hitex

AURIX KNOWLEDGE LAB 2024

ETAS HIGHTEC imagimob An Infineon Technologies Company

infineon pls Development Tools TRUST IN SOFT

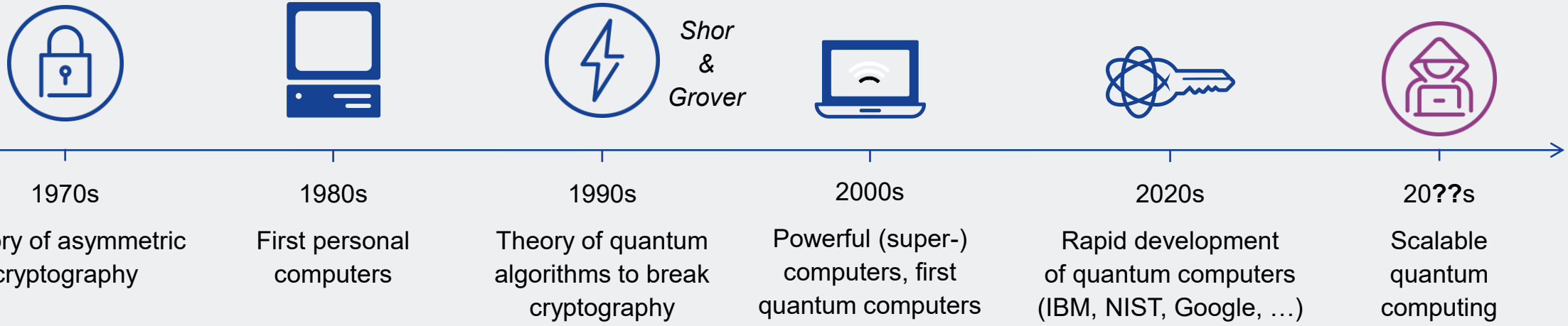
Post-quantum cryptography - ESCRYPT CycurHSM for TC4xx

Rohan Pandit, Product Manager ETAS

ETAS

Evolution of quantum computing

The quantum threat



Increasing system complexity

Increasing connectivity

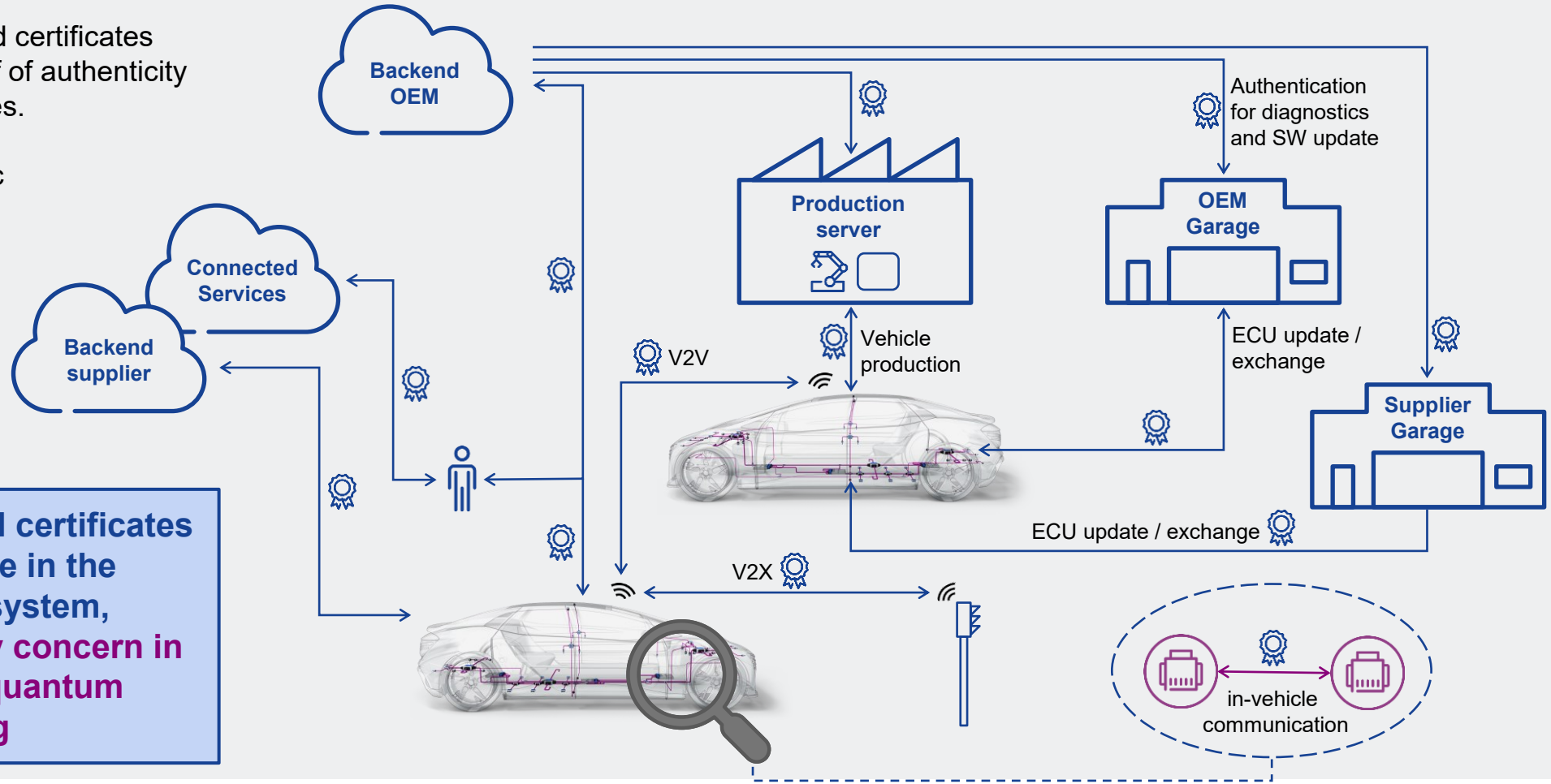
Increasing advances in quantum computing

Fields of Application in the Automotive Security

Example communication flow for a future car

Digital signatures and certificates used to provide proof of authenticity for all these use cases.

→ Flow of cryptographic information/material



Digital signatures and certificates play a central role in the automotive ecosystem, but are main security concern in the presence of quantum computing

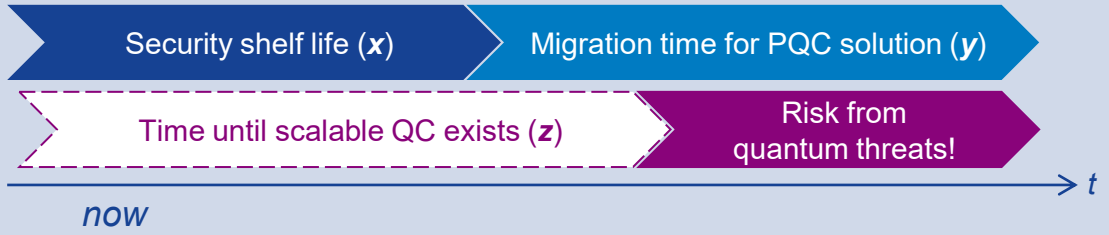
When do we handle the situation?

A decision based on limited information

Mosca's Theorem: Time to react (t)

- Your product lifetime (x) and migration time (y) **is foreseeable**
- Time until scalable Quantum Computing exists (z) **is uncertain**

Do not let quantum technology get ahead of your timeline!



Act now!

- **First standardized algorithms are available**
  - NIST selection of encryption and signature schemes (2022)
  - Early selection of stateful signature schemes
- **Recommendations of national institutes already exist**
  - BSI Handlungsempfehlung / Technische Richtlinie
  - AVID PQC Migration Handbook [4]
  - NIST Migration Project [5]
- **Remaining problems**
  - Algorithm selection is ongoing and difficult, there is **no scheme that fulfills all requirements**
  - General confidence in cryptography can only grow over the years

ETAS recommendation:
"Act now and wait"

Security threats based on quantum computing

Current trends in automotive security based on quantum computing

Reduced security due to quantum computing

– Lowers the security level of AES by factor 2

– Easy to break all existing asymmetric crypto algorithms (ECC, RSA)

Updated OEM specifications

– Major OEM‘s (e.g. Daimler) include Post Quantum Cryptography(PQC) in their security requirements for future vehicles

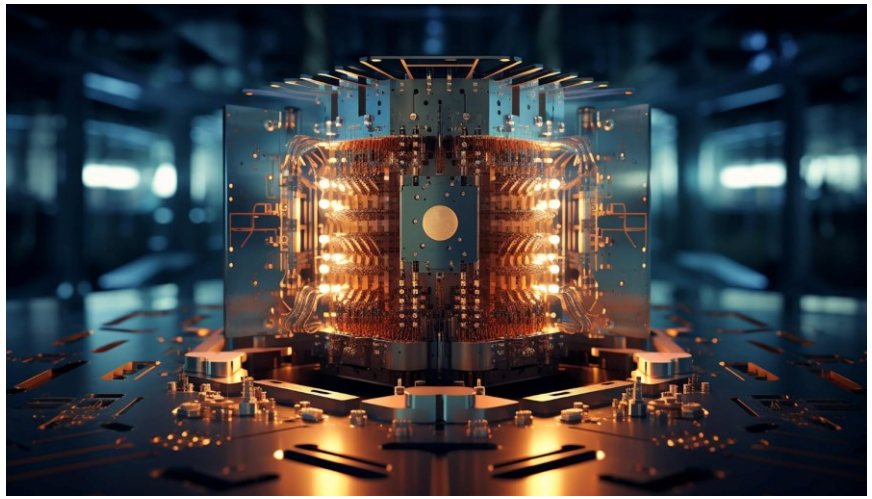
Leads to the need for

– New crypto algorithms prepared for quantum computer attacks

– Crypto agile solutions to ensure robust security throughout the long lifetime of ECU’s

– Several PQC algorithm candidates selected by NIST

  – Hash tree based, Code based, Lattice based => Major processing load for hashing (SHA2-256, SHA3,..)



What actions can we start with?

Resolutions using ETAS security expertise and product portfolio

Consulting services:

- Project partner in funded research project FLOQI (Full Lifecycle PQ PKI)
  - Analysis, research, development, benchmarking towards a quantum computer-resistant public key infrastructure(PKI)
- Guidance for management (workshops, recommendations on points of action, establishment of a timeline, etc.)
- Development of specific technical quantum safe solutions (analysis of specific systems, design of migration and transition solutions e.g., for PKI or key management)

Software solution:

- ETAS offers a cryptographic library i.e. ESCRYPT CycurLIB which already supports
  - PQC CRYSTALS-Dilithium (PQC Signature Algorithm)
  - CRYSTALS-KYBER (PQC Key Exchange)
- Sphincs+(PQC Hash based signature): Outlook 2025

PQC algorithms accelerated by Aurix TC4x security cluster

Escrypt CycurHSM 3.x + Aurix TC4x solution

Cyber security satellite (CSS) for parallel computation*

- Parallelization of HW accelerators to avoid performance bottlenecks by
  - Increasing throughput
  - Minimizing latency

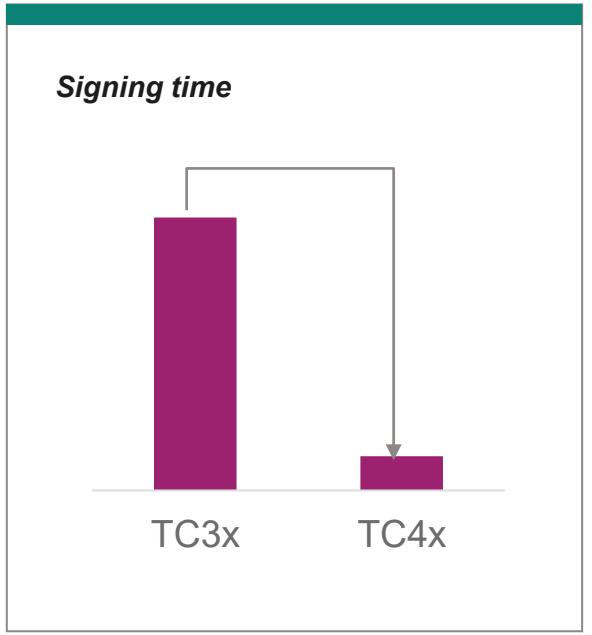
Cyber security real-time module (CSRM) for performance increase*

- Up to 15x more performance vs. ARM M3 TC3x HSM
- CSRM as trusted secured HW environment supporting new security standards (e.g. ISO 21434)

Hardware accelerated solutions for NIST selected PQC algorithms

- PQC CRYSTALS-Dilithium (PQC Signature Algorithm)
  - AES-256 HW acceleration using TC4x
- Sphincs+(PQC Hash based signature)
  - SHA2-256 HW acceleration using TC4x
  - SHA3 HW acceleration using TC4x
- CRYSTALS-KYBER (PQC Key Exchange)
  - AES-256 HW acceleration using TC4x

RSA 2048 on TC3x vs. PQC Dilithium 2 on TC4x*



8x faster

*Source: Webinar - Next level security using ESCRYPT CycurHSM on AURIX™ TC4x devices

ETAS offers sophisticated security solutions for PQC optimized using Infineon TC4x HW accelerators

Any Questions?