Atalla AT1000

Atalla Hardware Security Module (HSM) is a payments security module for protecting sensitive data and associated keys for non-cash retail payment transactions, cardholder authentication, and cryptographic keys.

Atalla
Innovation in Payments

Product Highlights

Atalla HSM enables data and ecommerce protection and key management operations for PIN translations, payment card verification, production and personalization, electronic funds interchange (EFTPOS, ATM), cash-card reloading, EMV transaction processing, and key generation and injection.

The PCI-DSS compliant Atalla HSM provides unrivaled protection for AES and other cryptographic keys when safeguarding payment transactions. The HSM protects and manages encryption keys needed for key derivation within the tamper-resistant hardware device.

The new-generation Atalla HSM AT1000 host commands are fully backward compatible with its previous generation models, incorporating more than three decades of expertise—enabling co-existence and easy migration.

Key Benefits

Advanced key management solution using Atalla Key Block. Atalla Key Block is a key block format approved by the ANSI standards community to support interchange of symmetric keys in a secure manner and with key attributes included in the exchanged data. The AES key-wrap process, also commonly known as ANSI Key Block (AKB), was the first market-specified standard that resolved this by hard binding the key with the intended attributes along with integrity to ensure that the cipher text hasn't been modified.

The key is protected by using the approved key bundling standard requirements thus greatly reducing Man-in-the Middle (MitM) attacks. Additionally, key usage attributes are securely bound to the key itself. This prevents misuse of the key type or its intended use for example, the key is identified as an encryption key and can't be used to decrypt data, key exportability, etc.

Key Features

- Atalla Key Block for AES and TDEA or 3DES key management
- Tamper-resistant security module (TSRM) for PCI PIN compliant remote key loading
- In-field scalable performance
- Highly scalable with more than 10,000 TPS in a single device
- Backwards compatible with the previous generation Atalla HSMs
- Easy to integration into your existing infrastructure (managed as an IT Security device)
- Optional customization

Contact

hsm@utimaco.com
hsm.utimaco.com

EMEA

Utimaco IS GmbH
Germanusstraße 4
52080 Aachen, Germany
Phone +49 241 1696 200

Americas

Utimaco Inc.
900 E Hamilton Ave., Suite 400
Campbell, CA 95008, USA
Phone +1 844 UTIMACO

APAC

Utimaco IS GmbH – Office APAC
One Raffles Quay, North Tower, Level 25
Singapore 048583
Phone +65 6622 5347

Product Highlights

Physical Security

- FIPS 140–2 Level 3 certification for physical security
- PCI-HSM certified (in process)
- Rack-mountable (1U), physically fortified form factor
- Dual redundant power supplies
- Double-locking bezel with Medeco pick-resistant locks
- Out-of-range temperature and voltage detection
- Low-battery voltage detection

Logical Security

- Dual control
- Industry-standard Atalla Key Block (AKB) key management technology
- Advanced security architecture that prevents retrieval of PINs, keys, and other sensitive data in clear text form
- Automated and manual key management options
- Encrypted, convenient configuration, management, and key loading via Atalla Secure Configuration Assistant (no clear text passing of keys or key components)
- ATM key initialization and remote key loading (RKL)
- Payment Card Industry (PCI) Security Standards Council PIN Transaction Security (PTS) approved device
- PIN security and key management implemented within a tamper-resistant hardware security module perimeter for protection against manipulation

Key Differentiators

- The unique flexible approach to HSM configuration and key management that enables a remote workflow-based model meeting the PCI Dual Control Requirement without the need to have all of the individual officers physically present
- Robust backup/restore capability with a user configurable policy to specify M of N smartcards required for a restore
- Full multi-domain key and policy enforcement enables enterprises to create and manage multiple segregated digital keys per business need while applying policy enforcement to govern the key on the HSM
- Integrated with the Voltage SecureData product portfolio by protecting the data encryption keys

Cryptographic Algorithms Supported

Cryptographic support

- Advanced encryption standard (AES), Data encryption algorithm (DEA) standard (ANSI X3.92-1987, ISO 10126-2), DES, and Triple DES; Banking procedures for message encipherment, general principles (ISO 10126-2); PIN management and security, part 1 and 2 (ANSI X9.8, ISO 9564–1 and 2); Message authentication (ISO 9797-1, ANSI X9.9-1987, ISO 9807); MasterCard CVC, Visa CVV, and American Express CSC; MasterCard CVC3, Visa dCVV, and Discover dCVV; Unique key per transaction (ANSI X9.24-2004); EMV-based smart card support

PIN block formats

- ISO 9564; PIN pad; IBM 3624 ATM PIN format; IBM 4731 PIN block; IBM Encrypting PIN pad; Unisys (Burroughs); Diebold; Docutel Olivetti

PIN verification methods

- IBM 3624; Visa PVV; Atalla Bi-Level DES; Diebold; NCR

Key management standards

- ANSI X9.24 Parts 1 & 2; ANSI X9.52; Triple DES derived unique key per transaction

Performance

- Rated at 10,000, 1060, 280, and 80 TPS (Visa PIN translates per second)

Note: Card validation code: (CVC), card verification value (CVV), card security code (CSC), card validation code 3 (CVC3), dynamic card verification value (dCVV), and PIN verification value (PVV)

More About Atalla Key Block

Atalla Key Block is the advanced key management complement to the Atalla HSM models. Leading financial industry independent software vendors (ISVs) have embraced Atalla Key Block. It has also been adopted as part of the industry-standard ANSI X9.24 Part 1-2009 Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques and ANSI X9.24 Part 2-2006 Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for Distribution of Symmetric Keys.

Technical Specifications

Physical Dimensions

- **Height**
  1.69 inches (4.3 cm)
- **Width**
  19.01 inches (48.3 cm)
- **Depth**
  30.87 inches (78.4 cm)
- **Weight**
  36.3 pounds (16.5 kg)
- **Controls**
  Power on/off switch, unit ID switch, LCD control panel

Electrical

- **Rated input voltage**
  100 to 127 VAC
  200 to 240 VAC
- **Rated input current**
  4.8 A at 100 VAC
  2.4 A at 200 VAC
- **Rated input frequency**
  50 Hz to 60 Hz
- **Rated input power**
  480 W at 100 VAC
  480 W at 200 VAC
- **BTUs per hour**
  1638 at 100 VAC
  1638 at 200 VAC
- **Rated steady-state power**
  250 W at 100 VAC
  250 W at 200 VAC
- **Maximum peak power**
  480 W at 100 VAC
  480 W at 200 VAC

Operating Environment

- **Temperature**
  10°C to 35°C (50°F to 95°F)
- **Relative humidity**
  5% to 95% Non-condensing

Certification/Compliance

- **Safety**
  UL, CSA, CE, TUV, GS, EAC, EK, CCC, BIS, BSMI, BIS, RCM
- **Emissions**
  FCC Class A, VCCI
- **Environmental**
  RoHS 2.07

Connectivity

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