MICRO FOCUS

Data Sheet
Security

Atalla HSM

Enhanced software for Atalla Ax160 HSM

Overview

The Atalla Ax160 HSM enhanced offering is loaded with features that enhance the Atalla Ax160, enabling organizations to reap expanded payment transaction protection. The Atalla Ax160 HSM enhanced version complements the Atalla Ax160 by providing key functionality for ATM/EFT/POS payment processing environments.

The Atalla Ax160 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. It enables data and ecommerce protection and key management operations for PIN translations, payment card certification, production and personalization, electronic funds interchange (EFTPOS, ATM), cash-card reloading, EMV transaction processing, and key generation and injection.

This PCI-HSM certified, tamper-resistant HSM is designed specifically for secure payments applications with compliance requirements, including Debit, EMVCo, and Cloud-based payments with FIPS 140-2 Level 3 appliance. It meets the critical PCI-DSS, NIST and ANSI standards required for security and compliance audits.

Powerful Features for Demanding Payments Environments

As an efficient platform for meeting the ANSI key block standard, the Atalla Ax160 HSM Enhanced platform derives the full security value of industry-known public key encryption technologies—DES, triple DES (3DES) and public key encryption The Atalla Key Block meets the mandates required by this industry standard.

As organizations comply and support PCI PIN, customers will find it easier to plan upgrades or deploy new solutions to meet the requirements for remote key loading. It supports the full set of the symmetric key block formats A/B/C required for the PCI PIN standard (ANSI X9 TR-31 format A/B/C).

The Atalla Ax160 HSM Enhanced platform enables trusted TLS connections and allows organizations to customize the security by configuring known IP addresses greatly reducing "insider" attacks. Automated health diagnostic checks can be captured and displayed—an important PCI HSM requirement—while administrators directly monitor HSM CPU utilization to ensure the Ax160 HSM use is not going to max out, potentially crippling transaction processing capabilities.

Multiple MFKs (Master File Keys) can be generated to enable resource efficiency by using a

Enhanced Software Features

- PCI-HSM certified
- Compliance with PCI PIN v3.0 requirements for ATM/POS remote key loading using Public Key (ANSI X9 TR-34)
- Compliance with new key block format for ATM remote key loading using symmetric key (ANSI X9 TR-31 format A/B/C)
- Generate/verify CMAC using 3DES
- DUKPT IPEK POS Support
- Expanded mPOS Terminal Support
- UPI Payment and PIN Change Transactions
- Generate/Receive/Verify APACS 40 messages

single unit while still maintaining compliance. This Multi-Domain Support with private keys and policies allows the customer to create and have multiple segregated private keys per business needs and apply the applicable policy to govern that key only on the same physical HSM.

Remote management, backup and restore including a configurable policy to be set to specify that M of N cards must be required for a restore. This approach provides increased robustness and policy control around recovery of sensitive encryption keys and configuration data.

Advanced Key Management Solution Using Atalla Key Block

The Atalla Ax160 HSM advanced key management supports the 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 Benefits

Logical Security

- PCI-HSM v1.0 certified
- ANSI standard Atalla Key Block 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
- GUI-based configuration, management, and key loading via Atalla Secure Configuration Assistant (no clear text passing of keys or key components)
- Remote ATM key initialization and Remote Key Loading (RKL)
- PCI Security Standards Council PIN Transaction Security (PTS) approved hardware
- UPI payment and PIN change transaction support
- Generate/Receive/Verify APACS 40 messages
- Support for DUKPT
- PIN and key component printing
- Enables P2PE v2.0 compliance with SecureData Payments

Flexibility and Extensibility

- Broad application support (ATM/EFT/POS, stored value, loyalty cards, EMV cards, transfer)
- Customer-defined security policies
- Command set customization
- Command set backwards compatible
- GUI-based management

Standards Support

Cryptographic Support

- Data encryption algorithm (DEA) standard (ANSI X3.92-1987, ISO 10126-2), DES, and 3DES
- Banking procedures for message encipherment, general principles (ISO 10126-2)
- PIN management and security, parts 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 Verification Methods

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

PIN Block Formats

- ISO 9564
- PIN pad

Contact us at:
www.microfocus.com

- IBM 3624 ATM PIN format
- IBM 4731 PIN block
- IBM encrypting PIN pad
- Unisys (Burroughs)
- Diebold
- Docutel Olivetti

Key Management Standards

- ANSI X9 TR-31
- ANSI X9 TR-34
- ANSI X9.24 parts 1 and 2
- ANSI X9.52
- 3DES
- DUKPT

Security—Data Security

Micro Focus® Data Security drives leadership in data-centric security and encryption solutions. With over 80 patents and 51 years of expertise, we protect the world's largest brands and neutralize breach impact by securing sensitive data at rest, in use, and in motion. Our solutions provide advanced encryption, tokenization, and key management that protects sensitive data across enterprise applications, data processing IT, cloud, payment ecosystems, mission-critical transactions, storage, and Big Data platforms. Security—Data Security solves one of the industry's biggest challenges: simplifying the protection of sensitive data in even the most complex use cases.

Learn More At

https://software.microfocus.com/products