

The Coming Crypto Crisis

Greece | Cyprus | Belgium | Romania | United States

Architecting Resilience for the Post-Quantum Era

Case Study: Μειώνοντας το Επιχειρησιακό Ρίσκο μέσω Ενιαίας Διαχείρισης Πιστοποιητικών (Public & Private), Κλειδιών, HSMs.

Andreas Tsiokanos
Product & Business Development Manager

Public Certificate Lifetime

Μείωση της Διάρκειας Ζωής των
Πιστοποιητικών συνεπάγεται αύξηση
Φόρτου Εργασίας (400%) οι ομάδες IT
πρέπει να εκτελούν την ίδια διαδικασία 4
έως 8 φορές συχνότερα ανά πιστοποιητικό

	Manual Management	Automated CLM
Labor required per 100 certificates/year	~500+ hours	10 hours or less
Outage risk due to certificate expiry	High	Near zero
Operator intervention per event	Multiple steps	Single click/minimal/no action
Ability to scale as environment grows	Difficult	High



Quantum Threat

Η Μετάβαση στο Post Quantum Cryptography.

- NIST ολοκλήρωσε τα επίσημα PQC προτυπα
 - ML-KEM, ML-DSA, SLH-DSA, LMS, XMSS
 - Κατάργηση RSA & ECC 2030-2035
- Google
 - Στο Android 17 ενσωματώθηκε PQC digital signature protection using ML-DSA
 - Google Chrome support for PQC
 - Αανακοίνωσε χρονοδιάγραμμα με ολοκλήρωση μετάβασης στο 2029
- MS ενσωμάτωσε PQC αλγόριθμους στα Windows 11 Και Server 2025



The perfect Storm

Όλα μαζί συνθέτουν την τέλεια καταιγίδα.

Έχουμε την πλήρη εικόνα των Crypto Asset ώστε να αντικατασταθούν ?

- Assymetric Keys/ Certificates
- Symmetric Keys
- Private CAs / PKIs
- Public CAs
- HSMs



Entrust Cryptographic Security Platform (CSP)

To fully address these challenges, centralized visibility and control **must be paired with a complete, unified stack of PQC-ready solutions**

PKI

Certificate Lifecycle
Management

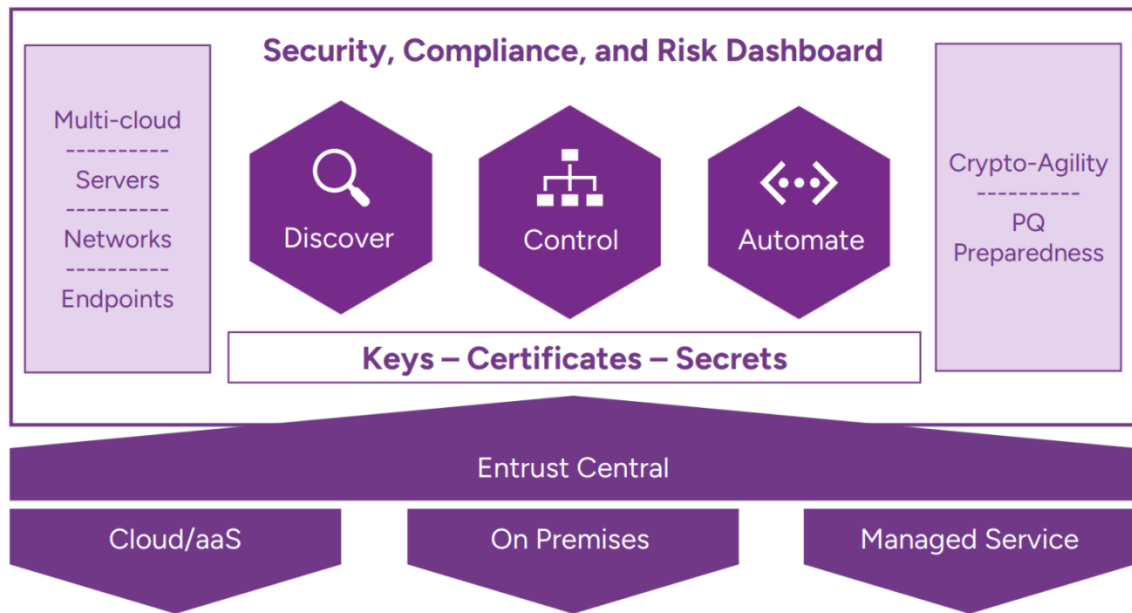
Key and Secrets
Management

HSM

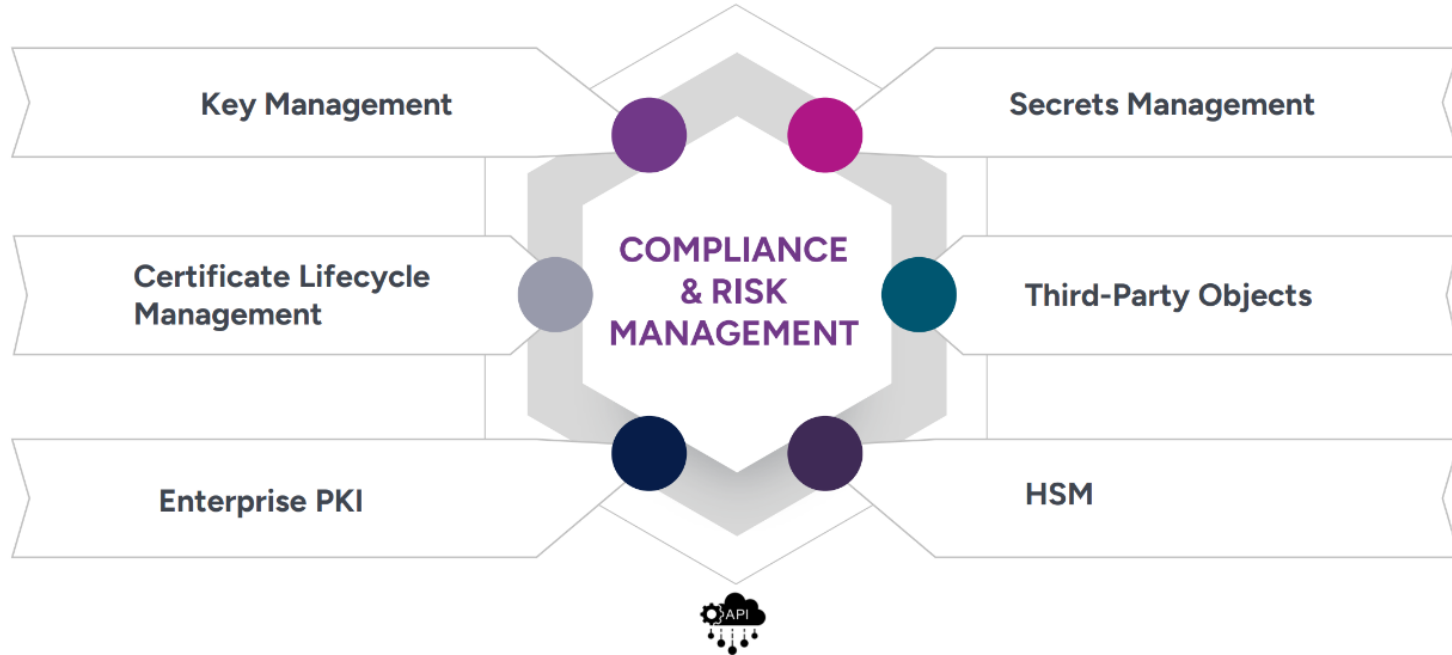
Complete Crypto Asset Single Pane of Glass: Entrust Cryptographic Security Posture (CSP)

- Discovery of Crypto Assets
- Secure key storage and cryptographic operations
- Automated issuance & management of public and private certificates
- Vulnerability and compliance monitoring
- Remediation of security issues and policy enforcement
- Available in SaaS, On-Premises and as a Managed Service

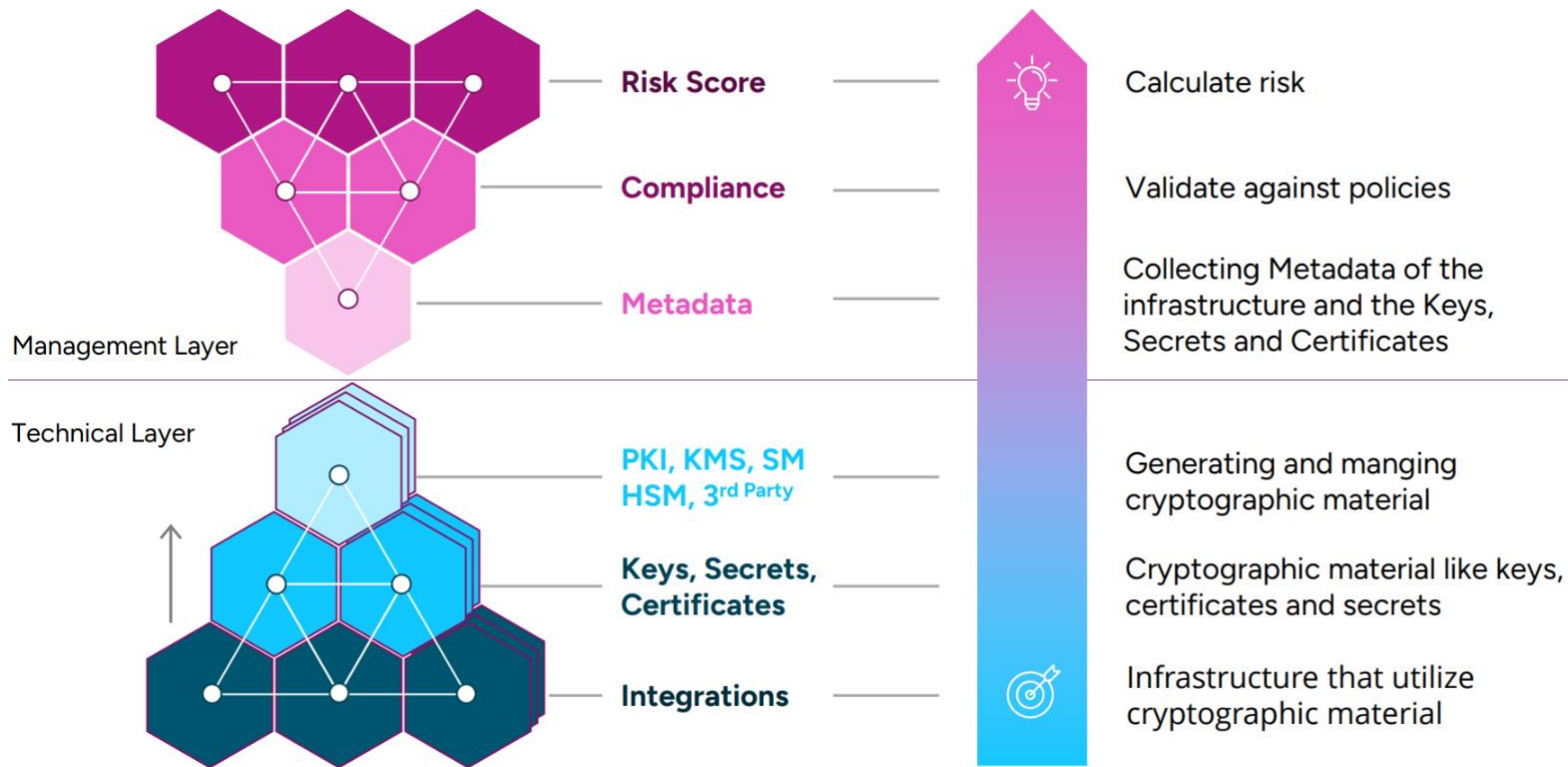
A Centralized Enterprise-wide Cryptographic Security Platform



Entrust CSP Single Pane of Glass: Compliance Manager



Complete Crypto Asset Single Pane of Glass: Entrust Cryptographic Security Posture (CSP)



Entrust CSP Success Story: Financial Institution



Financial institution providing personal and business banking services, operating in a highly regulated sector.

Old Status and the Discovery Questions

- ✓ What are the challenges with the current Microsoft CA and manual certificate processes? Considering to transition from self-hosted Microsoft Certificate Authority (CA) to a cloud-hosted Public Key Infrastructure (PKI). The IT team, manages a PKI with one offline root CA, two offline policy CAs, and two online issuing CAs, supporting roughly 1,200 workstations and 700 users with auto-enrolled (via AD) certificates
- ✓ How would automating certificate lifecycle management impact the operations? Challenges with manual certificate issuance for code signing and internal web servers (IIS, Apache, Tomcat), which creates inefficiencies and risks of service disruptions due to expirations.
- ✓ What's our timeline for consolidating external SSL certificates and budgeting for 2026? The external SSL certificates, currently managed via GoDaddy, are siloed, and Bank was exploring consolidation pending senior management approval to get a lower expiration risk posture and clearer ownership.
- ✓ What other vendors are we considering for PKI and key management?
- ✓ With Microsoft Intune handling mobile device management for MacBooks and (BYOD) policy, a hosted PKI as a Service was considered, Certificate Lifecycle Management, and key management to support up to 2,500 certificates, ensuring compliance with PCI DSS and other standards.

Criteria

Applicable Value Driver

- ✓ Optimize Operational Efficiency
- ✓ Reduce Risk of Data Loss
- ✓ Achieve Compliance

Required Capabilities

- ✓ Hosted PKI to manage device and user certificates, code signing, and internal web services.
- ✓ Certificate Lifecycle Management (CLM) to automate issuance, renewal, and tracking of certificates, integrate with Intune, AD, and future HRIS systems.
- ✓ A unified "single pane of glass" dashboard for centralized certificate oversight.
- ✓ Post-quantum readiness to secure the operations and prepare for regulatory changes.

Implementation & outcome

Solution Deployed

- ✓ Entrust CSP that included: PKI Private CA , CSP CLM selected for seamless cloud integrations, automation capabilities, and roadmap for public CA support (DigiCert and GoDaddy), CSP Vault (KMS), HSM, CSP Compliance Manager

Positive Business Outcome

- ✓ Centralized dashboard for certificate and compliance oversight reducing our risk and creating better control
- ✓ Enhanced security for code signing and web servers to lower security risk
- ✓ Guaranteed SLA and scalability for the future expansions
- ✓ Improved compliance with PCI DSS and NIST
- ✓ Future-proofing with post-quantum cryptography.

Sustainable Cyber Resilience

Greece | Cyprus | Belgium | Romania | United States



Thank You!

Andreas Tsiokanos
Product & Business Development Manager

www.besecuregroup.com