PCI Security Standards Council®

2025 EUROPE COMMUNITY MEETING

2025
EUROPE
COMMUNITY
MEETING

Hybrid Quantum-Safe Authentication in Digital Payments

Ensuring Security in the Quantum Age

PCI Security Standards Council

Dr. Kalpana Singh

Expert in Cryptography and Blockchain privacy

Cryptography expert

Worldline

Isil Ugurlu

CISM, PCIP

Head of PCI Program

Worldline

Worldline

Worldline is a **global payments technology company**

We cover the full payments value chain. And more.

- **#1 PSP** in Europe and #4 worldwide.
- **131M+ active cards** under management.
- **Over 1.4M customers** in **170+ markets**.
- **~ €250M** annual investment in products & technology.
- Global tech community of **7000+ engineers**.
- **100+ products**, backed by **180+ patents**.

PCI Security Standards Council

Agenda

- Overview of the Importance of Cryptography in Payments
- The Threat Landscape: Quantum computing risks to current cryptographic methods
- Global Perspectives and Transition Strategies for Post Quantum Cryptography (PQC)
- The Need for **Post-Quantum** Authentication Solutions
- Challenges & Takeaways

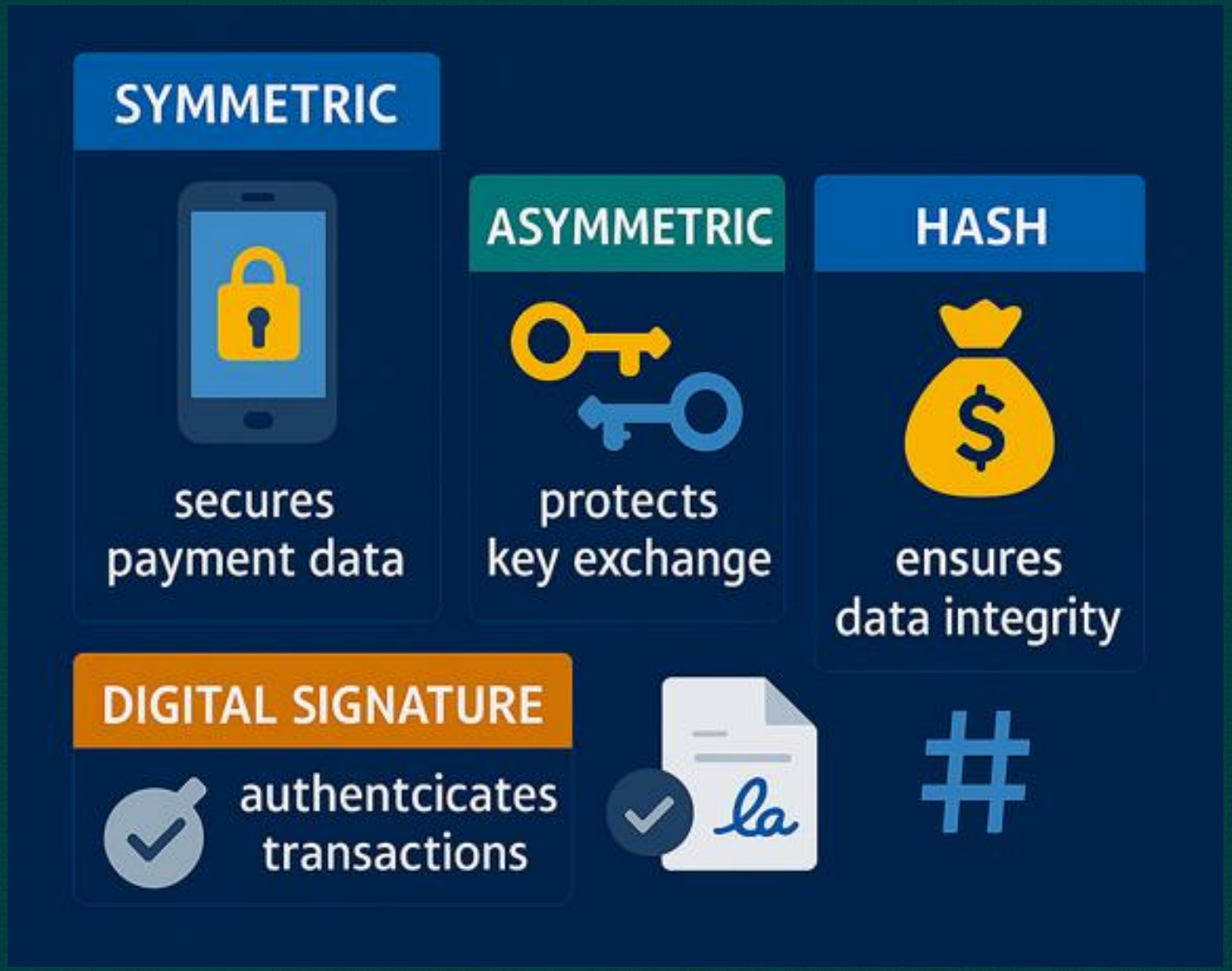
PCI Security Standards Council

The Uses of Cryptography in Payments

- SSL/TLS
  - Used in online banking, e-commerce, and
  - payment gateways.
- EMV Protocol (EuroPay)
  - Uses cryptography for card authentication
- 3-D Secure Protocol
  - Uses cryptographic challenge-response
- ISO 20022 and SWIFT Protocols
  - cryptography for secure messaging and authenticity.
- Cryptography in Mobile Payment Protocols
  - Near Field Communication (NFC) payment protocols
- Digital wallets

PCI Security Standards Council

Cryptography Algorithms in Digital Payments



PCI Security Standards Council

Quantum Threats

Current Digital Payment Systems

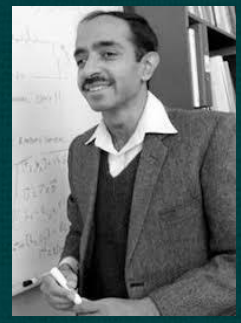
PCI Security Standards Council

Impact of Quantum Computer on Cryptography

A large-scale quantum computer **can break cryptography that's in use today**.

Algorithm	**Shor (1994)**	**Grover (1996)**
Impact	Asymmetric Cryptography	Symmetric Cryptography
Consequence	No longer secure	Easier to break than expected

P. Shor



L. Grover

- Quantum computers will have a **tremendous effect on the security of many cryptosystems that are massively deployed** all around the world.

PCI Security Standards Council

Quantum Threats

Current Progress in Quantum Computers

November 2022
IBM
claimed to have achieved to develop a 433 qubits quantum processor named Osprey

March 2023
Pasqal, a french start-up,
announced to have developed 100 qubits quantum processor

March 2023
Fujitsu and associates claim to have successfully develop the first Japan quantum computer with 64 qubits power

BY 2025
IBM
announced a 4000+ qubits quantum processor

By 2030
CNRS, INRIA and CEA
collaborate to develop quantum computing solutions

Global Perspectives and Transition Strategies for Post Quantum Cryptography

NIST

recommendation to transition to quantum-secure algorithms by 2030.

UK the National Cyber Security Centre (NCSC).

proactive strategy for transitioning to quantum-secure encryption

by 2035

The German Federal Office for Information Security (BSI)

emphasizes a risk-oriented approach to PQC migration, recommending that systems handling sensitive data be protected no later than the end of 2030

The European Commission

published recommendation on a **Coordinated Implementation Roadmap**, with timeline to begin national PQC strategies by end of 2026

PCI Security Standards Council

Success Metrics in Short-run

Cryptographic Inventory

NIST IR 8547 (2024) recommends organizations begin with a **comprehensive inventory** of cryptographic assets and dependencies

Risk Assessment

Conduct **risk assessments** to prioritize systems based on sensitivity and exposure to long-term data confidentiality threats.

Awareness Training

Cross-departmental training to build awareness of quantum risks and cryptographic agility

Pilot

ETSI TR 104 016 outlines the importance of **sandbox testing environments** to validate hybrid cryptographic implementations before production

PCI Security Standards Council

Post-Quantum Cryptography

Quantum-Safe Solutions

PCI Security Standards Council

Post-Quantum Cryptography Standards

Key encapsulation

Module-Lattice-Based KEM derived from **CRYSTALS-KYBER FIPS 203**

Signature

Module-Lattice-Based Digital Signature derived from **CRYSTALS-DILITHIUM FIPS 204**

Signature

Stateless Hash-Based Digital Signature based on **SPHINCS+ FIPS 205**

HQC was selected for standardization on March 11, 2025. NIST IR 8545

PCI Security Standards Council

Addressing the Challenges of Using Post-Quantum Cryptography

Impact of PQC on performance

PQ algorithm		Memory vs RSA/ECC
Signature	Dilithium	x5 to x8
Key exchange	Kyber	x4 to x6

Challenges in PQC

- Demand on memory & computation
- Manage lack of confidence in PQC
- Standardization and Interoperability

Current status

- Hardware with more RAM & power Impact on « 300ms »?
- Hybridation

PCI Security Standards Council

Hybridation

Towards Quantum-safe solutions

PCI Security Standards Council

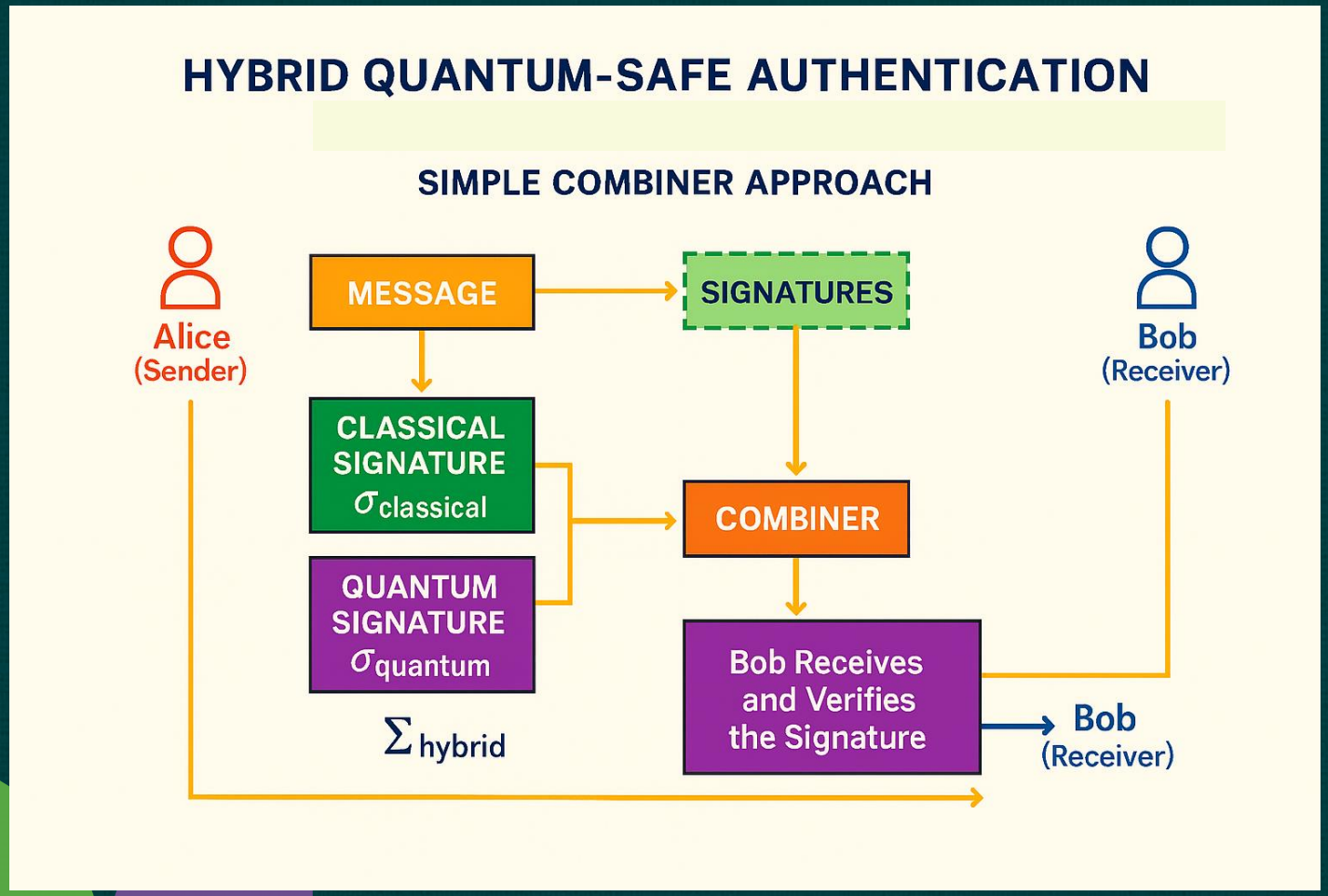
Hybridation

Towards Quantum-Safe solutions

Hybrid Quantum-Safe Authentication approach combines multiple cryptographic methods to ensure security against both current classical cyber threats and future quantum computing attacks

Hybrid Quantum-Safe Authentication

Simple Combiner Approach

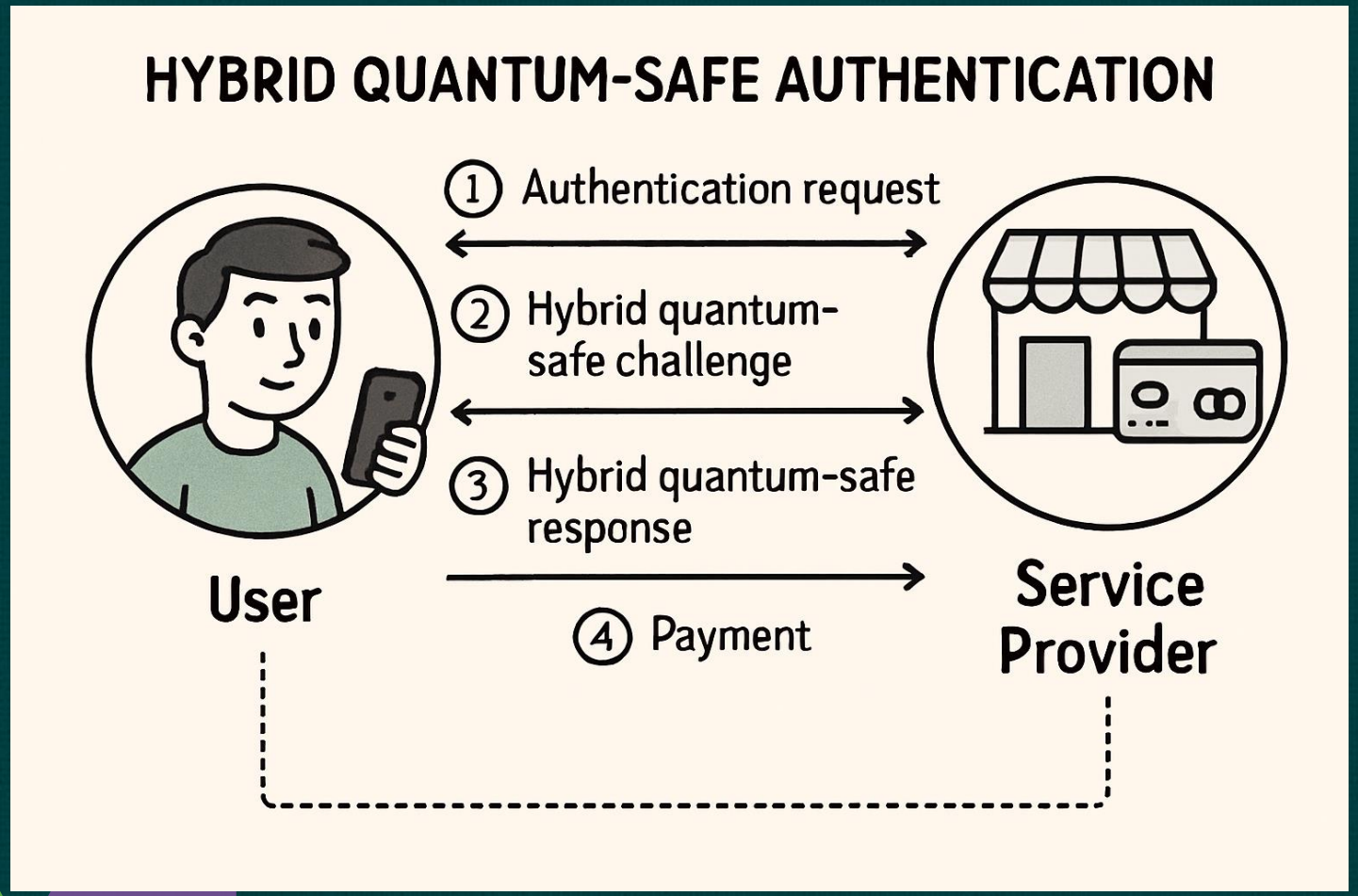


Benefits of Hybridation

- Future-proof security: Layered Security
- Gradual Transition
- Enhanced Integrity

PCI Security Standards Council

Hybrid Quantum-Safe Authentication in Payments



Integrating hybrid schemes into:

- Point-of-Sale (POS) terminals
- Mobile payment apps
- Payment gateways & backend systems

- Ensuring compliance with standards like PCI DSS

PCI Security Standards Council

Challenges for Companies in Payment

In implementation of Hybrid Quantum-Safe Authentication

- **Overarching Complexity and Scope of Migration**
- **Technology Maturity and Trust**

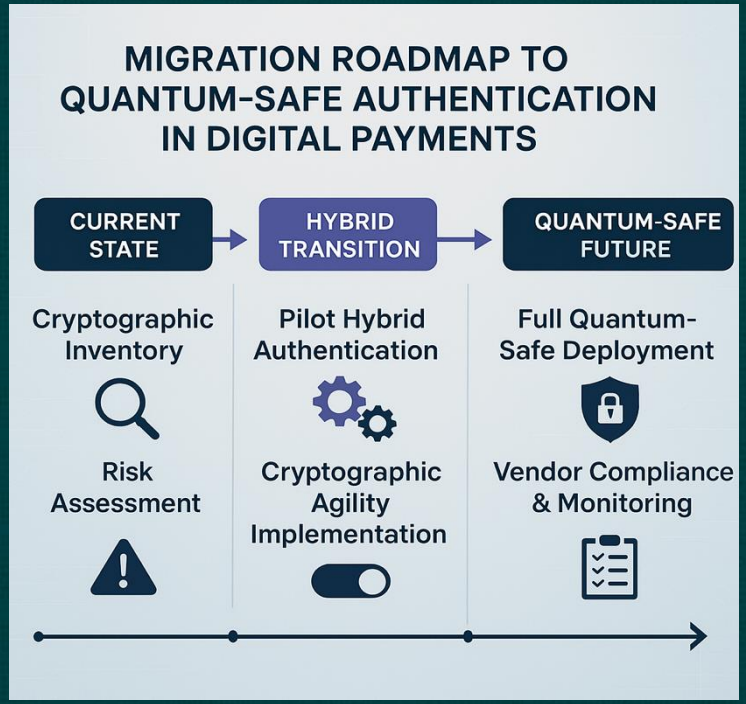
- **Impact on Specific Authentication Methods in Payments**
- **Integration and Interoperability with Existing Systems**

- **Regulatory and Compliance Pressure**
- **Significant Financial and Resource Investment**

Takeaways

Strategic Planning and Proactive Steps

- Risk Assessment
- Vendor Exploration
- Strategic Roadmap Creation
- Budget Alignment



- Develop cryptographic agility guided by the latest security research
- Create robust evaluation and testbeds
- Align and collaborate with standards bodies and governance

Long-term cryptographic strategy is an investment for future resilience

PCI Security Standards Council