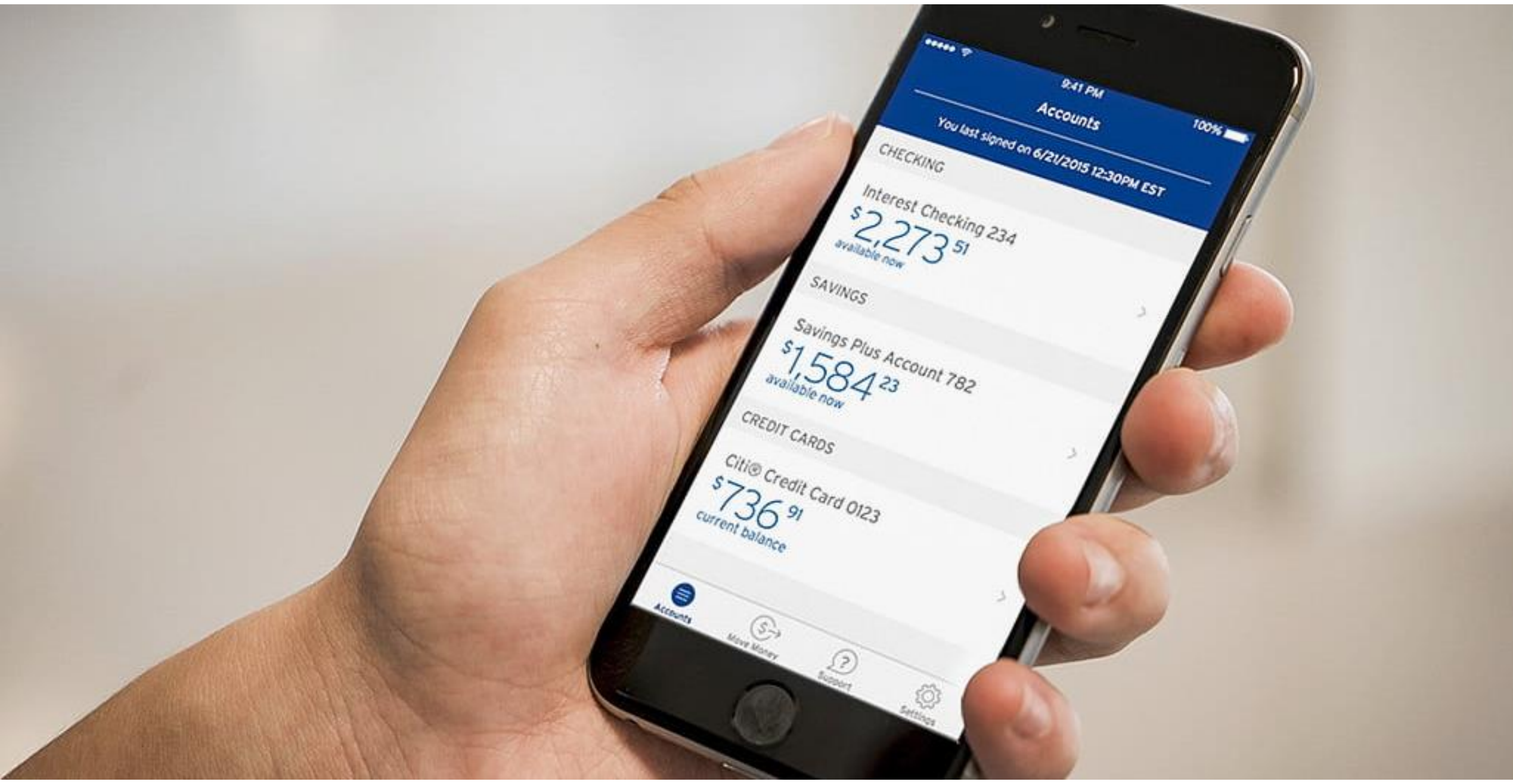
White Paper

Choosing the Right Hardware Security Module (HSM) for Your Bank



Introduction

The payment ecosystem contains some of the most complex and vulnerable processes that we have today. It involves many players and layers, as well as highly sensitive data, making it a prime target for complications and attacks. All these stakeholders must work together to provide a security solution that protects customer information because this entire system is only as strong as its weakest link. At the heart of this security landscape sits a Hardware Security Module (HSM). Most likely many HSMs.

An HSM provides cryptography for transaction processing, including endpoint authentication, secure communications and card/PIN verification. Using strong cryptographic algorithms, they store and generate keys, ensuring that the master key never leaves the vault. These keys are used to validate customer card details and determine if transactions should be authorized or declined. HSMs are considered the highest level of security and are rated and certified using the FIPS 140-2 standard. At a glance, a “good” bank HSM must secure the financial information in transit during a transfer from one bank to another, translate PINs between different time zones and securely protect cryptographic keys; which are in transit inside payment networks.

Adding to the requirements of protecting all this data are the expectations that the banking industry be able to accommodate rising customer expectations. Consumers expect anytime, anywhere banking with refined websites and applications. So, as security requirements, such as the new PCI 3.0 mandate become more stringent, banks will still need to find a way to be nimble.

In this article, we will **provide greater insight into the payment ecosystem, outline recent changes and new security requirements, as well as make recommendations around choosing the best HSM.**

Contents

Pre-Requisites: Bank’s Security Background for Financial Network Transactions

What is the Payment Value Chain?

The Payment Value Chain refers to an intricate ecosystem where devices and applications of differing levels of security are trusted to ensure that payments reach their intended party. These payment transactions involve the consumer, merchant, acquirer, network (e.g., MasterCard, Visa), issuer and switch, as well as multiple third-party service providers. The data associated with these transactions is encrypted and decrypted multiple times throughout this process, briefly exposing it and leaving it vulnerable to attack. Further adding to this complicated process is the fact that the various elements of this ecosystem may be owned by multiple third-party vendors. *To begin, let’s review some basic terminology.*

Electronic Fund Transfers (EFT)

This is the operation of an automated transfer of money between a bank account to another bank account via a network of computer-operated devices without human intervention. The EFT network can connect ATMs, POS financial terminals, and multiple switches between different processors and financial institutions.

Automated Teller Machines (ATM)

ATMs, also known as “cash dispensers” are autonomous telecommunication computer devices that allow customers to independently perform various financial operations. The most important operation is cash withdrawal from their bank account using a credit or debit card, which is usually PIN-protected.

Point-of-Sales (POS) Financial Terminals

A POS financial terminal, also known as EFTPOS terminal is a telecommunication computer device. It interfaces credit or debit cards to make electronic fund transfers at the point-of-sale terminal (cash register).

Payment Gateway

A payment gateway is an internet server that captures payment authorization and other payment-related flows emitted from internet or point-of-sale web clients or point-of-sales financial terminals.

Acquiring Bank

The acquiring bank (also merchant bank or acquirer) is a financial institution that holds the bank account of the merchant. Acquirer contracts allow merchants to process credit and debit card transactions. The acquirer holds the merchant's bank account and accepts payments on the merchant's behalf through the switch. The acquirer also deposits funds and may provide the hardware and software to enable the merchant to process transactions.

Payment Switch

A payment switch is a foundational element of all modern payment architectures. It's a smart processing software that enables communication between a multitude of payment providers to process payments in the most efficient way possible. The switch is an organization contracting with the acquirer to process transactions on a merchant's behalf. These are the intermediaries doing most of the information processing from the POS / ATM data collection level to the acquiring bank and beyond.

Credit Card Network

There are four major credit card networks – Visa, Mastercard, Discover, and American Express that serve as links between the merchant and the bank or the issuing bank.

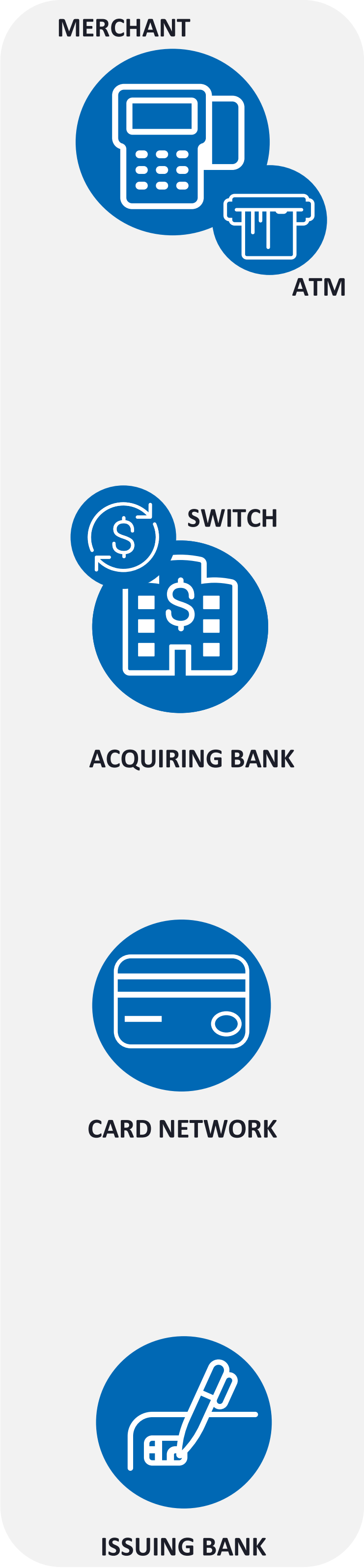
Issuing Bank

The issuing bank is a financial institution, such as a bank or credit union, issuing credit cards on behalf of the card networks. In the value chain of payments, the card issuer pays the acquiring bank for the cardholder's purchases of goods and services. The cardholder then repays the issuing bank based on contract terms.

Note: Some financial institutions are both acquirers and issuers. These banks operate for the consumer and the merchant. Bank of America, Citibank, Barclays, Chase, and Wells Fargo are examples of such financial institutions.

Payment Ecosystem Process

The consumer will initiate the process when using a credit /debit card to pay for goods and services by entering payment information into an ATM pin pad, POS terminal, or online portal. The entered information travels through a series of networks to a card issuer for authorization to access the cardholder's record and verifications.



1 *The merchant must have the technology in place to accept all payment methods, process the card and facilitate the transfer of funds, forwarding transaction information to the payment switch/ gateway / processor.*

2 *The switch forwards transaction data to the card network. Payment switches usually operate in the background, and a merchant seeking a POS set up to accept card payment may not have to work directly with payment switches as they typically partner with the acquirer directly.*

3 *The Card Network routes transaction data to the correct issuing bank. There are four major credit card networks – Visa, Mastercard, Discover, and American Express that serve as links between the merchant and the bank or the issuing bank.*

4 *The issuer receives and verifies the data, then returns an authorization message to the network.*

5 *Card Network receives the message from the issuer, then forwards it to the switch. Issuing banks typically manage cards on behalf of networks. However, Discover and American Express are both the card network and the issuing bank; their own financial institutions issue credit cards to consumers.*

6 *The switch receives the authorization message from the network and then forwards it to the ATM or POS.*

7 *The merchant receives the message, then completes the transaction and batches it with the rest of the day's sales to send to the acquiring bank.*

8 *The acquirer receives the batched transactions, deposits the amount into the merchant's account, minus applicable fees.*

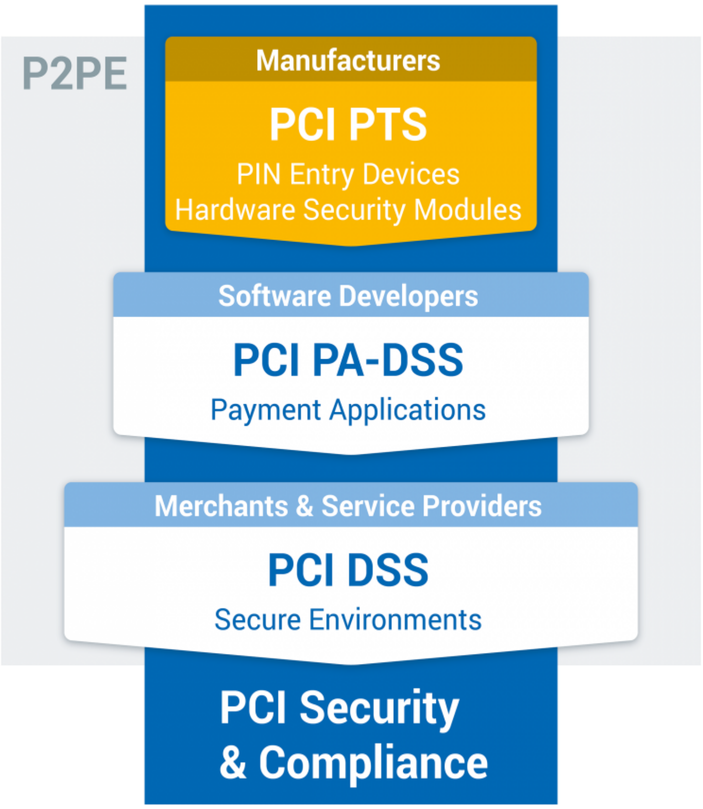
PCI Security and Compliance

Background

PCI standards define the minimal functional security requirements for the ecosystem surrounding electronic fund transfers (EFT). The Payments Card Industry Security Standards Council (PCI-SSC) is here to help protect cardholders' private information. They continually set and enforce global security standards applicable to all organizations that store, process or transmit cardholder data, as well as software developers and manufacturers of applications and devices used in payment transactions. There are three major standards:

Payment Card Industry Security Standards

Protection of Cardholder Payment Data



Ecosystem of payment devices, applications, infrastructure and users

- ***PCI-PTS applies to manufacturers who manufacture POS devices used for payment card financial transactions***

- ***PA-DSS is for software developers and integrators of payment applications that store, process or transmit cardholder data as part of authorization or settlement***
- ***Most card brands encourage merchants to use payment applications that are tested and approved by the PCI-SSC***

- ***PCI-DSS applies to all entities that store, process, and/or transmit cardholder data***
- ***This covers technical and operational system components included in or connected to cardholder data, for example - If you are a merchant who accepts or processes payment cards, you must comply with the PCI DSS***

Reference: PCI Security Standards - https://www.pcisecuritystandards.org/minisite/en/pci-dss-supporting-docs-v30.php

Version 3.0 of Payment Card Industry (PCI) PIN Security Requirements

The Council updates the PTS Standard every three years and POI device approvals expire six years after the retirement of the security requirements against which they were validated. The following security requirement versions are set to expire:

- PCI v1 – security requirements retired – **2013**, devices expired – March 2019
- PCI PTS v2 – security requirements retired – **2017**, devices will expire – April 2023

To be PCI-PTS v3.0 compliant, customers must upgrade to the key bundling method. Key bundling, sometimes referred to as "key blocks" significantly enhances the protection of symmetric keys shared by payment system participants to protect PINs and other sensitive data. Key use must be cryptographically linked to a master key using the following accepted methods:

- *A MAC calculated through the concatenation of the clear-text attributes and the enciphered portion of the key block, including the key.*
- *An integrity check, which is an inherent part of the key-encryption process, such as what is used in the AES key-wrap process.*

New implementation dates were split into three phases, each with its own effective date. This will allow organizations to focus their resources on addressing environment-specific implementation tasks and support smooth migration across the payment network.

Phases and revised effective dates:

- **Phase 1** — Effective June 2019: Implementation of key blocks for internal connections and key storage within service provider environments. This includes all applications and databases connected to HSMs.
- **Phase 2** — Effective June 2021: Implementation of key blocks for external connections to associations and networks.
- **Phase 3** — Effective June 2023: Implementation of key blocks to extend to all merchant hosts, POS devices, and ATMs.

Reference: PCI Security Standards - https://www.pcisecuritystandards.org/minisite/en/pci-dss-supporting-docs-v30.php

Payment Card Industry PIN Transaction Security Hardware Security Module (PCI-PTS HSM)

Now that we have a better understanding of how the payment ecosystem works and its security requirements, let's dive into how an HSM systematically protects every vulnerability point within the value chain. All device vendors and manufacturers must enlist the help of a Payment Card Industry PIN Transaction Security Hardware Security Module (PCI-PTS HSM) to be compliant. At a high-level, an HSM should provide the following:

- *Secure the payment value chain*; meaning that it must secure the financial information in transit during a transfer from one bank to another in the EFT network.
- *Effectively translate PINs* between different zones in the EFT network.
- *Securely protect cryptographic keys*; which are in transit inside payment networks.
- *Be accessed only via a very secure authentication.*
- *Have an anti-tampering system* to protect its electronic components against unauthorized access, side channel attacks and attempts to reveal secrets by opening the hardware.
- Be able to be *batch managed* and have simple and secure ways to receive batches of commands or function calls to process.
- Scale to the requirements of the bank's ATM network.
- Establish secure tunnel between HSM and the host application.
- Support legacy TDES and NextGen AES Keys for payment processing.
- Should support Payment industry standards and crypto operations.
- Be compliant and certified by FIPS and PCI Council.

PIN Transaction Security and PIN Translation

The PIN Security Personal Identification Number (PIN) is a method for verifying the cardholder at the point of transaction. Card issuers expect their customer PINs to be protected through the interchange process, while acquirers rely on consumer confidence to facilitate their desired volume. Ensuring cardholder PIN confidentiality throughout the interchange cycle requires adherence to a set of globally recognized security requirements.

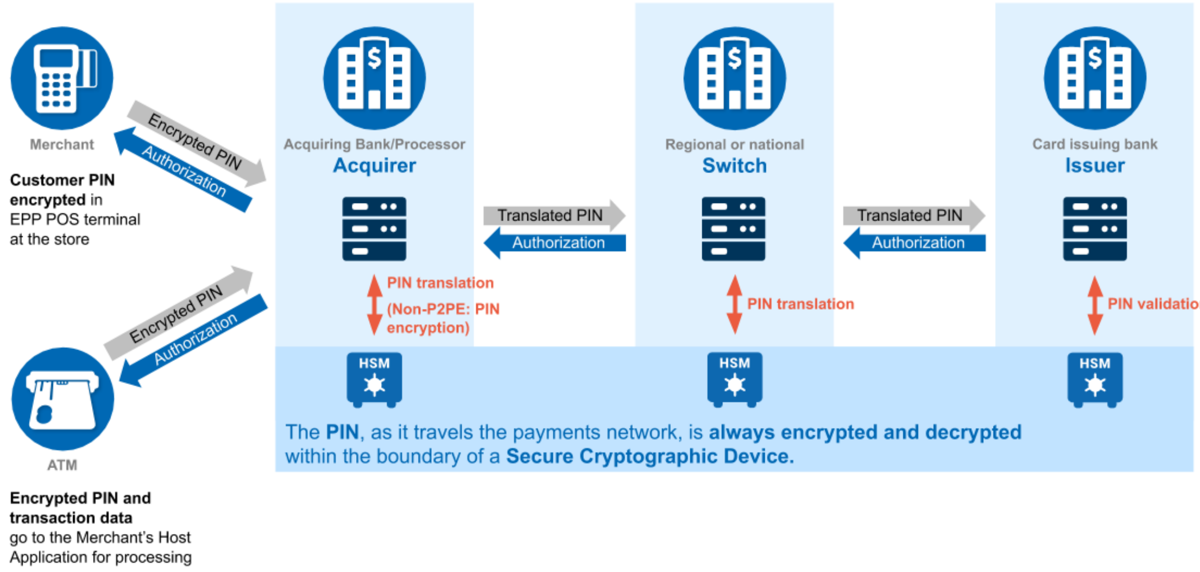
The International Organization for Standardization (ISO) defined a standard for systems that exchange cardholders' electronic information using payment cards. This system, called “ISO 8583,” outlines a structure for successful communication between different parties.

With all parties having a standard messaging format, there is a need for a way to securely communicate the PIN entered for authentication by the cardholder at the terminal. This is accomplished through the '**PIN translation**' process, which ensures point-to-point encryption. The cardholder's PIN is encrypted by the terminal and passed on to the acquiring bank.

Assuming this transaction is initiated at an ATM, it reaches the ATM interface at the 'Acquirer' bank. This is where a converter decrypts the input key and encrypts it into a new output key using an HSM.

The output key is then sent to the router identifying the card's payment scheme, again translating the key to a new output key to be sent to the network.

This key translation at each communication node ensures that the PIN is securely validated by the issuing bank, which upon the cardholder's authentication, returns an authorization code to the acquirer via the network to complete the transaction.


Merchant
Customer PIN encrypted in EPP POS terminal at the store
Encrypted PIN
Authorization
Encrypted PIN
Authorization
ATM
Encrypted PIN and transaction data go to the Merchant's Host Application for processing
Acquiring Bank/Processor
Acquirer
Translated PIN
Authorization
Regional or national
Switch
Translated PIN
Authorization
Card issuing bank
Issuer
PIN translation
(Non-P2PE: PIN encryption)
PIN translation
PIN validation
HSM
HSM
HSM
The PIN, as it travels the payments network, is always encrypted and decrypted within the boundary of a Secure Cryptographic Device.

In the ecosystem described by the illustration, ISO PIN blocks are being transmitted from one network to another for various reasons where the keys that are used on one network cannot be used on another network. Encrypted PINs that are transmitted across these networks must be securely “translated” from one encryption to another encryption.

For example, a bank customer who is outside his country of residence is withdrawing money from an ATM. The ATM needs to access the customer's bank account in his country of residence. The PIN that is entered at the ATM is encrypted locally and then sent through various financial networks until it reaches the customer's home bank. The home bank must verify the PIN ("online PIN") and return authorization before the ATM can allow access.

During transit on the intermediate systems (between networks), the different parties can use the PIN translation service to re-encrypt a PIN block from one key to another. The PIN Translation service ensures that PINs never appear in the clear and that the keys for encrypting the PIN are isolated on their own networks.

Symmetric Key Management and Security Package

ANSI X9.24-1/ANSI X9.24-2/ASC X9 TR 31

ANSI X9.24 Standards Security Package provides guidance on managing symmetric keys using symmetric techniques as well as asymmetric keys distribution techniques. It also sets methods for secure key exchange and sensitive data using a symmetric key-exchange key. This is also the standard asymmetric key storage method.

The ANSI X9.24 standard for retail financial key management mandates
that 3-DES keys must:

- *Be protected against disclosure and misuse*
- *Exist in a "key bundle"*
- *Be secret and randomly or pseudo-randomly generated; have integrity, so that each key in the bundle cannot be altered in an unauthorized manner*
- *Be used as specified by the particular mode*
- *Be considered as a fixed quantity, in that it is not possible to manipulate part of the key, and that the key cannot be "unbundled"*

These standards require cryptographic protection of cardholder PINs. Such protection requires specific controls to ensure all participants achieve the intended level of safety.

Successful management of the payment system depends on cooperation between all participants. Failure to meet the requirements increases the risk of compromise, resulting in monetary losses associated with investigating fraud claims and eroding consumer confidence in the payment system.

Although the standard mainly concerns 3-DES keys, clearly the same requirements make sense for any secret or private key. The security policy of the HSM should be configured as "tightly" as possible, subject to applications calling the HSM. Only HSM features necessary for security should be enabled; this includes HSM commands, PIN block formats, PIN algorithms, etc.; all other features should be disabled.

Secure Access for Loading Key and Configuration

There are three PIN procedures for high-security interchange operation. First, the PIN is encrypted at the entry terminal, using a secret cryptographic key during this step. Besides other transaction elements, the encrypted PIN is transmitted to the acquirer's system. Next, the encrypted PIN is routed from the acquirer's system to a Hardware Security Module. Within the HSM, the master key decrypts the PIN. The decrypted key is immediately re-encrypted and is routed to the issuer's system via secure channels. Finally, the routed PIN is decrypted in the issuer's security module and validated in the financial institution's database with the recorded reference PIN. Note, any network malfunction within this process will make an ATM unusable until fixed. This is where remote key loading comes into play.

Remote Key Loading

The payment card industry requires systems to encrypt the PIN when captured. **The HSM keys used to encrypt and validate PINs must regularly rotate** to meet PCI requirements and maintain high-level of security. Using manual methods for key loading requires unnecessary effort and cost, making proving compliance an onerous task. With multiple key custodians entering secret keys in an ATM's PIN pad, there is an increased risk for error and collusion. **Remote key loading provides a secure, efficient, and cost-effective way to load and manage ATM encryption keys across ATM networks**. Before remote key loading became accepted, key holders had to visit each ATM in-person to alternate network keys. This process was cumbersome, and operating costs increased significantly as ATMs continued to grow.

With over 4 million devices forecast worldwide by 2020, ATM growth is still swelling. **A remote key no longer requires two key custodians to visit the ATM when a key change is physically needed.**

Utimaco Atalla AT1000 is the Right Hardware Security Module for your Bank

Look to the *Utimaco Atalla AT1000* to Secure the Payment Ecosystem

Almost every banking transaction taking place in the world today touches a Utimaco Atalla HSM! It's an HSM with a long-standing history that provides a complete set of cryptographic functions to secure the Payment Ecosystem. Atalla HSMs implement a TLS tunnel in between the HSM and the host application which works as a brain in the banking infrastructure. The encrypted PIN received from the ATM network, an acquirer or a payment network is then sent to the HSM along with account validating information that is stored locally or on a translating key.

Achieved using command 31, the HSM securely decrypts the PIN inside the secure boundary and then encrypts it under the next level transport key. When this PIN reaches the issuing bank, its validated by the HSM against the known secrets at the bank level by using command 32.

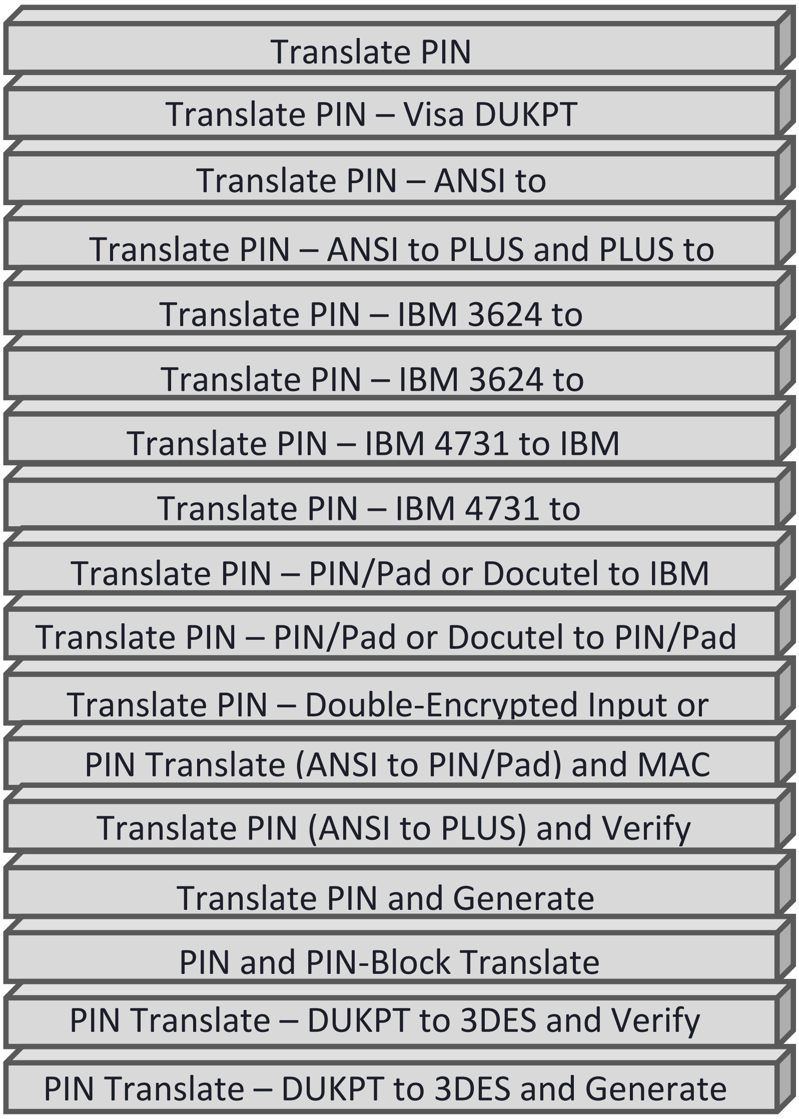
In the next few sections, we will outline how the Utimaco Atalla AT1000 uniquely addresses the following core elements within the payment ecosystem:

- *Advanced PIN translation, generating varying types of encryption keys, as well as performing a multitude of key operations in several models of ATMs.*
- *Processing many EMV operations present within segments of the Payment Value Chain.*
- *Managing and securing the cryptographic keys (often 3DES) using the famous Atalla Key Block.*
- *Remote accessibility through a hyper-secure device, the Secure Configuration Assistant (SCA), which is completely tamper-resistant.*

Utimaco Atalla AT1000 and PIN Translation

Utimaco Atalla HSMs are very good at PIN translation (Mohamed Atalla pioneered the use of the PIN in the banking industry). The AT1000 has a capacity of PIN Translation of more than 10,000 TPS (Translation per Second) in a single device.

The Utimaco Atalla AT1000 allows robust PIN translation via the following commands:



Translate PIN

Translate PIN – Visa DUKPT

Translate PIN – ANSI to

Translate PIN – ANSI to PLUS and PLUS to

Translate PIN – IBM 3624 to

Translate PIN – IBM 3624 to

Translate PIN – IBM 4731 to IBM

Translate PIN – IBM 4731 to

Translate PIN – PIN/Pad or Docutel to IBM

Translate PIN – PIN/Pad or Docutel to PIN/Pad

Translate PIN – Double-Encrypted Input or

PIN Translate (ANSI to PIN/Pad) and MAC

Translate PIN (ANSI to PLUS) and Verify

Translate PIN and Generate

PIN and PIN-Block Translate

PIN Translate – DUKPT to 3DES and Verify

PIN Translate – DUKPT to 3DES and Generate

The Utimaco Atalla AT1000 Uses the Atalla Key Block (AKB)

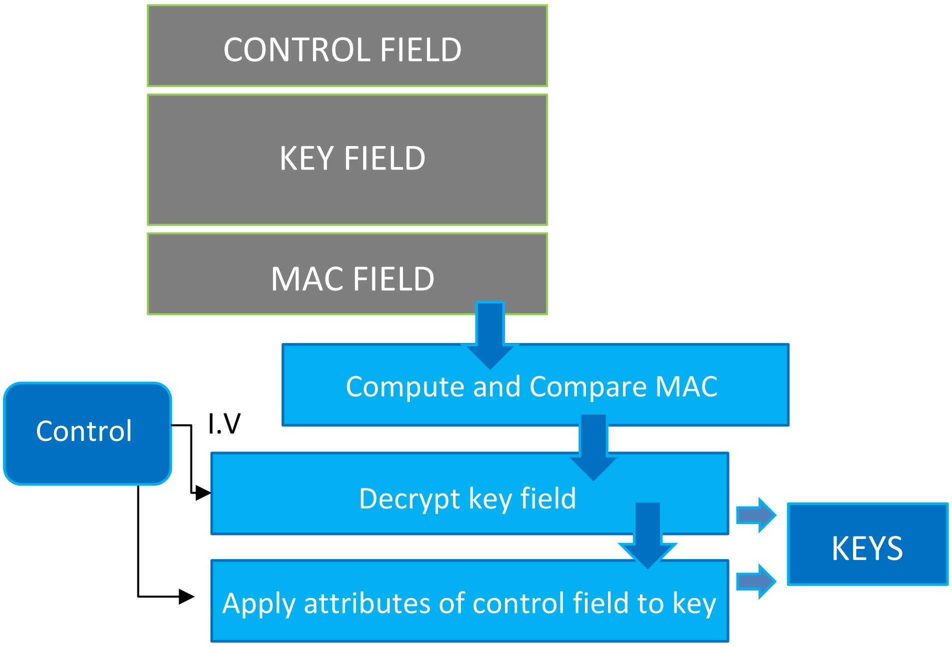
The Utimaco Atalla Key Block used by the AT1000 is the root of all the cryptographic block formats found in PCI or ANSI standards. **It solves key security issues when in transit within a potentially hostile environment**. The Atalla Key Block (AKB) was the first market-specified standard to bind the key with the intended characteristics and integrity to ensure that the ciphertext was not modified.

AKB is de facto integrated to the following standards:

- *ANSI X9.24 Part 1-2009 Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques;*
- *ANSI X9.24 Part 2-2006 Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for Distribution of Symmetric Keys;*
- *ANSI X9 TR-31, Interoperable Secure Key Exchange Key Block Specification.*

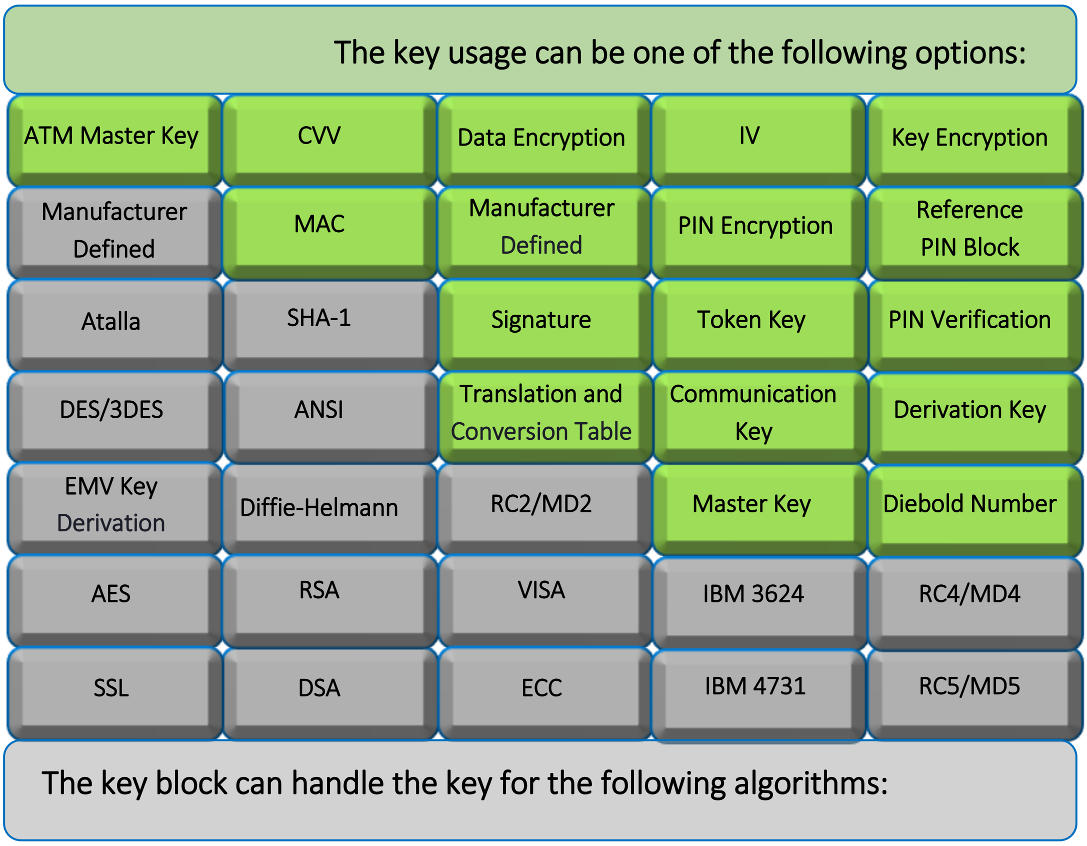
The key is protected by the approved bundling standard requirements, significantly reducing man-in-the-middle (MitM) attacks. Additionally, key usage attributes are bound to the key itself. For example, the key is identified as an encryption key and cannot be used to decrypt data, key exportability, etc.

Here we detail how the Atalla Key Block is processed by a receiver to extract the key (or PIN) it protects.



First, the AKB is checked for integrity by computing the MAC and comparing it to the presented MAC field. If the MACs are the same, the operation continues.

The key is then decrypted using the Control Field Initialization Vector I.V and the first variant of the master file key. Keys are then resolved and used following the data from the control field. The control field is an 8-byte header which details all the information about the key within the block.



The key usage can be one of the following options:

ATM Master Key	CVV	Data Encryption	IV	Key Encryption
Manufacturer Defined	MAC	Manufacturer Defined	PIN Encryption	Reference PIN Block
Atalla	SHA-1	Signature	Token Key	PIN Verification
DES/3DES	ANSI	Translation and Conversion Table	Communication Key	Derivation Key
EMV Key Derivation	Diffie-Helmann	RC2/MD2	Master Key	Diebold Number
AES	RSA	VISA	IBM 3624	RC4/MD4
SSL	DSA	ECC	IBM 4731	RC5/MD5

The key block can handle the key for the following algorithms:

Utimaco's solution integrates terminal master keys to any remote key enabled ATM with any host platform.

Remote loading benefits include:

- *Comprehensive remote key loading solution for ATM networks*
- *PCI 3.0 requirements and network standards*
- *Reduces manual steps and eliminates the potential for key management fraud*
- *Improves ATM upgrades and simplifies installations*
- *Includes remote key loading for ALL remote key enabled ATM*

Atalla HSMs utilize RSA keys for initializing remote devices. These commands generate RSA key pairs, import public keys, generate message digests, encrypt an ATM Master key using the public key stored in the Electronic PIN Pad, and generate and verify digital signatures. The following are high-level steps on how an Atalla AT1000 HSM engages in remote key loading.

Initial Setup per Certificate Authority (CA)

1. Use command 12A to get the CA's public key into AKB format with a header of 1RRVN00k. This AKB is used as field 8 in command 123. The CA's public key is required to verify the recipient's certificate (which contains the recipient's public key).
2. Use command 120 to generate a public and private key pair. Field 1 of the command 120 will contain the letter "w". The private key will have a header of 1wRGE000, for use as field 9 in command 139. The public key will have a header of 1wRVE000 (however this AKB is not used as the HSM does not supports receiving TR-34 key blocks). The public key must be provided to the recipient, so they can use it to verify the message signature created by command 139.
3. Use the public key information from the step 2 to create a KDH certificate request message. This step is performed by the host application.
4. Sign the certificate request message using command 139.
5. Receive the KDH certificate from the CA and store it on the host for use in the TR34 protocol.

TR-34 Bind Phase

6. Receive CRD Credential Token (terminal certificate). The host application parses the certificate to find the modulus and public key. Use command 123 to get the recipient's public key into AKB format, the header is 1kREE000. This AKB is used as field 7 in command 136. The host application sends the KDH certificate (from step 5) and current CRL to the Terminal.

Symmetric Key Transport Phase

7. The host application optionally receives Random Number Token and saves for inclusion in step 10.
8. Use command 136 to:
   a. Generate a key in AKB format (TR-34 Step B2)
   b. Generate an ephemeral key (TR-34 Step B3)
   c. Generate an IV
   d. Use the ephemeral key and IV to 3DES-CBC encrypt the key block (version, IDKDH, Kn, KBH). In other words, encipher the BE data supplied as field 4, the key generated in the first bullet and the header supplied as field 2. (TR-34 Step B4)
   e. Encrypt the ephemeral key under the recipient's public key. (TR-34 Step B5)
   f. Generate an AKB of the signing key token with a header of 1bRVN000, for use as field 8 in command 139.

9. The host application builds the data to sign for the key token, including optional random number from step 8, the envelop data, ephemeral key encrypted under the recipient’s public key, IV, and encrypted BE value from step 9, timestamps, etc.
10. Use command 139 to hash and sign the ‘to-be-signed’ data from step 10 using the private key created in step 2 above.
11. The host application constructs the key token from the formatted data from step 10, the signature created in step 11, and any appropriate CRLs. The host application then sends the key token to the terminal.

The Atalla Secure Configuration Assistant (SCA)

The Atalla Secure Configuration Assistant used by the AT1000 also named the SCA, is a secure terminal dedicated to interfacing Utimaco Atalla HSMs; especially for loading remote keys.

The SCA is a special piece of hardware consisting of:

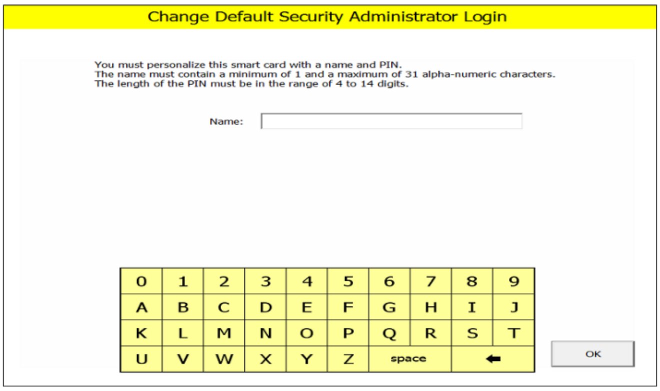
- *A tablet;*
- *A PIN pad equipped with a smartcard reader (the Atalla Secure Keypad (ASK));*
- *Cables that connect to the HSM either remotely or locally via a serial port.*

The SCA connects to the HSM and is used to perform initialization and general management in a secure way. It achieves many of the concepts of hyper-security.

Connecting a terminal to a secure system is not easy. By definition, allowing remote access is insecure. Of course, remote access is usually protected by a password or by keys and might also be protected by IP restrictions. But if the security of the terminal is not at least equal to the security of the system it must connect to, it then creates a security problem because compromising the terminal is compromising the entire system. Hence, such a terminal used to connect to an HSM must be hyper-secure in many ways.

Atalla Secure Keypad

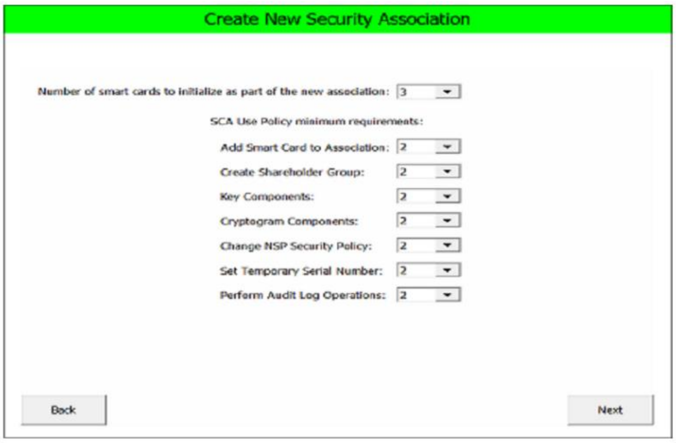
The SCA uses the Atalla Secure Keypad, which is a secure cryptographic device with anti-tampering capacities. It is designed to meet the security requirements of PCI, x9.24, as well as other financial standards regarding the manual entry of PINs. All the keys and smart card PINs are entered into the Atalla Secure Keypad and are communicated securely to the smart card, thus isolating all security items.



Change Default Security Administrator Login

You must personalize this smart card with a name and PIN.
The name must contain a minimum of 1 and a maximum of 31 alpha-numeric characters.
The length of the PIN must be in the range of 4 to 14 digits.

Name:


Create New Security Association

Number of smart cards to initialize as part of the new association: 3

SCA Use Policy minimum requirements:

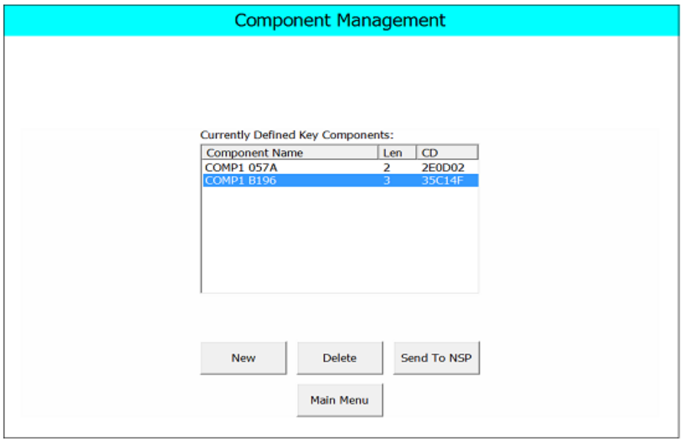
Add Smart Card to Association:	2
Create Shareholder Group:	2
Key Components:	2
Cryptogram Components:	2
Change NSP Security Policy:	2
Set Temporary Serial Number:	2
Perform Audit Log Operations:	2

Security Association

One of the main reasons why SCA achieves some hyper-security is its ability to create security associations. In its configuration, more than one administrator is needed to perform certain management operations. For instance, three administrators will take part in a security association defined by the security policy. Each will use their smart cards, one after the other to unlock the system with their own secret PIN secret.

Loading of the HSM MasterKey(s) from the Administrators Smartcards

The HSM MasterKey is the root of all keys. It must be remotely transmitted to the HSM in a hyper-secure way. Loading such a key is performed via the administrators' smartcards, which are as secure as the HSM. These smartcards are provided with sophisticated anti-tampering systems and are resistant to all sorts of attacks (DPA, SPA, glitch, DTA, laser, chemical, EM, environmental attacks, etc.). Therefore, this is the ideal way to carry cryptographic keys.


Component Management

Currently Defined Key Components:

Component Name	Len	CD
COMP1 057A	2	2E0D02
COMP1 B196	3	35C14F

The Atalla Command Language

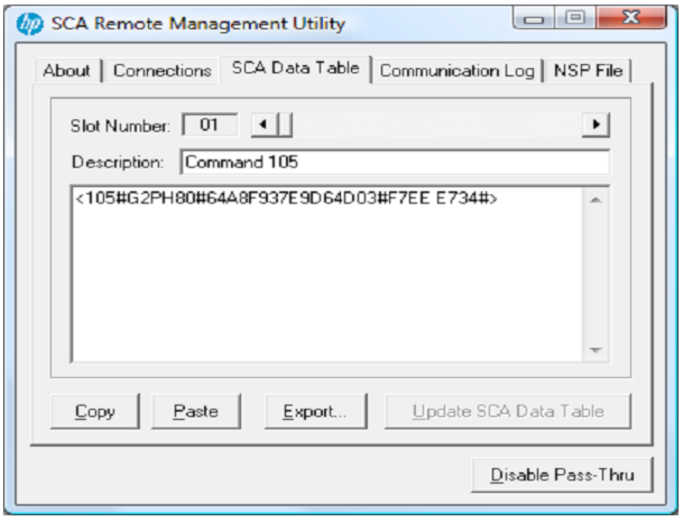
The Atalla command language is a secure and efficient way to communicate with the Utimaco Atalla HSM. It contains everything that is needed to perform banking operations in financial networks. One day, it may become a standard in how to interface HSMs, and potentially could be used in the future by other HSM vendors.

Atalla developed a text-based command system that is similar to a command shell (e.g. DOS or BASH) with a specific format. It can be considered as a Client Line Interface (CLI). It has an optimal use in the context of interfacing HSMs, including Utimaco Atalla HSMs.

There are more than 200 commands in the Atalla Command language. This makes the command shell quite a complex language. Anything that is needed to interface payment networks, ATMs, and EFTs, among others, is present in the command set.

Users communicate with the Atalla HSM via the secure Configuration Assistant (SCA), a hardware system that authenticates users via smartcards and lets them interface with the HSM.

The sending of direct commands to the Atalla HSM via the SCA is presented in the following picture.



Slot Number: 01

Description: Command 105

```
<105#G2PH80#64A8F937E9D64D03#F7EE E734#>
```

For example, the SCA implements a visual user interface to help the end-user generate or verify cryptograms. Under the hood, these are the Atalla commands that were sent.

The commands have different levels of security policy:

- *Standard commands that do not represent a risk in terms of security exposures, usually these are “global purposes” functions;*
- *Security exposure commands that may represent a risk, so they are disabled by default;*
- *Premium value commands that are highly exposed commands and can be activated only by a special set of commands.*

In terms of functionalities, the commands are divided into two groups:

- *Utility commands, consisting mainly of general operations, configurations, and diagnostics;*
- *Cryptographic commands, consisting of operations involving encryption, decryption, key generation, etc.*

Formatting of the Commands

Atalla commands are text-based and tokenized, meaning that the different parameters they carry are identified by separators, ‘tokens’, which are special reserved symbols. The commands follow a special syntax (or grammar) as follows:

A command will look like text data that is separated by the starting tag ‘<’ and the closing tag ‘>’ :

```
<_CMD_ID_#_FIELD1_#_FIELD2_#...#_FIELDN_#[^_CONTEXT_TAG_#]>
```

The `_CMD_ID_` value is a number representing the number of the command (ex: ‘105’)
The `_FIELD1_,_FIELD2_,...,_FIELDN_` are the values of the `N` parameters of the command

The `_CONTEXT_TAG_` value is a 5,000-word maximum data field, optional, and, which can have various usages.

All the parameters are separated by the token ‘#’.

An answer to the command will have the same format as the command, which means that several values may be returned in the answer.

Example of a command and response:

```
<10#1#F6F4D93F55860571#^Generate PIN ENCRYPTION KEY for ATM
NEWYORK_STAR_344#>
```

```
<10#1#F6F4D93F55860571#^Generate PIN ENCRYPTION KEY for ATM
NEWYORK_STAR_344#>
```

Utility Commands

Atalla’s utility commands do not require the loading of a master key file into the HSM. Therefore, they can be used even if the ATM has been zeroized. They allow access to system information about the CPU and RAM usage or battery status. Generally, these commands can be used for the HSM configuration, changing security policies, and running several self-check tests.

Conclusion:

There is a huge transformation taking place within the banking industry. As organizations try and deal with this digital disruption, the need for more secure, but flexible HSMs is a must!

The Utimaco Atalla AT1000 is known for its superior hardware security. It's PCI-PTS Certified for the most demanding application profile, focusing on physical security when used in controlled and uncontrolled environments like non-ISO certified data centers. It also provides unrivaled protection for AES and other cryptographic keys safeguarding payment transactions.

It's no wonder that global payment leaders and card brands continue to secure their payment ecosystem with Utimaco Atalla HSMs. Whether by industry or stakeholder need, this HSM secures a full breadth of use cases. They play a crucial role in securing inter-banking communication, user and card authentication, as well as focus on user data protection for both in-person (card present) and remote payments (online or card not present) transactions. Some key use cases include:

PIN Processing	3-D Secure	Card / User Verification	ATM Interchange	Data Integrity
Processing Transaction Data	Data Encryption / Decryption	Initialize Remote Payment Devices	PIN Translations and Authorization	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
Inter-banking, Clearing and Settlement	Card Issuance	Mobile and e-Wallets	Contactless Payments	Cloud Payment Standards

For more information or to speak with a representative, please contact *hsm@utimaco.com*.

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