Security Evaluation and Certification of Post-Quantum Crypto Implementations

Miquel Piris – Brightsight

European Conference on PQC Migration

December 3rd, 2025

brightsight

By SGS

Classification Policy: UNCLASSIFIED

Our numbers

10
Locations around the globe

50+
Security standards and schemes recognitions

40
Years of experience in security evaluations

250+
Security evaluation experts

700+
Security projects performed each year

High assurance security evaluation and certification

brightsight

By SGS

Agenda

01 PQC migration status

02 Implementation security

03 Certification

04 Challenges

05 Collaboration

06 Conclusions

brightsight

By SGS

PQC Standardization status and transition guidelines

NIST PQC Standardization Process (USA)

European Guidelines

PQC Standardization status and transition guidelines

1. **New algorithms** will be standardized to ensure **cryptographic diversity** and to meet **different application requirements**.

2. **EU** generally **adopts NIST-standardized algorithms** but **is not limited to them**.

3. Recommendations during the transition period:
   1. **Risk-based approach**
   2. **Cryptographic agility**
   3. **Hybrid cryptographic approaches** (classical + PQC)

4. **Secure implementation of PQC algorithms** is of critical importance.

5. The importance of **adapting certification schemes** to consider the quantum threat.

> *While **PQC algorithms** are inherently designed to resist quantum threats, their **implementation** can still be **vulnerable to practical attacks**, such as side-channel analysis (SCA) and fault injection attacks (FIA).*

Practical attacks against PQC implementations

- **NIST PQC standardization project** primarily focused on evaluating the **mathematical security** of algorithms.
- The **implementation security was largely left to developers and the community**.

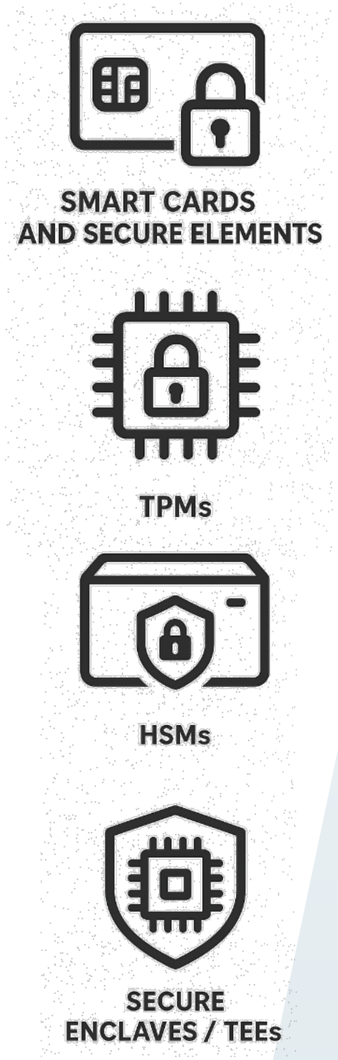
These attacks are of **important consideration for products that require high assurance.**

Side-Channel Analysis (SCA)

Passive attacks that **exploit information leakage** through power consumption, EM emissions or timing variations.

Fault-Injection Analysis (FIA)

Active attacks using techniques such as voltage glitches, laser pulses or EM pulses on a device to **introduce faults** aimed at bypassing security checks or extracting secrets.



brightsight
By SGS

Practical attacks against PQC implementations

Side-Channel Analysis (SCA)

- ML-KEM, ML-DSA: operations like **Number Theoretic Transform (NTT)** and **noise-sampling routines** can exhibit data-dependent leakages that allow **recovering secret coefficients** or **noise values.**
- Leakage sources include microarchitectural footprints from **polynomial arithmetic** and **timing differences in rejection-sampling loops.**

Fault-Injection Analysis (FIA)

- ML-DSA Signature Generation/Verification: **Faulting** during **nonce generation, coefficient computations**, or **rejection sampling** can lead to **signature forgery** or **key recovery.**
- ML-KEM Key Generation: **Faulting** during **sampling** or **matrix operations** can lead to **weak keys** or **secret key disclosure.**

PQC's **complex operations introduce new attack vectors** compared to classical algorithms. Moreover, **they have not yet been examined as thoroughly** as them.

brightsight
By SGS

Adapting Certification Frameworks for PQC

EU Cybersecurity Certification Scheme on Common Criteria (EUCC)

- **EUCC can be used** to evaluate and certify the security of **ICT products**, that implement cryptographic algorithms.
- ENISA publishes **State-of-the-Art (SotA) and Guidelines for EUCC evaluations:**

EU CC Common Criteria
CYBERSECURITY CERTIFICATION

ECCG Agreed Cryptographic Mechanisms

- Provides **recommendations regarding the cryptographic mechanisms** that should **preferably** be used **in ICT products** submitted to certification.
- Version 2 of this document **includes PQC algorithm recommendations**.
- Promotes **hybrid mode**: “This approach provides **assurance against the quantum threat** as well as assurance **against security issues** that might affect the **newer standardized post-quantum mechanisms**.”

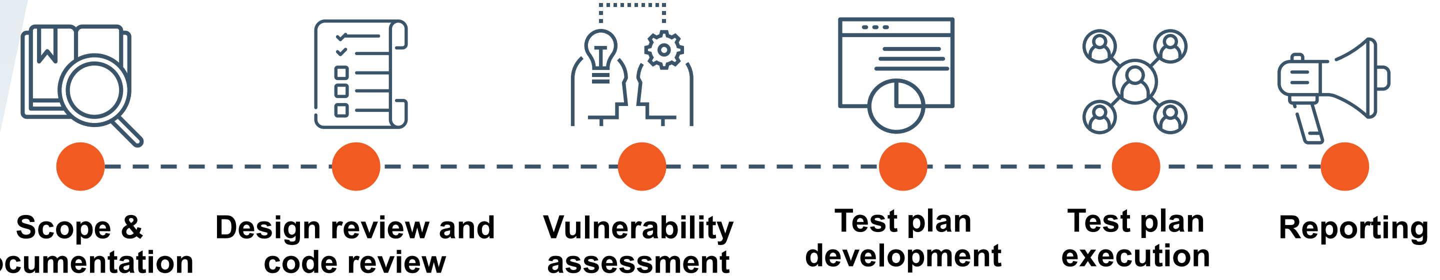
Security evaluations… Why?

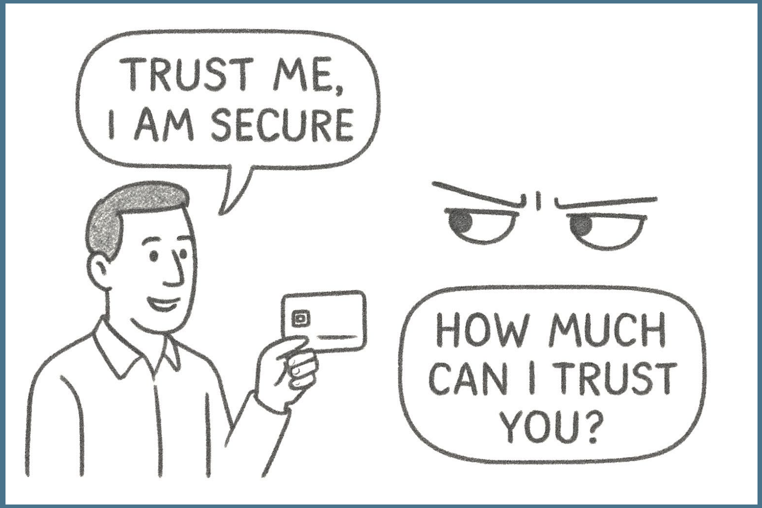
Developer:

1. **Develop PQC implementations** supported by robust security measures.
2. Define the **security claims** (e.g., ML-DSA, ML-KEM) of the product and **targeted assurance leve**l (EAL-1-7), which dictates the depth and rigor of the evaluation.

Third-party (ITSEF):

- **Independent Validation:** product's security claims are independently evaluated and verified by the lab.
- **Formal Process:** comprehensive approach that addresses both **theoretical and practical vulnerabilities**.





***EUCC evaluations** provide the **right methodology** to ensure that PQC solutions **follow the security standards**, while being robust and **secure against implementation attacks**.*

Status of PQC certified solutions

Brightsight had the honor to **evaluate the first ever secure IC implementing PQC** certified at the Common Criteria (CC) EAL5+ level.

Secure Sub-System (3S) integrated in a system-on-chip (SoC) following PP0117, for mobile applications, that **implemented ML-DSA**, as defined in FIPS204.

November 2024

TRUSTCB
TRUST AND VERIFY

Certificate

Standard: ISO/IEC 15408-1 :2009, -2 :2008, -3 :2008, Common Criteria for Information Technolo Security Evaluation (CC) v3.1 rev 5 and ISO/IEC 18045 :2008, Common Criteria Evaluation Methodology for Information Secur Evaluation (CEM) v3.1 rev 5

Certificate number: **NSCIB-CC-2300085-02**

TrustCB B.V. certifies:

Certificate holder and developer: **SAMSUNG Electronics Co. Ltd.**
IP Development Team
DSR, Samsungjeonja-ro 1-1, Hwaseong-si, Gyeonggi-Do, South Korea

Product and assurance level: **STRONGV4P00 of S5E9945 with Specific IC Dedicated Software Revision 1.2**
Assurance Package:
- EAL5 augmented with AVA_VAN.5, ALC_DVS.2 and ALC_FLR.2

Protection Profile Conformance:
- Secure Sub-System in System-on-Chip (3S in SoC), BSI-CC-PP-0117, Version 1.5, 28 February 2022

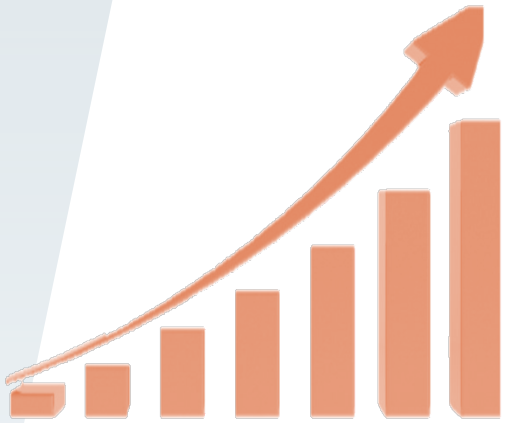
Project number: **NSCIB-2300085-02**

Evaluation facility: **SGS Brightsight BV located in Delft, the Netherlands**
Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5 (also published as ISO/IEC 18045)

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 5 for conformance to the Common Criteria for IT Security Evaluation versio 3.1 Revision 5. CC and CEM are also published as ISO/IEC 15408-1 :2009, -2 :2008, -3 :2008 ISO/IEC 18045:2008. This certificate applies only to the specific version and release of the prod in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme fo certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TrustCB B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TrustCB B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Validity:
Date of 1st issue : **26-03-2024**
Date of 2nd issue : **28-11-2024**
Certificate expiry : **28-11-2029**

Wouter Slegers, CEO
TrustCB B.V. Van den Berghlaan 48, 2132 AT Hoofddorp, The Netherlands



- **Very few products** implementing PQC have been **certified to date.**
- Brightsight sees an **increased adoption in products:**
  - **Several ongoing evaluations of products that will be certified in 2026.**
  - Developers requesting **preliminary security assessments** of PQC implementations that will be integrated in their **next generation ICs** to be certified.

brightsight
By SGS

Challenges in PQC Implementation

- **Risk assessment and product roadmap definition**
  Not easy in a changing eco-system, where requirements and constraints are often imposed by the market.
- **Fundamental constraints of embedded systems**
  These have tight limits on memory, processing power and energy consumption.
- **Increased Development & Testing Time**
  - **Performance Optimization:** PQC demands higher computational resources, often requiring hardware-accelerated implementations.
  - **Countermeasures Development:** Design and implement robust SCA and FIA countermeasures (e.g., masking, shuffling, integrity) specific to PQC operations.
  - **Testing secure implementations:** Requires extensive testing for correctness and security.

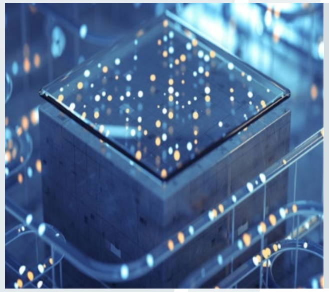
Smartcards & Secure Elements
Very limited memory and low clock speeds; PQC keys/signatures are large.

IoT Devices
Battery-powered; Higher PQC computation drains energy, low-power MCUs may struggle

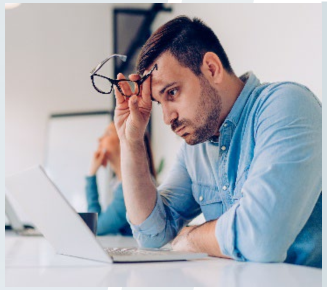
Network Devices
Multiple concurrent connections; PQC latency reduces throughput

Automotive systems
Safety-critical-real-time; PQC requires extensive validation

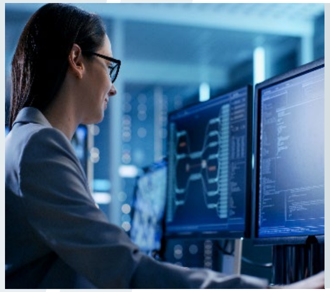
Challenges in PQC Certification



New Expertise
Need cryptographers and engineers specialized in PQC algorithms, their vulnerabilities and attack paths.



Methodology Adaptation
Develop and validate new test vectors, attack lists and evaluation methodologies tailored for PQC.



Tooling Development
Tools need to be upgraded to offer support for PQC algorithms and attacks against them.

Knowledge Sharing
Collaboration in industry working groups to facilitate recognition of PQC certifications.

R&D
State-of-the-Art monitoring and development of new attacks targeting PQC algorithms.

New Schemes / NCCAs Guidelines
Follow new guidelines on PQC implementations and migration.

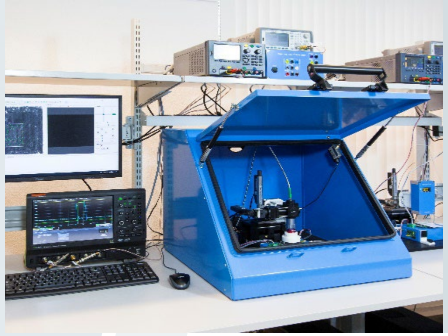
brightsight

By SGS

How can Security Labs support Developers?

Workshops and Trainings

To understand evaluation **requirements** or **technical** security trainings.

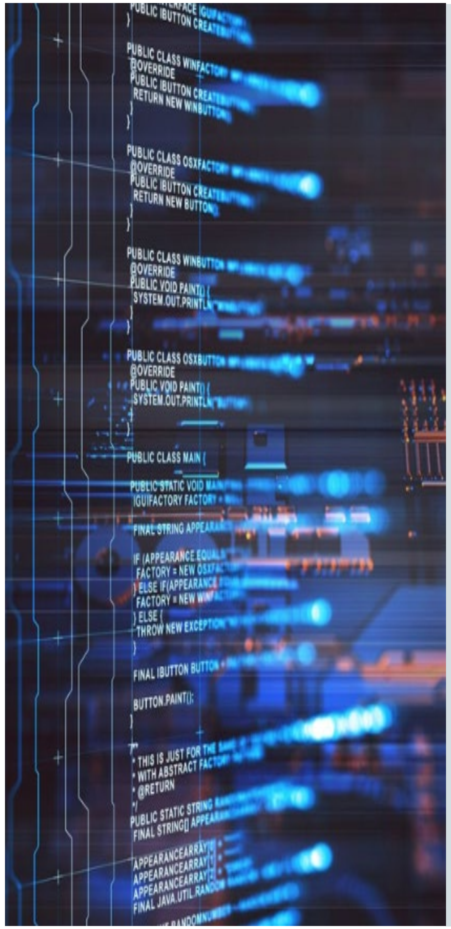


Testing

SCA and FIA testing of PQC implementations to meet the expectations of high-assurance evaluations.

Certification Readiness

Support for teams **preparing** for formal evaluations including PQC solutions.



Implementation Review (Hardware & Software)

Source code review to identify architectural flaws, implementation pitfalls, and **potential vulnerabilities before physical testing.**

Vulnerability assessment considering the latest **State-of-the-Art in attacks** on PQC implementations.

Conclusions

The **roadmaps** for the transition to PQC are set.

Collaboration among developers, labs, and certification authorities is a must.

Significant **implementation challenges** are present, especially in resource-constrained embedded systems.

Security evaluations where the implementation security against SCA and FIA is verified are essential.

Past cryptographic transitions have taken >10 years, so **start** integrating PQC solutions now.

Security labs like **Brightsight can support** developers in their PQC migration.

The **hybrid approach** is the most recommended now and the one proposed by national schemes.

brightsight

By SGS

Thank you! Questions?

Contact us:
miquel.piris@sgs.com
brs.sales@sgs.com
+31 (0) 15 269 2500
www.brightsight.com

brightsight
By SGS

Building digital trust

brightsight

By SGS