Certified physical security of PQ solutions

Peter Pessl

3.12.2025

Embedded Security Controllers

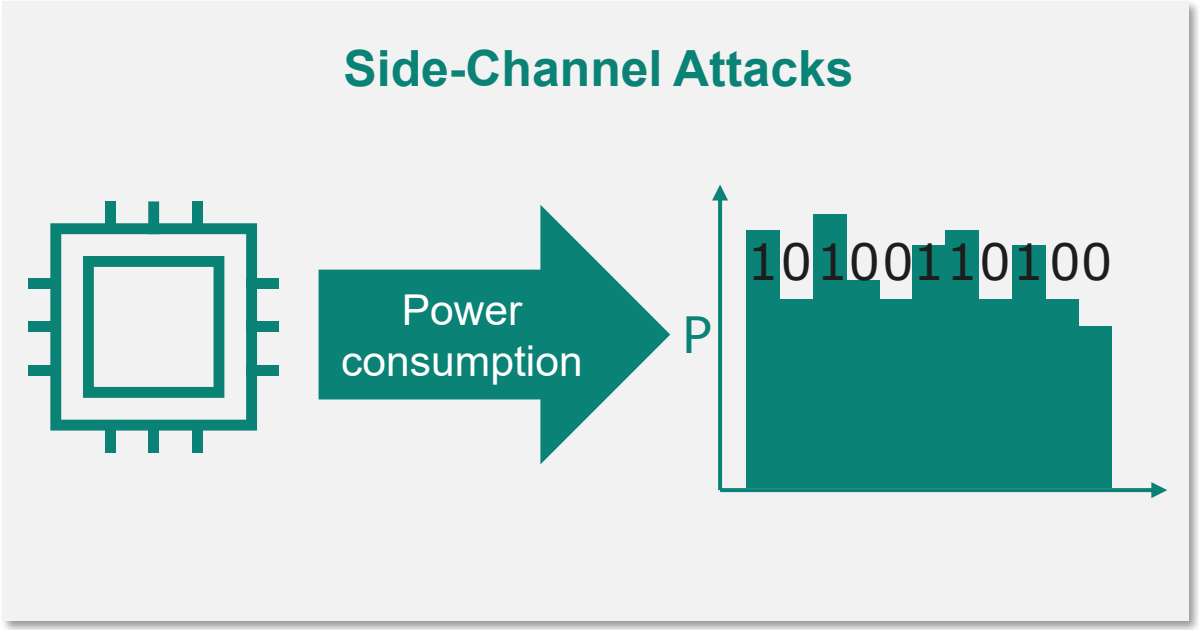
…enable a plethora of applications

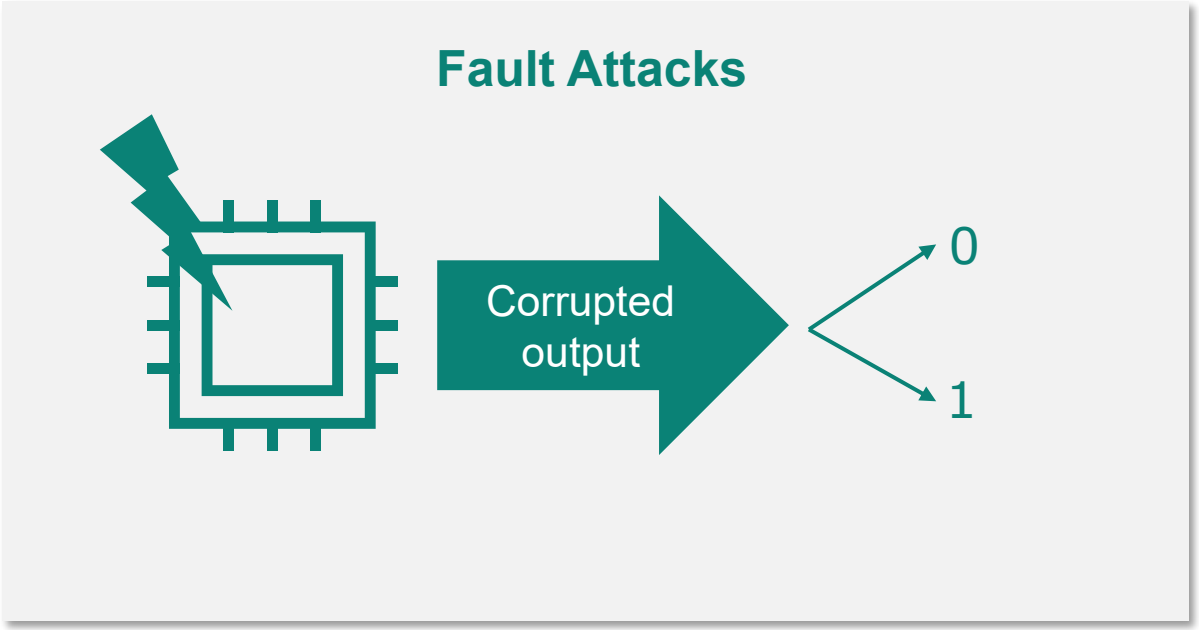
- from SmartCards (eID, payment, eHealth, ticketing, …)
- to embedded security (eSIM, FIDO, TPM, …)
- and IoT (industrial sensors, smart meters, …)

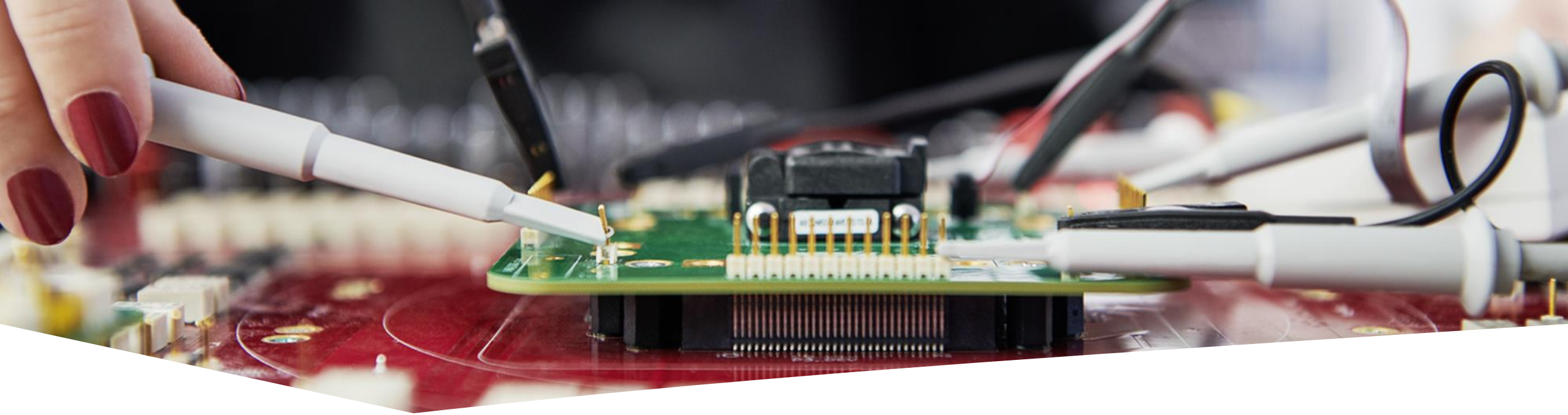
…need to fulfill high security requirements

- to provide security-relevant features, they need to support a huge range of cryptographic services, now including PQC
- provide resilience against unauthorized extraction of sensitive data (personal data, encryption keys, …)

Implementation/physical attacks on cryptography







Implementation Security of PQC: a Pressing Matter

- Security ICs and applications with considerable development efforts and long lifetimes
  - typically difficult to patch software, cannot patch hardware
- Requires holistic security concepts as well as
  - anticipation of future attacks
  - while fulfilling stringent resource requirements
- Need strong evidence for achieving security targets: **certification**

Certification landscape

- Large range of possible scopes: functional correctness, logic (SW-based) attacks, **physical security**
  - range of certification depths also for physical security

- IoT certification schemes covering physical security
  - Platform Security Architecture (PSA) Level 3 + Level 4
  - Security Evaluation Standard for IoT Platforms (SESIP) Level 3

- High-security (SmartCards etc.) certification
  - Common Criteria (CC) with “Security IC” protection profile, EAL5/6, AVA_VAN5 penetration testing
  - … sophisticated attack setups, extensive penetration testing with long-running evaluations

Infineon and the BSI pave the way for a quantum-resilient future: World's first Common Criteria Certification for post-quantum cryptography algorithm on a security controller

Jan 23, 2025 | Business & Financial Press

First CC certificate for a security controller running secured ML-KEM (Kyber)

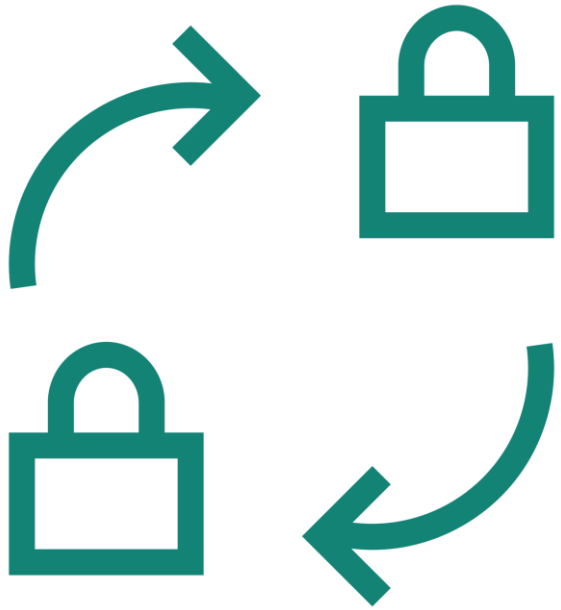
Recently: CC certificate for a security controller running ML-KEM and ML-DSA (Dilithium)

Understanding the attack surface

- Huge body of work analyzing threats and novel attack paths
  - large number of (academic) publications, including our contributions

- Fundamentally different algorithms → fundamentally different attack landscape
  - side-channel attacks more akin to those on symmetric cryptography (rather than those on RSA/ECC)
  - fault-attacks still underdeveloped

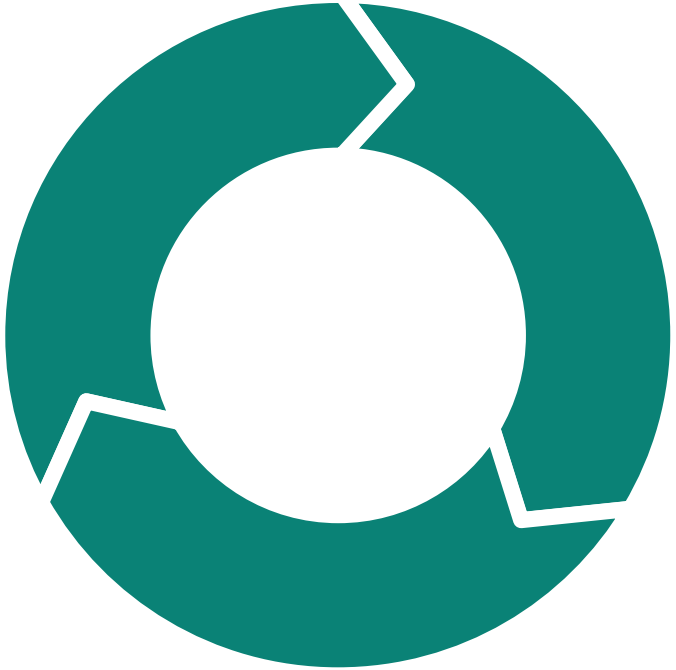
- New attack settings/targets can emerge, e.g., “re-encryption”
  - re-encryption used by ML-KEM to prevent certain cryptographic attacks
  - enables powerful side-channel attacks using chosen ciphertexts
  - implicit hardening against fault attacks, but dedicated attacks still possible



Types of operations within ML-KEM/ML-DSA

Hashing (SHA3/SHAKE)

– short seeds to long pseudorandom sequences



Pre/postprocessing

– non-linear processing of integers
– decoding (range checks), compression, comparison, random sampling…

Polynomial/modular arithmetic

– polynomials/vectors of integers modulo a fixed q (12/23 bits)
– modular multiplication, modular addition etc.
– RSA/ECC: a few very big integers vs.
ML-KEM/ML-DSA: a large number of smaller integers

Countermeasure Toolbox

- Hiding
  - weaken the link between processed values and side-channel leakage
  - example: shuffling order of element-wise operations in a large vector
- Masking
  - break link between secret value and processed value

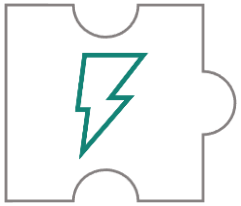
    …by splitting a sensitive value into two or more randomized shares,

    e.g., $r = r^{(0)} + r^{(1)}$

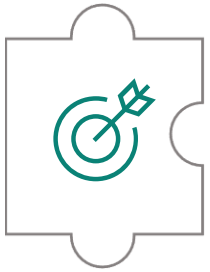
    …operate on shares such that they are never directly combined
- Redundancy
  - integrity protection by adding/checking redundant information
  - generic example: double computation

High-Level Challenges in Protecting ML-KEM/ML-DSA

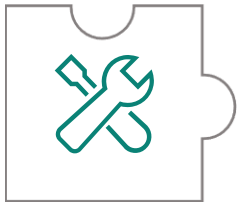
All algorithm components need to be considered
- different operation profiles, protection requirements and approaches
- require seamless protection without gaps at interfaces
- several different components are significant contributors to runtime



No “nice” algorithmic faulting countermeasures covering entire algorithm
- fault-sensitivity not fully researched, let alone countermeasures
- generic “double computations” is expensive in SW and might not be sufficient



Defense-in-depth with limited resources
- at each point in time: layering of countermeasures
- without incurring inhibitive costs (runtime, memory, etc.)

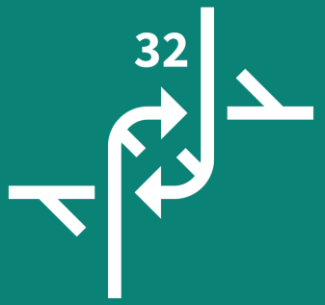


Provide high level of flexibility
- different customer requirements
- cryptographic agility and updateability

Our approach: secured SW and hardened HW

→

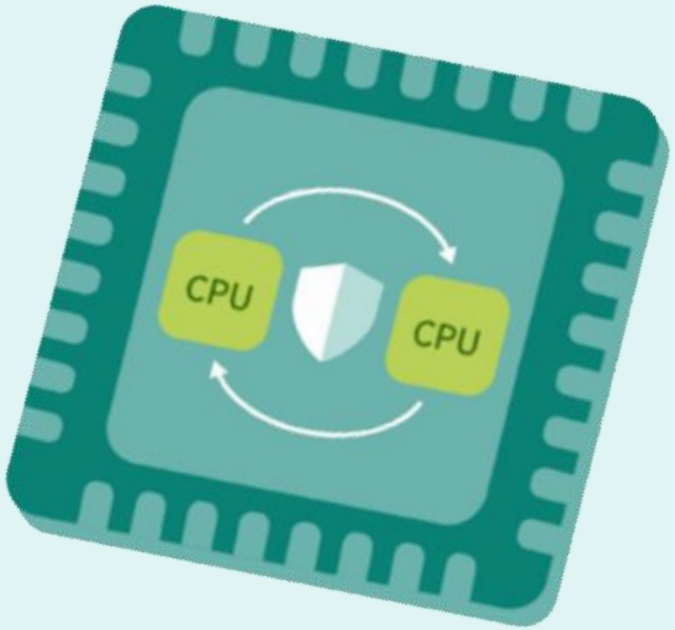
Software for the TEGRION platform with Integrity Guard 32



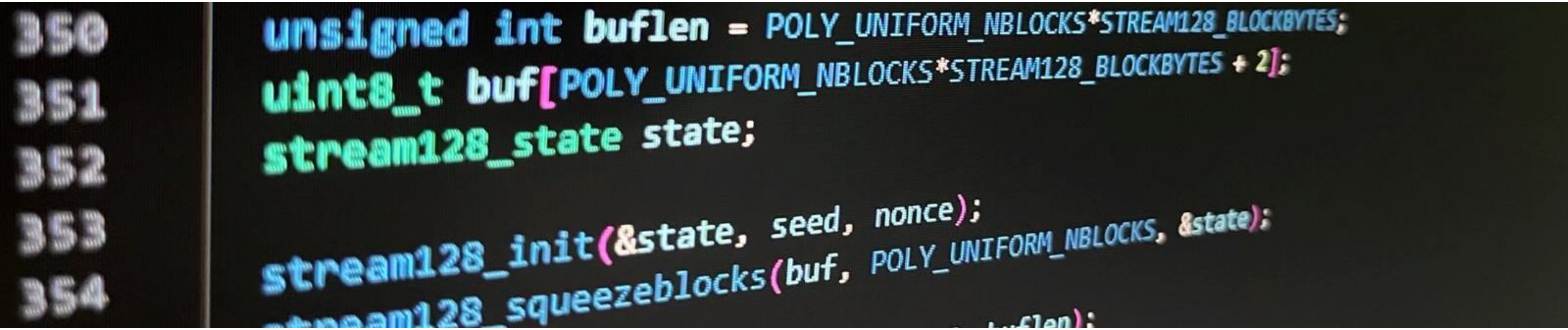
Integrity Guard 32

TEGRION with Integrity Guard 32

- Arm®v8-M compliant security controllers
  - custom design, thanks to ARM architecture license
- Comprehensive integrated fault-detection capabilities
  - e.g., self-checking dual-core design,
    error detection/correction codes
  - dealing with fault attacks on the hardware level
- Features supporting development of hardened SW
  - e.g., encrypted memories, custom instructions,
    architecture enabling efficient SW-masking
  - strong foundation for developing hardened SW



Software Design



- Software countermeasures built atop the hardware features
  - masking, hiding, etc.,
  - innovative countermeasures making best use of hardware capabilities
  - countermeasure layering throughout algorithm execution

- Optimized tradeoffs
  - physical security, runtime, temporary memory requirements (RAM), codesize (NVM), …

Certification and Conclusion

Bundesamt für Sicherheit in der Informationstechnik

Deutsches IT-Sicherheitszertifikat
erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1249-2024 (*)

Smartcard Controller

IFX_CCI_000068h, IFX_CCI_000080h design step G12 with firmware version 80.505.04.1, optional PQ Crypto Suite v5.00.012, optional HSL v04.05.0040, optional UMSLC v02.01.0040 and user guidance documents

from	Infineon Technologies AG
PP Conformance:	Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 6 augmented by ALC_FLR.1
valid until:	16 December 2029

SOGIS Recognition Agreement

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations, by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents as listed in the Certification Report for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 5.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) 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 the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria Recognition Arrangement recognition for components up to EAL 2 and ALC_FLR only

Bonn, 17 December 2024
For the Federal Office for Information Security

DAkkS Deutsche Akkreditierungsstelle D-ZE-19615-01-00

Sandro Amendola
Director-General

L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

Certified Devices

- Dec. 24: **First CC-certificate for ML-KEM** on a security controller (Security IC Platform Protection Profile, Assurance Level EAL6)
- Oct. 25: CC certificate for contactless (dual-IF) security controller with ML-DSA and ML-KEM library

Conclusion

- Providing hardened solutions for PQC is a pressing matter
- … and comes with many challenges
- … but first certified solutions are ready, enabling a timely transition


Infineon