ETSI/IQC Quantum Safe Cryptography Conference 2026

GlobalPlatform PQC migration of protocols managing Secure Elements

Presented by: Beatrice Peirani

18/06/2026

Agenda

GlobalPlatform introduction

Quantum computing threat

PQC standards

PQC national recommendations

GlobalPlatform Crypto Task Force

GlobalPlatform Secure Element Committee

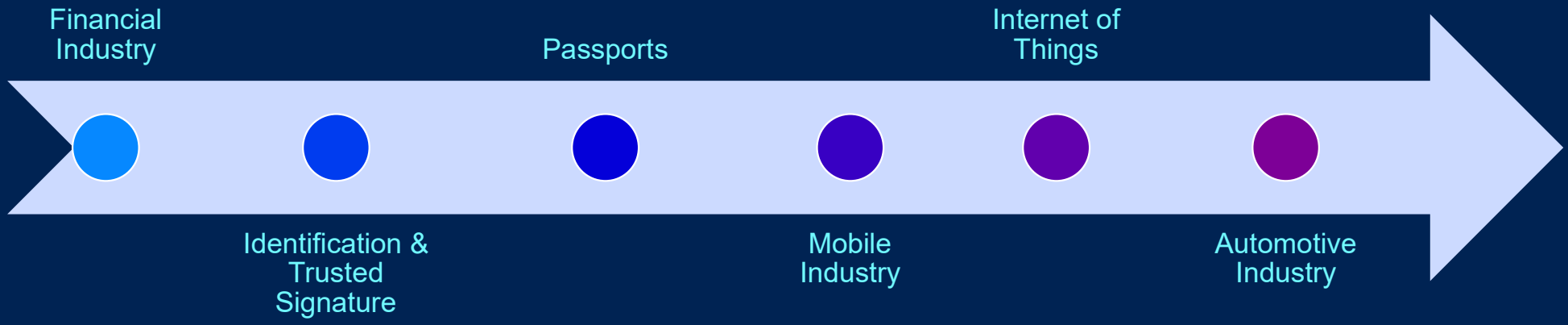
New Secure Channel Protocol SCP12

Conclusion

GlobalPlatform

THE standard for managing applications on secure chip technology, with over 25 years of experience

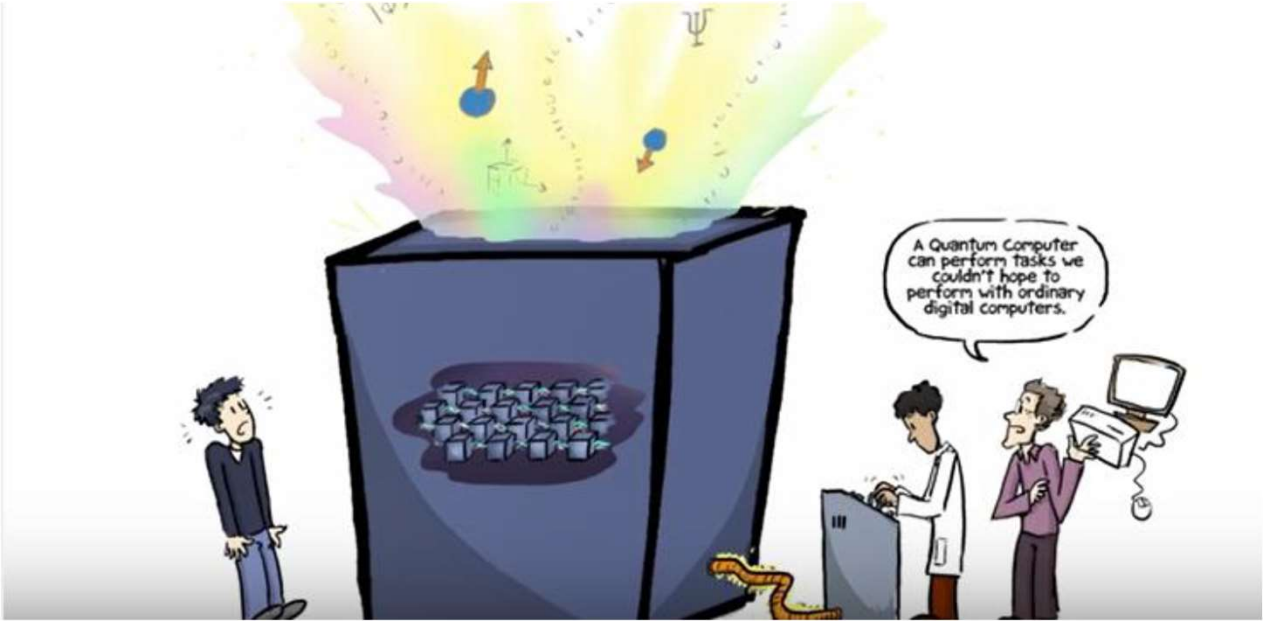
- **70 billion+ Secure Elements shipped worldwide are based on GlobalPlatform specifications**
- **Over 17 billion GlobalPlatform-compliant Trusted Execution Environment in the market today**



With 90+ Members, covering Silicon Providers, Software, Financial Services, Automotive Industry, Governments, Laboratories around the world

GlobalPlatform Specifications: https://globalplatform.org/specs-library/

Quantum computing, myth or reality?



Standardizing PQC Algorithms (not exhaustive!)

US – NIST & NSA

NIST PQC project

Russia

China

NGCC

S. Korea

KpqC

ISO/IEC JTC1
SC 27 WG2

IETF

ETSI Cyber QSC

Global Platform®

National Transition Regulations

Canada – Cyber Center
2031: high priority systems
2035: complete migration

US – NIST & NSA

2030: RSA/ECC deprecated
2035: Full transition to PQC
(non PQC-safe prohibited)

UK - NCSC
2031-2035:complete migration to PQC.

EU (18 Member States)
ANSSI : Increase algorithms size
Promotes Hybrid Crypto
Full transition to PQC **2035**.

Timeline for the transition to PQC

1. By **31.12.2026**:
   - At least the *First Steps* have been implemented by all Member States.
   - Initial national PQC transition roadmaps have been established by all Member States.
   - PQC transition planning and pilots for high- and medium-risk use cases have been initiated.
2. By **31.12.2030**:
   - The *Next Steps* have been implemented by all Member States.
   - The PQC transition for high-risk use cases has been completed.
   - PQC transition planning and pilots for medium-risk use cases have been completed.
   - Quantum-safe software and firmware upgrades are enabled by default.
3. By **31.12.2035**:
   - The PQC transition for medium-risk use cases has been completed.
   - The PQC transition for low-risk use cases has been completed as much as feasible.

Australia
2030: Full transition to PQC

PQC-able by 2030 – PQC Native by 2035

Global Platform®

GlobalPlatform Secure Element dependencies

- Secure Elements (SE), as standardized by GlobalPlatform and Java Card, are used in Payment, Mobile Networks, Government ID, …
- These infrastructures come with different requirements
- Therefore, our development depends on a range of external standards
  - NIST Post Quantum Crypto standards
  - IETF and ITU standards for X.509 or PKI infrastructure in general
  - ETSI / 3GPP / GSMA for security standards related to mobile communication (SIM/UICC)
  - ETSI and IETF for combiner functions in Hybrid solutions
- and Regulations
  - NIST, BSI, ANSSI, EU for security regulation and especially PQC transition
- …

GlobalPlatform Crypto Task Force

- « Cryptographic Algorithm Recommendations » document
  - See GP_TEN_053
  - The latest version 3.1 (May 2025) includes PQC algorithms and hybrid constructions
- Monitoring new trends
  - e.g., lightweight cryptography (ASCON for the next steps)
- Support the Committees and TFs on cryptographic topics
- Liaise with NIST, ISO/IEC JTC1 SC27 WG2, ETSI CYBER QSC
  - December 2024 to NIST: LS about SP 800-131Ar3 on the approval status of block cipher algorithms used for key wrapping
  - July 2024 to ETSI CYBER QSC: Request for details on hybrid schemes for KEMs

- What's in the revision
  - Definition of Hybrid PQC and Standalone PQC schemes
  - Legacy date (112 bits of security) moved to 2030
  - Deprecation of 3DES, SHA-224 and all ECC-224 based
  - Addition of NIST PQC algorithms ML-DSA and ML-KEM, with security strength category 3 and 5
  - Addition of LMS/XMSS
  - A new section on Hybrid construction, recommending KDF (HKDF, KMAC128 and KMAC256)
  - A new Annex for the comparison of legacy algorithms
  - A new Annex for ANSSI, BSI and ETSI recommendations on hybrid construction (for KEM)

GlobalPlatform Secure Element Committee

- GlobalPlatform main specification define how to establish a secure communication between an off off-card entity and the SE to perform management operations:
  - Load new keys
  - Manage applications in the SE (load, install, personalize, update, delete)
  - Load software updates
  - Configuration updates
- Transition to PQC means integration of PQC Signatures and Hybrid Signatures with the existing Card content management operations
  - Signing the load files, load data and the management commands
- Creating a new Secure Channel Protocol (SCP)
  - New protocol switching to KEM based Authentication and KEM based shared secret derivation
  - In Hybrid as well as PQ only modes

Constraints of Secure Element

SE specificities (compared to « computer »)

- Low computing capacity (CPU, RAM)
- Communication rates (pretty slow < 100 kB/s)
- Performance constraints (e.g., contactless banking transaction < 300 ms)

Performance can be improved with dedicated HW (e.g., RNG, AES block encryption, modular multiplication for RSA)

- Current Hardware has not support for PQC algorithm but next generation secure chips will

Security

- Specific side-channel / fault attacks, with impacting countermeasures (on performance, on RAM size…)

SE Committee – Crypto agility is the new mantra

- New crypto agile SCP04 Amendment K (symmetric secure channel protocol, June 2025)
  - SCP04 is composed of building blocks, configurable to allow for cryptographic agility of the protocol specification
- High level decisions for the new asymmetric SCP12
  - Crypto agility
  - Follow IETF wording for Hybrid and Composite mechanism
  - All new asymmetric schemes will support Hybrid (T/PQC now, in the future PQC/PQC), PQC standalone and Traditional
  - ML-DSA and ML-KEM as cryptographic primitives, with all security levels
- Two main documents are currently under discussion for PQC adoption
  - New Amendment P to the Card Specification to define new PQC certificates and signatures
  - New Amendment O to the Card Specification to define a new secure channel protocol based on PQC algorithms

Signatures and certificates

Signatures

- Combined Signature format from IETF https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-sigs/
  - Concatenation of the two Signatures
    - Traditional signature (RSA or ECC) with PQC signature (ML-DSA, FIPS 204)
    - In the future, it could be PQC signature with PQC signature
  - Weak non separability between the two Signatures
  - Specification allows to support new Signature algorithm and Signature format when they become available

Certificates

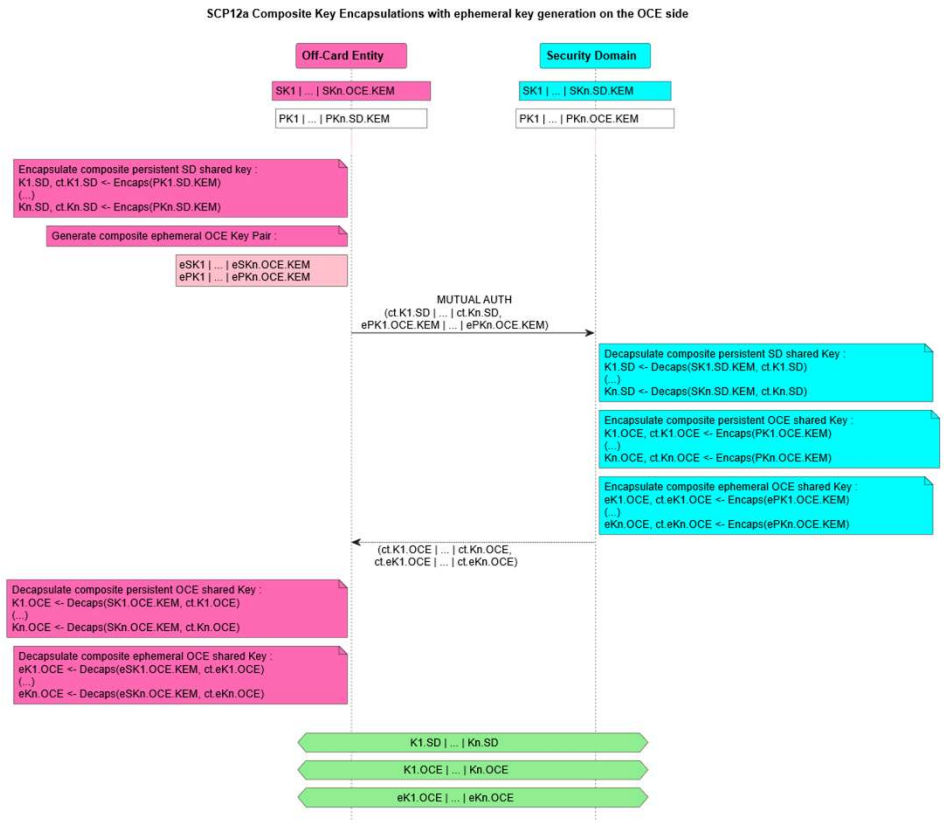
- Support of X509v3 certificates
  - To ease migration, we support Certificates with PQ or Hybrid PublicKey only signed by a Traditional Signature
- Certificates follow IETF specifications
  - Baseline is RFC 5280, waiting for IETF LAMPS Hybrid certificates with ML-KEM or ML-DSA keys

New Secure Channel Protocol SCP12

- Asymmetric SCP (based on challenge/response for authentication and key exchange for establishing the secure channel)
- For Hybrid KEM operation, the combiner function will be based on
  - ETSI TS 103 744 v. 1.2.1 (March 2025), "*Quantum-safe Hybrid Key Establishment*"
    - CatKDF
  - NIST SP 800-227 (September 2025), "*Recommendation for Key-Encapsulation Mechanisms*"
    - Focus is on Combiners that can be optimized for the memory constraints of the SE

SCP12 protocol with KEM

- Adoption of Key Encapsulation Mechanism is the main challenge
  - It means definition of a new protocol flow for the setup of a Secure Channel
  - Large amount of data within exchanges
- Design and optimization
  - ML-KEM keypair generation and decapsulation
    - Private key based operations are SE costly operations
    - SCP12 requires only one ML-KEM decapsulation operation on the SE side
    - Ephemeral ML-KEM key-pair generation to ensure forward secrecy is done outside the SE
  - SCP12 Mutual Authentication
    - PQC key, signature, certificates and ciphertext are much bigger than traditional crypto components
    - Authenticated KEM reduces the overall amount of data exchanged between the terminal and the SE
- Agility is a core requirement to adapt to new algorithms
  - Configurability will allow to adopt new algorithms in the future



Global Platform®

Key takeways

- Migration takes time and maybe complex
  - 2030/2035 is an aggressive target
- Crypto agility is key
- Ecosystem is large, standardization is not yet fully ready
  - *Store now, decrypt later* attack is a priority
- Hybrid is key for European markets
  - Configuration allows for standalone PQC or hybrid PQC
- SE constraints imply optimizations

GlobalPlatform is committed to provide updated specifications on time,
to allow its members deploy quantum-safe products, compliant with worldwide regulations

Global Platform®


Global
Platform®
Securing the digital future
globalplatform.org