based upon agreement (Business use) Free for personal use (no trial period required)



LAN Crypt 2Go

LAN Crypt 2Go can be seamlessly integrated into LAN Crypt File and Folder Encryption and as a Service, along with the option for importing password-based keys. LAN Crypt 2Go licenses are always included in the LAN Crypt File and Folder Encryption purchase; however, the enterprise version can also be purchased separately. LAN Crypt 2Go is free for personal use.



Learn more about LAN Crypt 2Go [here](#).

File and Folder Encryption as a Service

This cloud-based service enables role-based encryption to protect data at rest and in motion. It supports in securing files and folders against unauthorized access across any storage location, enabling sensitive data protection, secure file sharing, compliance requirements, and client confidentiality.



Get a [30-day free trial](#).

LAN Crypt File and Folder Encryption – Technical Specifications

Client 64 Bit

- Windows 10/11 Pro/Enterprise 1809 and later
- Windows Server 2022 and 2025
- Supported Citrix Environments
Citrix Virtual Apps and Desktop 7 1912 LTSR CU2 on WS 2019
- macOS 14 Sonoma and later

Administration 64 Bit

- Windows 10 Pro/Enterprise*
- Windows 11 Pro/Enterprise*
- Windows Server*

* See client versions for supported versions

Operating Systems

- Windows 11, 10
- macOS 26, 15
- Android 16, 15, 14, 13, 12
- iOS/iPadOS 26, 18

Supported Media and Platforms

Media

- Network drives
- Local hard disks
- Optical Media
- USB
- Flash drives
- Memory cards

Platforms

- Microsoft Terminal Server
- Virtual Machines
- OneDrive
- Azure SQL
- Dropbox
- Google Drive
- MS Azure (e.g. Clients, Azure, DB)

Supported Databases

- Microsoft SQL Server 2019, 2022 and 2025
- Oracle Database 19

Supported Algorithms

Encryption

- AES 128 Bit and 256 Bit
- 3DES 168 Bit
- DES
- IDEA 128 Bit
- XOR

Certificates

- RSA up to 4096 Bit
- Self-generated or via involvement of a PKI
- Soft certificates
- Smartcards
- Tokens

Recommended algorithm

- AES-256

Recommended encryption format

- XTS-AES

Hash

- MD5
- SHA256

LAN Crypt 2Go System Requirements

- Windows 10 and higher (later)
- macOS 13 and higher (later)
- iOS and iPad OS 16 and higher (later)
- Android 8.1 and higher (later)
- Ubuntu 20.4 and Debian 11 and higher (later)
- State-of-the-art browser for web portal

EMEA

Utimaco IS GmbH

📍 Krefelder Str. 220,
52070 Aachen,
Germany

☎ +49 241 1696-0
✉ 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

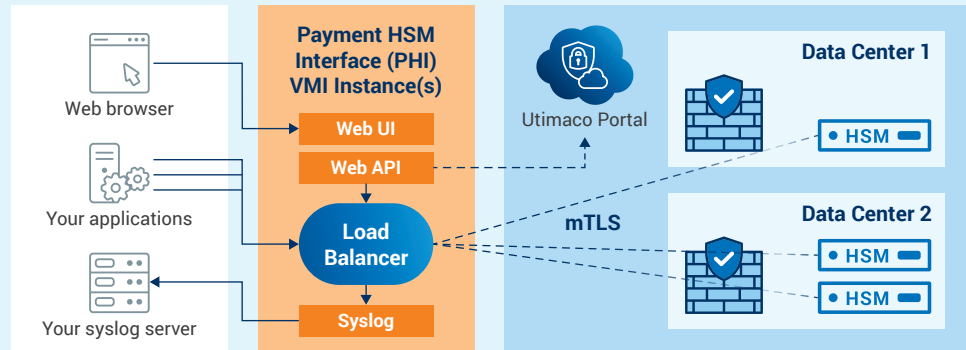


Ensure PCI Compliance and Scalability with High-Performing Payment HSM as a Service

Reduced Costs • Fully Managed Service • PCI certified • Multi-Cloud • High Availability

Access fully managed Payment HSMs hosted in resilient data centers for secure payment use cases. This service eliminates the need for hardware ownership, offering fast way to comply with the PCI standards.

The service is equipped by default with the optional PHI load balancer capable of significantly scaling throughput without increasing per-command latency.



Supported Use Cases

Transaction Processing	Issuer and Acquirer Payments Processing	Data Encryption/Decryption
Payment Card Verification		Realtime Payments Messaging
PIN Translations and Authorization	Card/User Verification	SoftPos Transaction Processing

Highlights

Reduced Costs

Reduce capital and operational expenses with a flexible subscription model.

Fully Managed Service

Eliminate operational complexity with a fully managed, cloud-hosted service.

PCI Certified

Accelerate PCI compliance with support for DSS, PIN, and P2PE standards.

Multi-Cloud

Securely deploy across public, private, hybrid, and multi-cloud environments with maximum flexibility.

High Availability

Ensure uninterrupted payment processing with 99.999% availability and high-performance HSM infrastructure.

Key Benefits

Reduced Costs

Lower the costs associated with purchasing, deploying, and maintaining on-premises Payment HSM infrastructure. Benefit from a predictable and flexible subscription model that eliminates large upfront investments and reduces ongoing operational expenses.

Fully Managed Service

Simplify operations with a fully managed Payment HSM service delivered from resilient, globally distributed data centers. Remove the complexity of hosting, maintaining, updating, and securing HSM infrastructure, while avoiding the need to recruit and retain specialized HSM expertise.

PCI Certified

Accelerate your path to PCI compliance. The service supports compliance with PCI DSS, PCI PIN, and PCI P2PE standards ensuring your payment environment remains secure and compliant.

Multi-Cloud

Unlock the full potential of your multi-cloud strategy. Payment HSM as a Service integrates with both public and private cloud environments, providing the flexibility of cloud deployment while maintaining the security required for hybrid and multi-cloud architectures.

High Availability

Benefit from Payment HSMs hosted in resilient global data center infrastructure designed to deliver 99.999% availability. Combined with high-performance HSM technology, the service provides reliable, always-on operation and the capacity to process high transaction volumes efficiently.



Service Benefits and Capabilities

- Low Latency
- High Availability (99.999%)
- Fully managed service, incl.: FW updates, Key Management, Operations and Maintenance
- Built on Utimaco's leading Payment HSMs
- Scale as you grow
- Global Coverage with Two Active DCs per availability zone
- MFK Key Exchange – compliant and fully managed by Utimaco in a secure environment, or performed by the customer.

Certifications and Compliance

- FIPS 140-2 Level 3 certified HSM
- PCI PTS HSM v3
- PCI DSS
- PCI PIN
- PCI P2PE
- TR-31 Key Block Support
- GBIC/ DK (Deutsche Kreditwirtschaft)
- ISO27001 compliant

Supported Cryptographic Interfaces

- Symmetric algorithms: DES, 3DES, AES
- Asymmetric algorithms: RSA 1024 to 4096
- Hashing algorithms: SHA-1 to SHA512
- MAC/sealing algorithms: MAC and HMAC, CMAC

Payment Standards

- ANSI X3.92, X9.52, X9.97, X9.8, X9.24, X9.17, TR31, TR34, TR39
- APACS 40 and 70
- ISO 9797, ISO 10126, ISO 9807, ISO 16609, ISO 9564
- NIST security standards SP800-90 (RBG), SP800-38A, SP800-67
- DUKPT X9.24, (DUKPT 2018)
- Visa, Mastercard, Amex, China Union Pay, JCB, Discover

Deployment Models

- Utimaco's data centers
- Hybrid cloud: private and public
- Multi-cloud
- IBM Cloud co-located data centers

Global and Regional Availability

Our services operate across multiple geographically separated data centers ensuring continuity even during major incidents or regional disruptions.

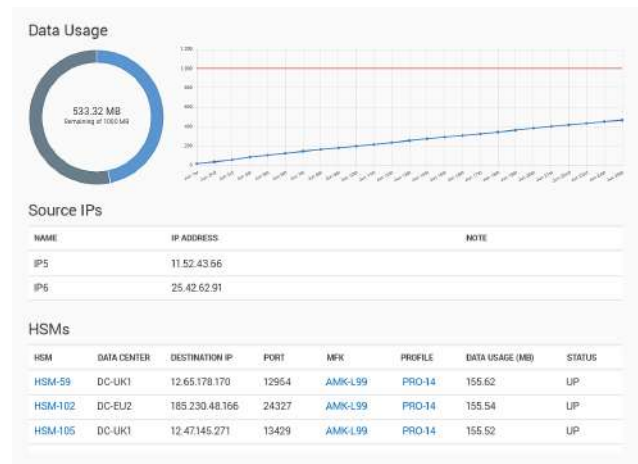


- ◆ SaaS
- ◆ IaaS

Service Management: Payment HSM as a Service

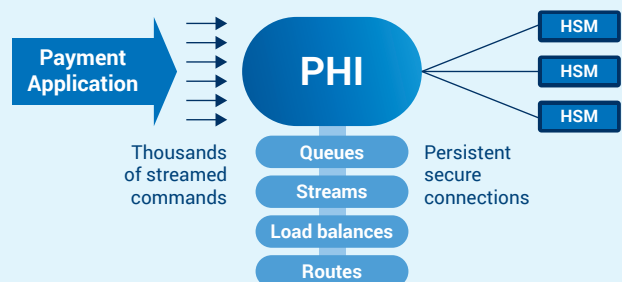
Manage and configure Payment HSM service from one central location. Perform tasks such as:

- Report collection
- Consumption view
- Service Administration
- User management



Payment HSM Interface (PHI)

The PHI model effectively breaks the traditional link between latency and throughput, letting systems scale transaction volumes without redesigning networks for ultra-low latency. PHI is available in CSP Marketplaces (IBM, Azure, AWS) as a load balancer for Payment HSMaaS. This capability is powerful yet optional.



EMEA

Utimaco IS GmbH

Krefelder Str. 220,
52070 Aachen,
Germany

+49 241 1696-0
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

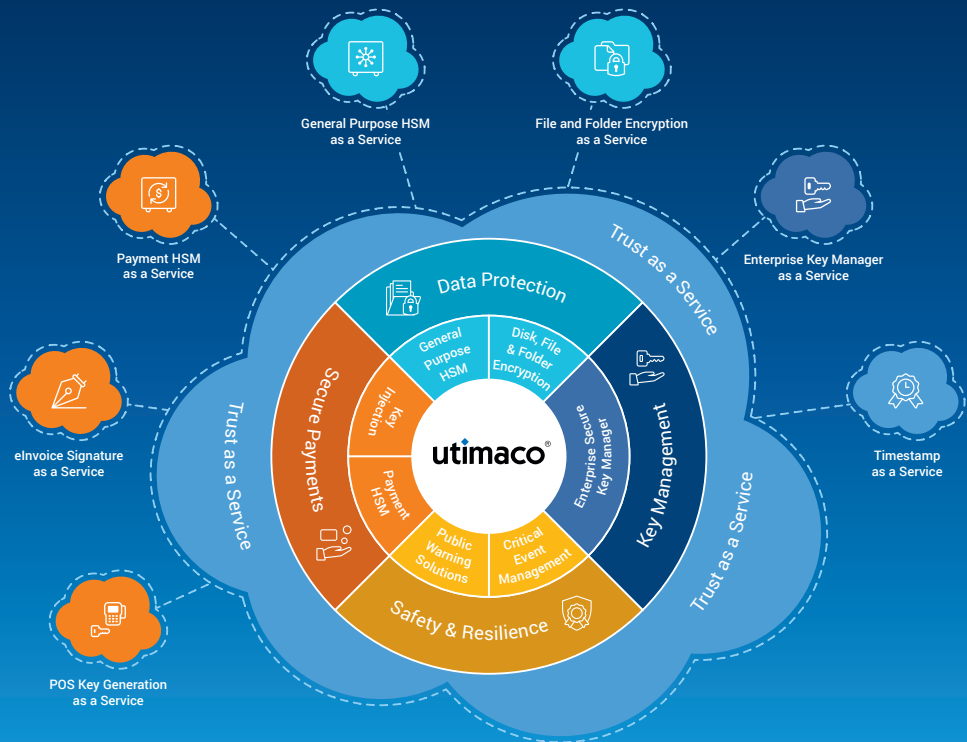


Enable Your Business with a Cloud-Based Services Portfolio

Lower TCO • Multi-Hybrid Cloud • Compliance and Availability • Flexible Deployment • Physical HSM Security

Utimaco's Trust as a Service (TaaS) delivers HSM-grade security, compliance, and data protection in a flexible, CAPEX-free subscription.

Cloud-agnostic and CSP-independent, it secures multi-cloud and hybrid environments with consistent control and simplified audits under GDPR, PCI DSS, and more. With 99.999% availability, 24/7 global services, and seamless integration, TaaS reduces costs, scales with your growth, and ensures uncompromised protection for your most critical data and transactions.



Highlights

Lower TCO

Cut costs with our managed cybersecurity service—no CAPEX, built to scale.

Cloud-Agnostic Security

Secure multi-cloud and hybrid environments with consistent protection, compliance, and control across all clouds.

Global Compliance & Availability

Stay compliant and operational with 24x7 global services, 99.999% uptime, and simplified audits.

Easy Deployment & Growth

Seamlessly integrate, adapt, and scale to meet evolving business needs with ease.

Physical HSM Security

Protect your data with enterprise-grade HSM technology and a high-security physical setup.

Key Benefits

Lower Total Cost of Ownership

Achieve a lower total cost of ownership with our fully-managed cybersecurity service that eliminates upfront CAPEX investment and additional staffing costs, while seamlessly scaling with your growth through comprehensive operations, maintenance, upgrades, monitoring, and lifecycle replacement.

Cloud-Agnostic Security for Multi-Cloud & Hybrid Environments

Empower your multi-cloud and hybrid strategies with a secure, cloud-agnostic trust layer that operates independently of any Cloud Service Provider (CSP). Achieve consistent security and compliance across public and private clouds while supporting BYOK, HYOK, and unified key management. Simplify deployments, enhance flexibility, and maintain control—no matter where your data resides.

Global Compliance and 99.999% Availability

Ensure your business stays compliant and operational with our globally available services. Designed to meet stringent standards like GDPR, DORA, and PCI DSS, we simplify audits with centralized reporting and proof of compliance. With a 100% uptime record since 2019 and industry-leading 24x7 availability, you can rely on rapid, reliable, and compliant protection—no upfront hardware investments required.

Flexible Deployment, Integration and Adaptive Growth

Experience a solution designed to seamlessly integrate with your existing business operations, ensuring minimal disruption and maximum efficiency. Adapt swiftly to evolving market conditions and business challenges with unmatched agility. Effortlessly scale up or down to meet the unique demands of your enterprise, all while maintaining seamless functionality and alignment with your goals.

High-Security Physical HSM Setup

Experience unmatched security with our services powered by Hardware Security Module (HSM) technology. Trusted by critical infrastructures worldwide, we deliver enterprise-grade protection with a high-security physical setup with an HSM-grade root of trust, ensuring your data remains safe and uncompromised.

Utimaco's Trust as a Service Solution Overview



General Purpose Hardware Security Module as a Service

Lower operational costs ♦ FIPS-certified ♦
No CSP vendor lock-in ♦ Fully hosted ♦ Zero-maintenance

Secure, FIPS 140-2 Level 3 certified HSMs are fully hosted in resilient data centers while remaining under your governance. This service ensures secure key generation, storage, and management with seamless integration into standard cryptographic interfaces, reducing costs and complexity while maintaining compliance and scalability.



Enterprise Key Manager as a Service

External Cloud KMS ♦ Data Sovereignty ♦
Customer-Owned MBK ♦ Integrated HSM ♦ Fully Managed

Secure your environments through advanced multi-cloud or hybrid deployment, supporting BYOK, HYOK, KMIP, TDE, KMS, and REST. Centralized key management ensures strict separation between your data and cryptographic material, while your exclusive-access Master Backup Key (MBK)—stored in HSMs—serves as your reliable Root of Trust.



Timestamp as a Service

Trustworthy proof of time ♦ Full eIDAS compliance ♦
High availability ♦ Easy integration

This service provides eIDAS-compliant Qualified Electronic Timestamps, offering legal proof of time and content integrity. It enables the generation, validation, and archiving of timestamps to ensure documents remain unchanged since issuance. Built for high availability and seamless integration, it embeds compliance, efficiency, and long-term trust into digital records and workflows.



File and Folder Encryption as a Service

Quick setup ♦ Role-based encryption ♦
Unauthorized access protection

Secure files and folders against unauthorized access across any storage location with role-based encryption. This service protects data at rest and in motion, ensuring the right users have the right access. It supports critical use cases such as sensitive data protection, secure file sharing, compliance requirements, and client confidentiality.



Payment Hardware Security Module as a Service

Reduced costs ♦ Fully managed service ♦ PCI certified ♦
Multi-cloud ♦ High availability

Access fully managed PCI PIN-certified HSMs hosted in resilient data centers for secure transaction processing, PIN translation, and key management. This service eliminates the need for hardware ownership or maintenance, ensuring compliance, scalability, and reduced total cost of ownership.



POS Key Generation as a Service

Key generation ♦ Key custodial services ♦ PCI-PIN certified ♦
High availability

This PCI-PIN certified service provides secure key generation, distribution, and storage for POS payment use cases. With 24/7 access to expert key custodial staff and automated or on-demand cryptographic key operations, it ensures maximum availability and resilience from geo-redundant data centers for a wide range of POS applications.



eInvoice Signature as a Service

Trusted eInvoicing ♦ full eIDAS compliance ♦
Seamless integration ♦ High Availability

Deliver eIDAS-compliant Qualified Electronic Signatures to ensure invoices and business documents meet European tax regulations. This service enables the generation, validation, and archiving of signatures to maintain authenticity and integrity under VAT Directive requirements. Designed for high availability and seamless integration, it secures invoices, orders, delivery notes, and financial records, ensuring compliance and legal confidence in digital workflows.

Discover Utimaco's Trust as a Service Offerings on

<https://utimaco.com/products/data-security/trust-as-a-service>



Technical Overview



General Purpose Hardware Security Module as a Service

Certifications and Compliance

- FIPS 140-2 Level 3 certified HSM
- GSMA SAS-SM (for selected DC and Customers)
- ISO27001 compliant

Service benefits and capabilities

- High availability, 99,999%
- Global coverage, with two DCs per availability zone
- Scale as you grow
- Latest cryptographic algorithms, including PQC, 5G protect, etc
- Fully Managed service, incl. FW updates, Operations and Maintenance
- Based on Utimaco's market leading GP HSM product suite

Supported cryptographic interfaces

- PKCS #11
- Java Cryptography Extension (JCE)
- Microsoft Crypto API (CSP), Cryptography Next Generation (CNG), and SQL
- Extensible Key Management (SQLEKM)
- OpenSSL
- Utimaco's comprehensive Cryptographic eXtended services Interface (CXI)

Supported Use Cases

- Data Encryption
- User and Device Authentication
- Document Signing
- Certificate Issuing
- Public Key Infrastructure
- Code Signing
- Blockchain Processes
- PQC and 5G protect applications



Payment Hardware Security Module as a Service

Certifications and Compliance

- FIPS 140-2 Level 3 certified HSM
- PCI PTS HSM v4
- PCI DSS
- PCI PIN
- PCI P2PE
- TR-31 Key Block Support
- GBIC/ DK (Deutsche Kreditwirtschaft)
- ISO27001 compliant

Service benefits and capabilities

- Low latency
- High availability, 99,999%
- Global coverage, with two active-active DCs per availability zone
- Scale as you grow

- Fully Managed service, incl. FW updates, Key Management, Operations and Maintenance
- Based on Utimaco's leading Payment HSM products
- Payment HSM Interface available in CSP marketplace (IBM, Azure, AWS) as load balancer towards Payment HSMaaS.

Supported Cryptographic Interfaces

- Symmetric algorithms: DES, 3DES, AES
- Asymmetric algorithms: RSA 1024 to 4096
- Hashing algorithms: SHA-1 to SHA512
- MAC/sealing algorithms: MAC and HMAC, CMAC

Payment Standards

- ANSI X3.92, X9.52, X9.97, X9.8, X9.24, X9.17, TR31, TR34, TR39
- APACS 40 and 70
- ISO 9797, ISO 10126, ISO 9807, ISO 16609, ISO 9564
- NIST security standards SP800-90 (RBG), SP800-38A, SP800-67
- DUKPT X9.24, (DUKPT 2018)
- VISA, MASTERCARD, AMEX, CHINA UNION PAY, JCB, DISCOVER

Application Programming Interfaces and Communication Protocols

- PTCP/IP sockets per device
- TLS sockets
- REST API
- PayShield and Atalla APIs

Supported Use Cases

- Transaction Processing
- Payment Card Verification
- PIN Translations and Authorization
- Issuer and Acquirer Payments Processing
- Data Encryption/Decryption
- Card/User Verification
- Realtime Payments Messaging
- SoftPos Transaction Processing



Enterprise Key Manager as a Service

Certifications and Compliance

- FIPS 140-2 Level 3 (for HSM)
- FIPS 140-2 Level 1 (for KMS)
- ISO 27001 Compliant

Service benefits and capabilities

- Multi-Cloud and Hybrid Cloud support (CSP independent)
- Mix of Cloud and Customer Datacenter support (Hybrid deployments)
- Key Management, with HSM root of trust
- Customer has full control of Master Key
- Support all Enterprise Key Management use cases from one service

Supported Use Cases

- Cloud Key Management (BYOK/HYOK)
- Multi-Cloud Key Mgm
- dB encryption (TDE)
- Enterprise Key Management for Applications/VMs/dB (KMIP, KMS)
- Converged Key Mgm and GP HSMaaS service over REST API

Supported Cryptographic Interfaces

- RESTful interface API
- KMIP, OpenKMIP and PyKMIP
- KMS
- TDE
- PKCS #11
- Java Cryptography Extension (JCE)
- Microsoft Crypto API (CSP), Cryptography Next Generation (CNG), and SQL
- Extensible Key Management (SQLEKM)
- Supports Azure, Google, and Amazon cloud integrations

Supported Cryptographic Algorithms

- Symmetric algorithms: AES, Triple-DES, DES
- Asymmetric algorithms: RSA, DSA, ECDSA with NIST and Brainpool curves, EdDSA
- Elliptic Curves: DH, ECDH with NIST, Brainpool and Montgomery curves
- Hashing algorithms: SHA-1, SHA-2, SHA-3, RIPEMD
- MAC/sealing algorithms: MAC, CMAC, HMAC
- Optional upgraded with blockchain-specific algorithms: BIP32/44 and SLIP-010



POS Key Generation as a Service

Certifications and Compliance

- PCI PTS HSM v4 compliant
- PCI PIN compliant
- PCI P2PE compliant
- ISO 27001
- ISO9001, 4001
- SOC2

Service benefits and capabilities

- PCI compliant key management service
- PCI compliant remote key generation & distribution to PoS devices or 3rd payment HSMs
- Key lifecycle management
- Component management
- Custodial services

Supported Cryptographic Interfaces

- RESTful API secured via TLS 1.2 communications security

Supported Cryptographic Algorithms

Asymmetric algorithms/lengths:

- RSA: 1024, 2048, 3072, 4096 Bits

- ECC: NIST, SEC 2 and Brainpool elliptic curves, 160 – 571 Bits
- Symmetric algorithms/lengths: DES, TripleDES, AES 128, 192, 256 Bits

Hash Functions:

- SHA1, SHA224, SHA256, SHA384, SHA512 Bits
- Message Authentication: CMAC, HMAC



eInvoice Signature as a Service

Supported Interfaces

REST Interface:

- REST interface with an encrypted connection (HTTPS) for transmission, pickup, and status query for data/documents to be signed, stamped, archived, and checked.

- Data traffic encryption via TLS

- Authentication via account credentials
- Maximum file size, unless otherwise agreed, 15 MB

Compliance

- Art. 41, Paras. 1,2,3 REGULATION (EU) 910/2014 eIDAS

Supported Use Cases

- eIDAS compliant Qualified Electronic Signatures,

- Legal authenticity and integrity of invoices and business documents according to European tax regulations.

- Generation, validation, and archive of signatures, to meet the VAT Directive's demands for authenticity of origin and integrity of content.



Timestamp as a Service

Supported Interfaces

RFC 3161 Interface:

- Standard interface to request timestamps
- Data traffic encryption via TLS

Compliance

- Art. 41, Paras. 1,2,3 REGULATION (EU) 910/2014 eIDAS
- Authentication using account credentials
- Transmitting of document HASH values

Supported Use Cases

- Safeguarding electronic documents
- Evidence of completion of time-critical transactions,
- Protection of business intellectual property

- Safeguarding patent-related information
- Standard interface to request timestamps



File and Folder Encryption as a Service

Certifications and Compliance

- GDPR
- CCPA
- TISAX
- HIPAA
- PDPA
- NIS2 Directive
- DORA, etc.

Supported Cryptographic Algorithms

- AES 256 Bit

Supported Platforms

- Microsoft Terminal Server
- Virtual Machines
- OneDrive
- Azure SQL
- Dropbox
- Google Drive
- MS Azure

Mobile Operating Systems

- Android (11,12,13,14)
- iOS/iPadOS (15,16,17)

Supported Media

- Network drives
- Local HDs
- CD/DVDs
- USB
- Flash drives
- Memory cards

Supported Directory Service

- Microsoft Entra ID

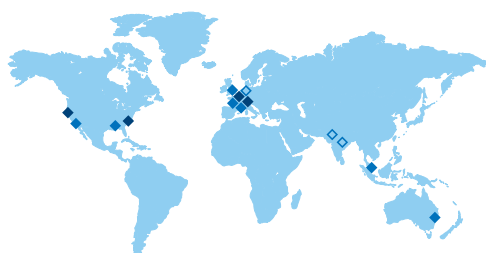
Technical Requirements

- 64-bit client: Windows 10 Pro/Enterprise
- Windows 11 Pro/Enterprise
- Windows Server
- macOS
- Support Citrix Environments

Datacenter Overview

Data Center Locations

- North America: West and East Coast
- Europe: UK, Netherlands, Germany
- Asia: Singapore
- Australia: Sydney
- India: Dehli and Mumbai regions



Service Setup

- Fully redundant per DC setup, fully Geo-redundant per availability zone
- State of the art IT design, enable local DR and full high-availability

- Highly fault tolerant service and infrastructure setup
- Secure server room with shared/dedicated HSM*
- Key security in your control with your master key**

Certifications and Compliance

Fulfilling relevant security and regulatory certifications as well as various data security requirements***

- ISO27001, ISO9001, ISO14001
- GDPR
- PCI DSS
- SOC2 (US DCs)

Compliant Cloud Personnel

- 24/7 onsite security personnel
- CCTV with 90-day backup
- Biometric/Photo badge access
- Crash-rated/Anti-climb gates
- 24/7 HSM vendor support*

Utimaco Datacenters
Backbone of our as a Service Offerings

* Applicable for HSM-based services

** Applicable for Enterprise Key Manager as a Service

*** Individual Certification varies on location

For more information about Utimaco products, please visit us at utimaco.com or send an e-mail to hsm@utimaco.com

© Utimaco IS GmbH 03/26 – Version 2.1

Utimaco® is a trademark of Utimaco GmbH. All other named trademarks are trademarks of the particular copyright holder. All rights reserved. Specifications are subject to change without notice.

utimaco®



The Multi-Tenant Hardware Security Module with Tamper-Active Physical Security

High Physical Security • Advanced Sensor Protection • Containerized Architecture • PQC-Ready • SDK for Customization

The u.trust General Purpose HSM CSe-Series is the latest addition to Utimaco's HSM portfolio, designed to meet the highest physical security requirements. It supports multi-tenancy and offers upgrade options for Post-Quantum Cryptography, ensuring future-proof protection for critical applications.



Utimaco
Quantum Protect



Utimaco
Blockchain Protect



Utimaco
5G Protect

Highlights

High security meets high performance and flexibility

Advanced sensor mechanism that removes sensitive key material in the event of an attack

Multi-tenancy with up to 31 fully isolated containerized HSMs in one platform

Crypto-agile and PQC-ready for future-proof applications

Software Development Kit for custom implementations

Application Packages and Add-Ons

- **Quantum Protect:** Post Quantum Cryptography algorithms
- **5G Protect:** Subscriber authentication and key agreement in mobile networks
- **Blockchain Protect:** Securing sensitive assets in blockchain processes
- **Software Development Kit:** The professional development kit for u.trust General Purpose HSMs

u.trust General Purpose HSM CSe-Series Models

	CSe100	CSe2k	CSe5k
Signature Creation (Signatures / s)			
RSA-2048	100	2,000	5,000
ECDSA P-256	1,000	4,300	10,500
Key Generation (Key / s)			
RSA-2048	2.8	9.5	10.8
ECDSA P-256	270	1,300	3,000
Encryption / Decryption (Mbytes / s)			
AES 256 – GCM	40	130	130
AES 256 – ECB	70	190	190
Containers			
	1	4	8, 16, or 31
In-field upgrade			
	Upgrade to CSe2k	Upgrade to CSe5k	Upgrade number of containers

Key Benefits

High security meets high performance and flexibility

This multi-tenant HSM delivers tamper-active physical protection for secure key generation, storage, and usage. Available in models ranging from entry-level to high-performance, it supports up to 31 containerized HSMs to accommodate a wide range of deployment needs.

Crypto-agile and PQC-ready

Designed with crypto-agility in mind, the HSMs are in-field upgradable with PQC CAVP validated algorithms. Patented state handling method for stateful hash-based signatures.

Advanced sensor mechanism against physical threats

The HSM offers an advanced sensor mechanism, which includes a sensor protection film, that reacts to all types of mechanical, chemical, and physical threats. In the event of an attack, sensitive keys and data stored within the HSM's internal memory are actively and quickly erased.

Containerized architecture for multi-tenancy, high availability, and scalability

Deploy cHSMs as a shared cluster to boost performance and resilience or leverage the strong isolation of the cHSMs and assign them individually or as a cluster per application to create a true multi-tenant solution. Choose between 1, 4, 8, 16, or 31 containers (cHSMs).

SDK for custom implementations

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

Cryptographic Algorithms

- RSA, DSA, ECDSA with NIST and Brainpool curves, EdDSA
- DH, ECDH with NIST, Brainpool and Montgomery curves
- Edwards curves Ed25519 and Ed448
- AES, Triple-DES, DES
- MAC, CMAC, HMAC
- SHA-1, SHA-2, SHA-3, RIPEMD
- Chinese Algorithms
- All algorithms included in the product price

Cryptographic Interfaces (APIs)

- PKCS #11
- Java Cryptography Extension (JCE)
- Microsoft Crypto API (CSP), Cryptography Next Generation (CNG) and SQL
- Extensible Key Management (SQLEKM)
- OpenSSL
- Utimaco's comprehensive Cryptographic eXtended services Interface (CXI)
- REST Cryptography API (RCAPI)

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.

Certifications

- FIPS 140-3 Level 4 (Physical Security)*
- Hash-based deterministic random number generator (DRG.4 acc. AIS 31/ NIST SP800-90B)
- True random number generator (PTG.2 acc. AIS 31; PTG 3 is achievable)

* In progress

Hardware

Network Appliance



PCIe Card



Physical Dimensions

Form factor	19" 1U	Half-length, full-height, PCI Express Card
Weight	22.05 lb (10 kg)	0.88 lb (0.42 kg)
Length	21.79 in (533.4 mm) excluding handles	6.60 in (167.65 mm) half-length excluding bracket
Depth/Width	17.56 in (446 mm) excluding handles	0.73 in (18.6 mm)
Height	1.73 in (44 mm)	4.38 in (111.15 mm) full height
Compatibility	Ethernet – 100/1000 mB/s	PCIe 1.1, PCIe 2.0 and PCIe 3.0 slots

Connectivity

Interfaces	2 RJ45, 2.5 Gb/s 2 SFP+ 10 Gb/s or 2 RJ45 1Gb/s network interfaces as optional extension	PCIe x4
-------------------	---	---------

Electrical Characteristics

Power Supply	Redundant field-replaceable, 2 x 100 ~ 240 V AC, 50 ~ 60 Hertz, 300 W	3.3 V, 12 V supplied by PCIe connector
Power Consumption	Typically 45 W / 66 VA, max. 50 W / 70 VA	Max. 20 W
Heat dissipation	Max. 171 BTU/h	Max. 69 BTU/h
Backup battery	Lithium battery LS14500 (3.6 V)	Lithium battery CR2032 (3 V)

Operating Environment

Operating temperature	+50°F to +104°F (+10°C to +40°C)	+50°F to +95°F (+10°C to +35°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	98,244 hours at 25°C / 77°F, environment GB, GC – Ground Benign, Controlled	360,000 hours at 25°C / 77°F, environment GB, GC – Ground Benign, Controlled

Certification / Compliance

Safety and Electromagnetic Compliance	IEC/EN 55011, IEC/EN 55032, IEC/EN 61000-6-4, IEC/EN 61000-3-2, IEC/EN 61000-3-3, IEC/EN 61000-6-2, IEC/EN 61000-4-2, IEC/EN 61000-4-4, IEC/EN 61000-4-8 IEC/EN 60950-1, IEC/EN 62368-1 UL, CB, CE, FCC Class B, BIS, KC	IEC/EN 55011, IEC/EN 55032, IEC/EN 61000-6-4, IEC/EN 61000-3-2, IEC/EN 61000-3-3, IEC/EN 61000-6-2, IEC/EN 61000-4-2, IEC/EN 61000-4-4, IEC/EN 61000-4-8 IEC/EN 60950-1, IEC/EN 62368-1 UL, CB, CE, FCC Class B, VCCI, KC
Environmental	RoHS III, REACH, SVHC, WEEE	RoHS III, REACH, SVHC, WEEE

Other specifications

TPP	~ 28.7
DDR bandwidth	~ 8.5 GB/s

EMEA

Utimaco IS GmbH

📍 Krefelder Str. 220,
52070 Aachen,
Germany

☎ +49 241 1696-0
✉ 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

© Utimaco IS GmbH 08/26 – Version 1.3

Utimaco® is a trademark of Utimaco GmbH. All other named trademarks are trademarks of the particular copyright holder. All rights reserved. Specifications are subject to change without notice.

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 140-3 Level 3 certified.

Highlights

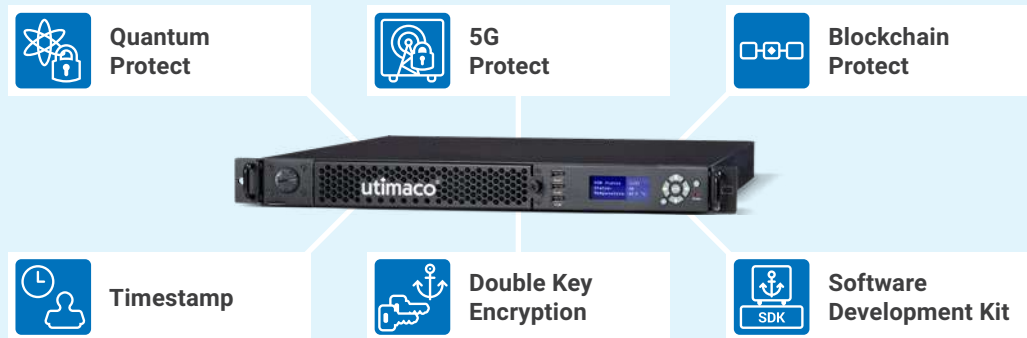
Performance of up to 40,000 RSA 2K operations per second

Multi-tenancy with up to 31 fully isolated containerized partitions

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

FIPS 140-3 Level 3 certified

Software Development Kit for custom implementations



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

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, 16, 31	4	8, 16, or 31
In field-upgrades	Upgrade path from Se100 to Se2k to Se5k			Upgrade path from Se15k to Se40k	

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.

Crypto-agile and PQC-ready

Designed with crypto-agility in mind, the HSMs are in-field upgradable with PQC CAVP validated algorithms. Patented state handling method for stateful hash-based signatures.

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, 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.

FIPS-certified up to 140-3 Level 3

The u.trust platforms are certified up to FIPS 140-3 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

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
- Utimaco's native Cryptographic eXtended services Interface (CXI)
- Utimaco's REST Cryptography API (in progress)

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.

Certifications

- FIPS 140-3 Level 3
- Common criteria EAL4+
- NITES
- Hash-based deterministic random number generator (DRG.4 acc. AIS 31/ NIST SP800-90B)
- True random number generator (PTG.2 acc. AIS 31; PTG.3 is achievable)
- VS-NfD*

* In progress

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 x D 21.79 in x H 1.73 in (W 446 mm x D 533.4 mm x H 44 mm) excluding brackets	W 4.38 in x D 6.60 in x H 0.74 in (W 111.15 mm x D 167.65 mm x 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	Typically 55 W / 78 VA, max. 65 W / 90 VA	Max. 25 W
Heat/battery	Heat dissipation: max. 222 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
--	--

Other specifications

TPP	~ 28.7
DDR bandwidth	~ 8.5 GB/s

EMEA

Utimaco IS GmbH

📍 Krefelder Str. 220,
52070 Aachen,
Germany

☎ +49 241 1696-0
✉ 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

© Utimaco IS GmbH 08/26 – Version 1.4

Utimaco® is a trademark of Utimaco GmbH. All other named trademarks are trademarks of the particular copyright holder. All rights reserved. Specifications are subject to change without notice.

utimaco®



Next-generation General Purpose Hardware Security Module

Superior Performance ♦ Multi-Tenant ♦ PQC-Ready ♦ VS-NfD Approved ♦ Free Simulator

u.trust General Purpose HSM VS-NfD combines superior performance with multi-tenancy.

From entry-level to high-performance use cases, all models are future-proof with post quantum cryptography readiness.

This product is made in Germany. It allows to secure data classified up to "VS-NfD", "EU restricted" and "NATO restricted" levels.



SecurITy
made
in
Germany

u.trust General Purpose HSM VS-NfD is approved for classified environments according to VS-NfD, RESTREINT UE/ EU RESTRICTED, and NATO RESTRICTED profiles. It is approved by the German Federal Office for Information Security (BSI).

u.trust General Purpose HSM VS-NfD 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, 16, 31	4	8, 16, or 31
In field-upgrades	Upgrade path from Se100 to Se2k to Se5k			Upgrade path from Se15k to Se40k	

Highlights

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

Multi-tenancy
with up to 31 fully
cryptographically
isolated cHSMs.

**Designed for
crypto agility**

VS-NfD approved

Key Benefits

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

u.trust General Purpose HSM VS-NfD is available in various performance options.

Crypto agility

Designed with crypto-agility in mind. Supports hardware accelerated ML-DSA/ML-KEM. Using SLH-DSA for quantum resistant firmware signing.

Multi-tenancy for high availability, scalability, and flexibility

Manage fully isolated, standalone processes in one cHSM with the containerization option. Choose between **1, 4, 8, 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.

VS-NfD Approved

BSI-approved, additionally enabling protection of data up to EU Restricted and Nato Restricted.

Flexible Key Storage

The u.trust platforms support both 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
- MAC, CMAC, HMAC
- SHA: SHA-256, SHA-512/256, SHA-384 and SHA-512, SHA3-256, SHA3-384, SHA3-512
- Minimum key size is 120 bits
- RSA key size = 3k
- Supports hardware accelerated ML-DSA/ML-KEM
- Using SLH-DSA for quantum resistant firmware signing

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
- Utimaco's native Cryptographic eXtended services Interface (CXI)
- Utimaco's REST Cryptography API (in progress)

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.

Certifications

- VS-NfD approved
- CC / NITES
- PCI PTS HSM v3
- Hash-based deterministic random number generator (DRG.4 acc. AIS 31/ NIST SP800-90B)
- True random number generator (PTG.2 acc. AIS 31; PTG.3 is achievable)

**Centrally
monitor and
manage your u.trust
GP VS-NfD HSMs
with 360 HSM
Monitoring**

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 x D 21.79 in x H 1.73 in (W 446 mm x D 533.4 mm x H 44 mm) excluding brackets	W 4.38 in x D 6.60 in x H 0.74 in (W 111.15 mm x D 167.65 mm x 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	Typically 55 W / 78 VA, max. 65 W / 90 VA	Max. 25 W
Heat/battery	Heat dissipation: max. 222 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
--	--

EMEA

Utimaco IS GmbH

📍 Krefelder Str. 220,
52070 Aachen,
Germany

☎ +49 241 1696-0
✉ 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

© Utimaco IS GmbH 06/26 – Version 1.1

Utimaco® is a trademark of Utimaco GmbH. All other named trademarks are trademarks of the particular copyright holder. All rights reserved. Specifications are subject to change without notice.

utimaco®