Product Brief

Utimaco Atalla AT1000

Atalla AT1000 is a FIPS 140-2 Level 3 & 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.

Unmatched Security with a Long-Standing History

The Utimaco Atalla AT1000 provides superior hardware security to deliver maximum privacy, integrity and performance for host applications. Our HSM has been using the Key Block structure for over 20 years and is the Payment Card Industry's de facto standard. Our newest model, the AT1000, is the fastest and most compliant payment HSM on the market.

Compliance-Driven
Tamper-responsive with the ability to act in response to side-channel attacks with FIPS 140-2 L3, **and FIPS 140-2 L4 (physical)**. 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. It 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.

utimaco®

Secure and Flexible Feature Set

Now manage your Atalla HSM from the convenience of your own Microsoft Windows computer! Our **Secure Configuration Assistant – Windows (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.

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
- 3-D Secure
- 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

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.

Cryptography

Symmetric Key management TR-31, X9.24 (incl. AES and TDES DUKPT), X9.17, APACS 40/70	**Data Encryption** AES, RSA OAEP, DES/ TDES (X3.92, ISO 10126-2, X9.52)	**Digital signatures** RSA PKCS#1 v1.5 and ISO 9796-2	**Payment Card Processing** MasterCard CVC, Visa CVV, American Express CSC, MasterCard CVC3, Visa dCVV, Discover DCVV, American Express Expresspay, Visa Cloud based payments
Asymmetric Key management TR-34, legacy RSA keying protocols including those for Diebold and NCR ATMs	**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)	**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	**EMV-based smart card support**

Please refer to the Utimaco Atalla AT1000 Datasheet for more detailed technical specifications.

utimaco®

Learn more about Utimaco Atalla AT1000

https://hsm.utimaco.com/products-hardware-security-modules/payment-hsm/utimaco-atalla-at1000/

About Utimaco

Utimaco is an international provider of IT security solutions with headquarters in Aachen (Germany) and Campbell, CA (USA). Utimaco develops hardware security modules and 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.

Over 260 employees have committed to the company's goal to protect people, ideas and data. Customers and partners value the reliability and long-term investment security of Utimaco's high-security products and solutions. Utimaco stands for recognized product quality, user-friendly software, excellent support and products that effectively meet market requirements.

For more information, visit hsm.utimaco.com

EMEA	Americas	APAC
Utimaco IS GmbH	**Utimaco Inc.**	**Utimaco IS Pte Limited**
Germanusstraße 4 52080 Aachen, Germany	900 E Hamilton Ave., Suite 400 Campbell, CA 95008, USA	80 Raffles Place, #32-01, UOB Plaza Singapore 048624
+49 241 1696 200	+1 844 UTIMACO	+65 6622 5347
hsm@utimaco.com	hsm@utimaco.com	hsm@utimaco.com