Product Brief

Atalla AT1000 – the fastest HSM in the Payment Industry

Secure and Compliant Payments with PCI PTS HSM v3

Ringing in at 10,000 TPS with global Support for Payment Standards

UTIMACO
Atalla AT1000

Creating Trust in the **Digital Society**

utimaco®

UTIMACO Atalla AT1000 is a **FIPS 140-2 Level 3 and PCI PTS v3 certified payment Hardware Security Module (HSM)** used to protect sensitive data and associated keys for non-cash retail payment transactions, cardholder authentication, and cryptographic keys by payment service providers, acquirers, processors, issuers, and payment networks across the globe.

The UTIMACO Atalla AT1000 provides superior hardware security to deliver maximum privacy, integrity and performance for host applications. Being the inventor of Key Block scheme which is later adapted by the industry as TR-31, our HSM family has been using the Key Block structure for over 20 years and is one of the only payment HSMs on the market that supports REST API. Our newest model, the AT1000, is the fastest and most compliant payment HSM on the market.

Unmatched Security with a Long-Standing History

Compliance-Driven

Tamper-responsive with the ability to act in response to side-channel attacks with **FIPS 140-2 L3 Compliance, FIPS 140-2 L4 (physical design) and PCI PTS HSM v3** certified for both **controlled and uncontrolled environments**, decreasing PCI scope and auditor analysis.

Easier Migration

Offered in both Variant and AKB (TR-31, TR-34) modes, the AT1000 is built to help clients transition from other non-compliant HSMs. Update legacy applications and streamline your HSM estate with our Payment Emulator. Atalla AT1000 is also fully-backward compatible with all Atalla HSMs.

Robust Backup and Restore

To offset the vulnerabilities associated with backing up an HSM, the AT1000 requires the participation of two or more parties, as well as limits the amount of times a restore can take place, recording each date and time as matter of record.

Redundancy and Failover

Thoughtfully crafted with the "worst case scenario" in mind, UTIMACO believes it's the small details that make the difference. Each HSM comes with Dual RAID1 hard drives and 4 NICs with NIC Bonding support for failover to ensure the HSM never goes down and the AT1000 always remains reliable.

Sleek New Design

Rack-mountable and physically fortified - now in a smaller 1U hardware package. Offering added security with dual-locking bezel and Medeco pick-resistant locks, with front panel display for easy deployment. Field upgradable performance provided, with no hardware replacement required. More energy efficient with enhanced battery life and voltage monitoring is included.

Secure and Flexible Feature Set

Now manage your Atalla HSM from the convenience of your own Microsoft Windows computer! Our **Secure Configuration Assistant – Windows (UTIMACO Atalla SCA-W)** provides encrypted, convenient configuration management and key loading remotely and locally, implementing an end-to-end encrypted tunnel between smart cards and HSM. Security administrators can easily interface with the AT1000 to configure commands, define parameters, calculate cryptograms, and inject keys.

This intuitive GUI is more secure than ever! It includes natural event and decision flow and enforces dual access and split knowledge, requiring more than one administrator to perform certain management functions and key loading.

True Remote Management

Unlike any other HSM on the market, key custodians can be geographically dispersed, working independently of one another. 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.

Payment Emulator

By leveraging the Payment Emulator, organizations can emulate other Payment APIs in the industry to communicate with the Atalla API and NextGen RESTful interface.

Capacity and Incident Monitoring

Robust audit log, reporting and alerts for the following: user access, connection attempts, error logging, crypto tests and audit operations while syncing its time with a trusted NTP server.

Out-of-the-Box Command Set

No feature enablement or additional licensing required; quickly repurpose your HSM for multiple use cases as needed. Optional customization and licenses offered for uncommon use cases and regional requirements.

Secure and Authenticated Communication Channel

Whitelist who can talk to the HSM and protect the communication over TLS 1.2 authenticated tunnel without any performance impact.

Proven Quality and Highest Performance

The AT1000 is an HSM that grows with your business. You no longer must decide between hardware models; simply upgrade your performance as needed.

Unrivaled Speed

With up to 10,000 TPS, the AT1000 is the fastest multi-core HSM on the market and can perform upgrades on the fly! That's four times the power of our closest competitor! Software upgrades in under five minutes – performance is never impacted.

Breadth of Solution

AT1000 is used by all the leading players within the payment ecosystem with close integrations with HPE NonStop Systems and MicroFocus Voltage Secure Data. Here are just a few of the use cases that can be fulfilled:

- PIN Processing
- 3D Secure v1 and v2 cryptography
- Card / User Verification
- ATM Interchange
- Data Integrity
- Processing Transaction Data
- Data Encryption/Decryption
- Initialize Remote Payment Device
- PIN Translations
- Payment Card Verification, Production and Personalization
- Electronic Funds Interchange (EFTPOS, ATM)
- Cash-Card Reloading
- EMV Transaction Processing
- Key Generation and Injection
- ATM Remote Key Loading
- AS2805 Host-to-host
- Supports JSON Web Tokens

Save Time and Reduce Costs

Consolidate HSMs, improve efficiencies and capitalize on the cloud.

Power of Partitions

Less to administer and operate. 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.

Cloud Ready

Emerge as a cryptography service provider to your internal customers. AT1000 is ready for HSMaaS model enabling multi domains that run independent of each other and supports multiple use cases at the same time.

REST API Support

REST API

Leverage the REpresentational State Transfer Application Programming Interface (REST API) to communicate with the Atalla HSM. With this flexible, stateless, easy to use and secure API, users can harness the unrivaled protection of an HSM in public, private and hybrid cloud environments. The REST API implementation also supports TLS, ACL, multiple domains and mutual authentication to further enhance security of the HSM.

Technical Specifications

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, ANS1 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 dCVV,
  Discover DCVV, American
  Express Expresspay, Visa Cloud
  based payments
- **EMV-based smart card support**

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
- **Dimensions (WxDxH)**
  19.0 x 26.0 x 1.75 in
  (48.26 x 66.04 x 4.45 cm)
- **Weight**
  27.8 lb (12.6 kg)

Connectivity

- **Communications Ethernet**
  TCP/IP, TLS 1.2 (only)
  With TLS Client Certificate
  Validation and CN Whitelisting
- **Connection**
  10/100/1000BASE-T (RJ45)
  auto-sensing
  Supports Static Routes
- **Communication Protocols**
  TCP: host and management
  commands
  UDP: host commands

Electrical and thermal characteristics

- **Rated input voltage**
  100 to 127 VAC
  200 to 240 VAC
- **Rated input current**
  5 A to 3 A
  2.4 A at 200 VAC
- **Rated input frequency**
  50 Hz to 60 Hz
- **Rated input power**
  350 W
- **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 (3 sec.)

Operating Environment

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

Certification/Compliance

- **Safety**
  UL/CUL, CE, TUV, BIS, BSMI, SII
- **Emissions**
  FCC Class B, VCCI, BSMI, C-Tick,
  IC, KCC
- **Environmental**
  RoHS, REACH

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 and key management solutions as well as compliance solutions for telecommunication providers in the field of regulation. UTIMACO is one of the world's leading manufacturers in both of these market segments.

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

Find out more on utimaco.com

Headquarters Aachen, Germany

Headquarters Campbell, USA

People and IDs

People and digital identities against terrorism and cyber crime.

Transactions

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

We protect

Data and Ideas

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

Investments

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

Contact us

EMEA

UTIMACO IS GmbH

Germanusstrasse 4
52080 Aachen,
Germany

+49 241 1696 200

hsm@utimaco.com

Americas

UTIMACO Inc.

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

+1 844 UTIMACO

hsm@utimaco.com

APAC

UTIMACO IS Pte Limited

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

+65 6631 2758

hsm@utimaco.com

For more information about UTIMACO® HSM products, please visit:
hsm.utimaco.com

© UTIMACO IS GmbH 08/21 – Version 1.0

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.

Creating Trust in
the **Digital Society**

utimaco®