Post-Quantum

Cryptography Conference

Crypto-Agility: How it’s both a Critical Component and a Complex Challenge

Samantha Mabey

Director of Product Marketing for the Data Security Solutions at Entrust

Matt Rose

Manager Sales Engineer North America at Entrust

KEYFACTOR CRYPTO4A SSL.com ENTRUST HID

October 28 - 30, 2025 - Kuala Lumpur, Malaysia

PKI Consortium

Crypto-Agility: How It's Both a Critical Component and a Complex Challenge

Greg Wetmore

VP Software Development

ENTRUST

SECURING A WORLD IN MOTION

What is Crypto-Agility?

At the simplest, crypto-agility is an attribute of a system that allows it to transition from one cryptographic system to another, by configuration or policy, without impacting all the infrastructure around it.

But Crypto-Agility is also…

Designing information systems to encourage support of rapid adaptations of new cryptographic primitives and algorithms without making significant changes to the system's infrastructure.

- Dr. Garfield Jones, Associate Chief of Strategic Technology, CISA

Cryptographic agility implies the ability to quickly respond to an algorithm being broken by switching to an alternative with minimal disruption. Because PQC algorithms are relatively new, crypto-agility is a key pillar of resilience in the quantum age.

- Dr. Michele Mosca, CEO evolutionQ

Crypto agility describes the capabilities needed to replace and adapt cryptographic algorithms for protocols, applications, software, hardware, and infrastructures without interrupting the flow of a running system to achieve resiliency.

- NIST CSWP 39, Considerations for Achieving Cryptographic Agility

Navigating Crypto-Agility

- Crypto agility is all of those, which can make it hard to define
- What we do know, it is so much more than just configuration and algorithms
- Today we're going to explore:
  - What's driving the need for crypto-agility
  - The different dimensions of crypto-agility
  - The benefits it delivers

ENTRUST

What’s Driving the Criticality of Crypto-Agility

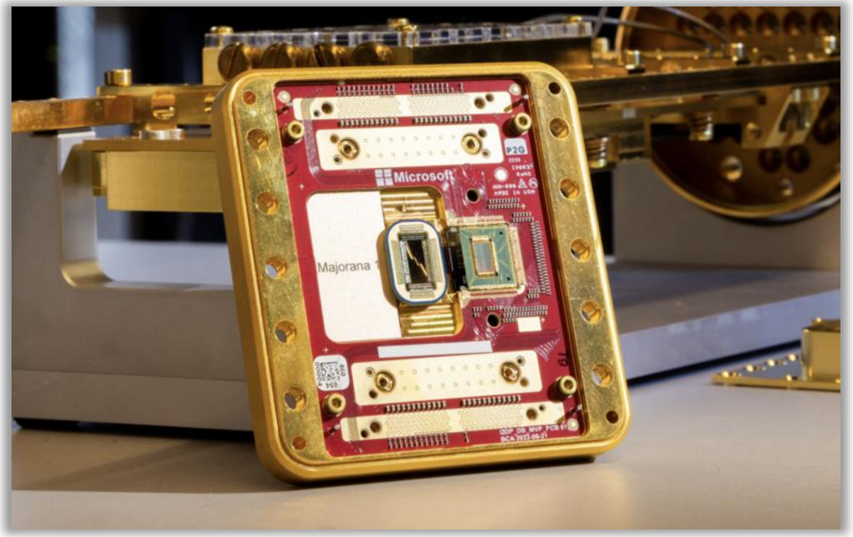
What’s Driving the Criticality of Crypto-Agility

Organizations face a myriad of challenges as the threat landscape continues to grow and operations become more complex.

- The Journey to Quantum Safe
- Data and Device Sprawl
- Organizational Complexity
- Short-life Certificates

The Quantum Threat

- Advances in quantum computing are accelerating
- The risk from harvest now, decrypt later (HNDL) attacks needs to be addressed today
- The deadlines to prepare are approaching…



2025 NSA (CNSA 2.0) requires software, firmware, and browsers to prefer and support quantum safe algorithms

2030 NIST deprecating classical asymmetric algorithms like RSA

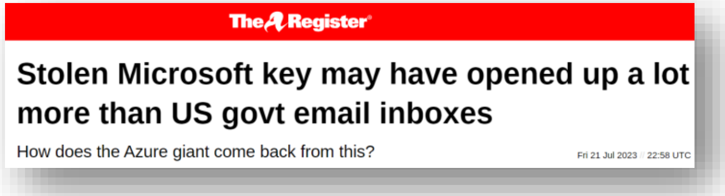
2033 NSA (CNSA 2.0) requires exclusive use of quantum-safe algorithms for software, firmware, and browsers

2035 NIST disallowing classical asymmetric algorithms

ENTRUST

Data and Device Sprawl

- The threat landscape is expanding:
  - **75B connected devices** by 2025, up from 31B in 2020
  - **175 zettabytes of data** needing protection, growing to 421ZB by 2030
- The explosion of data and devices results in an explosion of crypto assets to secure them
- Attacks on cryptographic systems are increasing in number and sophistication

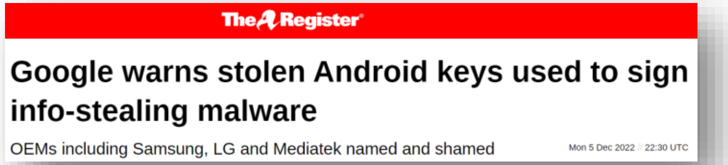


The Register

Stolen Microsoft key may have opened up a lot more than US govt email inboxes

How does the Azure giant come back from this?

Fri 21 Jul 2023 // 22:58 UTC



The Register

Google warns stolen Android keys used to sign info-stealing malware

OEMs including Samsung, LG and Mediatek named and shamed

Mon 5 Dec 2022 // 22:30 UTC

Operational Complexity

- Multiple, fragmented tools used to manage cryptography enterprise-wide
- Tools, assets, and data managed by independent teams
- Accelerating pace of change

Top Challenges in Deploying and Managing PKI

No clear ownership

51%

Insufficient skills

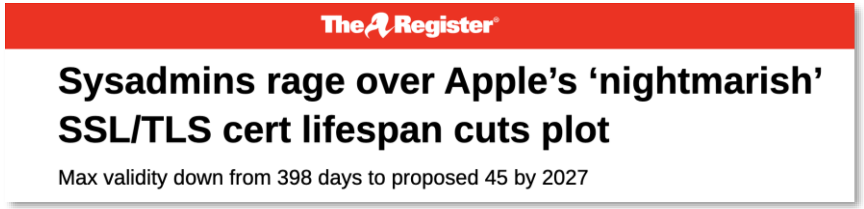
43%

Source: 2024 Ponemon PKI & Post-Quantum Trends

ENTRUST

Short-Life Certificates

- Growth of the certificate landscape makes manual processes unsustainable
- Lack of visibility creates an increasing risk of outage or expiry
- Compliance and security challenges
- The number one cause of breaches is credential compromise
- Reputational damages



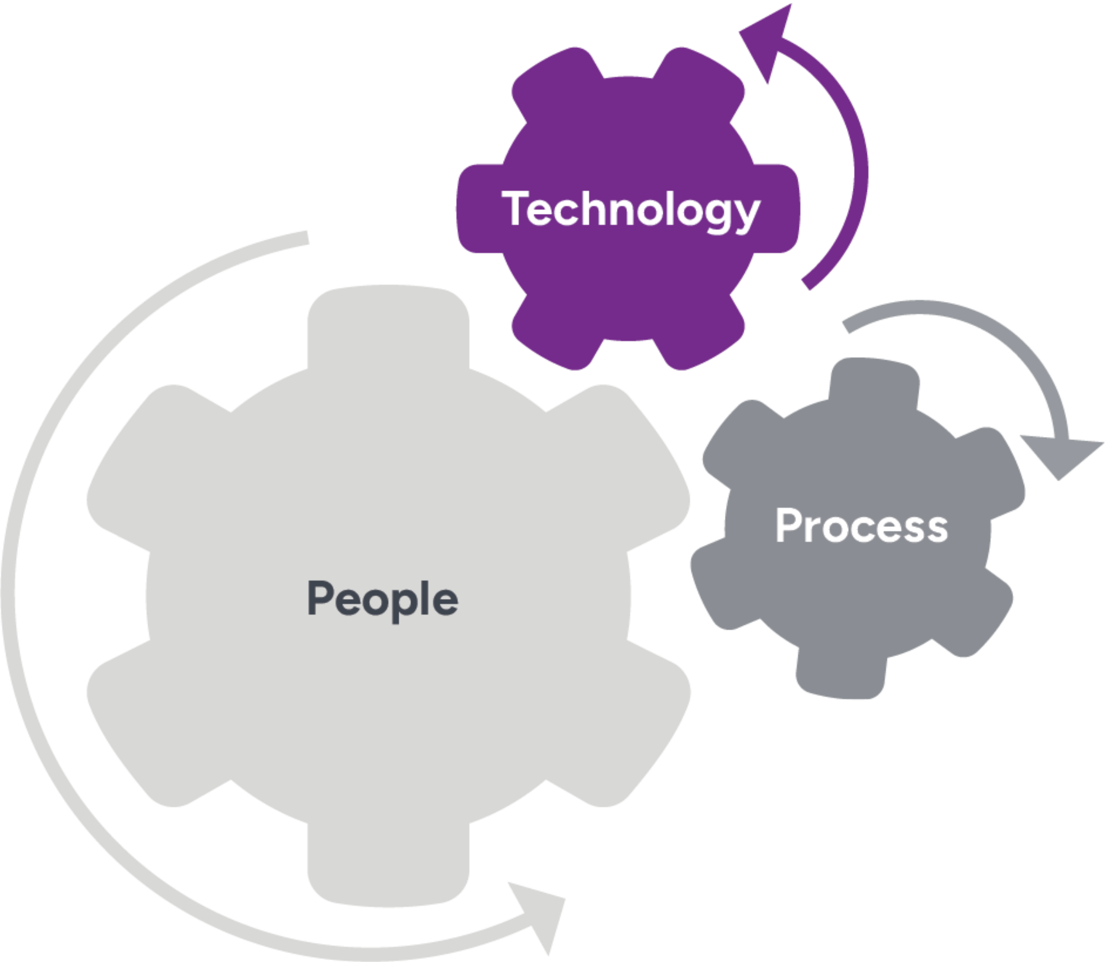
The Register

Sysadmins rage over Apple's 'nightmarish' SSL/TLS cert lifespan cuts plot

Max validity down from 398 days to proposed 45 by 2027

The Different Dimensions of Crypto-Agility

Crypto-Agility at the Organizational Level



People - role that people play in an organization’s cryptographic agility

Process - how governance, compliance, policies, processes, and procedures influence cryptographic agility

Technology - the influence and importance of technology on cryptographic agility

Crypto-Agility: People

Even the best technology fails without informed and engaged teams…

- Accountability
- Training and Awareness
  - IT, Development, Operations
  - Legal, Compliance
  - Business Stakeholders
- Executive Leadership

Crypto-Agility: Process

Process informs how governance, compliance, policies, processes, and procedures influence cryptographic agility.

- Policy Management and Governance
- Risk and Compliance
- Vendor and Ingredient Technology
- Change Management and Incident Response
- Traceability and Audit

Crypto-Agility: Technology

VISIBILITY

Inventory certificates and crypto assets across your organization.

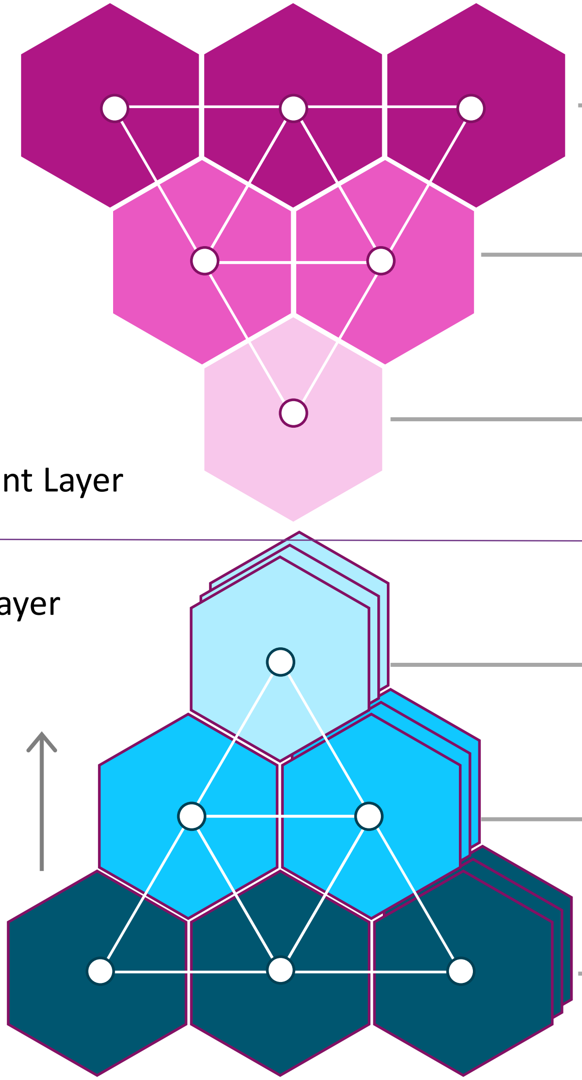
POLICY & CONTROL

Centrally manage policy, issuance, & access to public & private certificates and keys.

AUTOMATE

Orchestrate deployment and manage lifecycle of certificates and keys.

Technology: Control Plane vs Data Plane



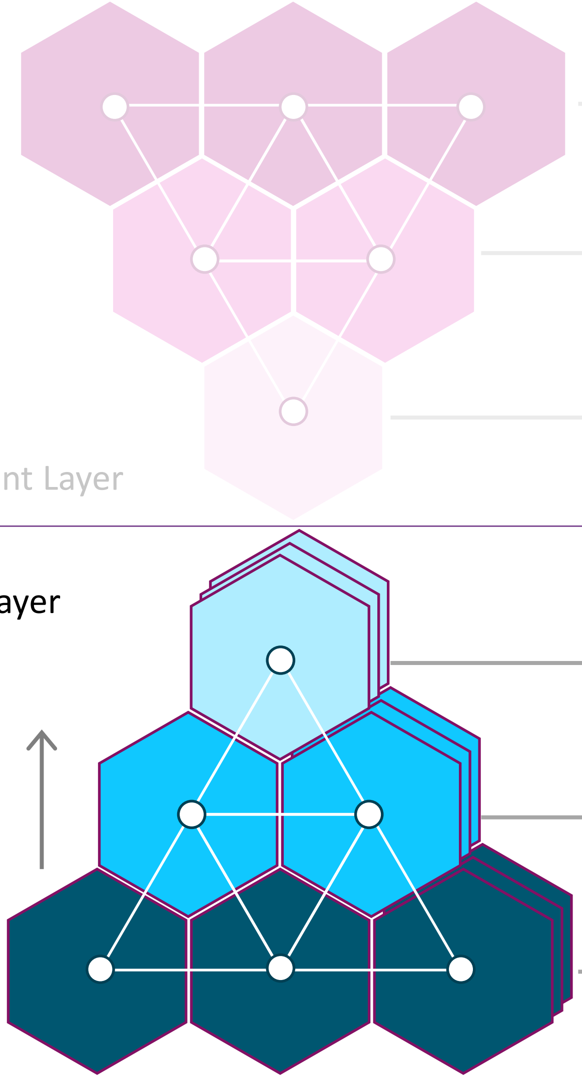
Management Layer

Risk Score	Calculate risk
Compliance	Validate against policies
Metadata	Collecting metadata of the infrastructure and the keys, secrets and certificates

Technical Layer

PKI, KMS, SM HSM, 3rd Party	Generating and manging cryptographic material
Keys, Secrets, Certificates	Cryptographic material like keys, certificates and secrets
Integrations	Infrastructure that utilize cryptographic material

Examining the Technical Layer



Risk Score — Calculate risk

Compliance — Validate against policies

Metadata — Collecting metadata of the infrastructure and the keys, secrets and certificates

Management Layer

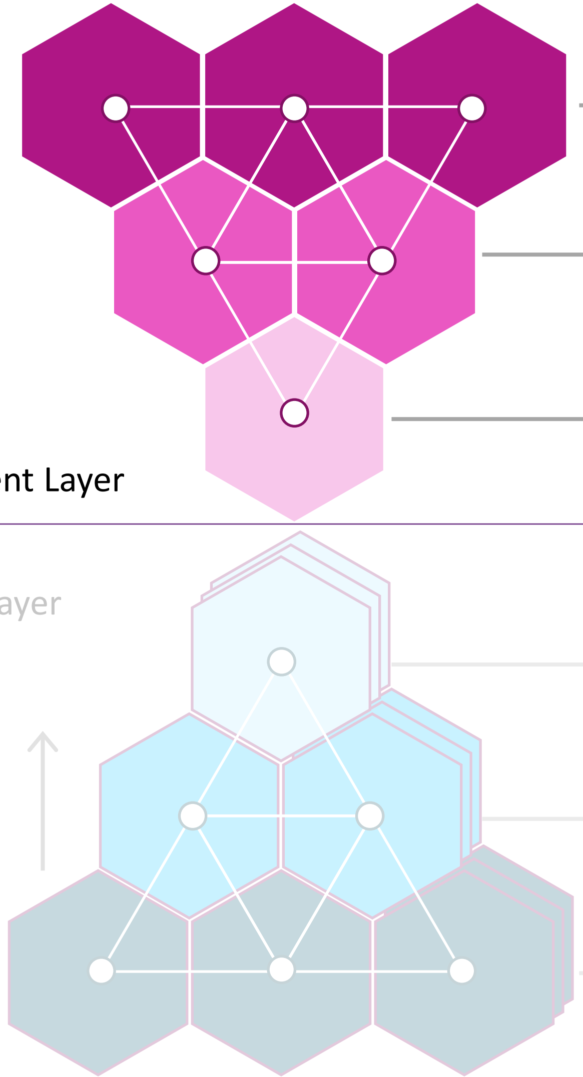
Technical Layer

PKI, KMS, SM HSM, 3rd Party — Generating and manging cryptographic material

Keys, Secrets, Certificates — Cryptographic material like keys, certificates and secrets

Integrations — Infrastructure that utilize cryptographic material

Examining the Management Layer



Management Layer

Risk Score — Calculate risk

Compliance — Validate against policies

Metadata — Collecting metadata of the infrastructure and the keys, secrets and certificates

Technical Layer

PKI, KMS, SM HSM, 3rd Party — Generating and manging cryptographic material

Keys, Secrets, Certificates — Cryptographic material like keys, certificates and secrets

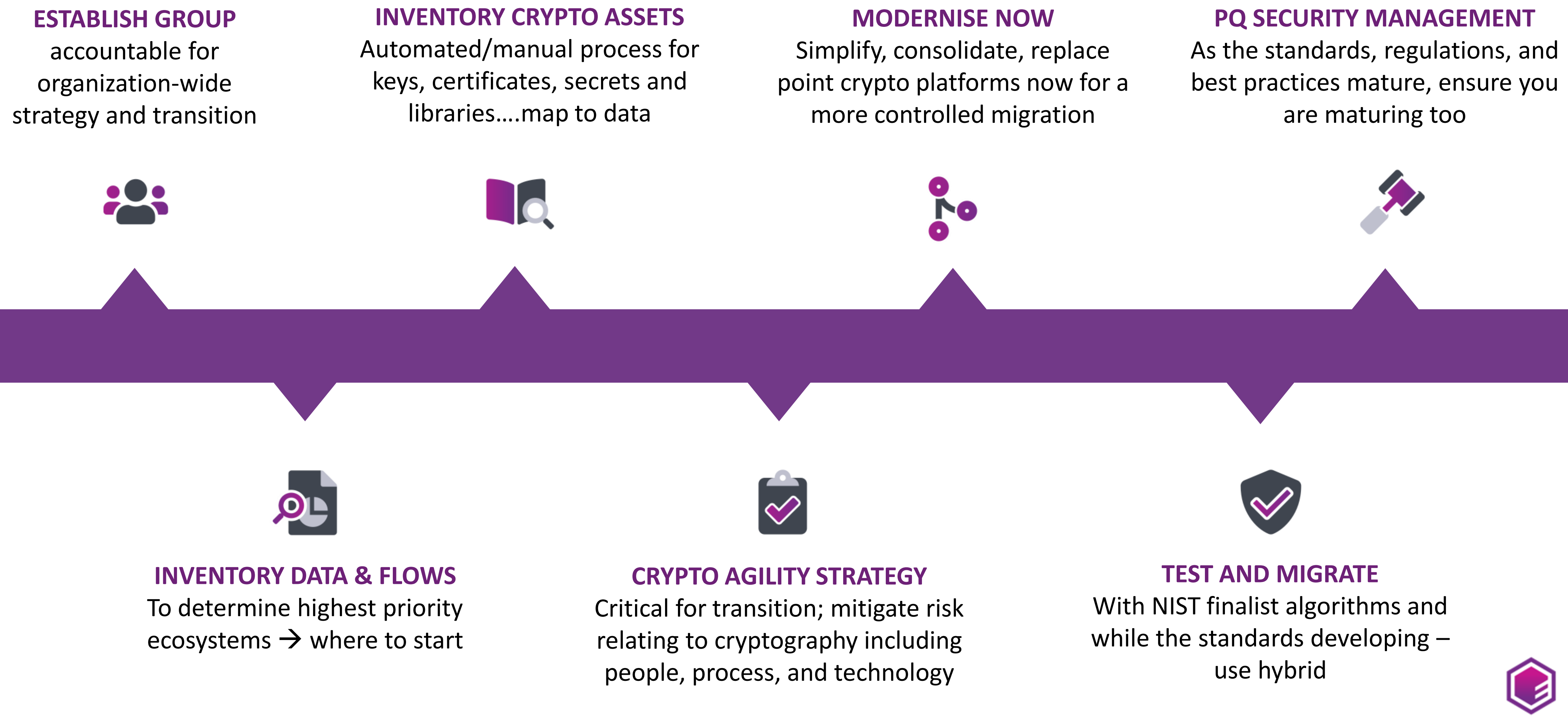
Integrations — Infrastructure that utilize cryptographic material

ENTRUST

The Value of Achieving Crypto-Agility

ENTRUST

Post-Quantum Preparedness Journey



ESTABLISH GROUP
accountable for organization-wide strategy and transition

INVENTORY DATA & FLOWS
To determine highest priority ecosystems → where to start

INVENTORY CRYPTO ASSETS
Automated/manual process for keys, certificates, secrets and libraries….map to data

CRYPTO AGILITY STRATEGY
Critical for transition; mitigate risk relating to cryptography including people, process, and technology

MODERNISE NOW
Simplify, consolidate, replace point crypto platforms now for a more controlled migration

TEST AND MIGRATE
With NIST finalist algorithms and while the standards developing – use hybrid

PQ SECURITY MANAGEMENT
As the standards, regulations, and best practices mature, ensure you are maturing too

Implement Cryptographic Guardrails

- How does CA help organizations move faster
- By applying security the right way, and having organization-wide policy, it applies guardrails to different groups who might work with cryptography
  - Improves efficiency
  - Allows for more innovative product development
  - Enables teams that aren’t crypto experts

“The most effective way to manage and control the use of cryptography is through establishing a single team that has the expertise needed to make effective policy for the organization.”

-Gartner, Report: Postquantum Cryptography: The Time to Prepare Is Now!, July 2024

Confidence with the C-Suite

Full discovery and centralized visibility of cryptographic assets:

- Keys, certificates, and secrets
- Tokens, cryptographic libraries, protocols, configs

Compliance & Risk Mitigation

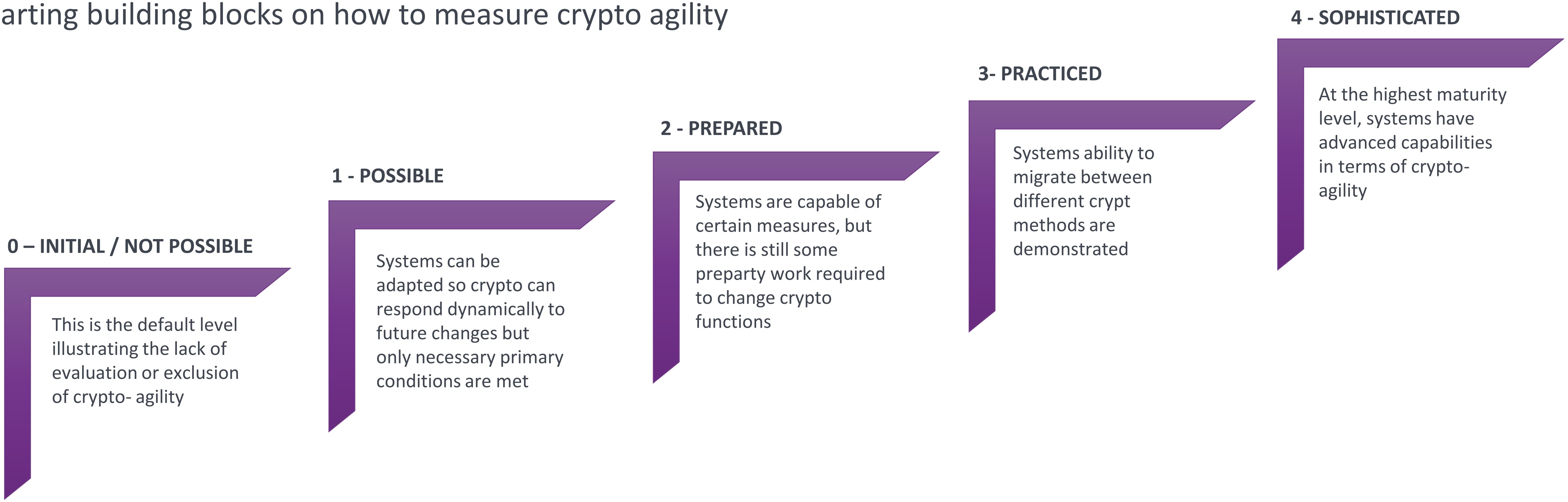
- Centralized compliance policy definition and management
- Priority remediation alerts
- Reporting and analytics

Key Takeaways: How to Apply

- Accountability
  - Determine who will be accountable within your organization
  - An individual or group needs to over see crypto agility and strategy
- Inventory
  - Discovery and inventory of cryptographic assets: keys, certificates, secrets, hardware, software, etc.
- Maturity
  - The secret to having an orderly and organized transition is crypto-agility
  - Develop capabilities around: find, control and automate
  - Figure out where your maturity is and build a plan to reach a higher level
- Implement and execute
  - Test and rollout into production

Crypto-Agility Maturity Model

Starting building blocks on how to measure crypto agility



0 – INITIAL / NOT POSSIBLE

This is the default level illustrating the lack of evaluation or exclusion of crypto- agility

1 - POSSIBLE

Systems can be adapted so crypto can respond dynamically to future changes but only necessary primary conditions are met

2 - PREPARED

Systems are capable of certain measures, but there is still some preparty work required to change crypto functions

3- PRACTICED

Systems ability to migrate between different crypt methods are demonstrated

4 - SOPHISTICATED

At the highest maturity level, systems have advanced capabilities in terms of crypto-agility

There's a need to further develop this model to include people and processes

Source: https://camm.h-da.io/model/

Thank You

Greg.Wetmore@entrust.com

entrust.com

ENTRUST

SECURING A WORLD IN MOTION