

Creating Trust in
the Digital Society

Gracias por acompañarnos.
El webinar comenzará en breve.

utimaco[®]

Creating Trust in
the Digital Society



Atalla AT1000

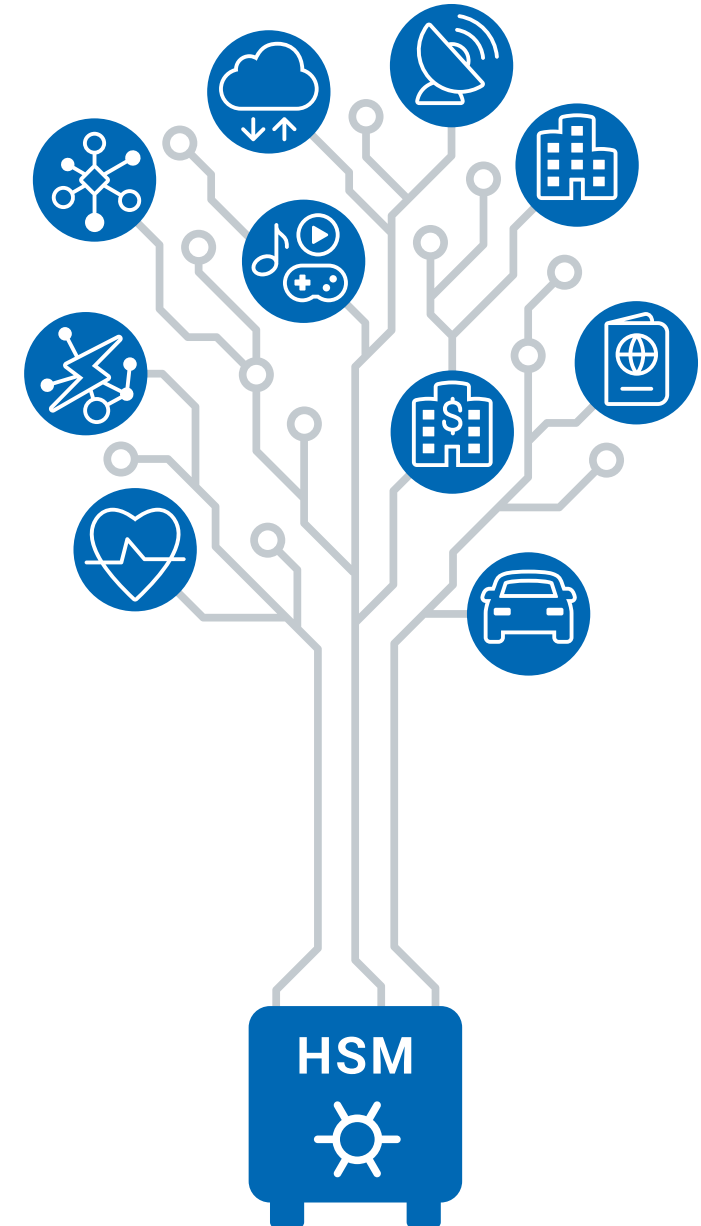


Is it Time to Upgrade your Ax160?

utimaco[®]

Focused around our customers' needs

- **Utimaco Portfolio & Atalla History**
- **Industry Challenges**
- **Current Status of Ax160**
- **Introducing AT1000**
- **PCI PTS Compliance Details**
- **AT1000 Enhancements**
- **Migrating to AT1000**
- **Atalla HSMs in the Cloud**



Utimaco is an international provider of
» **cyber security & compliance solutions** «
with headquarters in Aachen, Germany
& Campbell, California



 **\$75M USD**
Revenue FY 19/20



331+ highly skilled experts



Founded **1964**
Private company



50+ years in IT and
35+ years in IT-Security

**Worldwide customer and partner
network** in more than **90** countries



Diversity and internationality are the key to our success



Information Security

Encryption-based,
high-security solutions



Hardware Security
Modules



Key
Management



Enterprise
Data Protection

against theft, abuse and
manipulation

Cyber Security & Compliance Solutions

Telecom Solutions

Compliance solutions for
telecommunication
providers



Lawful Interception
Mediation System



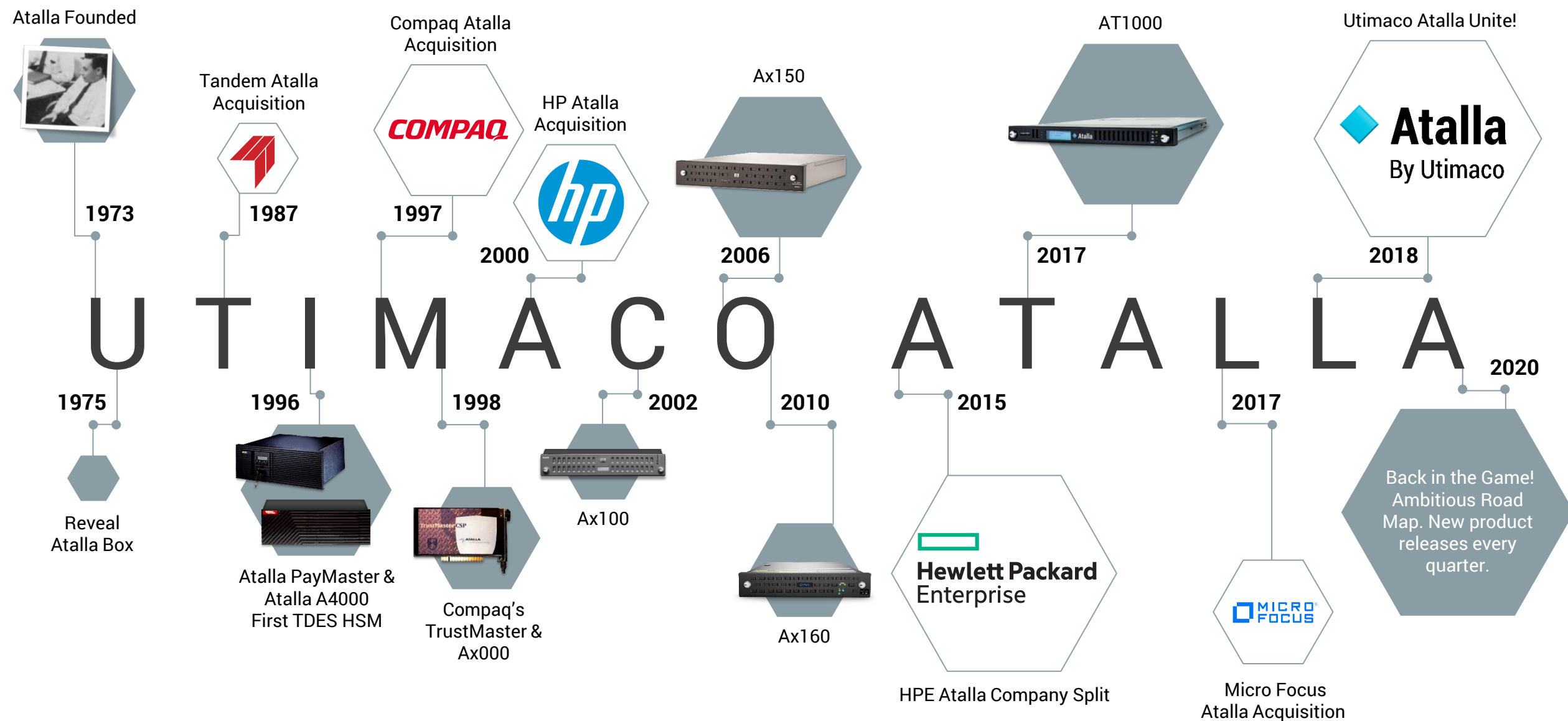
Data Retention Suite



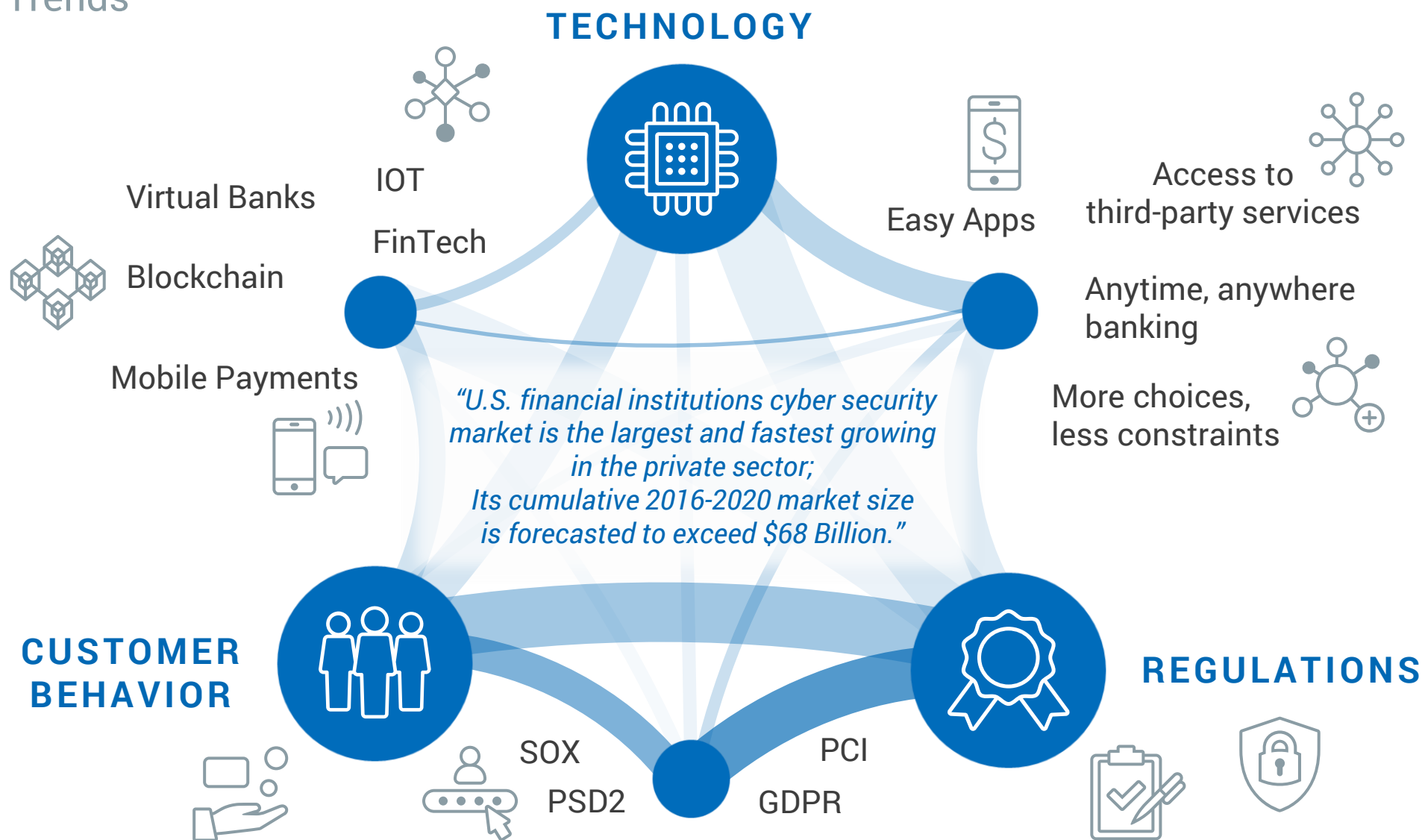
Lawful Interception
Test Suite

solutions that meet regulation &
compliance standards

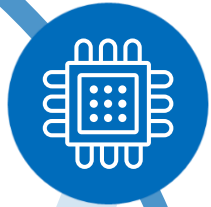
A History Steeped in Innovation



Market Trends



Within the Banking Industry



Adopting **New Technologies**



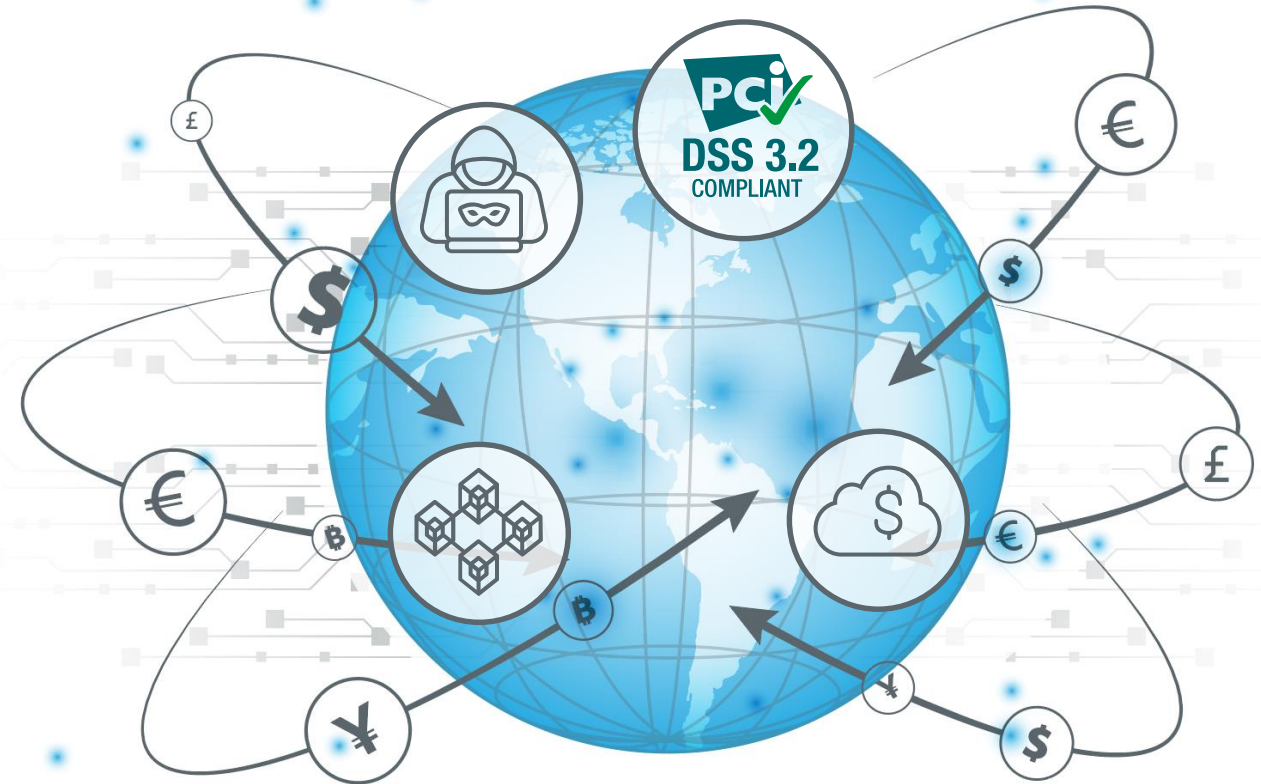
Competing Against
New Entrants



Protecting Against
New Security Threats



Staying Compliant as
Mandates Grow and Change



AX160 first launched in 2010!

Ax160



No Longer Compliant
PCI PTS v1

End of Sale Announcement

January 7, 2019

End of Sale Last Order

June 6, 2019

End of Support

July 1, 2024

Introducing Utimaco Atalla Payment Solutions

Banking transactions in 34 countries around the world are secured with an Utimaco Atalla AT1000!



Atalla AT1000



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.

Key Use Cases

Credit, Debit/ATM cards:

Acquirer,
Issuer,
Merchants



Key Injection: ATM/POS/ Terminals



Tokenization, IoT, Card Personalization



E-Wallets, Online and Mobile Payments



Key Verticals: Financial Services, Retail, Payment Processors



Meeting Standards and Compliance

PCI PTS HSM

Ensures logical and physical security to protect cardholder data

FIPS 140-2 Level 3

Set of standards that define encryption algorithms and physical security

TR-31 Key Block

Key Blocks protects the secrecy and integrity of encrypted keys

Payment Processing Standards

MasterCard, Visa,
American Express, Union Pay,
Discover, Rupay, EuroPay

- 01 **ENHANCED SECURITY** | Built using the Atalla Key Block (AKB), the AT1000 offers **AES Master File Key support** and meets the **TR-31 requirements** for key lifecycle management.
- 02 **HIGH PERFORMING & CLOUD READY** | **Leverage up to 10,000 TPS throughout 10 partitions** – separate environments; utilize HSM in multiple ways.
- 03 **EASY MIGRATION** | **Backward compatible** and offered in both Variant and AKB modes allowing you to **easily replace** outdated key block & variant-based HSMs over to the AT1000.
- 04 **TRUE REMOTE MANAGEMENT** | Compliant, remote management lets you **control HSMs from multiple locations**, as well as monitor audit logging using remote syslog and SNMP alerts.
- 05 **COMPLIANCE DRIVEN** | **FIPS 140-2 Level 3** and **PCI PTS v3 certified** in both **controlled** and **uncontrolled environments**. One of the highest security and compliance levels in the industry.

Which regulations drive the HSM

Track record of leading, defining and shaping standardization and regulations and these are the ones that AT1000 adheres to today.

PCI PTS HSM 3.0

Atalla AT1000
is certified –
Certificate 4-80041



pci-pin compliant

Hardware Part #: HW-AT-HSM-V1,
Firmware #: 8.22, 8.30

https://www.pcisecuritystandards.org/pops/pts_device.php?appnum=4-70041

FIPS 140-2 Level 3

Atalla AT1000
is certified –
Certificate # 3059



<https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3059>

P2PE

Validation, can be
achieved using Atalla
HSMs



Point to Point Encryption

https://www.microfocus.com/media/analysispaper/hardware_security_module_lead_ership_atalla_hsm_analysis.pdf

SP800-90A Rev. 1

Modern Random
Number Generator



<https://csrc.nist.gov/publications/detail/sp/800-90a/rev-1/final>

PCI PTS

In order for cryptographic keys to provide reliable security, two areas must be addressed:

Protect the integrity of the key

including the order of the key parts for algorithms that require multiple key parts, for example TDEA.

Associate the type/purpose of key to ensure that the key isn't used for any other designated purpose, for example as a key-encrypting-key or as a PIN-encrypting key.

2014

A new precedent was set by PCI to improve security of keys with the implementation of key blocks. Also known as key bundling, this greatly improves the security of symmetric keys that are shared among payment participants to protect PINs and other sensitive data.

2017

This requirement was modified to ensure its achievability – Implementation is to be done in three phases. The first phase deadline was June 2019.

What do I need to do to prepare?

2019 Local Key Storage

All locally stored keys must be managed in Key block format.

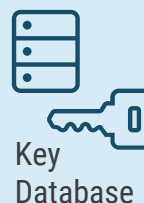
MFK



Stage 1 – Internal Key Storage / Usage

E.MFK (KEK)

E.MFK (KATM)



Key Database

Header

Encrypted Key

MAC



2021 Stage 2 – Network Key Exchange

Keys we share for translation (send and receive or verify / decrypt) need to be in Key block TR-31 format.

E.KEK (WK) TR-31



Header

Encrypted Key

MAC



2023 Stage 3 – POS/ATM Key Management

All keys must be in Key block format.

E.ATM (PIN)

E.KEK (KATM) TR-34

KEY ATM
ENCIPHERING
PIN PAD (KEK)



Header

Encrypted Key

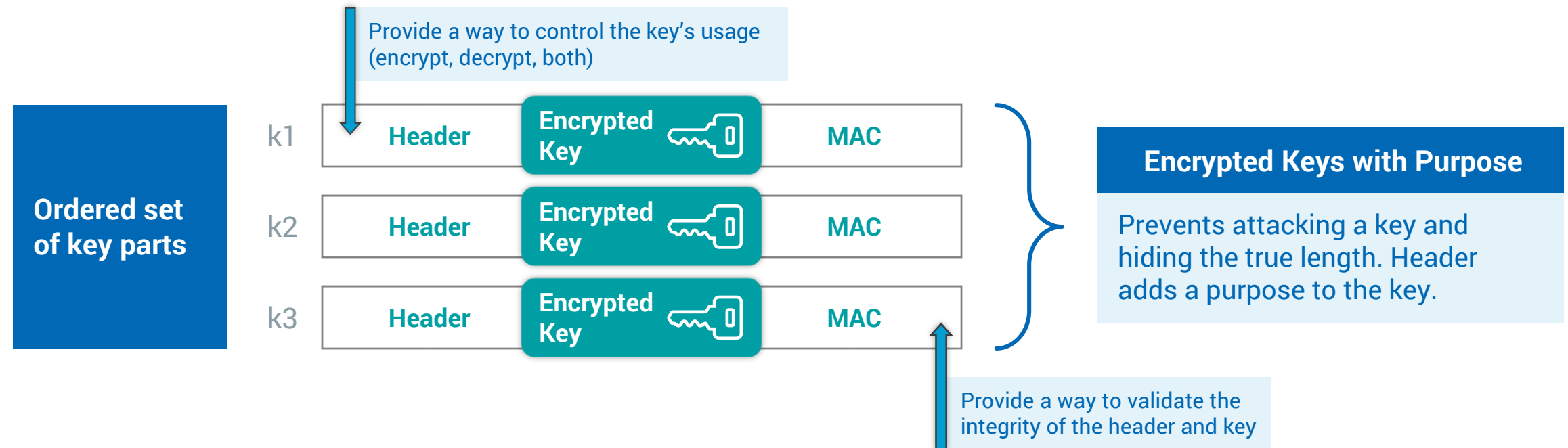
MAC



Note, while Ax160 does support key blocks, it is not PCI PTS v3 certified and therefore out of compliance.

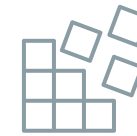
Key Bundling

- A **Key block** is a means of using one or more blocks to bind key parts to additional information about the resulting key.
- **Key bundling** is the use of key blocks. An encrypted key not be protected from modification or tied to a purpose. When it's bundled or wrapped into a key block, cryptographic operations are performed to provide both confidentiality and integrity protection and key cannot be manipulated.



Highest performing HSM
on the market at 10,000 TPS

10,000



More **flexibility**,
greater partitioning power!

Experience
upgrades in real time

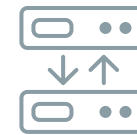
1,080



Now **10x faster**
than before!

If you need more throughput,
simply upgrade TPS on the fly

280



Only use **what** you need,
when you need it!

Buy AT1000, complete
with out-of-the-box commands

80



NO more having to decide
between hardware models!



Ax160 Comparison

A8160

A9160

**Extended
performance**
in increments of
500 TPS, up to
10,000 TPS!

AT1000



Performance Licensing

80 TPS

280 TPS

1,080 TPS

1,500 – 9,500 TPS
10,000 TPS

Host Connection Licensing

1 Host
(Default license)

8 Hosts
(License)

64 Hosts
(License)

128 Hosts
(License)

Domain Licensing

2 Domains
(Default license)

5 Domains
(license)

10 Domains
(license)

NEW! Secure Configuration Assistant – Windows

Configure commands, define parameters, calculate cryptograms, and inject cryptographic keys.

User-friendly Design



Say goodbye to traditional tablets.

Now delivered on a USB form factor, the SCA-W, implements the well-regarded SCA-3 onto a user-friendly application form that **runs on your own company managed Microsoft Windows computer.**

True Remote Management



Not offered by any other HSM on the market - Loading MFKs and lower-level keys does not need to be done at the same time at the same location. Key custodians can be geographically dispersed.

Even More Secure



Delivered on FIPS 140-2 level 3 certified platform and conforms to best security practices, keeping it secure against corruption and potential malware injections. Supports identity-based authentication, encrypted communication and protected cryptographic key component storage.

Capacity & Incident Monitoring



Robust audit log, reporting and alerts while syncing its time with a trusted NTP server.



Moving to Multi Domains: We're Ready When You Are!

Partitioning Capabilities of the AT1000

1 Partition = 1 Master File Key (MFK)

Separate environments, different TCP ports

PIN translations
Key generation
Key injection

ACI
FIS
Diebold

Security Admin 1
Security Admin 2

MFK

MFK

MFK

Enable multi domains that run independent of each other and support multiple use cases at the same time.

Consolidate multiple payment applications onto one HSM.

Isolate access, security policies and separate administrative access per partition.

1. Begin to **adopt partitioning capabilities**.
2. Leverage within the **cloud**.
3. Emerge as a cryptography service provider to your internal customers providing an **HSMaaS** model.



Legacy Ax160 vs. Next Generation AT1000

Legacy

Ax160



AT1000



Next Gen

Legacy Ax160 vs. Next Generation AT1000

Legacy

Ax160



(SCA-3) Local administration
(PCI HSM Mode); cable clutter

No SNMP support

Performance upgrade
requires hardware exchange

1,080 TPS

Separate license required for base
or enhanced firmware; **additional licenses**
required for custom commands

Software upgrade 45-60 minutes
USB required for SW updates,
config files and log files


ADMINISTRATION


MONITORING


**PERFORMANCE
UPGRADES**


PERFORMANCE


LICENSING


**SOFTWARE
UPGRADES**

AT1000



(SCA-W) Full remote administration
after initial network settings; no cables

SNMP support & syslog

Field performance upgrade
via license without hardware exchange

10,000 TPS

All commands included out-of-the-box
(both base and enhanced)

Software upgrade 5 minutes
2 HDDs for storage;
USB optional for config files

Next Gen

Let Us Help You Make the Transition

We continue to migrate customers over to the Utimaco Atalla AT1000!

Step 3

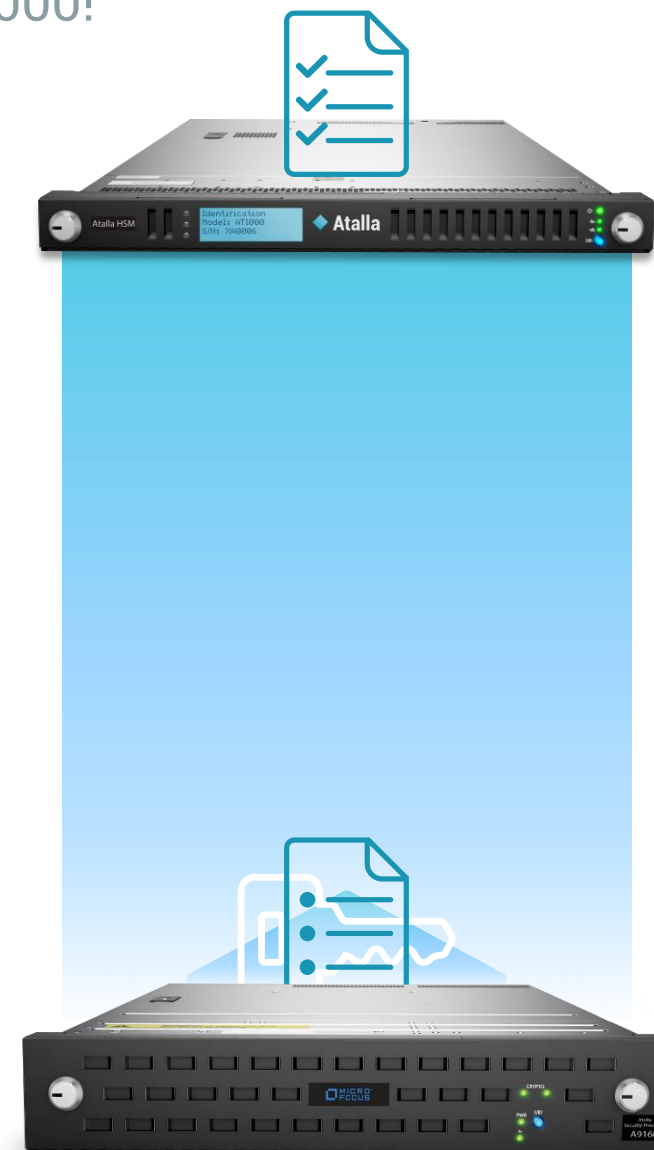
Finally, we generate a report outlining the **cryptographic functionality enabled on existing Ax160 HSMs** and map it to your new AT1000 HSMs.

Step 2

Next, **we help you transfer MFK components**. Some customers have the information readily accessible and can transfer **manually**. In other circumstances, we can perform a **card-to-card migration** or **create a new MFK**.

Step 1

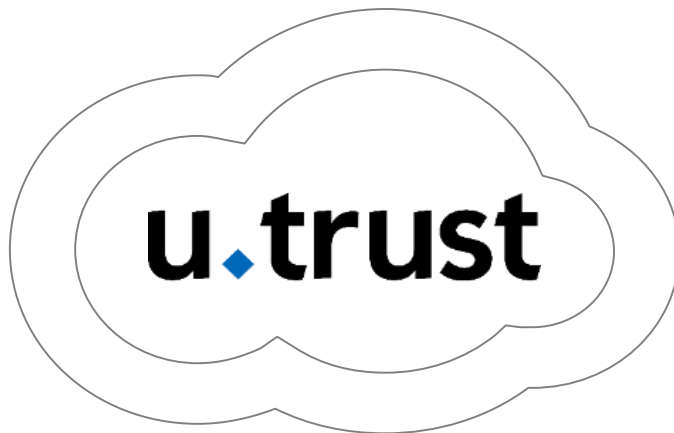
Decide if AT1000 will fully replace legacy HSMs or operate in a mixed environment. **The sooner you start the upgrade, the more flexibility you have for the implementation** – adding a phased approach or testing environments.



Utimaco's vision to enable customer transition to the hybrid cloud

Move

- Move Keys To/From On-Prem to the Cloud.
Transport Keys Across Public Clouds and hybrid environments.
- Manage Keys: Create, Store, Rotate & Protect

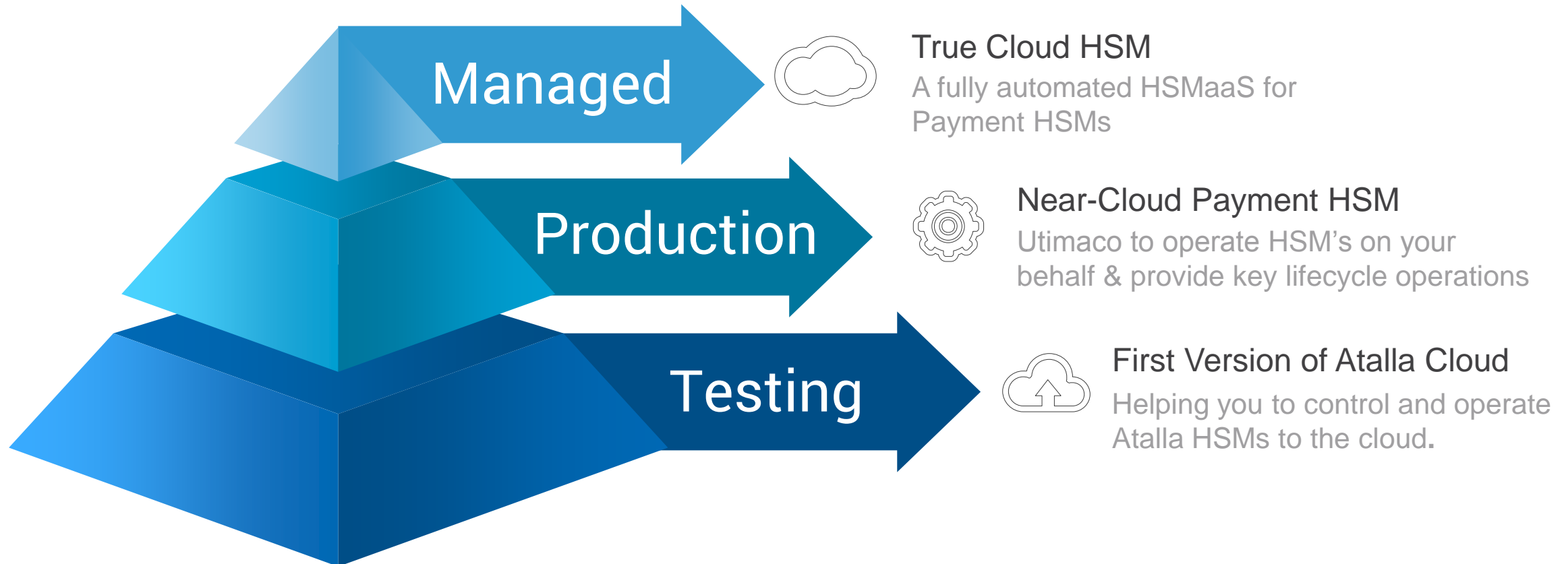


Run

- Secure Key Escrow & Exchange Services
- Operate HSM's on behalf of the Customer

Build

- Enable Private & Public Cloud Service Providers to Build their own IaaS & PaaS Cryptographic Services.



Industry Leading Payment Hardware Security Module

Value Proposition

- Industry's leading payment API and command set
- True remote management capabilities
- Integration with all major payment and switching applications
- Close integration with HPE NonStop Systems to provide a fully redundant payment solution
- Performance driven – up to 10,000 TPS
- Customization to adapt your requirements
- Legacy TDES and future-proof AES support



Get Started with AT1000 today

- **HW demo:** Easy to evaluate, on-prem and cloud
- **Easy deployment:** Install and configure quickly and remotely
- **Simple licensing:** Field upgradeable performance and comprehensive command set
- **Reliable:** Decades of innovation in payment security
- **Grows with your business:** TR-31, AES keys

How do we lead?

Innovation 50+ Patents

Creative engineers delivering security inventions and driving security thinking

Rock-solid security FIPS 140-2 validated Level 2, 3, and 4

Our Key Management Solutions are built for the highest standards

Trusted name since 1972 \$ Trillions

Utimaco Atalla secures 1 in 3 card transactions; also processes billions of card transactions annually

Q&A

Presenter: Ricardo Trujillo

Email: Ricardo.Trujillo@utimaco.com

Latam Team

Manuel Alonso Manuel.Alonso@Utimaco.com

Mónica Flórez Monica.Florez@Utimaco.com

Ismael Valencia Ismael.Valencia@Utimaco.com

...and we invented security that you can take for granted!!!