

Creating Trust in
the Digital Society

The Path for Cloudifying Payment HSMs

Cloud Webinar Series

August 2020

utimaco[®]

- About Utimaco
- *Trends in the Banking & Financial Industry driving cloud adoption*
- Evolution of HSM's over time
- Considerations when moving HSMs to the cloud
- Utimaco's offerings for PaymentHSMs in the cloud
- Bringing on-prem Legacy HSMs into the cloud: Different Service Models



Vaughn Eisler
Director of Business Development - Equinix

A recognized sales and business development executive, Vaughn is a Director of Business Development at Equinix, establishing and leading an ecosystem of security partners delivering enterprise security solutions to customers.

Prior to joining Equinix, Vaughn led numerous innovation efforts at Symantec during his 6+ years there. Primarily, he was responsible for establishing and driving global partnerships in the fast growing Internet of Things (IoT) space.

Also during his time at Symantec Vaughn helped drive enterprise mobility solutions into new routes to market. Before joining Symantec, Vaughn worked in the Business Solutions Organization at Nokia Siemens Networks selling network infrastructure and consulting and systems integration sales.

Overall, Vaughn has over 15 years of experience in business development, technical sales and product management roles within the CSP vendor community.



Haris Sethi **Global Strategy Manager, Payments**

Haris Sethi, Global Strategy Manager in Utimaco today has 10 years of experience in the Payments/Cybersecurity domain. He started his journey as a Payments experts working for large financial institutions such as Barclaycard and MasterCard giving him a holistic view of the Payment Ecosystem.

He has vast experience in the underlying security mechanisms that are mandated by PCI DSS and currently is a Certified Cloud Security Professional (CCSP).



Eyal Worthalter **VP Platform Solutions & Growth**

Eyal spends his time in Utimaco leading digital transformation in order to turn products into solutions and services that can be delivered digitally and as-a-service. He's also responsible for driving technology alliances and integrations with Cloud Service Providers and MSP's.

Prior to joining Utimaco, Eyal had a successful track record as an Enterprise Sales Executive and Sales Director, his last role was as Head of Sales Enablement at a VC-backed Israeli tech startup focused on data management and protection. Eyal holds an MBA from Hult IBS.



HQ Location
Aachen, Germany

UTIMACO is a global **platform solution leader** of trusted Cybersecurity and Compliance solutions.

We are driven to take a leading market position by providing uncompromised Cyber Security solutions fulfilling the highest standards.


With responsibility for global customers and citizens we create innovative solutions to protect data, identities and communication networks.



HQ Location
Campbell, USA

 **70 Mio US\$**
Revenue FY 19/20

 **330** highly skilled experts

 Founded **1964**
Private company

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

UTIMACO is an international provider of
cyber security & compliance solutions
with headquarters in



Milestones



Founded
as data center
for enterprises



Re-focused
on providing
IT security
and **encryption**
solutions



1st Generation
KryptoServer
(HSMs)



UTIMACO
HSMs are
chosen for
the **German**
road-toll
system



UTIMACO
starts
partnership
with **leading**
Asian network-
equipment
vendor



US-based **world**
leader in electric
vehicle
manufacturing
selects UTIMACO
HSMs to secure
connected cards



UTIMACO
exceeds 150
employees
and wins
TOP JOB
award



New product
innovations
for **Cloud** and
post-quantum
safe
encryption



GEOBRIDGE
by **utimaco**

UTIMACO
acquires
GEOBRIDGE

1964



1983



1991



2002



2006



2012



2015/16



2018



2020



2018

UTIMACO
acquires
Atalla
Business



2000

HP
acquires
Atalla



2002

Atalla
invents
Keyblock



2010

Atalla
Ax160
HSM



2017

Atalla
AT1000
HSM



Information Security

Encryption-based,
high-security solutions



Hardware
Security Modules



Key
Management



Enterprise
Data Protection

Cyber Security & Compliance Solutions

Payment Security

Compliance solutions
for the Payment Industry



Payment Hardware
Security Modules



Key Management
POI/POS Devices



PCI Compliant
Tokenization

Protect the Payment Ecosystem

Utimaco offers a variety of Hardware Security Modules to protect your most valuable data within the payment ecosystem.

Secure and Manage Keys Used Across Multi Channel Payment Platforms

From key injection to key escrow services, Utimaco helps organizations simplify and automate the process for cryptographic key management.

Transition to the Cloud

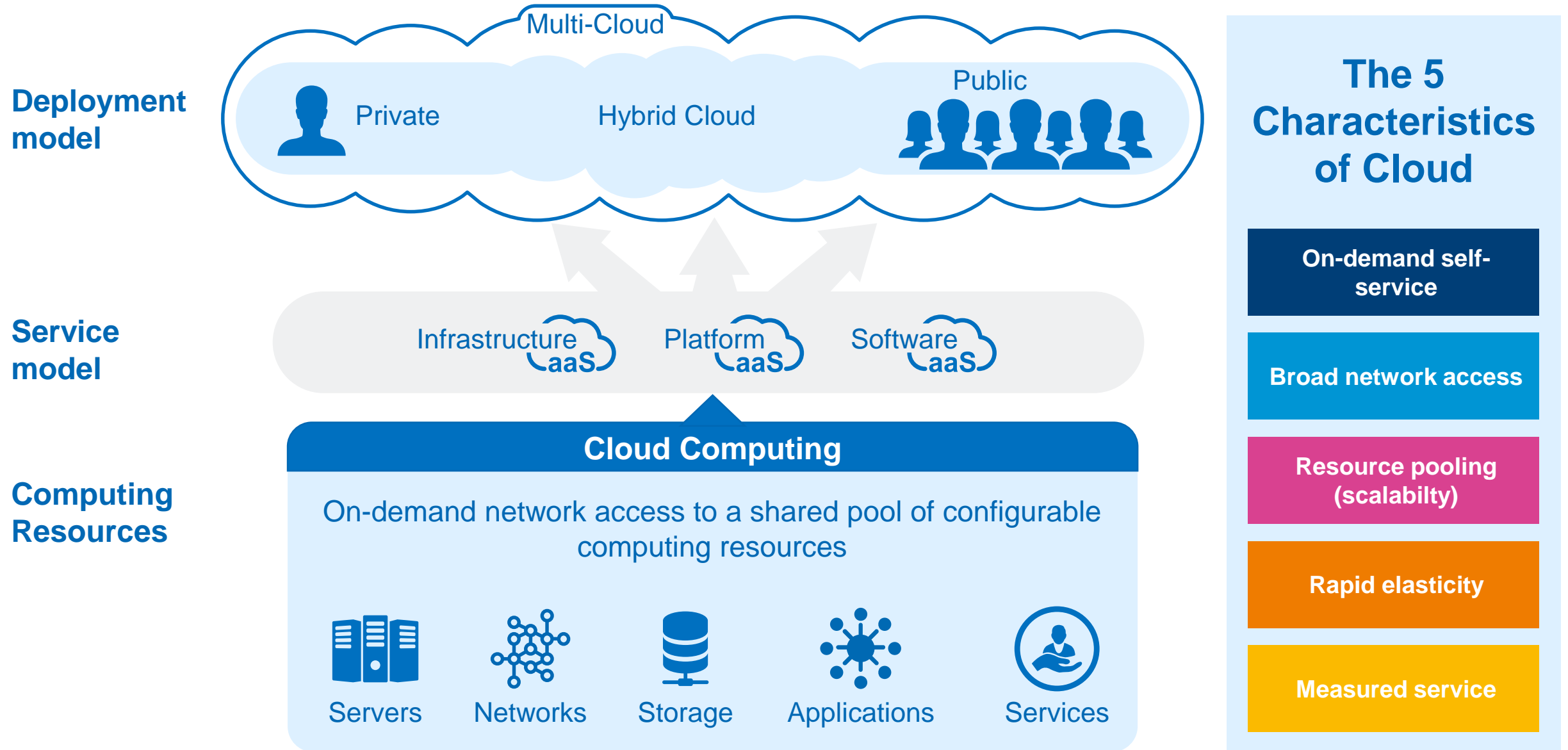
We provide a phased and flexible approach for moving keys across on-prem and cloud environments, as well as enabling private or public cloud services securely.

Solutions

- PIN Verification & Transaction Processing
- ATM Network / Interchange
- Mobile & Card Provisioning / Issuing
- Security & EMV Payment Tokenization
- Enterprise Key Management
- Remote Key Loading/Injection
- Key Escrow Services
- Cloud Data Protection

- Enterprise Banking, Fintech & Retail
- Device and Equipment Vendors (ATM, POS/POI)
- Key Injection Facilities

Markets



Market evolution is moving toward more frictionless transactions and expanding services

Industry Trends

INSTANT

Real-time Payments
Cross-border payments
Real-time Analytics &
Fraud detection

OPEN

Open Banking
Partner Ecosystems

EVERYWHERE

Global Delivery
SaaSification
Consistent UX
Data Sovereignty

Tech Enablers

Open APIs
Tokenisation

Key Management
DLT / Blockchain

Cloud Technologies
AI / ML capabilities

Digital Infrastructure

Networks

Clouds

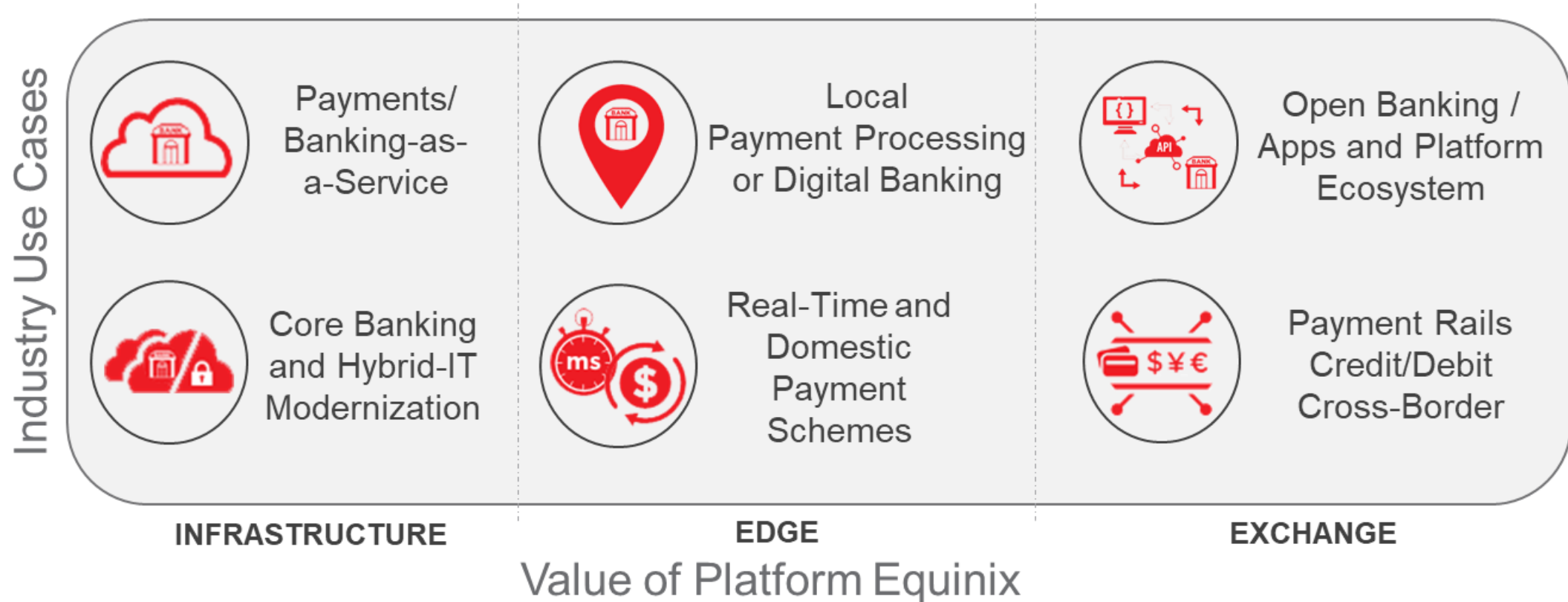
Data

Security



PLATFORM
EQUINIX™

Many of these use cases require the use of a Payments HSM

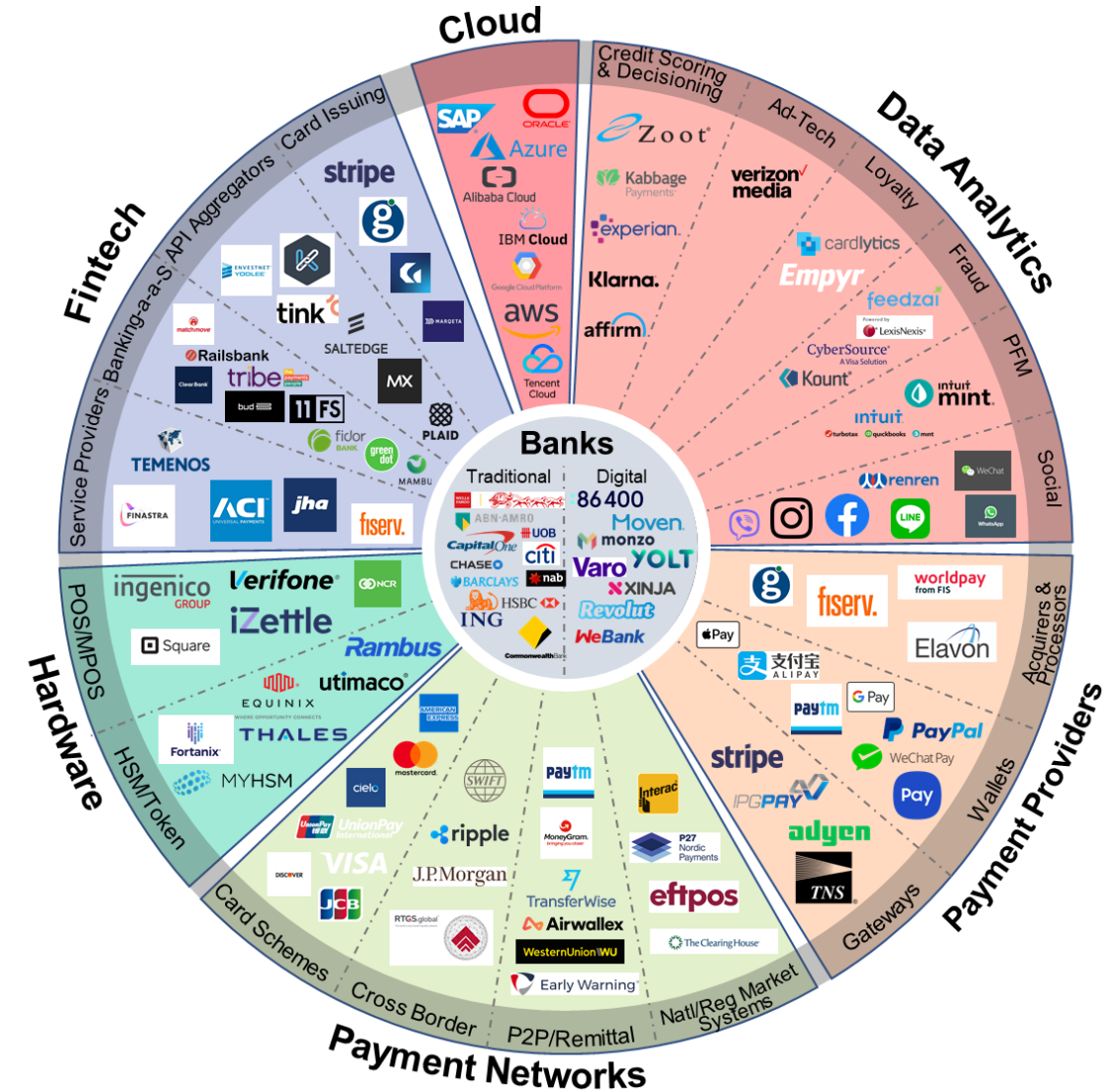


Infrastructure increasingly dependent upon cloud service providers. Deployments are typically in Equinix metros with robust choices of low latency connections to cloud providers on ECXF

Infrastructure that needs to be in a particular country or region due to local partnerships, data sovereignty or latency requirements.

Infrastructure that benefits by being adjacent to a large number of ecosystem participants that share standardized messaging formats and protocols.

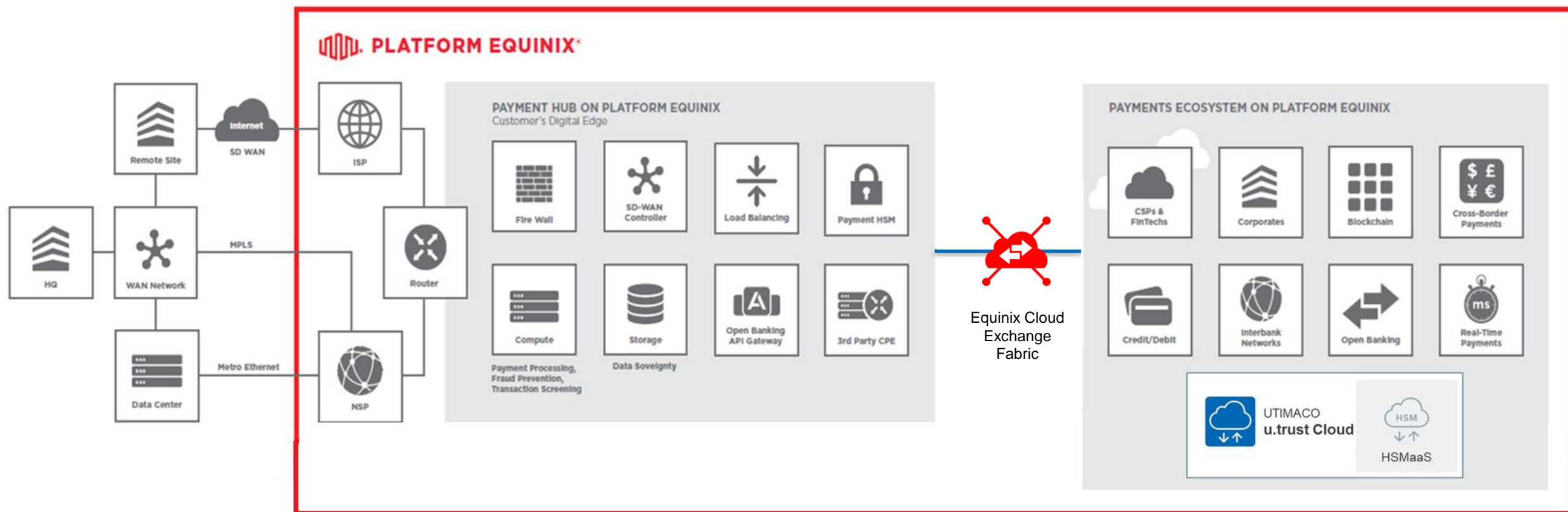
- 1250+ Financial Services customers
- 250+ payment specific customers
 - 6 card schemes / 4 of the top 6 card networks
 - 5 domestic payment schemes
 - 1 central bank
- 350+ banks
 - 6 of the top-10 global banks
 - 9 of the top-15 payment card issuers
- 25 of the top 25 mobile network operators
- Most of whom are interconnecting to each other, clouds, and services such as Payments HSMs



Logos on this slides are illustrative of the ecosystem

Payment Hubs Deployed At Equinix

As payments and banking services move to the cloud the non-cloud infrastructure is moving to the digital edge



Ecosystem Participants

Ability to efficiently interconnect to payment rails and other payment participants in the cloud or in Equinix

Edge Services

Consume edge services such as NFV or Payment HSM-aaS with low latency adjacency to the cloud

Distributed Architectures

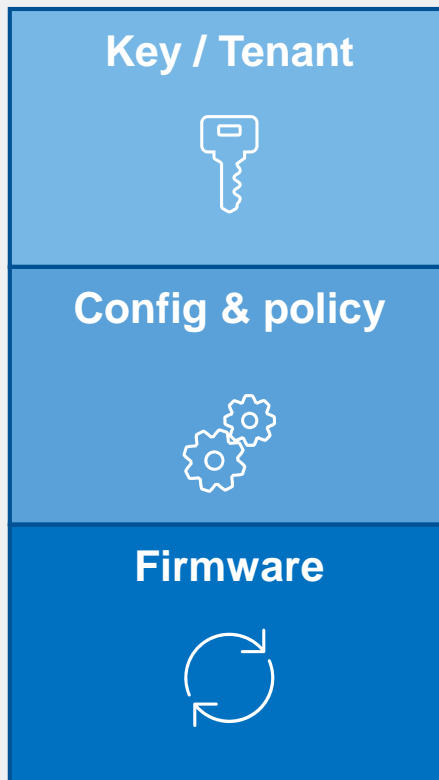
Repeatable architecture that can be deployed in new markets for new business opportunities, data sovereignty or lower latency

Evolution of HSM's in the Cloud

How technology & service offerings have evolved over time to match customer needs

2013: CloudHSM Classic, CSC

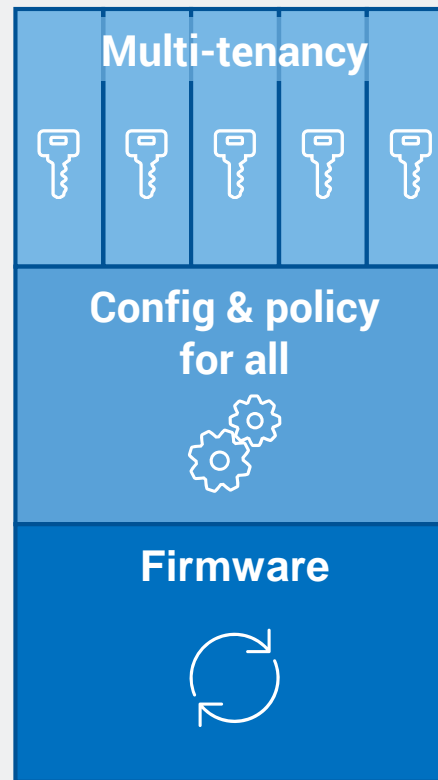
 **Gen 0**
Dedicated HSM



Benefit: On-demand & measured service

2017-18: SmartKey, GCP & AWS

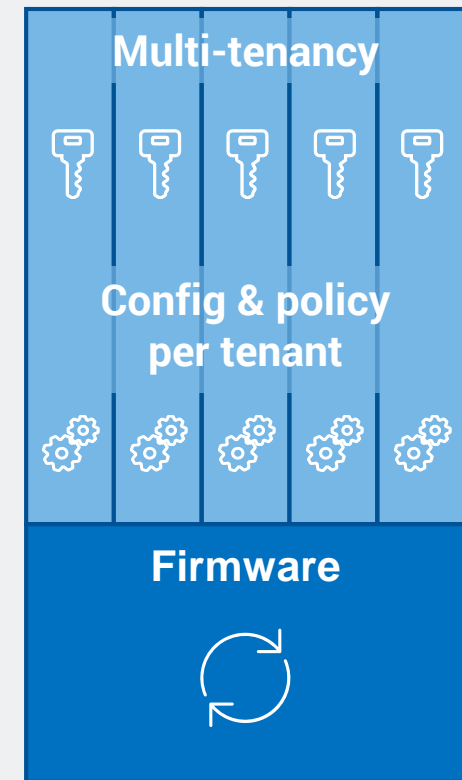
 **Gen 1**
Partitioned HSM



Benefit: Resource Pooling (Scalability) & Elasticity.

2019-20: u.Trust Cloud

 **Gen 2**
Partitioned + Payment



Benefit: Enables paymentHSMs to be deployed in cloud

 **CryptoServer Cloud**
HSM as a Service



aws




EQUINIX

aws

The main reason why cloudifying HSMs is not a straightforward path

Security

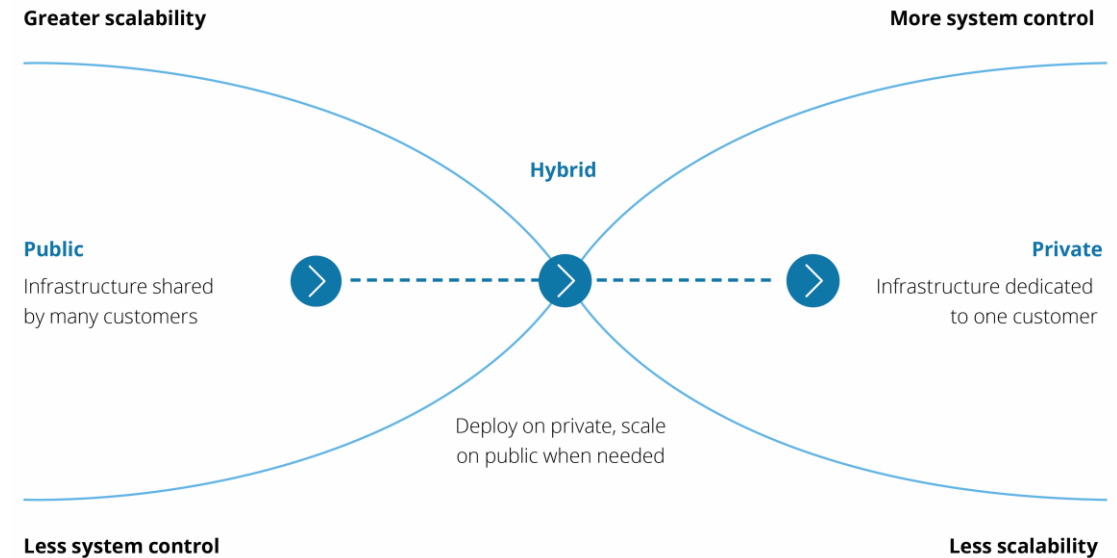
- ♦ *"Security is different in the cloud"*
- ♦ Cloud providers typically take responsibility for the security of the lower-level infrastructure layers.
- ♦ **Who has access to cryptographic keys?**

Benefits of Cloud

- ♦ Cloud enables organizations to rapidly scale, which is important for the agile delivery of new products/services.
- ♦ **The tradeoff of scalability is to have more control.**

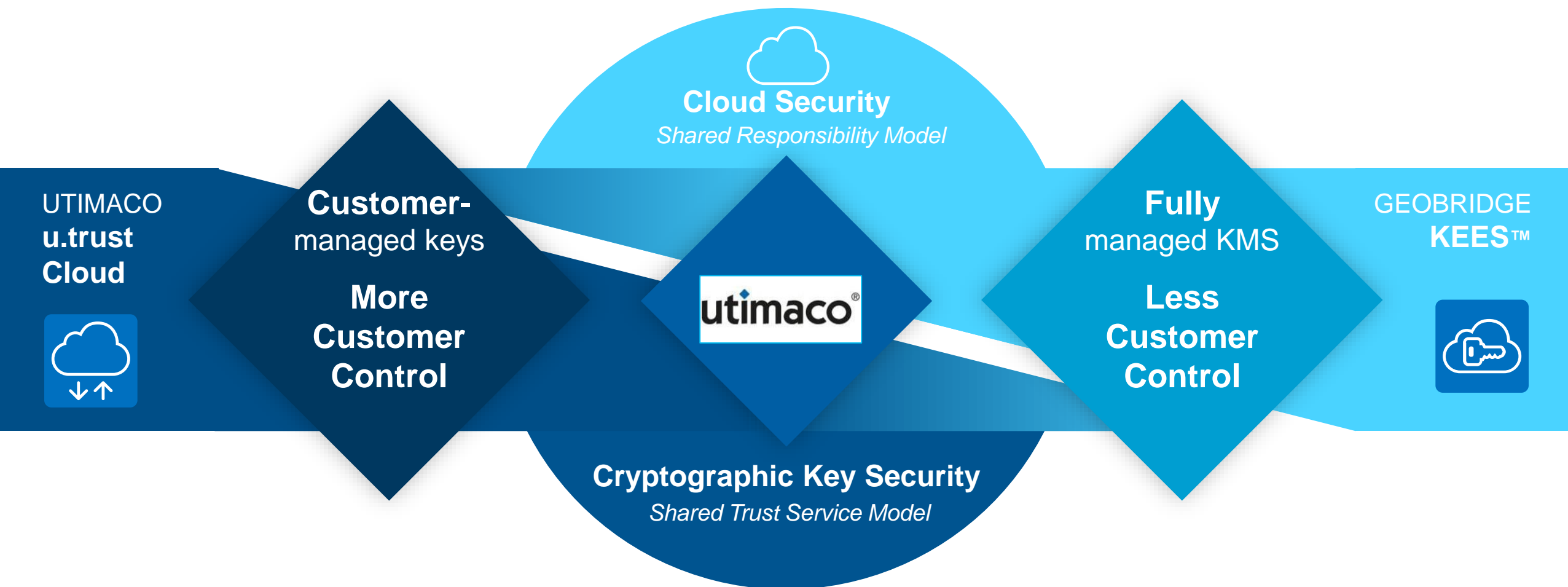
Trade-off of Control & Scalability

- ♦ Defining how cryptography is elevated to the cloud means changing the way your organization considers 'control'



<https://www2.deloitte.com/global/en/pages/financial-services/articles/bank-2030-financial-services-cloud.html>

Overcoming Compliance challenges requires a different approach



Decision based on customer situation in terms of
Regulatory Requirements / Compliance • Data Sensitivity • Risk Propensity • TCO • ...



UTIMACO Atalla AT1000

PCI HSM for Acquiring &
Processing Card Transactions



ATM/POS
Networks
PIN Translation
PIN Verification
Remote Key
Loading



E-Wallets, Online
and Mobile Payments



Transaction Processing
Credit, Debit/ATM cards,
Acquirer, Issuer,
Merchants

Secure your payment data using
a root of trust and centrally manage
your keys, on premise or in the cloud.



UTIMACO u.trust Cloud



HSMaaS



GEOBRIDGE by utimaco®

KeyBRIDGE

Turnkey solution for payment
related crypto operations



Key Lifecycle
Management



Key Injection:
POS / POI



HSM Migration
& Management



Secure
Tokenization



GEOBRIDGE KEES™



Key Escrow
Exchange
Service



u.trust Cloud - Atalla PaymentHSM



Agile Delivery

Leverage advantages of cloud services such as on-demand scaling to focus on getting your products to the market faster.



Lowered TCO

Reduce cost of legacy Payment HSM, staffing overhead and surrounding IT infrastructure with monthly OPEX.



Reduced PCI Compliance Scope

Maintain HSM infrastructure under PCI PIN 3.0 without challenging audits.



What is u.trust Cloud - Atalla PaymentHSM?

u.trust Cloud – Atalla PaymentHSM is a managed service from Utimaco for paymentHSM's based on Atalla AT1000 HSM. It enables customers to move payment keys and HSM workloads from on premise to the public/private/hybrid cloud, gaining the advantages of cloud-delivered IaaS. Since customers have varied needs over cryptographic key ownership and in order to provide flexibility we have come up with the following HSM consumption models:

Consumption Model

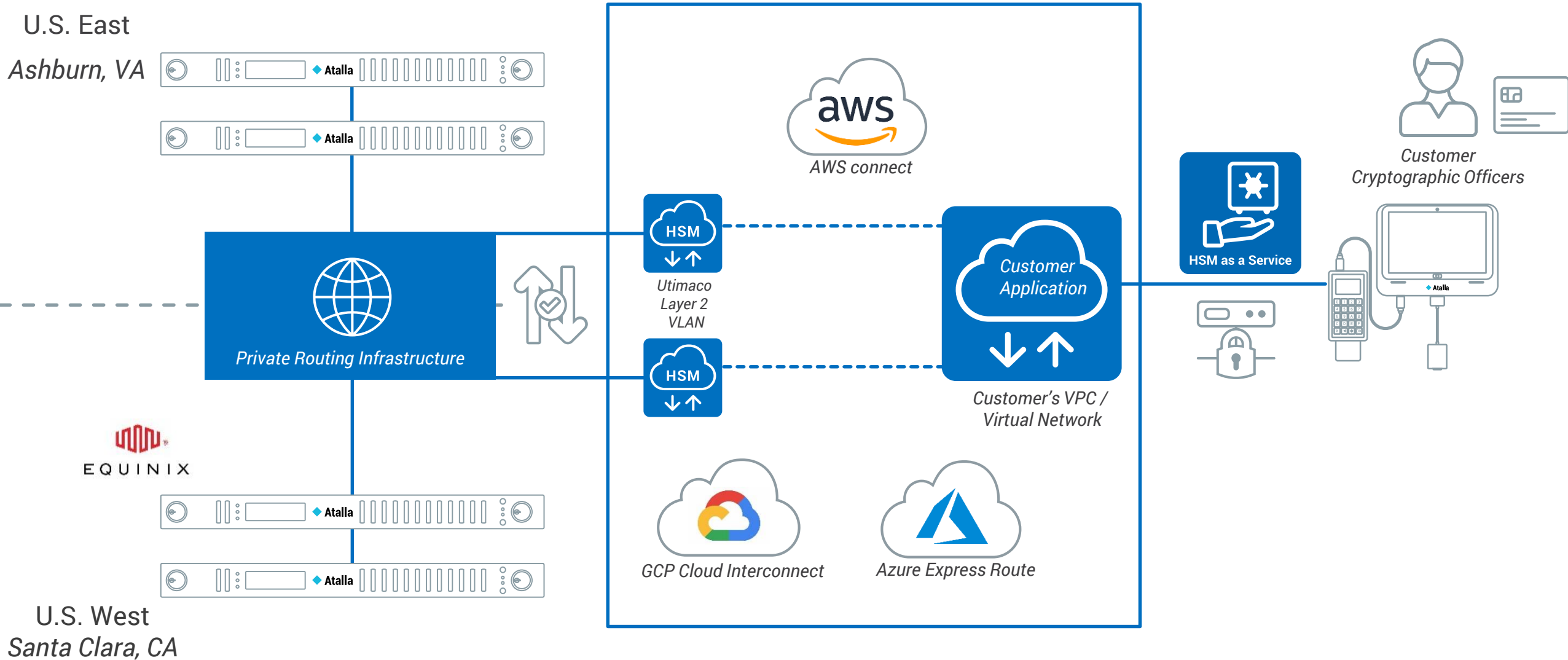
Dedicated or
Containerized (Shared)

Hosted Service Model

Hosted Service Model: Customer
can control and operate HSM
100% on their own.

Managed HSM

Initialization & On-Boarding
Backups & FW Updates
Select Key Lifecycle Mgt. Operations



Step 4 Migrate Keys

Once all schemes are interoperable, Utimaco will setup Key Encryption Key (KEK) between the legacy HSM's and u.trust Cloud HSMs. Then, it will automatically migrate all working keys using the KEK.

Step 3 Analyze Key Types (conversion of key inventory)

Most of the time, we are dealing with four schemes for LMK encryption of keys (X,R,U,S). X,R are interoperable and already in the format that Atalla can convert. We will export U,S into an interoperable format.

Step 2 Mapping Commands (application programming)

Typically, there are 10-15% of payment commands used from a Payment HSM. We assist by creating a document that maps each command from legacy HSM's to Atalla AT1000.

Step 1 Identify Current HSM Environment & Key inventory

Utimaco will help identify the customers current HSM deployment as well as understand where keys are stored and what are they used for. This can be done with existing Utimaco HSM's, as well as legacy HSM's from other vendors.



KeyBRIDGE UKM 4100

- PCI-PIN Certified Policy based **Key Life Cycle Management including Distribution Control**
- **Unify** your existing HSM key management landscape
- **Remote** HSM Operation & Management

Unify the lifecycle management of keys in your organization



Customer Profile

Regional Bank in Canada

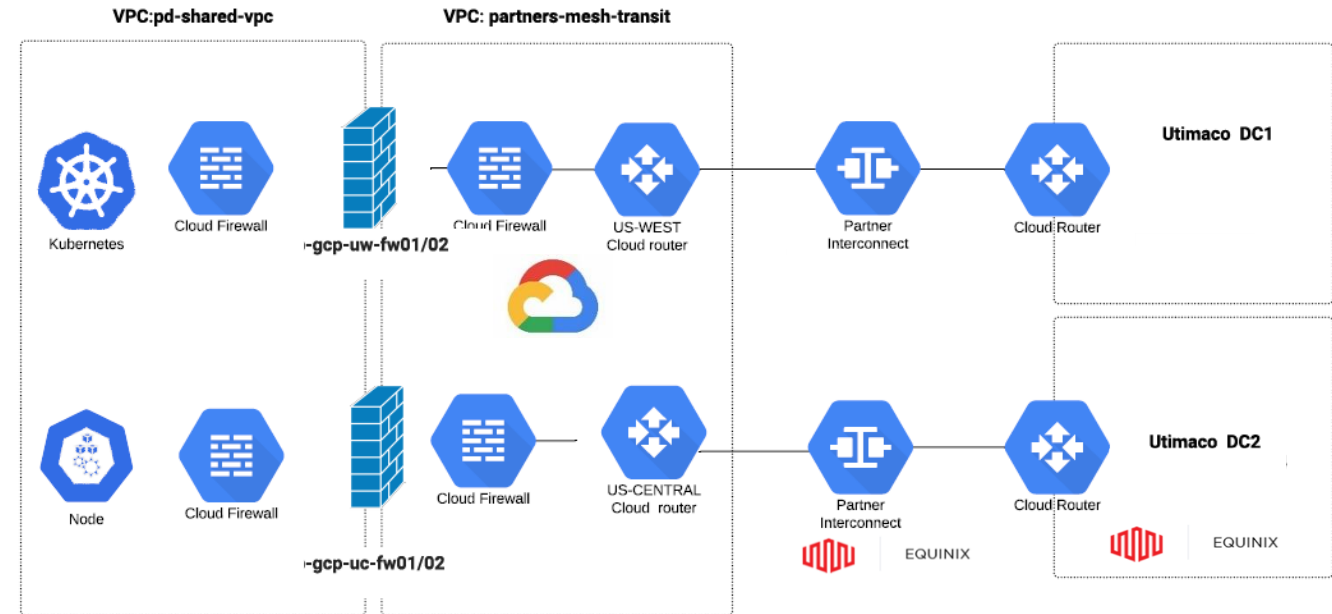
~6000 employees & <1M users

Business Challenge(s)

- Moved most applications to the cloud but still require PCI compliant PaymentHSM
 - Team is mostly remote (all over Canada)
 - Google Cloud as primary cloud

HSM Cloud Migration Journey

1. Established Test / POC in one datacenter
2. Setup a redundant connection in 2ndary DC via direct cloud connection
3. Performed fail-over tests
4. Exploring expansion and ECX connection



Solution

- U.trust Cloud setup with direct cloud connection to Google Cloud
- Customer has dedicated HSM for test and for live environments

Customer profile

Major Retailer

Merchant Acquirer

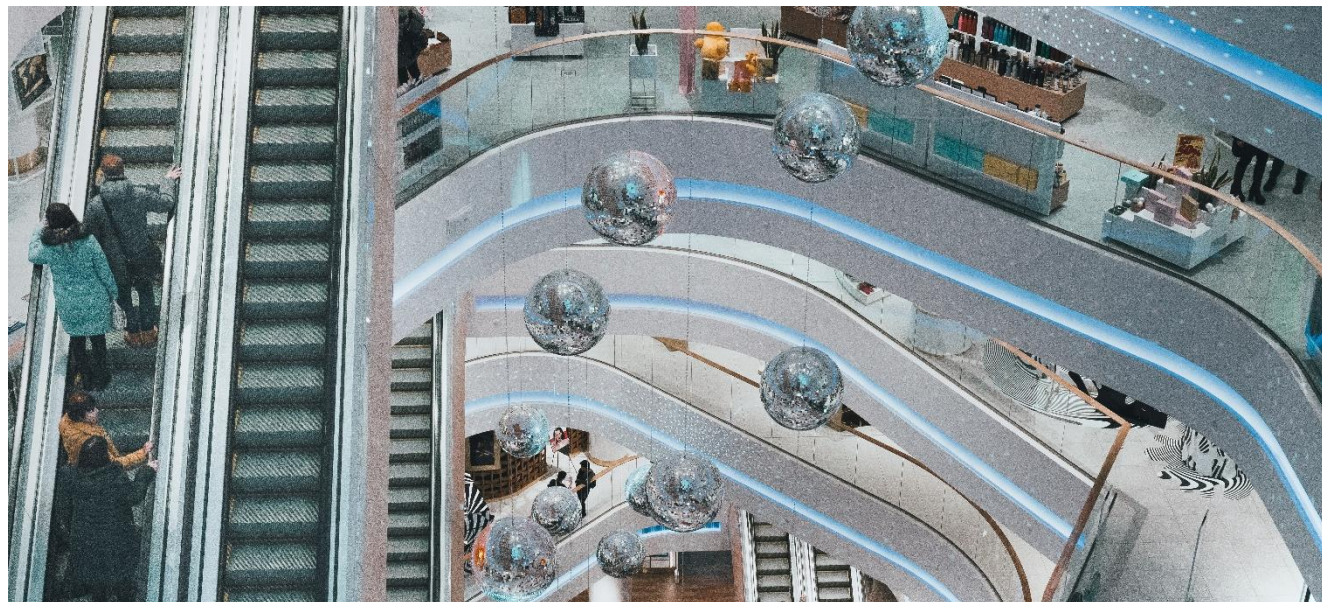


Business Challenge

- Managing 70,000 POI Terminals
- Deployment Center (Primary – Mid West)
- Key Custodian backup team in Corporate HQ created compliance challenges.
- Looking for specific key management operation to be managed by Utimaco.

Reduce Audit Footprint

- All of HQ was in scope for PCI
- Operations did not need to leverage HQ



Solution

- KEES™ for storing backup data in a PCI-PIN certified site.
- Eliminate HQ as PCI Scope

u.Trust Cloud Test: Payment HSM Service



HSM as a Service

Separate your live/production environment from your testing infrastructure. Rapidly reduce your TCO by avoiding purchasing equipment for non-production keys.

Design cloudHSM operations with **Utimaco & Equinix**



Private Routing
Infrastructure

Utimaco will help your organization plan a staged approach to the cloud in collaboration with Equinix.

GO LIVE!



Go Live!

Leverage u.trust Cloud & KEES™ PCI-PIN certified offering to operate as primary on behalf of you or augment your organization with qualified backup personnel.

Upcoming topics to continue educating users on their journey to the cloud

- **The Path for Cloudifying PaymentHSMs** – *Featuring End Users & Payment Application Vendors* – Coming in the fall
- **Key Migration & Key Lifecycle Management** – September 10th
- **Introducing KEES™** –
<https://hsm.utimaco.com/downloads/webinars/>

Thank you for your attention!

Utimaco Inc.

900 E Hamilton Ave., Suite 400
Campbell, CA 95008
USA

Phone +1 (844) UTI-MACO

<https://hsm.utimaco.com>

hsm@utimaco.com

To offer a „crypto as a service“ business to drive growth and differentiate themselves



Cloud

Build, migrate and manage the use of cloud service through Hardware based **Crypto as a service**



Key Escrow



Payment



Cloud based Key management

Managing data security across multiple public clouds is complex. Fulfilling customer expectations concerning cloud elasticity and flexibility is demanding and sometimes reaches the limits of technical feasibility.

We help those managing complex projects fulfil customer expectation by pushing the boundaries of what has been technically possible with regard to **cryptographic materials as a service**.

Discover how the new platform architecture from UTIMACO for “**encryption as a service**” allows you to **drive your business** by adopting this offering to your customers.

Manage

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

Migrate

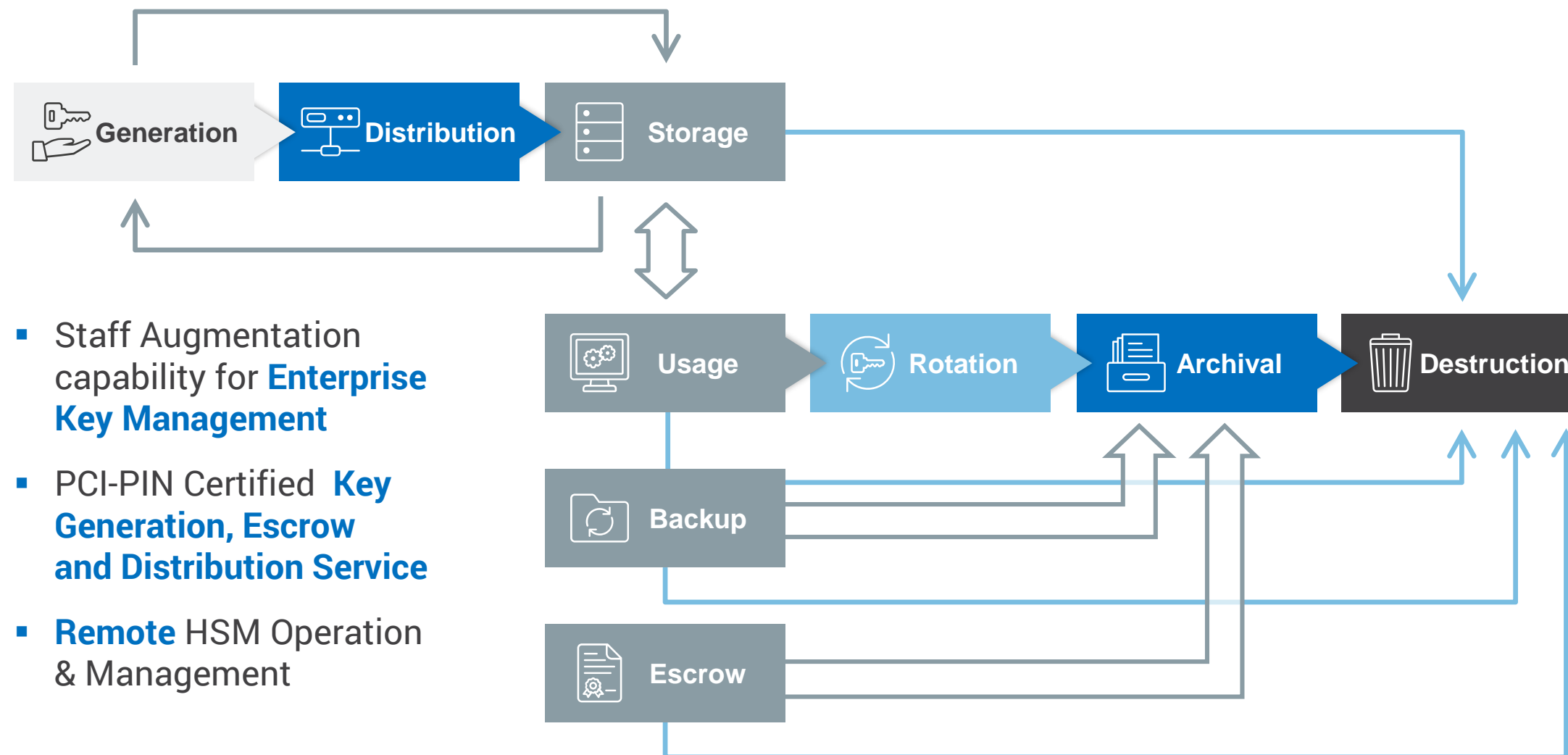
- ◆ KEES Key Escrow & Exchange Services
- ◆ Operate HSM's on behalf of the Customer

Build

- ◆ Enable operators of Private & Public Cloud Services, MSPs, CASBs to build and use Hardware based Crypto as a Services.

Introducing KEES™ Key Exchange & Escrow Service

KEES™ redefines the lifecycle management of keys in your organization



- Staff Augmentation capability for **Enterprise Key Management**
- PCI-PIN Certified **Key Generation, Escrow and Distribution Service**
- **Remote** HSM Operation & Management