A bouquet of crypto flowers

Dieter Bong, PM Hardware Security Modules @ Utimaco

Creating Trust in the Digital Society

utimaco®

A bouquet of crypto flowers

utimaco®

Agenda

- About Utimaco
- PQC Standardization Process @ NIST … and beyond
- A bouquet of crypto flowers … where do we go from here
- Q&A

UTIMACO is a **global platform solution leader** of trusted Cybersecurity and Compliance solutions.

We are driven to take a leading market position by providing **uncompromised Cyber Security solutions** fulfilling the highest standards.

38 years in IT security

500+ highly skilled experts

100 million Euro revenue

A bouquet of crypto flowers

utimaco®

Agenda

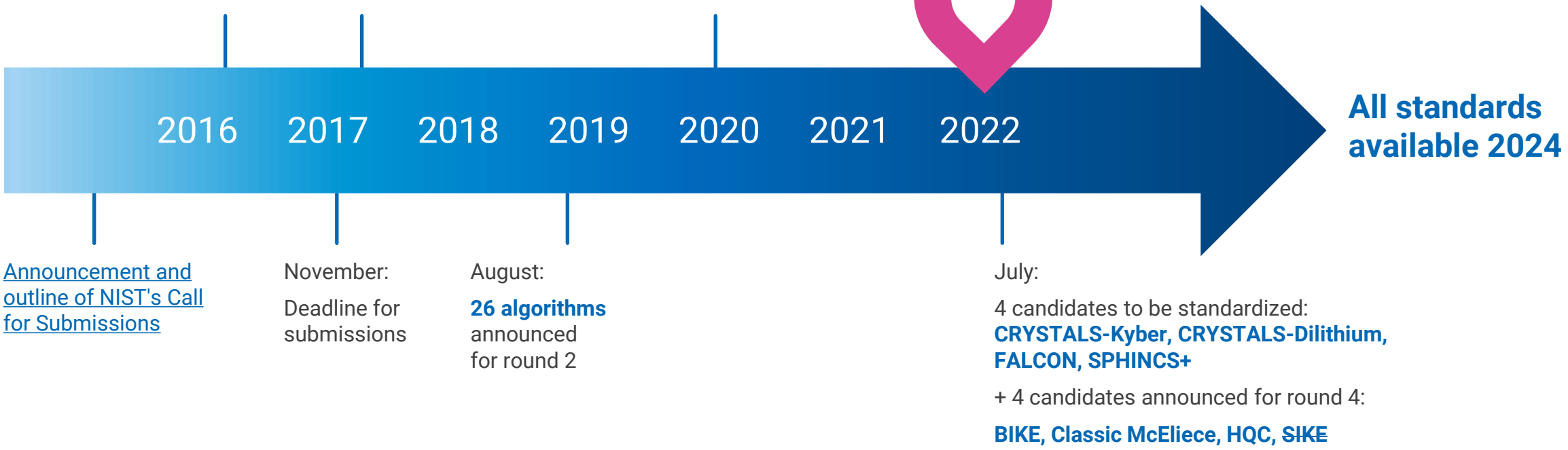
- About Utimaco
- PQC Standardization Process @ NIST … and beyond
- A bouquet of crypto flowers … where do we go from here
- Q&A

PQC Standardization Process @ NIST … and beyond

utimaco®

The NIST standardization process

Start: Collecting proposals | Round **1** | Round **2** | Round **3** | Round **4**



PQC Standardization Process @ NIST … and beyond

utimaco®

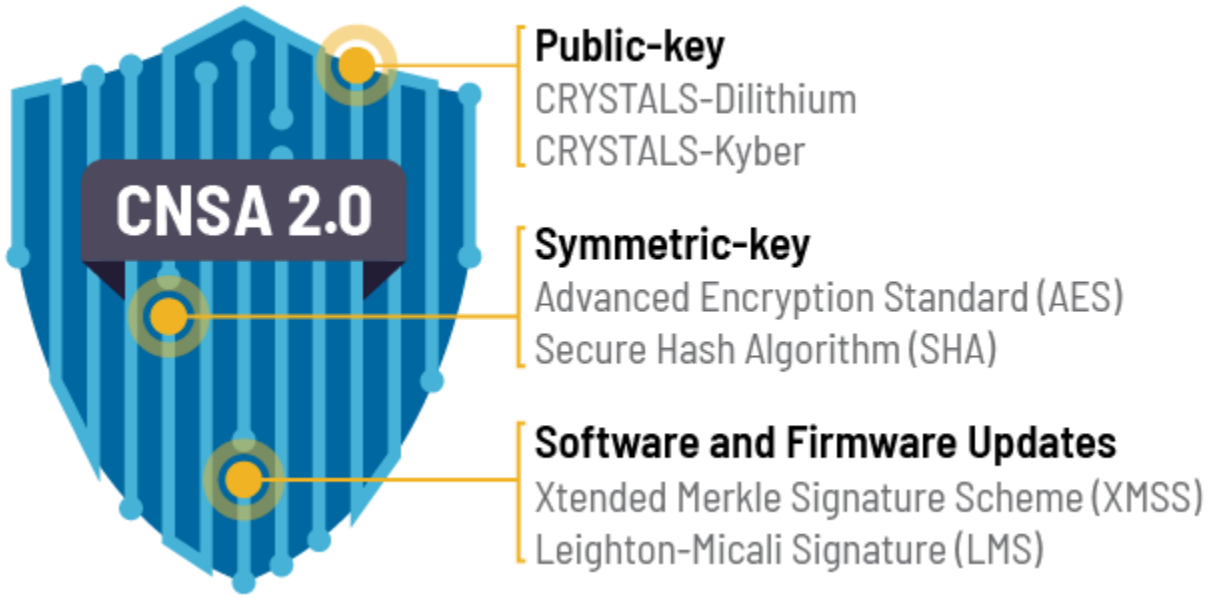
The NIST standardization process

PQC Standardization Process @ NIST … and beyond

utimaco®

Beyond the NIST standardization process

- USA, NSA Cybersecurity Advisory
  - Commercial National Security Algorithm Suite 2.0 specifies that *"The algorithms chosen for software- and firmware-signing are those specified in NIST Special Publication 800-208. NSA recommends Leighton-Micali with SHA-256/192 …"*



- Germany, Technische Richtlinie BSI TR-02102-1 recommends the following PQC algorithms:
  - Signature
    - XMSS, XMSS-MT, LMS, HSS
  - Key encapsulation mechanisms
    - Lattice-based **FrodoKEM**
    - Code-based **Classic McEliece**
  - BSI maintains recommendation after NIST's Round 3 selection: high security margin

PQC Standardization Process @ NIST … and beyond

utimaco®

Beyond the NIST standardization process

- Protocol and Interface standardization in progress … a few examples

- Internet Engineering Task Force (IETF)
  - Jake Massimo, Panos Kampanakis, Sean Turner, Bas Westerbaan, Sep 29, 2022, Internet X.509 Public Key Infrastructure: Algorithm Identifiers for Dilithium
  - Christine van Vredendaal, Silvio Dragone, Basil Hess, Tamas Visgrady, Michael Osborne, Dieter Bong, Joppe W. Bos, Oct 23, 2022, Quantum Safe Cryptography Key Information for CRYSTALS-Dilithium
  - Mike Ounsworth, Massimiliano Pala, June 8, 2022, Composite Signatures For Use In Internet PKI

- Organization for the Advancement of Structured Information Standards (OASIS)
  - PKCS #11 Specification 3.1, Committee Specification 01 defines mechanisms for HSS signature scheme
  - PKCS #11 Specification 3.2 will define mechanisms for further quantum-safe algorithms

PQC Standardization Process @ NIST … and beyond

utimaco®

Beyond the NIST standardization process

- Protocol and Interface standardization in progress … a few examples

- European Telecommunications Standards Institute (ETSI)
  - ETSI TR 103 617 Quantum-safe virtual private networks
  - ETSI TS 103 744 Quantum-safe hybrid key exchanges

- No standardization, but very good overview
  - European Union Agency for Cybersecurity (ENISA), PQC Integration study

A bouquet of crypto flowers

utimaco®

Agenda

- About Utimaco
- PQC Standardization Process @ NIST … and beyond
- A bouquet of crypto flowers … where do we go from here
- Q&A

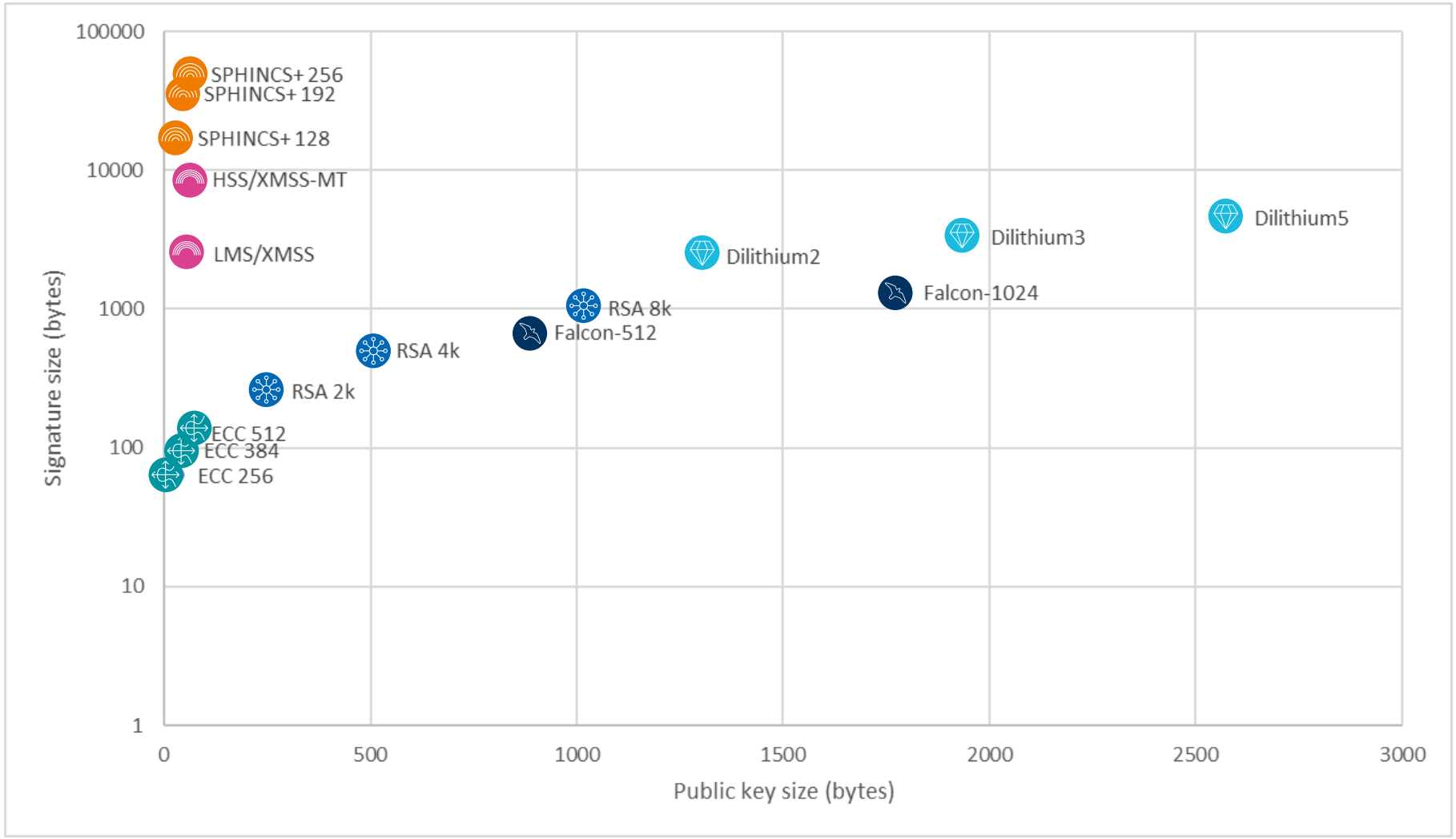
A bouquet of crypto flowers

A bouquet of crypto flowers … where do we go from here

A bouquet of crypto flowers … where do we go from here

utimaco®

PQC signature algorithms compared to ECC / RSA



A bouquet of crypto flowers … where do we go from here

utimaco®

PQC signature algorithms

	CRYSTALS-Dilithium	FALCON	SPHINCS+	LMS,HSS,XMSS,XMSS MT
Method	Lattice-based	Lattice-based	Hash-based	Hash-based
Strengths	Creates relatively small signatures, fast, easy to implement	Fast verification, fast signing, very compact	Stateless, small keys, overlap with XMSS, use of established building blocks possible	Small keys
Weaknesses	Quite large keys which are still too large for some use cases	Very delicate signing procedure, floating-point arithmetic required	Very large signature, speed	**Stateful signature schemes**, quite large signature
Good to know	NIST declares Dilithium as a **primary algorithm** to be implemented for most use cases.	NIST recommends FALCON for **use cases where Dilithium may be too large**.	SPHINCS+ will be standardized to **not rely solely on lattice-based algorithms**. NIST asks for a version with a lower number of maximum signatures.	Standardized in NIST Special Publication 800-208 since 2020

Take away:

- **Stateful hash-based signature schemes require careful state management!**
- **There is no one-size-fits-all signature algorithm!**
  - **E.g. Suitability of 3rd Round signature candidates for vehicle-to-vehicle communication : as replacement for ECC, only Falcon-512 fits due to message size limitations … but not in dense environments due to slow verification; only Rainbow-I is fast enough for dense environments**

A bouquet of crypto flowers … where do we go from here

utimaco®

PQC key encapsulation mechanisms

	CRYSTALS-Kyber	FrodoKEM	Classic McEliece
Method	Lattice-based	Lattice-based	Code-based
Strengths	Fast	Quite fast	Quite short ciphertext, slow key generation
Weaknesses	Quite large key sizes, quite large ciphertext	Large key sizes, large ciphertext	Very large public key, quite large secret key
Good to know	NIST declares KYBER as a primary algorithm to be implemented for most use cases.	Limited to German (European?) deployments.	Limited to German (European?) deployments.

Take away:

- **We don't have many choices today** 

Don‘t wait until 2024

What now?

Think about your options now!

“The transition to post-quantum encryption algorithms is as much dependent on the development of such algorithms as it is on their adoption. While the former is already ongoing, planning for the latter remains in its infancy. We must prepare for it now to protect the confidentiality of data that already exists today and remains sensitive in the future.”

U.S. Secretary of Homeland Security,
Alejandro Mayorkas, March 31, 2021

https://www.dhs.gov/quantum

A bouquet of crypto flowers … where do we go from here

utimaco®

Think about your options … needs … limitations

- Needs
  - Use-case driven needs
    - E.g. code signing
    - Decide for one signing algorithm
  - Operational needs
    - E.g. clustering for high availability and load balancing
    - Weight challenges of stateful hash-based signatures
  - Solution / portfolio needs
    - Smartcard may only need one signing and one KEM algorithm
    - Crypto library or HSM must support all
- Limitations
  - Memory
    - Larger keys & certificates
    - Larger signed documents
  - Compute resources
    - Server: use more powerful CPU
    - Battery-backed devices???
  - Bandwith, timing, latency
    - TLS
    - V2x communication

A bouquet of crypto flowers

utimaco®

Agenda

- About Utimaco
- PQC Standardization Process @ NIST … and beyond
- A bouquet of crypto flowers … where do we go from here
- Q&A

Thank you

for your attention!

UTIMACO IS GmbH

Germanusstraße 4
52080 Aachen
Germany

Phone +49 241 1696-0
Web hsm.utimaco.com
E-Mail hsm@utimaco.com

UTIMACO Inc.

900 East Hamilton Avenue
Campbell, CA-95008
United States of America

Phone +1 (844) UTI-MACO
Web https://hsm.utimaco.com
E-Mail hsm@utimaco.com