Payment HSM as-a-Service

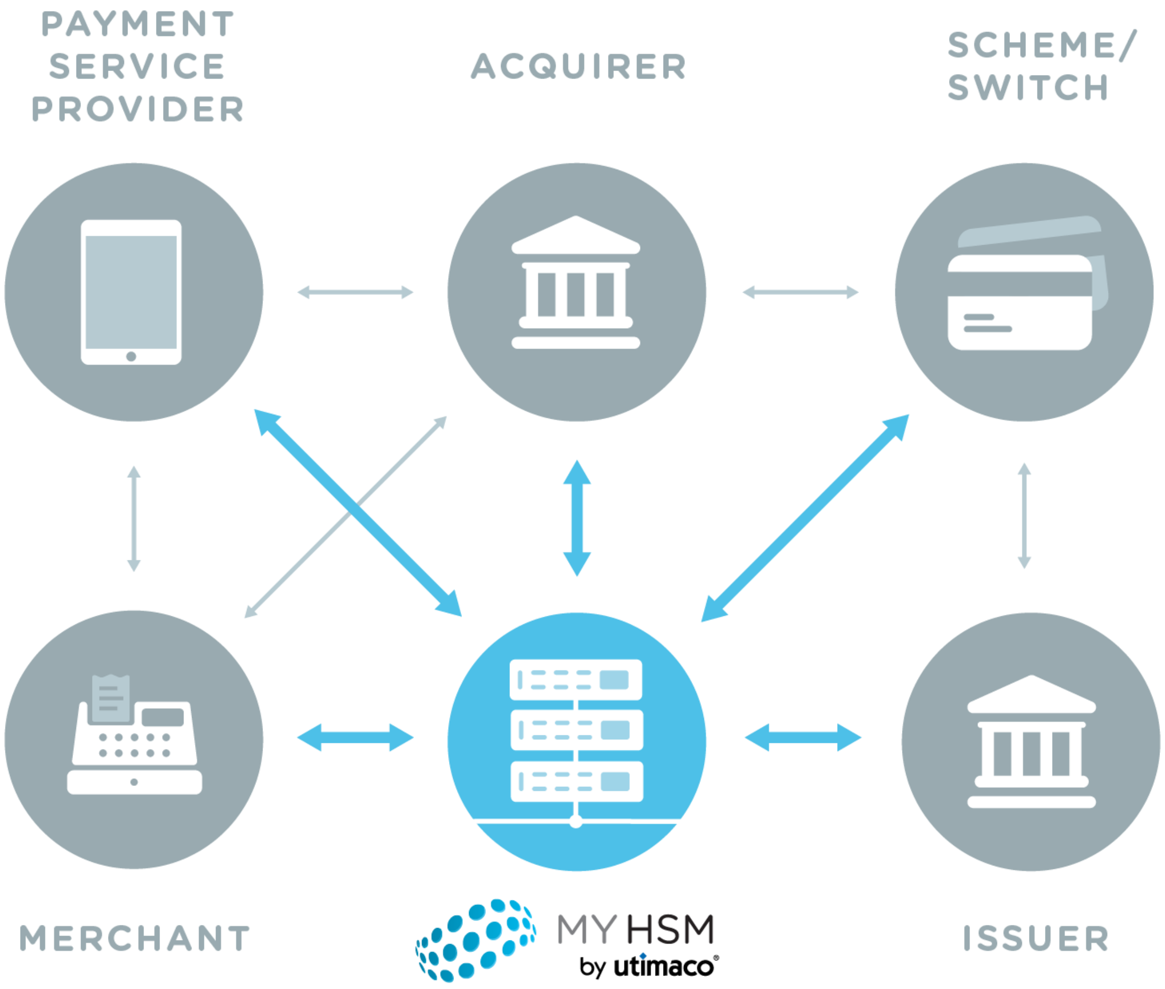
MY HSM
by utimaco®

Why MYHSM?

Creating Trust in
the **Digital Society**

utimaco®

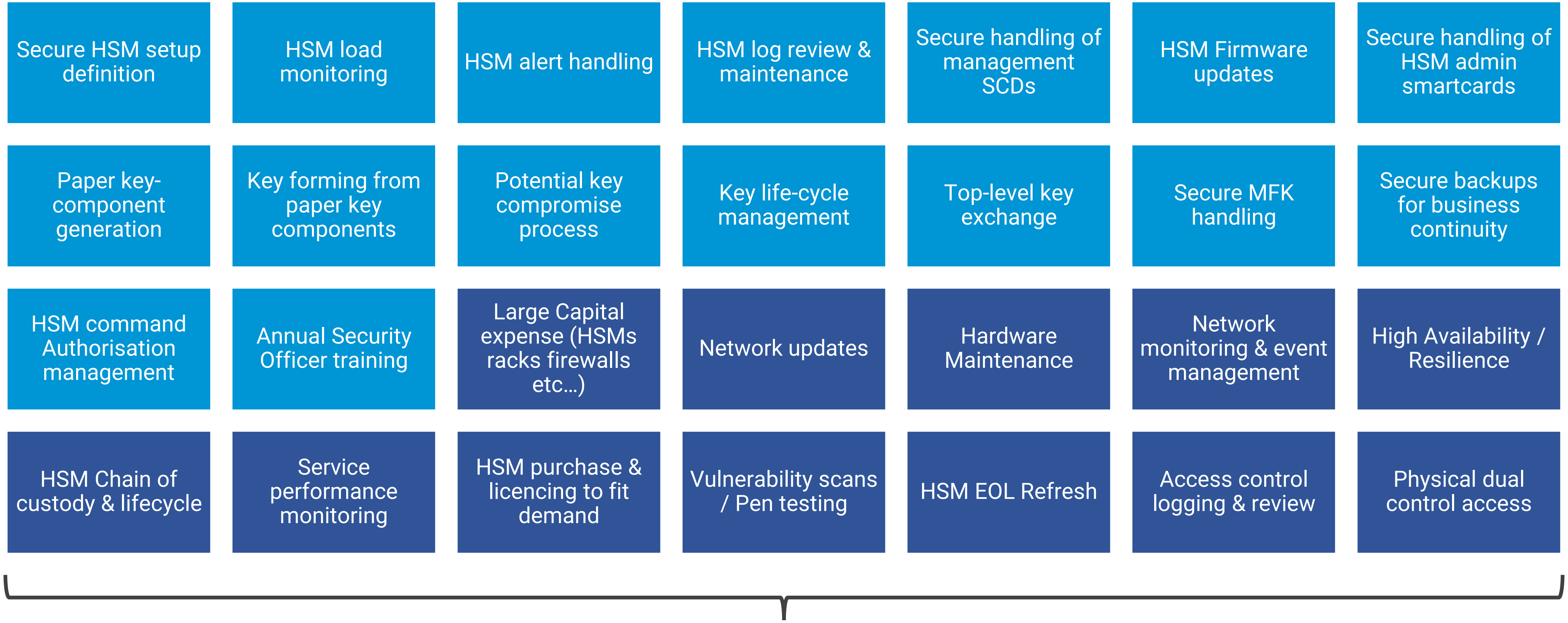
Where MYHSM Fits



Payment HSM Management: What is Involved?

Light blue relates to managing a Payment HSM, dark blue relates to hosting one.

MYHSM does all of this for you.



Secure HSM setup definition	HSM load monitoring	HSM alert handling	HSM log review & maintenance	Secure handling of management SCDs	HSM Firmware updates	Secure handling of HSM admin smartcards
Paper key-component generation	Key forming from paper key components	Potential key compromise process	Key life-cycle management	Top-level key exchange	Secure MFK handling	Secure backups for business continuity
HSM command Authorisation management	Annual Security Officer training	Large Capital expense (HSMs racks firewalls etc...)	Network updates	Hardware Maintenance	Network monitoring & event management	High Availability / Resilience
HSM Chain of custody & lifecycle	Service performance monitoring	HSM purchase & licencing to fit demand	Vulnerability scans / Pen testing	HSM EOL Refresh	Access control logging & review	Physical dual control access

Plus skilled staff, detailed procedures & audit logging to cover all of the above

What is MYHSM?

- **Fully managed** Payment HSM as-a-Service
- **Globally** accessible, multiple data centres
- **Secure**, active-active service with **99.999%** availability
- **PCI PIN** and **PCI DSS** certified
- Multi-vendor: **Atalla AT1000 and Thales payShield 10K**
- **Subscription-based** pricing
- Customers now in over **40 countries**
- **Partnered** with industry leaders
- Online **customer portal**

Test and Live Service Options:

Shared Test

Develop / test payment applications and run POC's in a separate environment using a group of 2 x HSMs with standard test keys

Shared Live

For **live production processing** using groups of 3 x HSMs shared by multiple users

Dedicated Live

For **live production processing** using groups of HSMs for **exclusive use** by those users who have non-standard configuration / exceptionally high volumes

MYHSM Service Benefits

Plug the Public Cloud Gap

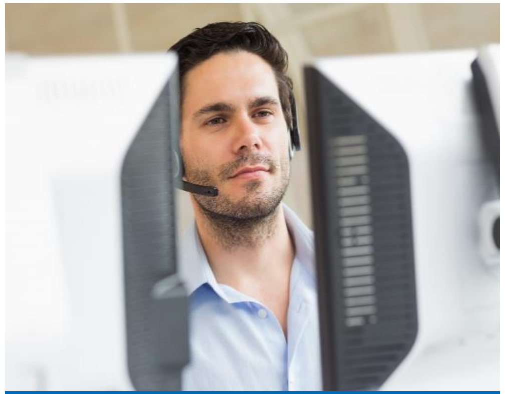
- Solves the challenges of deploying payment HSMs natively in the cloud with PCI-PIN compliance
- MYHSM is cloud agnostic "edge of cloud"
- Increases speed to market, resilience and scalability

Focus on your core business

- Leave MYHSM to manage your Payment HSMs
- Fully managed service, not just hosting
- Utilize latest firmware, security updates, and hardware
- You focus on your Business success

Reduce TCO

- Remove capex for opex
- Reduce overall costs around hardware, networking, datacenters, maintenance, staff, audits and infrastructure



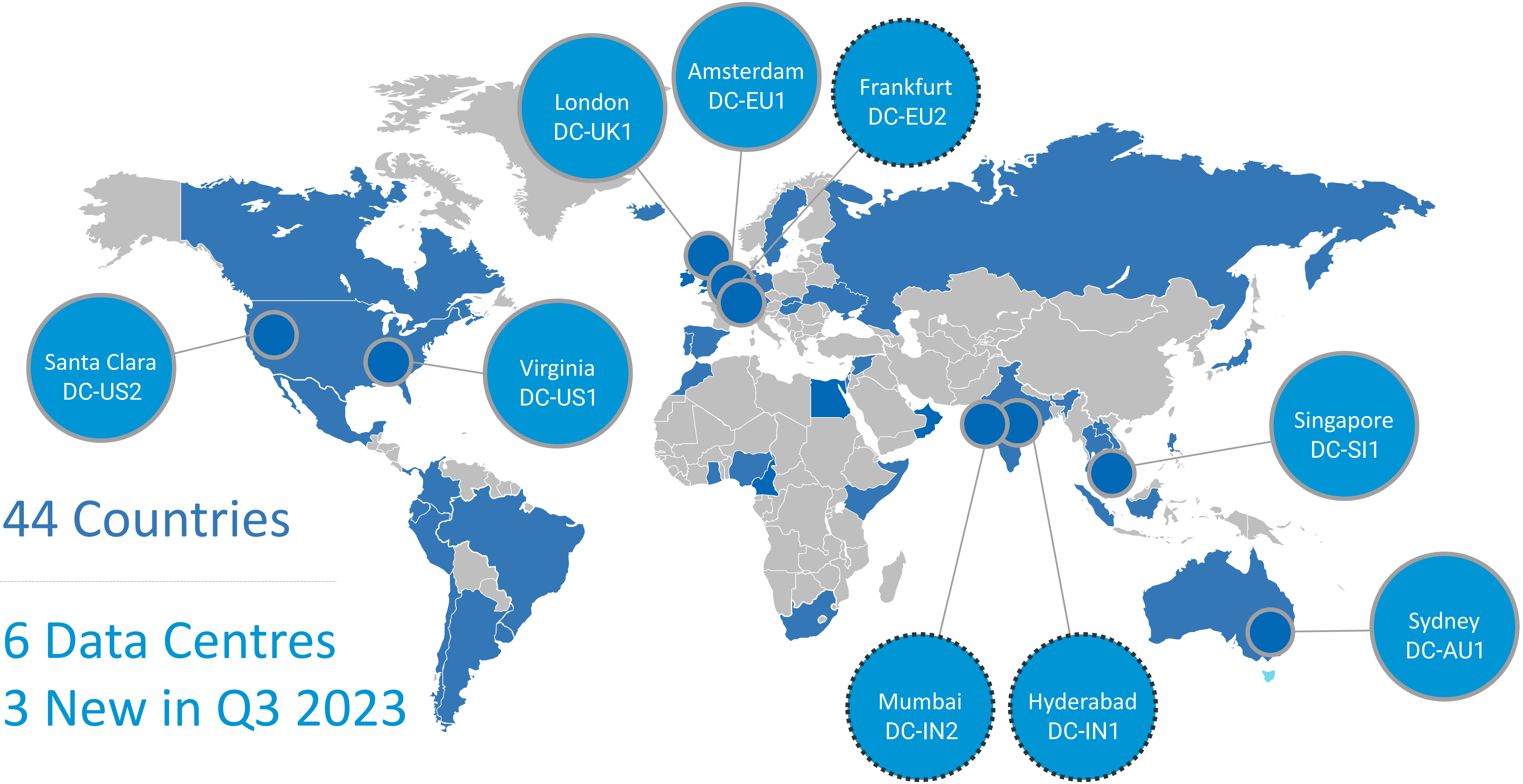
Agility & Global Footprint

- Ability to increase capacity as and when required
- Reducing time to market
- Gain immediate access to Fully certified infrastructure
- Globally accessible
- Low latency

Future proof

- Avoid future HSM refreshes, and service disruption when your Payment HSMs go end-of-life
- Limitless expansion as and when required anywhere Globally
- All infrastructure running on latest proven firmware

MYHSM Global Footprint and Datacentres



44 Countries

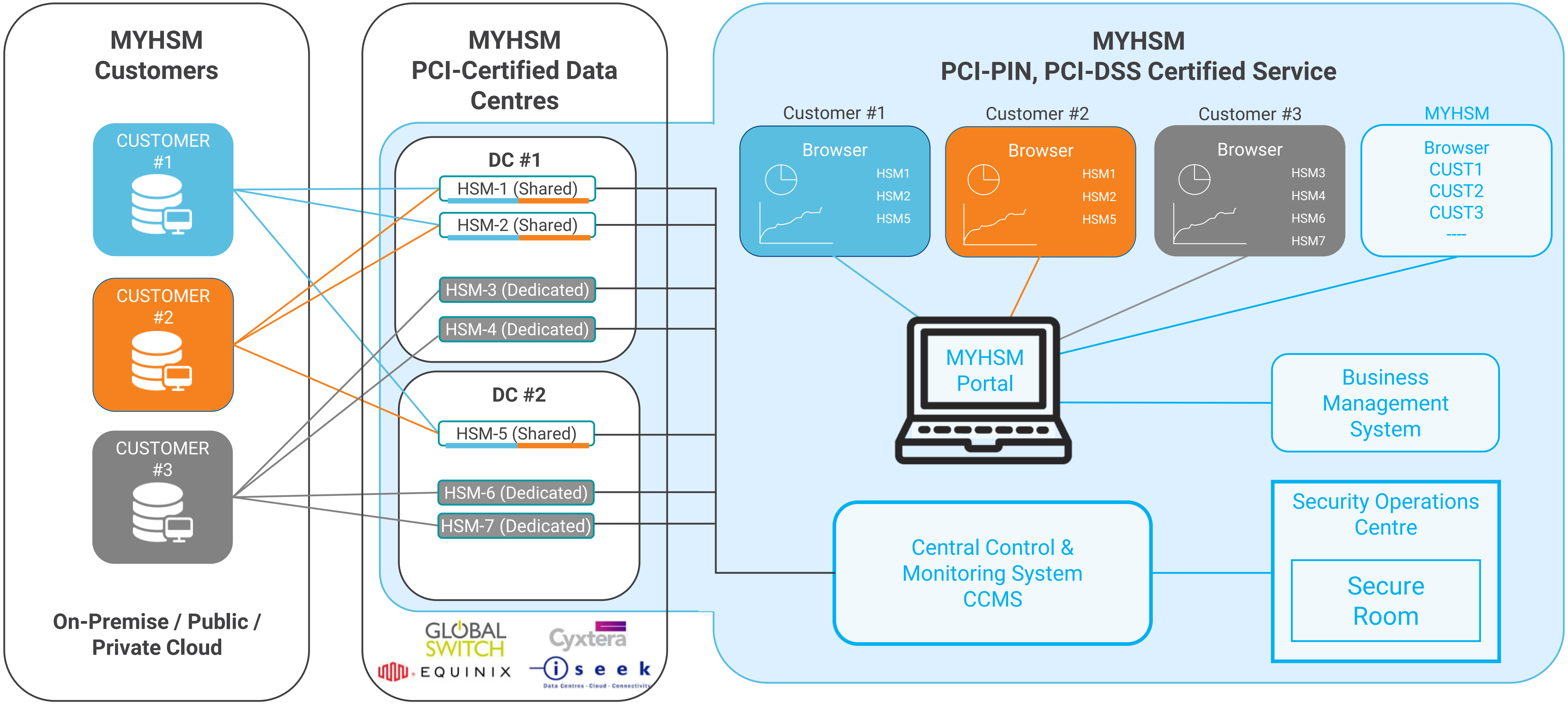
6 Data Centres

3 New in Q3 2023

Service Architecture

Creating Trust in
the **Digital Society**

MYHSM Portfolio and Services



MYHSM Customers

CUSTOMER #1

CUSTOMER #2

CUSTOMER #3

On-Premise / Public / Private Cloud

MYHSM PCI-Certified Data Centres

DC #1

HSM-1 (Shared)

HSM-2 (Shared)

HSM-3 (Dedicated)

HSM-4 (Dedicated)

DC #2

HSM-5 (Shared)

HSM-6 (Dedicated)

HSM-7 (Dedicated)

GLOBAL SWITCH

Cyxtera

EQUINIX

iseek Data Centres · Cloud · Connectivity

MYHSM PCI-PIN, PCI-DSS Certified Service

Customer #1: Browser, HSM1, HSM2, HSM5

Customer #2: Browser, HSM1, HSM2, HSM5

Customer #3: Browser, HSM3, HSM4, HSM6, HSM7

MYHSM: Browser, CUST1, CUST2, CUST3, ----

MYHSM Portal

Business Management System

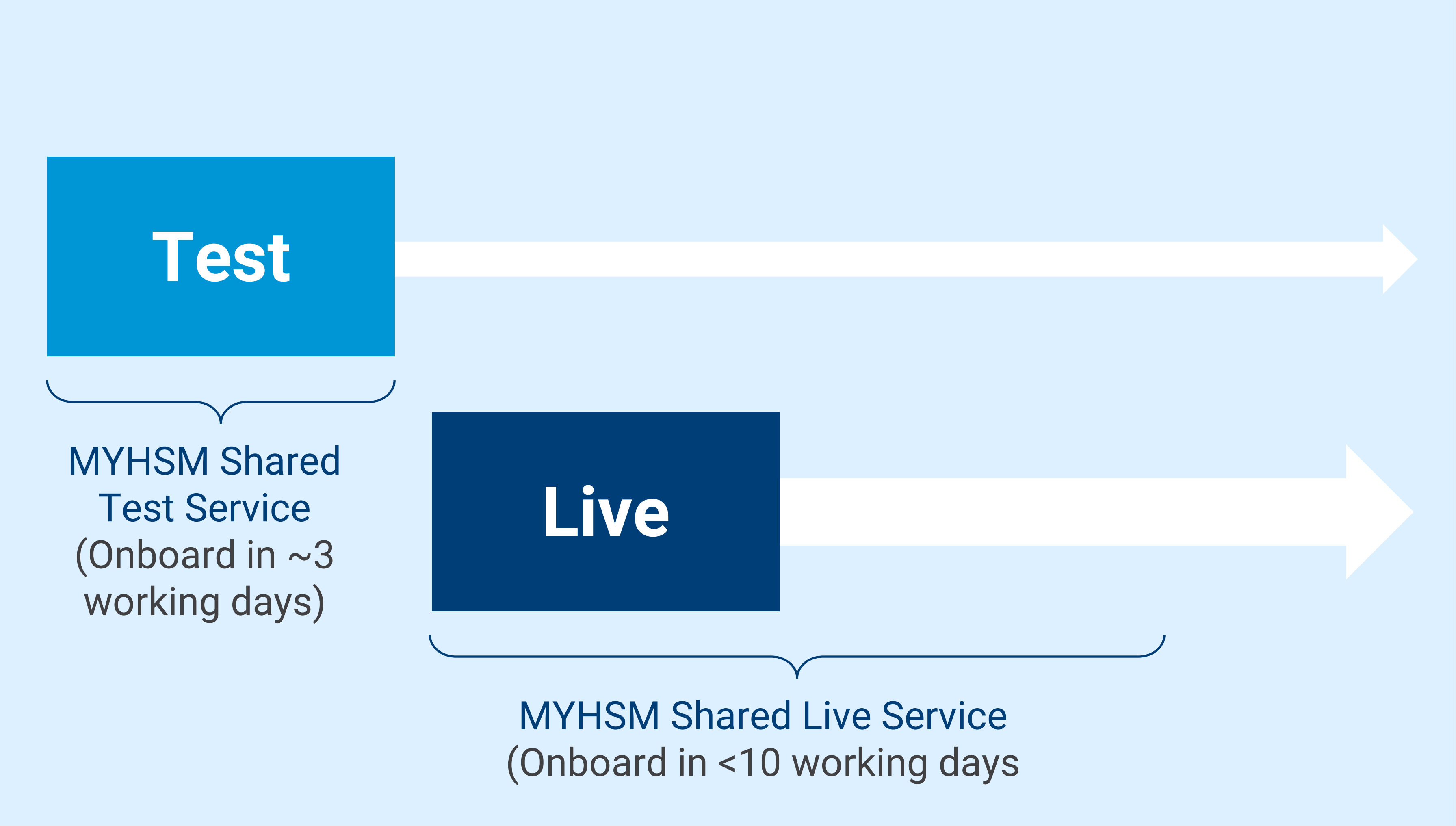
Central Control & Monitoring System CCMS

Security Operations Centre

Secure Room

Preparing for Live Service

MYHSM enables a seamless rollout from test to a production live service



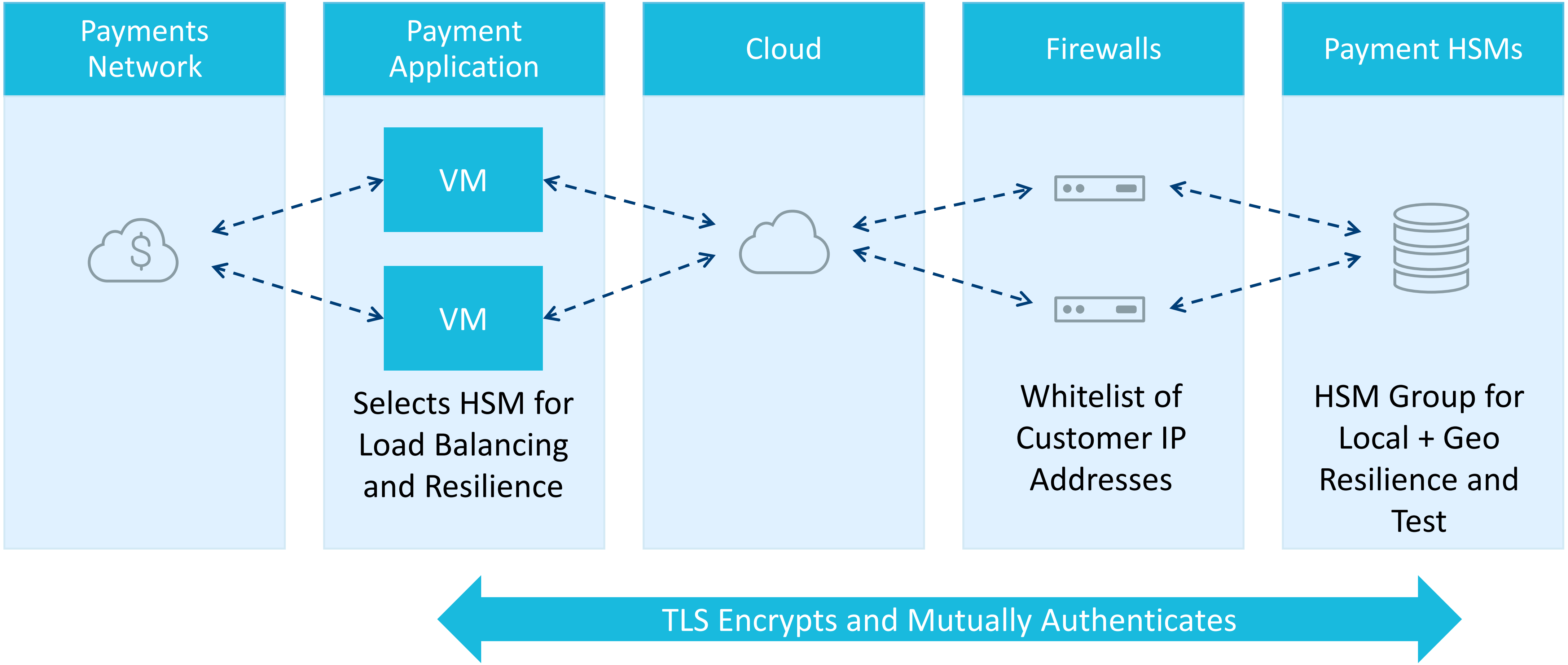
Test

MYHSM Shared Test Service (Onboard in ~3 working days)

Live

MYHSM Shared Live Service (Onboard in <10 working days

Connectivity



Payments Network

Payment Application

Cloud

Firewalls

Payment HSMs

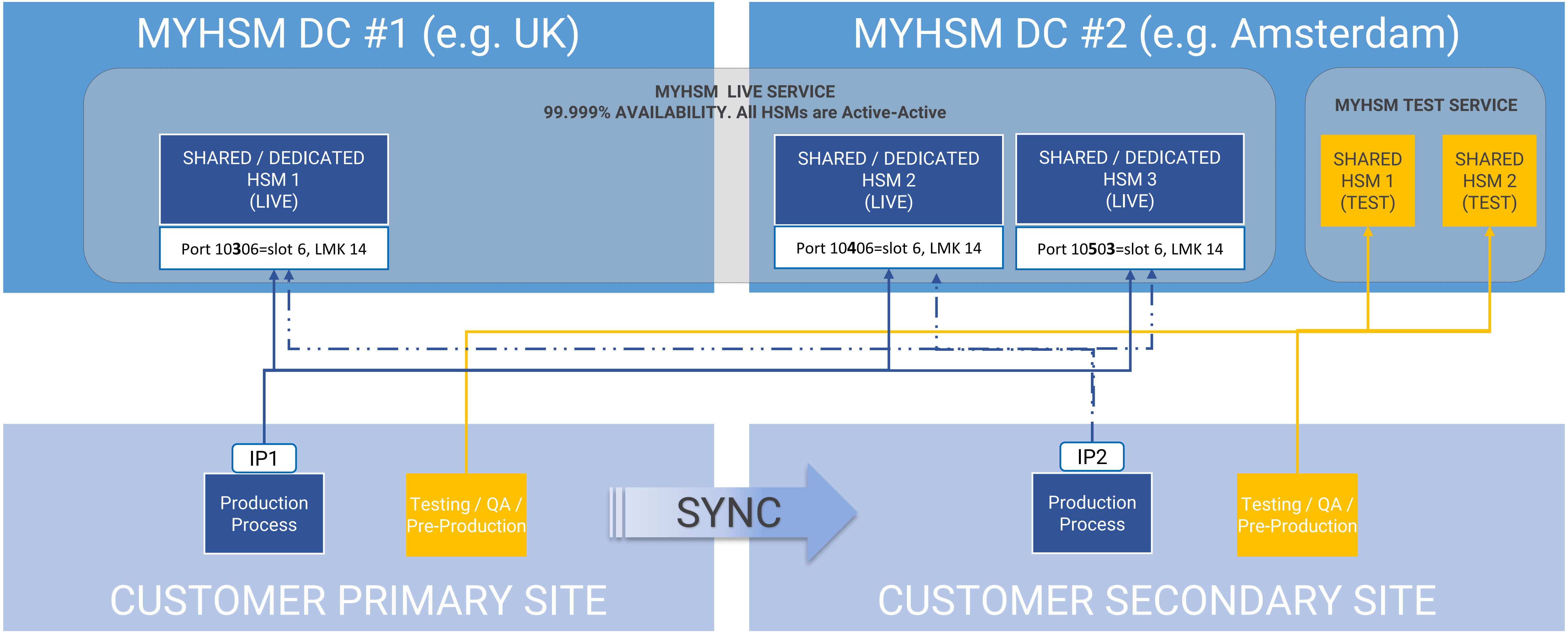
Selects HSM for Load Balancing and Resilience

Whitelist of Customer IP Addresses

HSM Group for Local + Geo Resilience and Test

TLS Encrypts and Mutually Authenticates

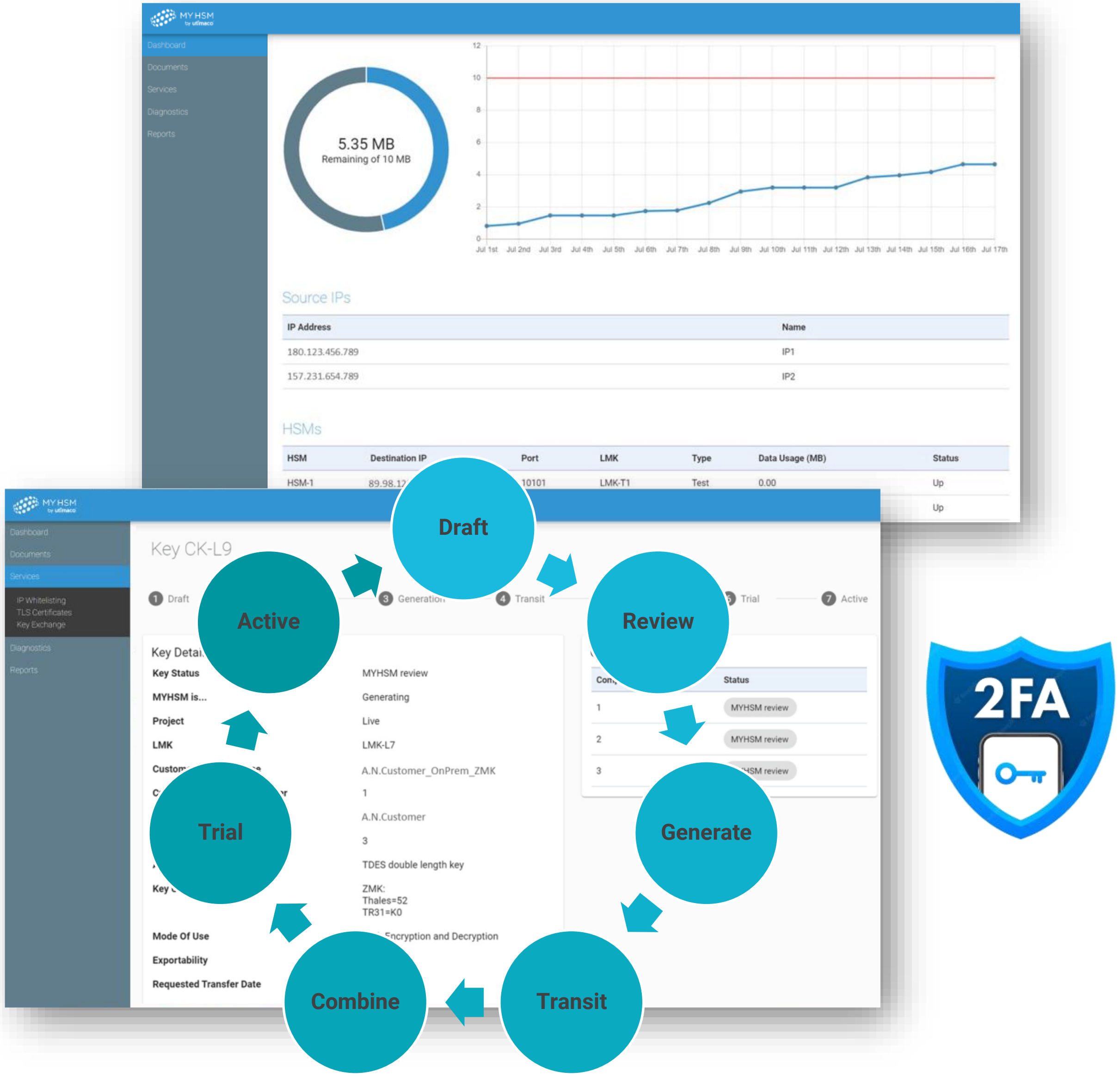
Typical MYHSM and Customer Setup


MYHSM DC #1 (e.g. UK)
MYHSM DC #2 (e.g. Amsterdam)
MYHSM LIVE SERVICE
99.999% AVAILABILITY. All HSMs are Active-Active
SHARED / DEDICATED HSM 1 (LIVE)
Port 10306=slot 6, LMK 14
SHARED / DEDICATED HSM 2 (LIVE)
Port 10406=slot 6, LMK 14
SHARED / DEDICATED HSM 3 (LIVE)
Port 10503=slot 6, LMK 14
MYHSM TEST SERVICE
SHARED HSM 1 (TEST)
SHARED HSM 2 (TEST)
IP1
Production Process
Testing / QA / Pre-Production
SYNC
IP2
Production Process
Testing / QA / Pre-Production
CUSTOMER PRIMARY SITE
CUSTOMER SECONDARY SITE

- **Pool of active-active HSMs, 99.999% availability.**
- **One (normally) Live LMK/MFK per customer per HSM, so one port per HSM**
- **Option of using MYHSM's MCI Load Balancer**

Customer Portal

- MYHSM customers can:
- Administer the organisation’s accounts including adding new Users /Org-admins.
- Access general documentation, general guidance & example source code
- Securely exchange customer-specific files with MYHSM
    - E.G: certificates, certificate signing requests and LMK/MFK-encrypted keys
- See information about their projects, HSM statistics and their status
- Request import of plain-text key components (MYHSM generating / receiving)



Source IPs

IP Address	Name
180.123.456.789	IP1
157.231.654.789	IP2

HSMs

HSM	Destination IP	Port	LMK	Type	Data Usage (MB)	Status
HSM-1	89.98.12	10101	LMK-T1	Test	0.00	Up
						Up

Key CK-L9

1 Draft — 3 Generation — 4 Transit — 6 Trial — 7 Active

Key Detai

Key Status	MYHSM review
MYHSM is...	Generating
Project	Live
LMK	LMK-L7
Custom	A.N.Customer_OnPrem_ZMK
C	1
	A.N.Customer
	3
	TDES double length key

Key	ZMK:
	Thales=52
	TR31=K0

Mode Of Use	Encryption and Decryption
Exportability	
Requested Transfer Date	

Com	Status
1	MYHSM review
2	MYHSM review
3	HSM review

Key Management

Creating Trust in
the **Digital Society**

Key Management Options

- HSM Master key (MFK)
  - A unique master key is created by MYHSM for each customer.
- Top level keys (e.g. ZMK)
  - These keys are exchanged as components between two entities when they set up a relationship.
- Working keys (e.g. ZPK)
  - Once two entities have shared a top-level key, they can use it to share other (working) keys programatically.

1 MY HSM by utimaco — We Do Your Key Ceremonies for you

2

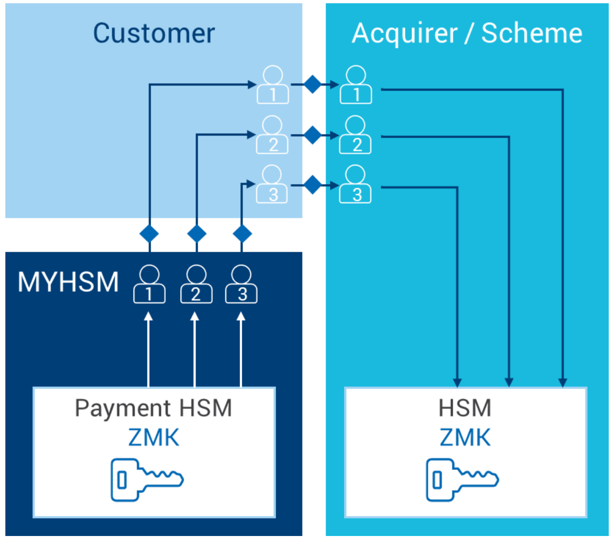
You Do Your Key Ceremonies Yourself

3 KEY Exchange & Escrow Services (KEES) — We Do All Of Your Key Mgt and storage for You

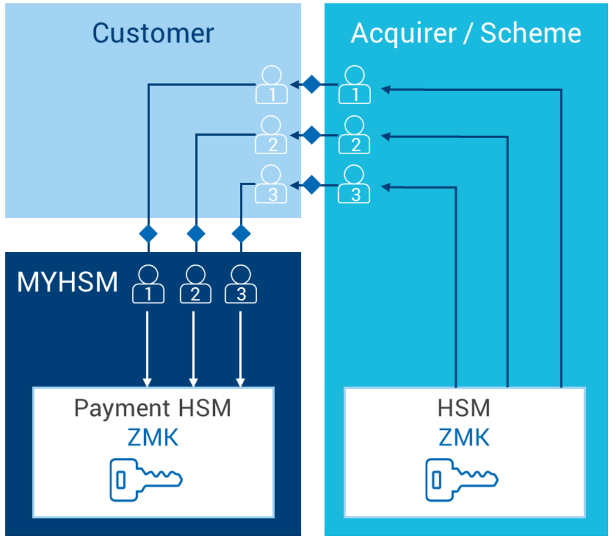
MYHSM Performing Top Level Key Exchanges – Indirect / Direct Model

Indirect Model

Key Exchange, MYHSM as Generator

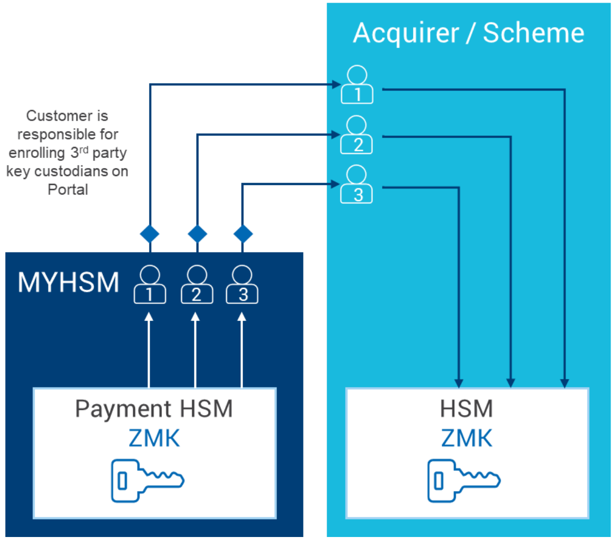


Key Exchange, MYHSM as Receiver

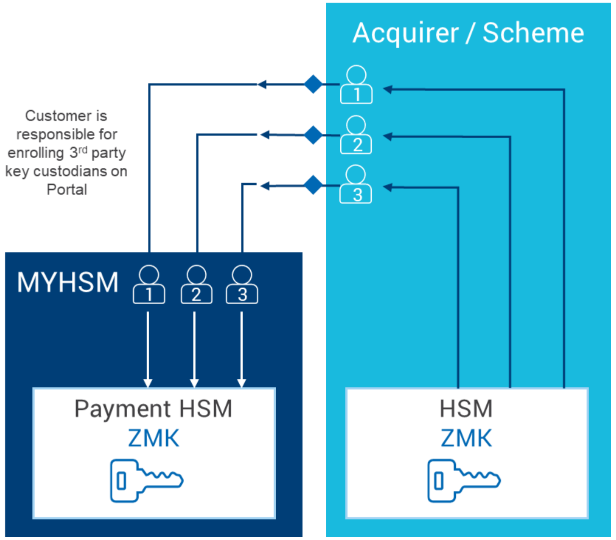


Direct Model

Key Exchange, MYHSM as Generator


Acquirer / Scheme
Customer is responsible for enrolling 3rd party key custodians on Portal
1
2
3
MYHSM
Payment HSM
ZMK
HSM
ZMK

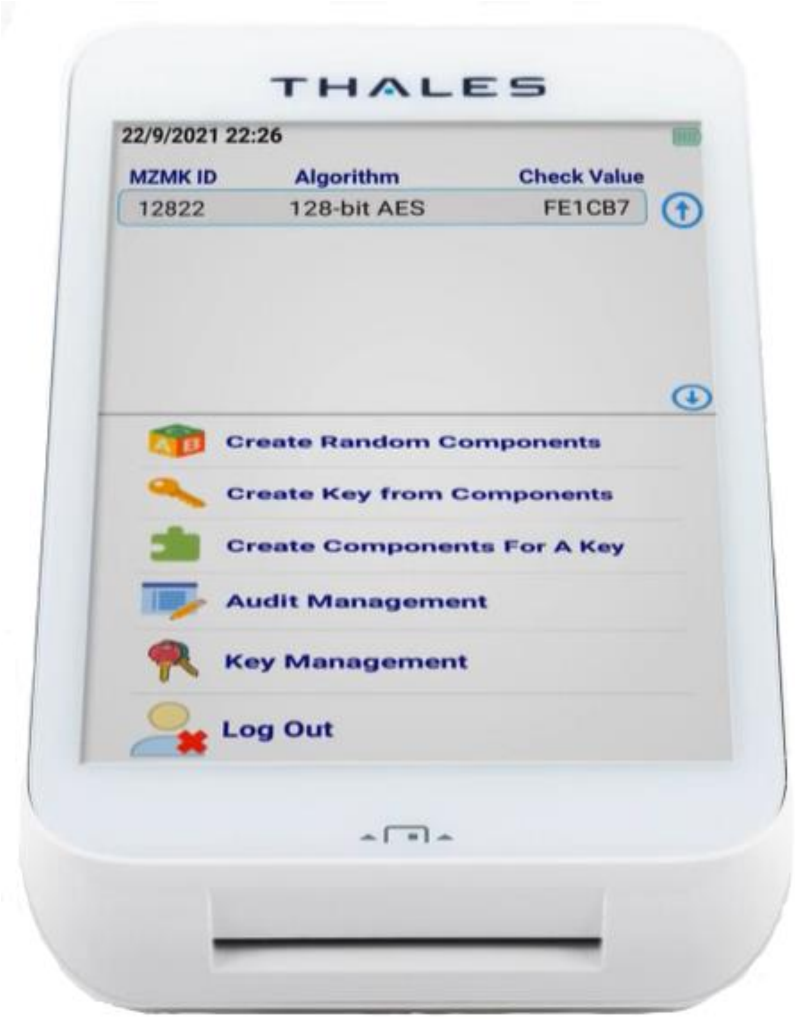
Key Exchange, MYHSM as Receiver


Acquirer / Scheme
Customer is responsible for enrolling 3rd party key custodians on Portal
1
2
3
MYHSM
Payment HSM
ZMK
HSM
ZMK

Customer Performing Inhouse Key Management using TMD’s

Trusted Management Devices

- Customers buy the TMD device(s) to perform their own key exchanges with 3rd parties.
- An initial key exchange is performed between MYHSM and the TMD
- Customers can then conduct key exchange by themselves using the TMD devices
- The TMD devices can be used with Thales PayShield 10K or Atalla AT1000 HSMs in MYHSM



22/9/2021 22:26

MZMK ID	Algorithm	Check Value
12822	128-bit AES	FE1CB7

KEES Full Key Lifecycle Management and ESCROW

KEES does all of this for you, so that you don’t have to:

Tracking all instances of imported and exported keys	Dual control enforcement	Maintaining a Key Inventory	Enforcement of key separation	Track key generation, import, export	Track key termination details and optional key expiration dates
Tracking all functional key management activities and access	Key Imports and Exports	Paper key-component generation	Key forming from paper key components	Potential key compromise process	Key life-cycle management
Top-level key exchange	Centralised management	Secure Key Storage for business continuity	Reliable Key Generation	Annual Security Officer training	Scheduled Back-ups

Plus skilled staff, detailed procedures & audit logging to cover the above

Roles and Responsibilites

Creating Trust in
the **Digital Society**

utimaco®

Roles and Responsibilities

MYHSM

- Provision of all hardware and software in the datacentre.
- Monitoring of MYHSM system components
- Security of the datacentre and equipment in the datacentre
- Maintenance of equipment in the datacentre, including the installation of firmware updates and replacing failed units
- Detection of and timely response to incidents involving MYHSM equipment
- All relevant security and regulatory certifications
- All HSM management operations, including MFK management and actions requested by customers
- All non-electronic key management (e.g. creating components, forming keys from components)
- Providing clear indication of the current status and health of the customer's HSMs
- Supporting customers experiencing issues with the MYHSM service
- Customer introduction to Thales for support with HSM commands
- Provision and Maintenance of Host TLS certificates
- Extraction and secure storage of audit logs
- Periodic HSM time sync as required
- Accurate and timely invoicing

CUSTOMER

- Export of any existing operational keys encrypted under a ZMK from the old HSM system and import the keys under the MFK provided by the MYHSM Service.
- Load balancing between the HSMs in their group, including failover if an HSM goes offline.
- All electronic key management, e.g. generation of operational keys, import/export of keys encrypted under master keys or asymmetric keys.
- Securely maintaining their own key databases (i.e. databases containing keys encrypted under their MFK).
- Notify MYHSM of events which might affect the operation or security of the MYHSM platform.
- Provision and maintenance of client TLS certificates.
- Understanding how to use the Atalla or payShield HSM API as required
- Providing timely information to enable MYHSM to fulfil customer service requests and to provide support.
- Operation, security, regulatory compliances, and resolution of issues outside of the control of MYHSM.

Pricing Model

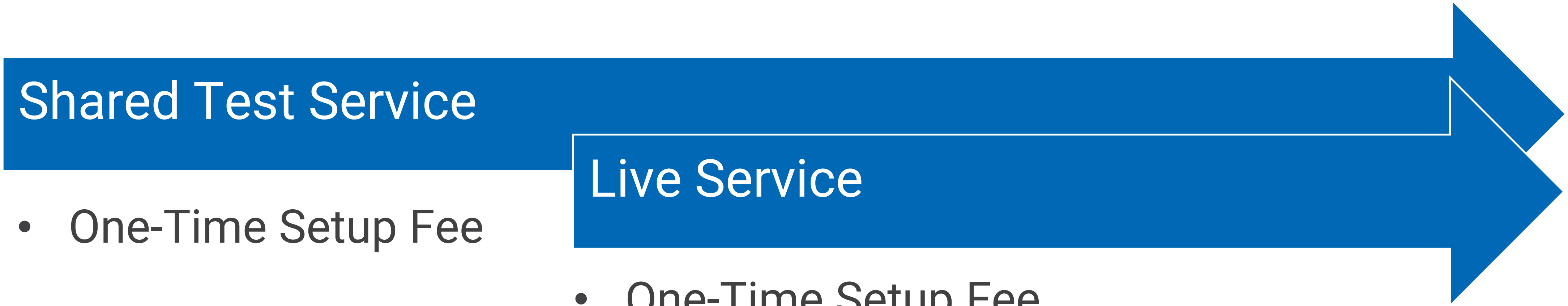
Creating Trust in
the **Digital Society**

MYHSM pricing is all-inclusive

Our pricing covers:

- Provision of all Payment HSM and associated networking hardware and firmware in the data centres.
- Built-in redundancy and disaster recovery facilities.
- Active-active HSMs deployed across physically separate data centres, with 99.999% availability
- Continual monitoring of the health and utilisation levels of all MYHSM system components and rapid response to incidents.
- Maintenance of all MYHSM equipment, including configuration updates, installation of latest firmware, equipment replacement, & capacity management.
- Management of HSM Master Keys (LMKs) for customers.
- Generating, receiving, and forming master keys (such as ZMKs, BDKs) used by the customer to exchange keys with their partners.
- 24x7 emergency support.
- Managing the security of the data centre and its equipment.
- Maintenance of relevant security and regulatory certifications, including PCI DSS and PCI PIN.
- Provision and Maintenance of Host TLS certificates for secure communications.
- Maintenance and recording of audit logs.

MYHSM Shared Service Pricing Model



Shared Test Service

- One-Time Setup Fee
- Flat Monthly Fee

Live Service

- One-Time Setup Fee
- Monthly Fee based on:
  - Shared Live = Data Usage Plans
  - Dedicated Live = HSM CPS Licenses

Shared Live Service: Monthly Data Plans

Data Plans:	1MB	10MB	100MB	1GB	10GB	20GB	30GB
PIN Translation (250 bytes)	4,000	40,000	400,000	4,000,000	40,000,000	80,000,000	120,000,000
MPOS PIN translation (440 bytes)	2,270	22,700	227,000	2,270,000	22,700,000	45,400,000	68,100,000
PIN Authorisation (230 bytes)	4,350	43,500	435,000	4,350,000	43,500,000	87,000,000	130,500,000
ARQC Verification (170 bytes)	5,880	58,800	588,000	5,880,000	58,800,000	117,600,000	176,400,000
EMV Card data prep (690 bytes)	1,450	14,500	145,000	1,450,000	14,500,000	29,000,000	43,500,000

Examples of Operations Possible per Month

Thank you

for your attention!

UTIMACO Inc.

900 East Hamilton Avenue
Campbell, CA-95008
United States of America

Phone +1 (844) UTI-MACO
Web https://hsm.utimaco.com
E-Mail hsm@utimaco.com

utimaco®