TeleTrusT-EBCA "PKI-Workshop" 2024

Berlin, 10.10.2024

A Journey to Post-Quantum Cryptography: Crypto-Inventory

Dr.-Ing. Fabrizio De Santis, Kristjane Koleci

Foundational Technologies, Siemens AG

Cryptographically Relevant Quantum Computers (CRQC) are a fundamental threat to cybersecurity

CRQCs exploit exponential speed-up for breaking universally used public key algorithms RSA and ECC.

Main threats:

- **“Intercepted now – decrypted later”**
  No confidentiality, e.g., “secret Coca Cola formula”, encrypted patient data

- **“Signed today – forged later”**
  No integrity and authentication: e.g., “signed malware”, manipulated audit trails

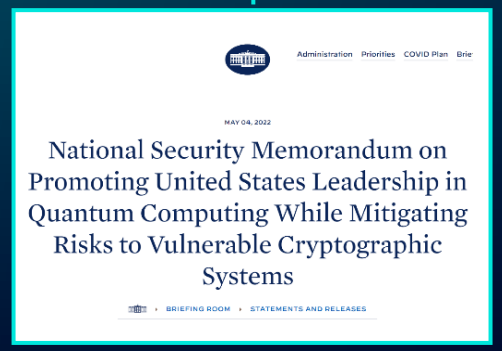
- **“Installed now – attacked later”**
  No availability, e.g., bypass of security measures, leading to disruption of critical infrastructures

SIEMENS

The transition to PQC must be prepared to meet upcoming regulatory requirements and customer demands, regardless of progress in the field of quantum computers

- US administration is pushing for the transition to post-quantum cryptography
- Initial focus on US NSS systems starting by 2025, e.g., armed forces, intelligence
- Private sector expected to follow soon afterwards
- Similar recommendations expected in other regions too, e.g., Europe, China, …
- US NIST have been published first PQC standards in August 2024

May 2022 — *National Security Memorandum*

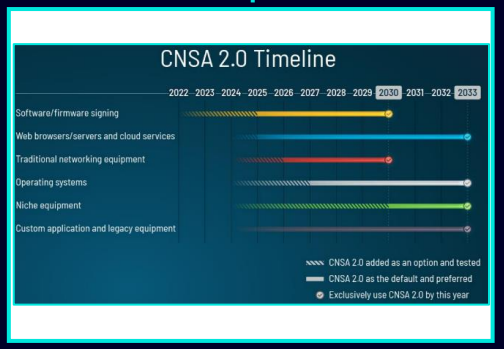


Mar 2023 — *US National Cybersecurity Strategy*

"… Federal Government will prioritize the transition of vulnerable public networks and systems to quantum-resistant cryptography [...] The ***private sector should follow the government's model*** *in preparing its own networks and systems for our post-quantum future"*

Apr 2024 — *EU: Recommendation on PQC*

Apr 2024 — *CNSA 2.0 Suite FAQ Update*



SIEMENS

The transition to PQC must be prepared to meet upcoming regulatory requirements and customer demands, regardless of progress in the field of quantum computers

A journey to post-quantum cryptography

Awareness

Establishment of a PQC Task Force and a PQC Community within the company

Crypto-Inventory

Identification of cryptographic assets and definition of transition priorities

Evaluation/PoC

Impact evaluation and design for PQC in IT/OT products, solutions, and infrastructures

Deployment

Deployment of PQC into products, solutions, and infrastructures

SIEMENS

Post-Quantum Cryptography Task Force @ Siemens Foundational Technologies

Cryptography lies at the foundation of cybersecurity. Products, solutions, and infrastructures must be transitioned to Post-Quantum Cryptography.

The **Challenge**

Regardless of when quantum computers will become available, the time to act is **now.**

- Experts predict cryptographically relevant quantum computers to be available by **2030**
- However, customer demand for PQC support will come in the near future, driven by upcoming **security standards and recommendations**
- A transition to post-quantum cryptography affects the **full ecosystem**

The **Offer**

A dedicated task force of technology experts, **supporting businesses** to

- **Identify** relevant elements within portfolio affected by the PQC transition
- **Prioritize** portfolio elements that need to be considered first in the PQC transition
- **Implement** comprehensive concepts for the transition of components, infrastructure, and processes to PQC

The **Benefits**

Time- & cost-efficient transition to PQC, by mitigating **capacity and know-how gaps.**

- **Guidance and best practice sharing** by technology experts
- Gain early experience on post-quantum cryptography from implemented proof-of-concepts
- **Quantum-safe** business portfolio

SIEMENS

What is a cryptographic inventory?

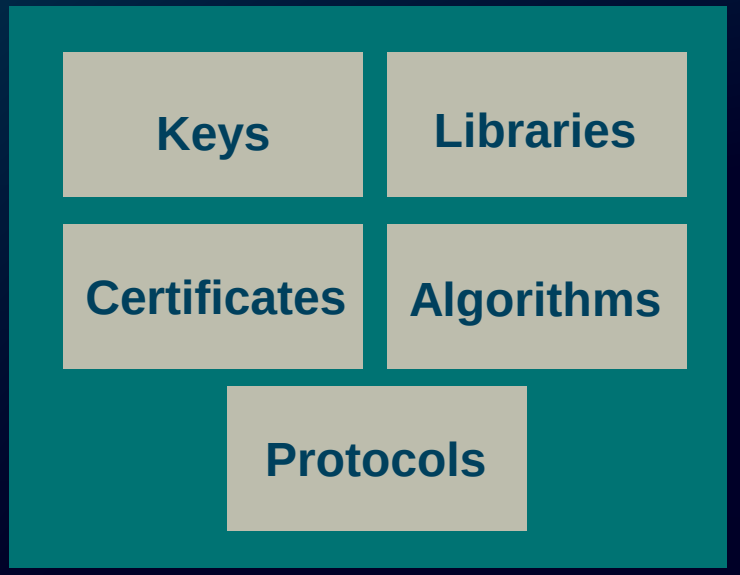
A cryptographic inventory is the record of the active cryptography included in a system or application.

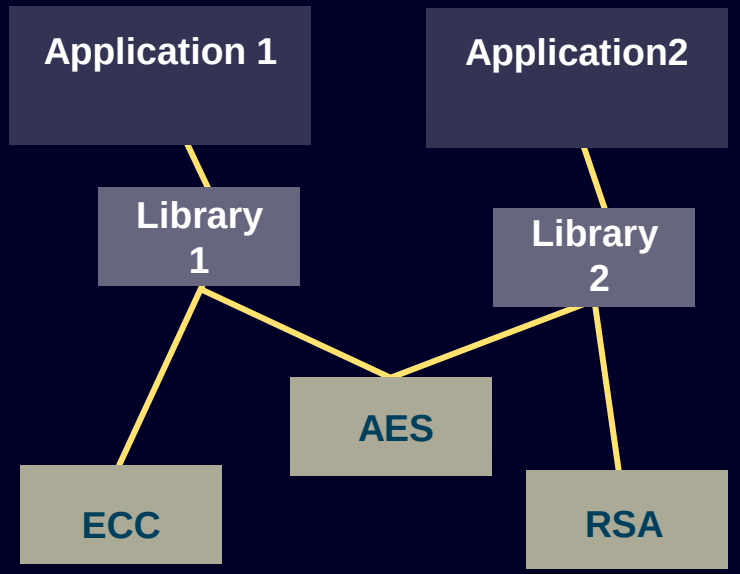
The cryptographic inventory:

- includes information on the **location and usages** of libraries, certificates, and keys.
- indicates **which protocols** and which algorithms is used.

A Cryptographic Inventory shows:

- the **dependencies** on the same libraries of different applications
- the parameters of an algorithm and its instances.





SIEMENS

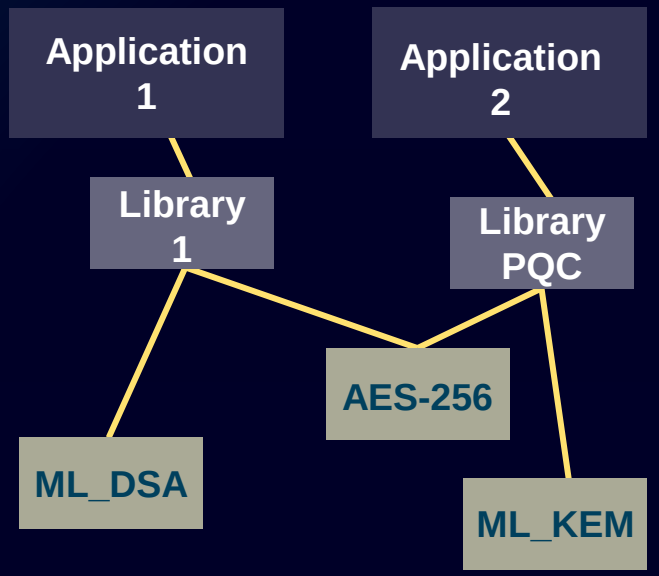
A cryptographic inventory for the transition to post-quantum cryptography

With a cryptographic inventory it is possible to:

- Define different **strategies** for algorithms, symmetric and asymmetric cryptography: to enable the **transition to PQC** and **crypto-agility**
- Define a timeline for the keys and certificates that must be updated, to address the harvest-now-decrypt-later attacks in time.
- Have an overview of libraries and be able to monitor their transition to post-quantum cryptography.

Further task to be performed before the transition to post-quantum cryptography:

- Monitor the transition plan of software providers to PQC;
- Monitor the status of libraries that implement PQC and their compliance with the standards.



SIEMENS

A cryptographic bill of materials for a cryptographic inventories

The Cryptographic Inventory format

- **C**ryptographic **B**ill **o**f **M**aterials (CBOM) is the format that describes cryptographic assets and their dependencies.
- The Cyclone DX 1.6 standard is the gold standard for the CBOMs.

The CBOM support:

- The CBOM is supported to generate the CI of a source code.
- A series of open-source tools can create a CBOM: cdxgen, sonar cube, CodeQL.

CDXGEN

sonarqube

CodeQL


```
"components": [ {
    "name": "RSA-2048",
    "type": "cryptographic-asset",
    "bom-ref": "crypto/key/rsa-2048@1.2.840.113549.1.1.1",
    "cryptoProperties": {
      "assetType": "related-crypto-material",
      "relatedCryptoMaterialProperties": {
        "type": "public-key",
        "id": "2e9ef09e-dfac-4526-96b4-d02f31af1b22",
        "state": "active",
        "size": 2048,
        "algorithmRef": "crypto/algorithm/rsa-2048@1.2.840.113549.1.1.1",
        "securedBy": {
          "mechanism": "Software",
          "algorithmRef": "crypto/algorithm/aes-128-gcm@2.16.840.1.101.3.4.1.6"
        },
        "creationDate": "2016-11-21T08:00:00Z",
        "activationDate": "2016-11-21T08:20:00Z"
      },
      "oid": "1.2.840.113549.1.1.1"
    }
```


Source: bom-examples/CBOM/Key at master · CycloneDX/bom-examples · GitHub

SIEMENS

PQC transition is an organization-wide transformation
The topic gained traction worldwide but still a lot to do

Raise awareness in your organization regarding upcoming post-quantum standards and requirements

Perform an inventory to understand how cryptography is used in your products/solutions

Perform a threat-and-risk analysis to define a migration strategy of your products/solutions

Engage with customers and suppliers to align roadmaps and requirements

Evaluate the impact of post-quantum cryptography on the requirements of your products/solutions

Prepare devices and infrastructure for a in-field migration to post-quantum cryptography

SIEMENS