

Security in the era of quantum computing technology

Tackle the massive quantum computing challenge

public

Quantum computers – far beyond just theory

- In January 2019, IBM presented the first commercially usable quantum computer i.e. outside of laboratory environments – the IBM Q System One
- Classical bits only know the state 1 or 0, a qubit can assume any superposition of the states "0" and "1"
  → This enables true parallelism in computing
- Quantum computers can solve special tasks in seconds while it would take conventional supercomputers many years to accomplish

Classical bit



Quantum bit



Copyright © Infineon Technologies AG 2025. All rights reserved.

Current cybersecurity measures may soon be inadequate

Due to the specialized computing capabilities of quantum computers, some common cryptographic ciphers will be almost useless soon

- **Asymmetric encryption algorithms** used today (e.g. RSA or ECC) will no longer be considered appropriately secure anymore:
  - For instance, the security of RSA relies on the difficulty of factoring the product of two large prime numbers (prime factorization)
  - With adequate key length used, prime factorization would be impractical on a conventional computer, while a suitable quantum computer could solve it in minutes, making unauthorized extraction effortless
- **Symmetric encryption**, such as AES, is considered less threatened by quantum computers. However, for higher security levels it is recommended to use longer keys, such as AES-256

Example

Prime factorization of an RSA encryption with a key length of 2,048 bits



Conventional computer	Quantum computer
~ 100,000 years	**< 2 minutes**

Source: EY

Copyright © Infineon Technologies AG 2025. All rights reserved.

The technology is not yet ready. So, no reason to worry?

Quantum computers **currently** only achieve a performance of around **10 – 40 high-quality qubits**

This is only around 0,3 – 1% of the amount required to crack current cryptography (*RSA 2048*)

However

The first universal **quantum computers** capable of breaking main encryption methods used today could be ready as early as **2030 – 2035**

Source: German Federal Office for Information Security (BSI)

Copyright © Infineon Technologies AG 2025. All rights reserved.

Thinking about tomorrow today



Harvest now – decrypt later: Attackers are already collecting and copying data today, to decrypt it tomorrow using quantum systems



Threat especially for sensitive data from governments and public institutions

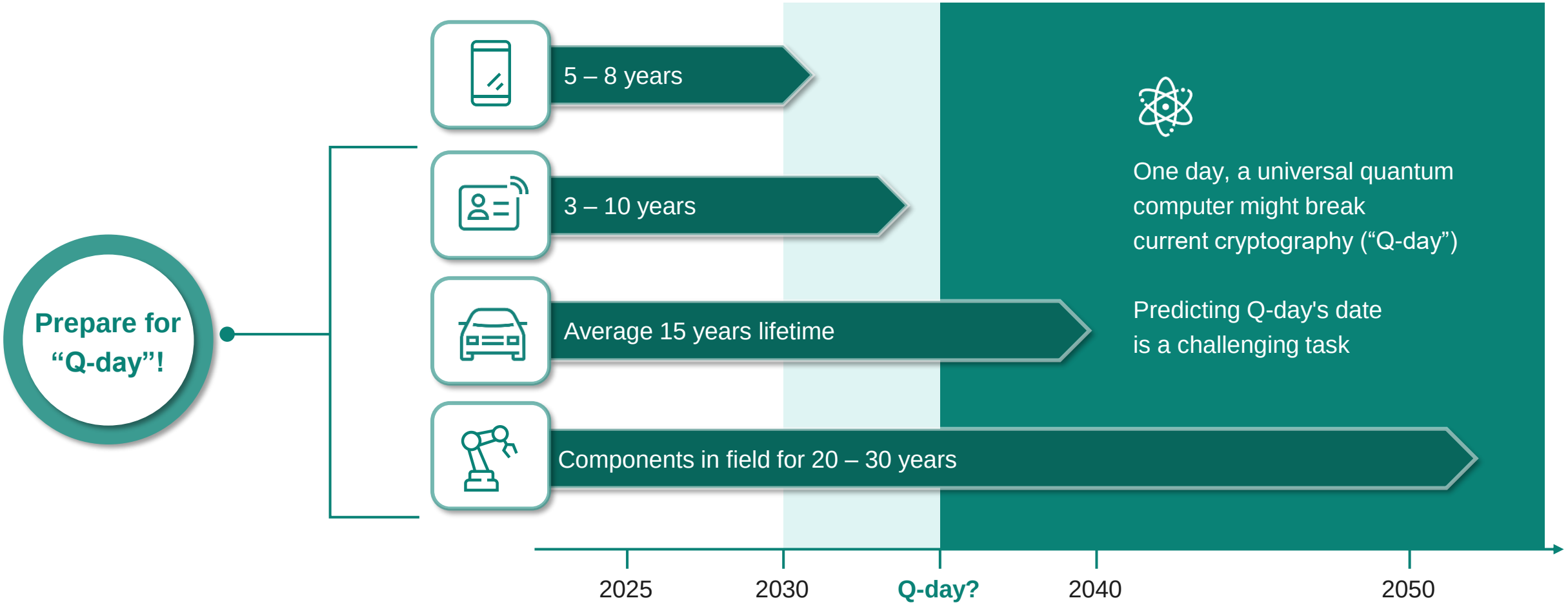




Threat to products with long research and development cycles, such as in the automotive, aerospace and life sciences sectors

Copyright © Infineon Technologies AG 2025. All rights reserved.

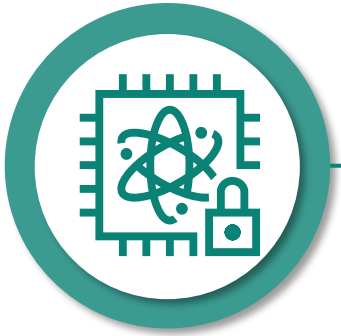
Assets with a long service life are particularly at risk



> Devices with over 10 years lifecycle must be prepared for the quantum computing age

Copyright © Infineon Technologies AG 2025. All rights reserved.

Post-quantum cryptography (PQC)



- Use of algorithms that are not threatened by prime factorization or other mathematical problems with similar complexity (e.g. discrete logarithm)
- Can be implemented on conventional hardware
- The first standards developed through a process organized by the US NIST were published in August 2024

Copyright © Infineon Technologies AG 2025. All rights reserved.

The quantum computer evolution does not wait. Deploy PQC-ready products today

The infrastructure challenge

- Any major change in larger infrastructures is complex and a long-term activity
- A full transition from today's cryptography to PQC will be gradual and typically require several years

Quantum computers evolution will not wait

- The threat of a quantum computer will not wait until all infrastructures are migrated and quantum-secured
- An expensive exchange of existing non-quantum secured products in the field needs to be avoided

The solution: Deploy today and update later

- PQC-ready hardware should be already deployed today (with sufficient computing power and memory configuration)
- The products (hardware and software included) need to be prepared for field-updates and crypto agility
- Once all standards and infrastructures are established, an easy and rapid transition to PQC can be performed

Field Update

Quickly and easily update embedded software (i.e. Operating systems) for already field-deployed products

Crypto agility

Quickly and easily exchange cryptographic functions without significant disruption

Copyright © Infineon Technologies AG 2025. All rights reserved.

Leading the way in post-quantum security

Infineon has been working with customers, partners and the academic community on all facets of PQC for years

- **As early as 2017**, Infineon implemented a post-quantum key exchange method based on the "New Hope" algorithm on a commercially available chip for contactless smart cards
- **Since 2018**, Infineon has been actively involved in several funding projects and has published numerous pioneering papers
- **In 2022**, Infineon released a quantum-resistant firmware upgrade path for OPTIGA™ TPM
- Infineon actively contributed to the development of the **SPHINCS+** stateless hash-based signature scheme, which has recently been **standardized by NIST as SLH-DSA**
- **December 2024, World's first Common Criteria Certification** for post-quantum cryptography (ML-KEM) on a security controller

Copyright © Infineon Technologies AG 2025. All rights reserved.

Infineon is ready: Worlds first CC certificate for PQC (ML-KEM)



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

SOGIS Recognition Agreement

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

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

Certification in December 2024

- **World's first CC-certificate for ML-KEM** on a security controller
- **Common press release** with German Federal Office for Information Security (BSI)

> The BSI consistently supports and demands the switch to post-quantum cryptography in order to make files and applications secure in the long term. **The availability of quantum-safe IT products, which can also be found in numerous everyday applications, is therefore a real milestone!**
>
> *Claudia Plattner, President of the BSI*

Copyright © Infineon Technologies AG 2025. All rights reserved.

Infineon – your trusted advisor for the PQC landscape

First market player to offer hardware with dedicated PQC coprocessor

Infineon TEGRION™ product family of next gen security controllers with Integrity Guard 32 for long-lasting security and superior fault protection

Partnering with customers, partners, and the academic community to prepare for a post-quantum future

Global team of experts and researchers dedicated to the PQC field

We can help you to bridge the gap between quantum theory and practical application

Copyright © Infineon Technologies AG 2025. All rights reserved.

Achieve future-proof security in the era of quantum computing now!




Infineon