SECURING THE FUTURE: POST-QUANTUM CRYPTOGRAPHY STANDARD DEVELOPMENT AND CHALLENGES

Joppe Bos, Senior Principal Cryptographer
Competence Center Crypto & Security

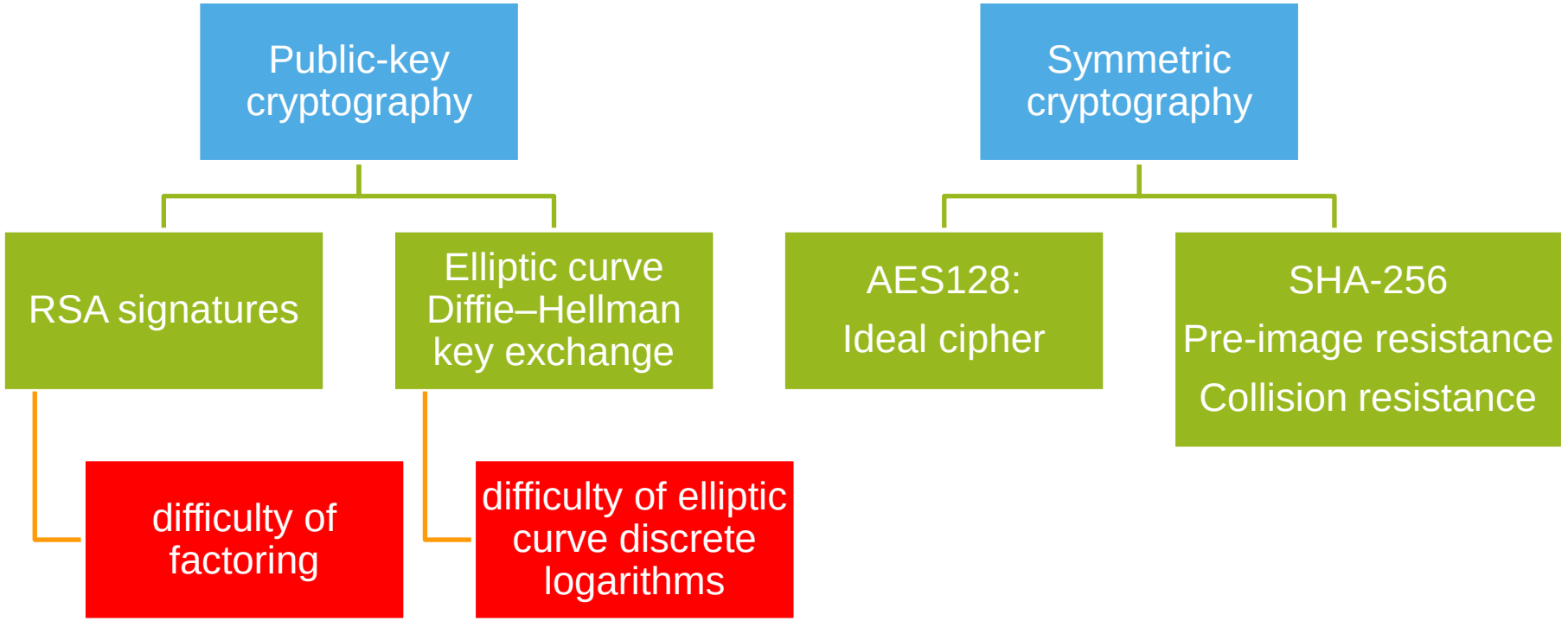
SEPTEMBER 2022

SECURE CONNECTIONS FOR A SMARTER WORLD

PUBLIC

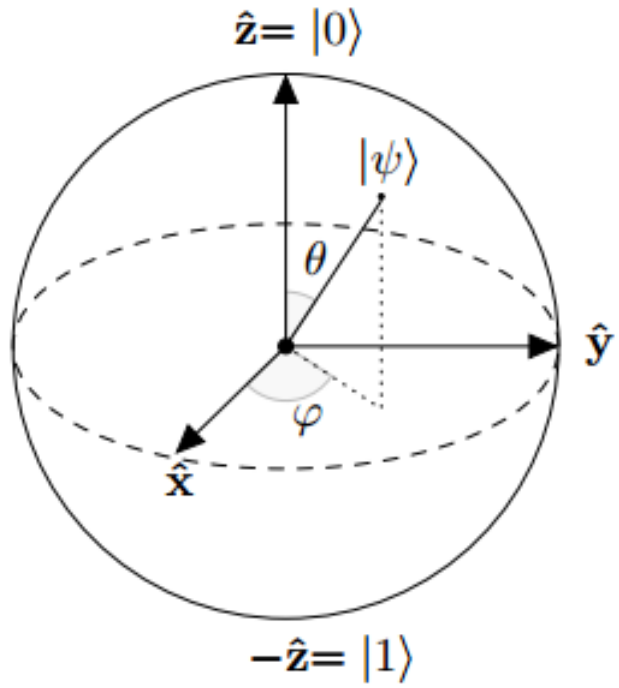
CONTEMPORARY CRYPTOGRAPHY

TLS-ECDHE-RSA-AES128-GCM-SHA256



QUANTUM COMPUTING

Computer systems and algorithms based on principles of quantum mechanics
- Superposition
- Interference
- Entanglement



- A classical bit can only be in the state corresponding to 0 or the state corresponding to 1
- A qubit may be in a superposition of both states
  → when measured it is always 0 or 1

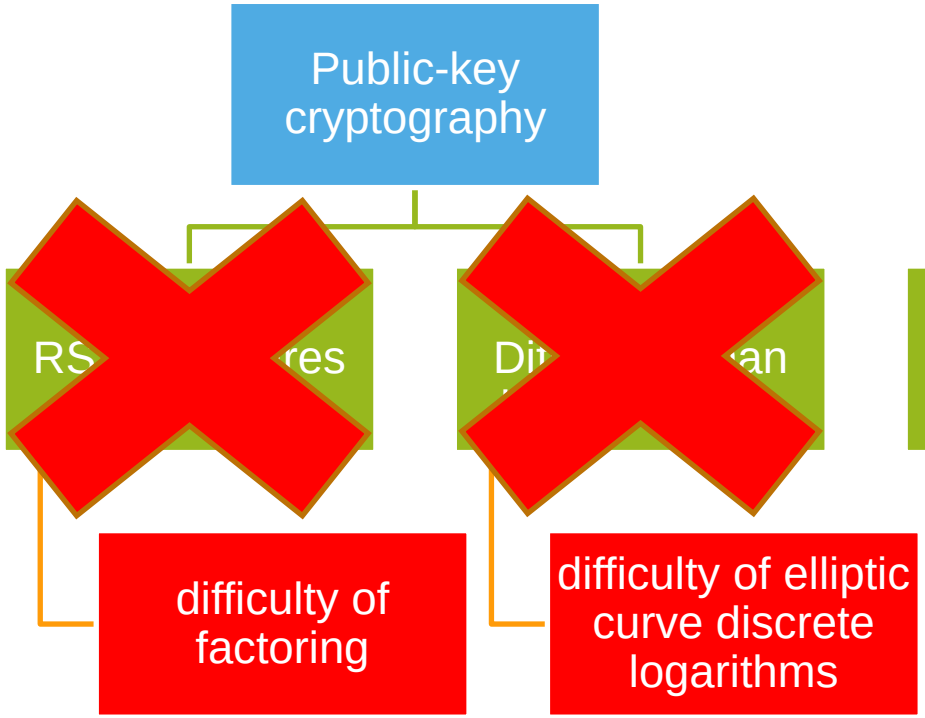
Shor's quantum algorithm (1994).
Polynomial time algorithm to factor integers.
Impact. If we assume the availability of a large quantum computer, then one can break RSA instantly.

State-of-the-art.
IBM's 127-Qubit Quantum Processor
Break RSA-3072:
~10,000 qubits are needed

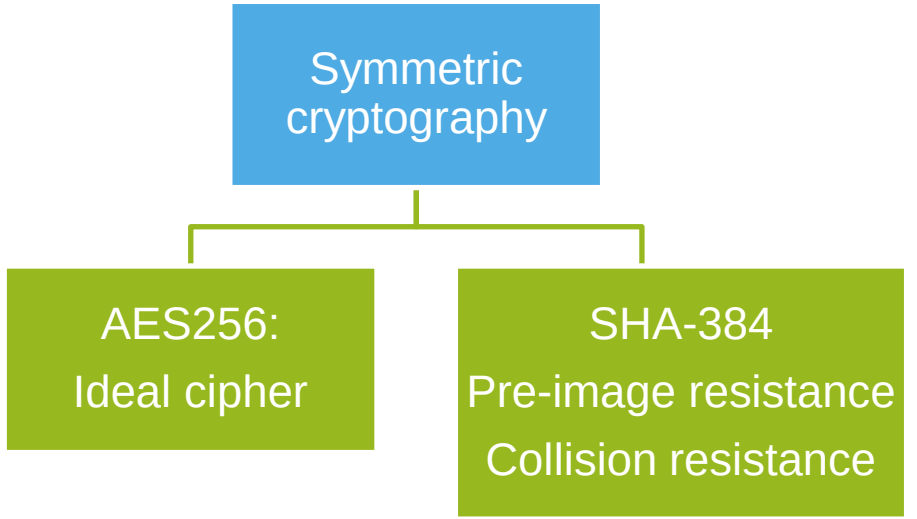
CONTEMPORARY CRYPTOGRAPHY

TLS-~~ECDHE-RSA~~-AES256-GCM-SHA384

"Double" the key sizes



Shor's algorithm (1994)



Grover's algorithm (1996)

Quantum Potential To destroy Security As We know it

Confidential email messages, private documents, and financial transactions
Secure today but may be compromised in the future, even if recorded & encrypted

Firmware update mechanisms in vehicles
May be circumvented and allow dangerous modifications

Critical industrial and public service infrastructure (for healthcare, utilities, and transportation using internet and virtual private networks)
Could become exposed – potentially destabilize cities

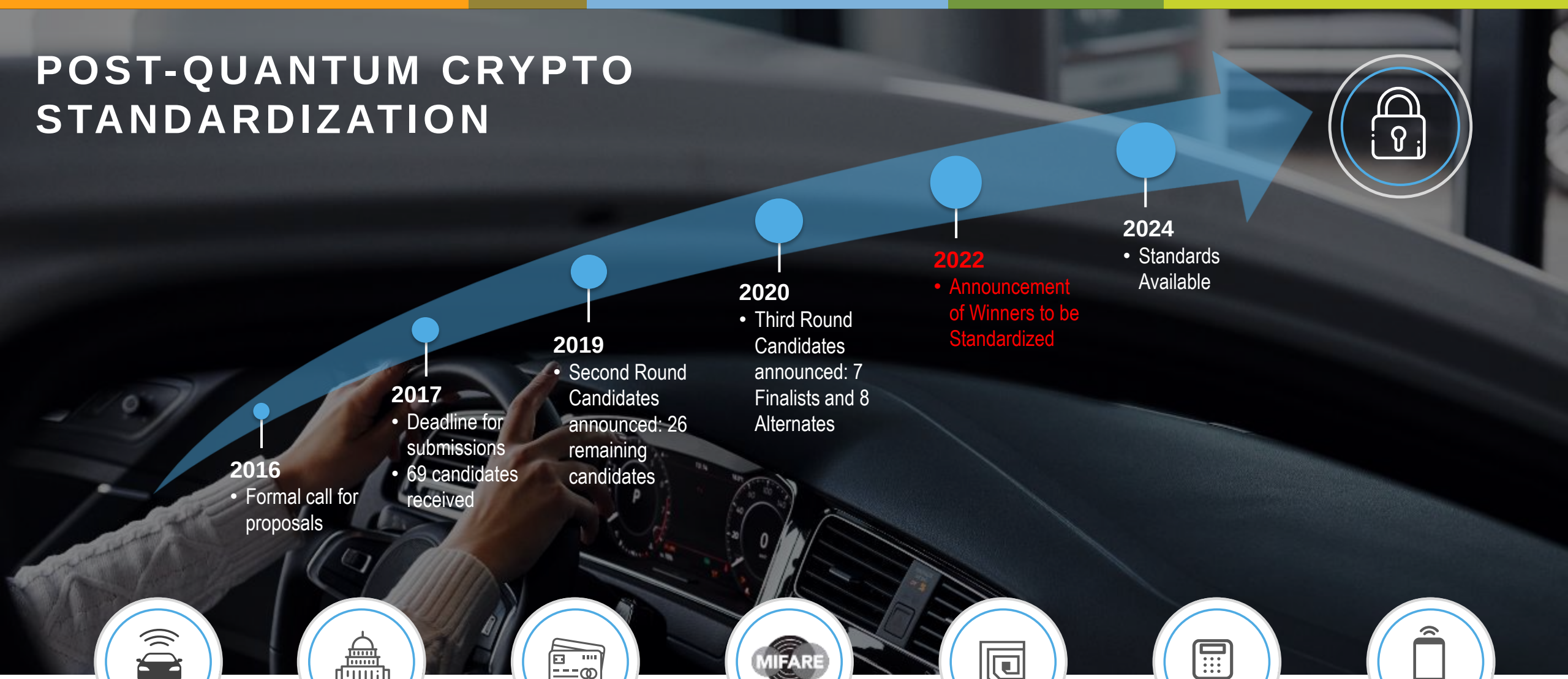
Audit trails and digitally signed documents associated with safety (auto certification and pharmaceutical authorizations)
Could be retrospectively modified

The integrity of blockchains
Could be retrospectively compromised - could include fraudulent manipulation of ledger and cryptocurrency transactions

POST-QUANTUM CRYPTO STANDARDS ARE COMING

IT DOESN'T MATTER IF YOU BELIEVE IN QUANTUM COMPUTERS OR NOT

POST-QUANTUM CRYPTO STANDARDIZATION



2016
- Formal call for proposals

2017
- Deadline for submissions
- 69 candidates received

2019
- Second Round Candidates announced: 26 remaining candidates

2020
- Third Round Candidates announced: 7 Finalists and 8 Alternates

2022
- Announcement of Winners to be Standardized

2024
- Standards Available

AUTOMOTIVE

EGOVERNMENT

BANK CARDS

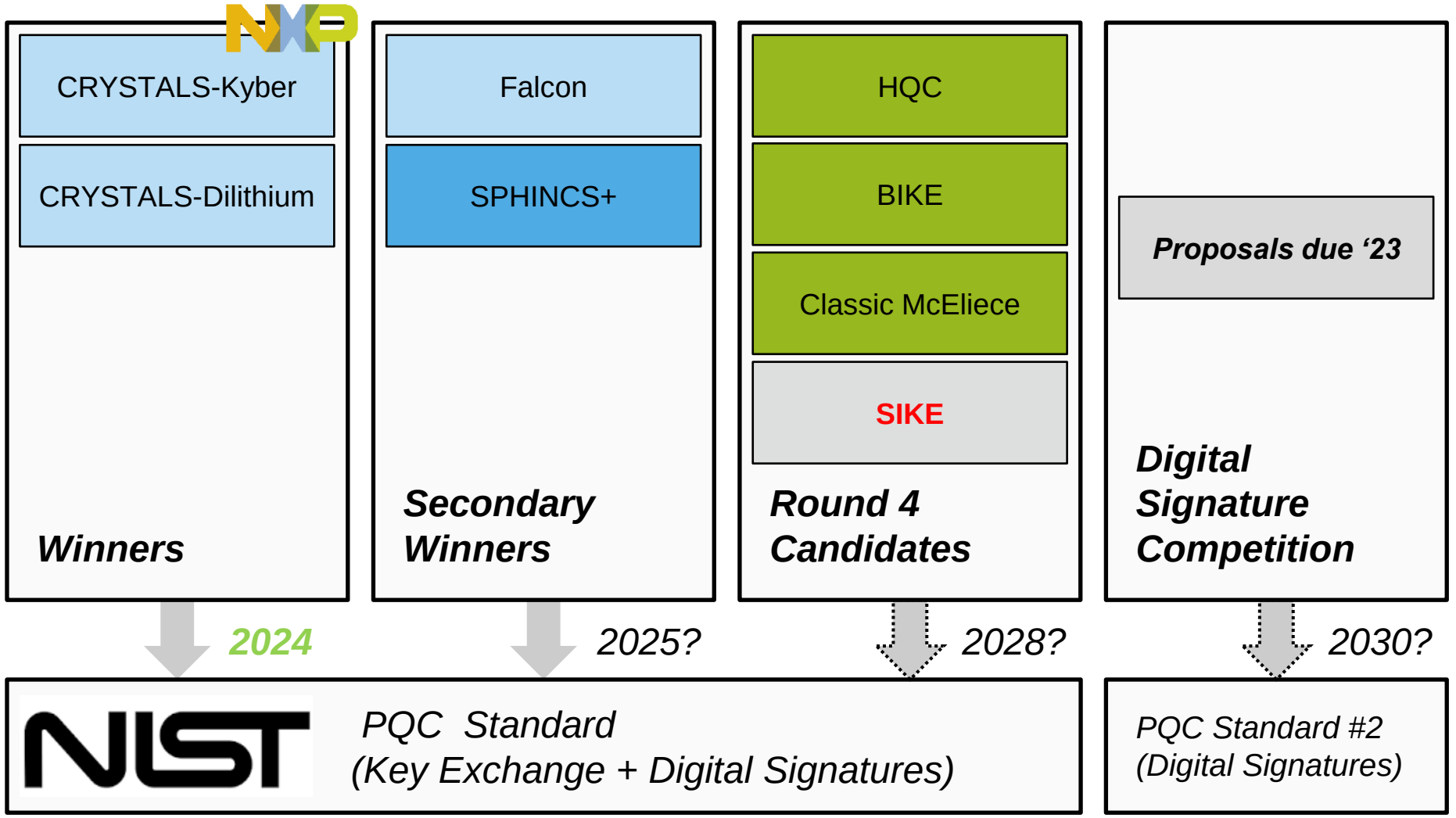
SMART MOBILITY (MIFARE) CARDS

TAGS & AUTHENTICATION

READERS

MOBILE

STANDARDS – NIST



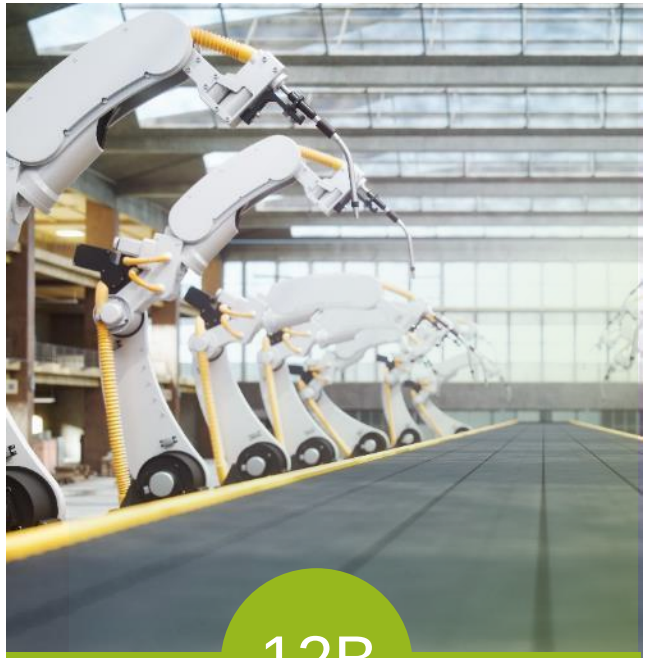
POST-QUANTUM CRYPTO IS ON THE HORIZON

AUTOMOTIVE

70%

70% connected cars by 2025

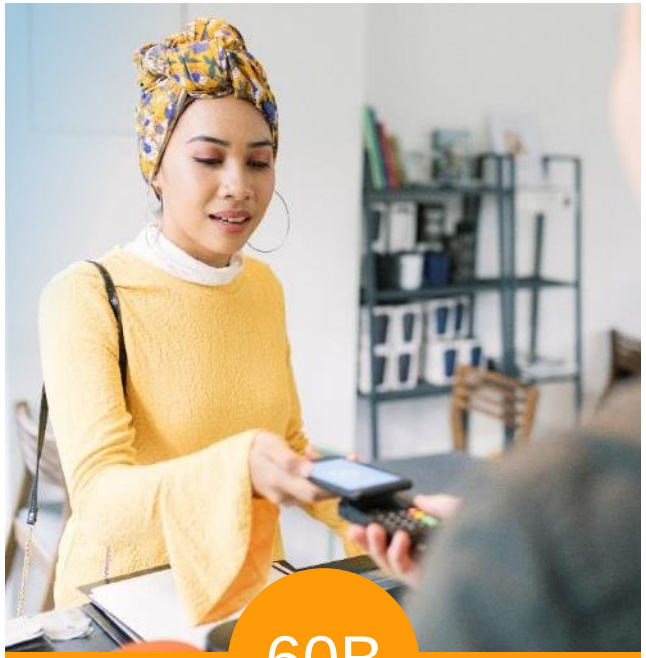
INDUSTRIAL & IOT



12B

IoT Edge & end nodes from 6B units in ‘21 to 12B units in ‘25

MOBILE



60B

Tagging 60B products per year by 2025

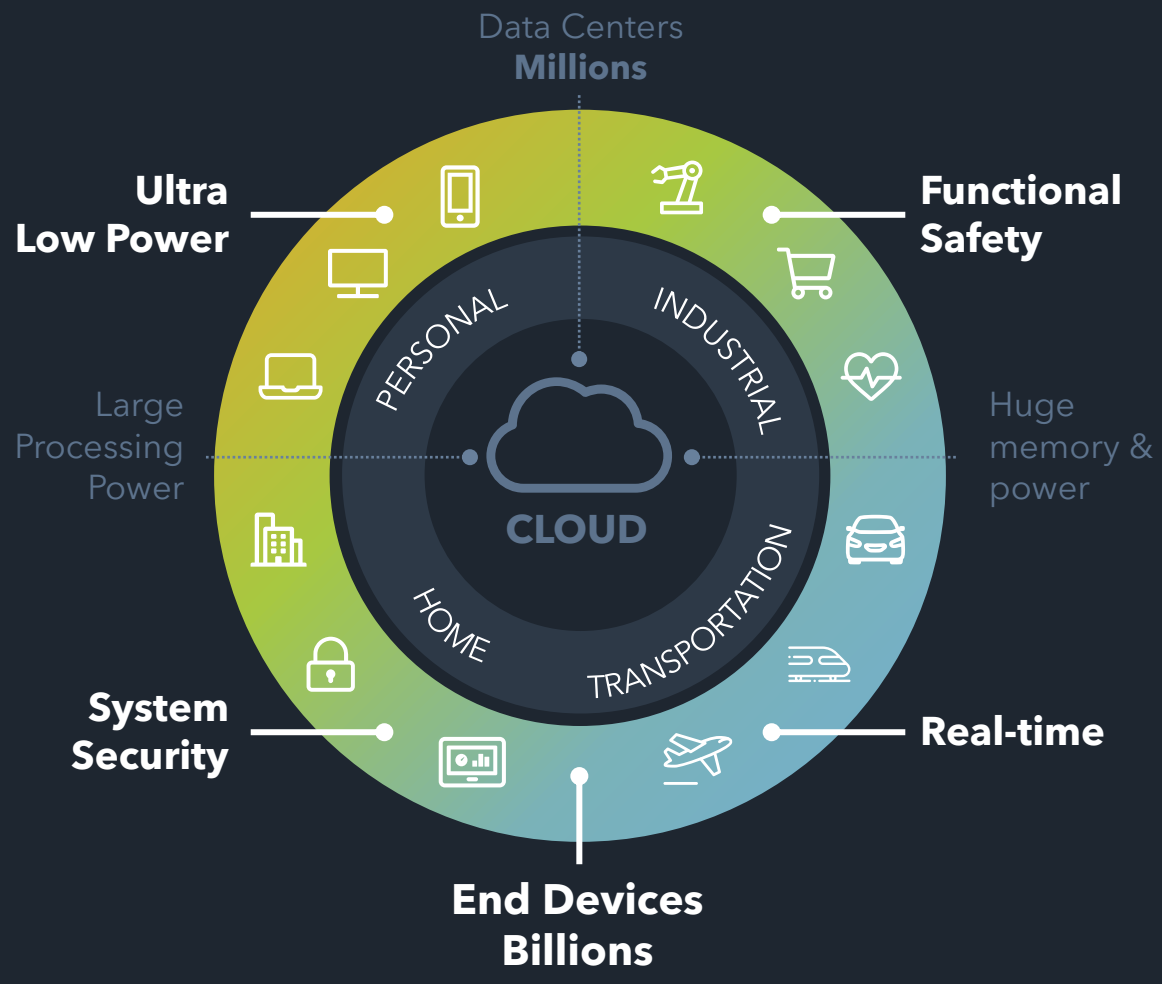
COMMUNICATION INFRASTRUCTURE

40B

Secure anchors & services for 40B processors

1. Source: NXP, Strategy Analytics, Evercore, Ericsson, IDTechex,

IMPACT PQC ON OUR ECO-SYSTEM



Data collection, processing and decisions at the edge
Devices securely connected to the cloud

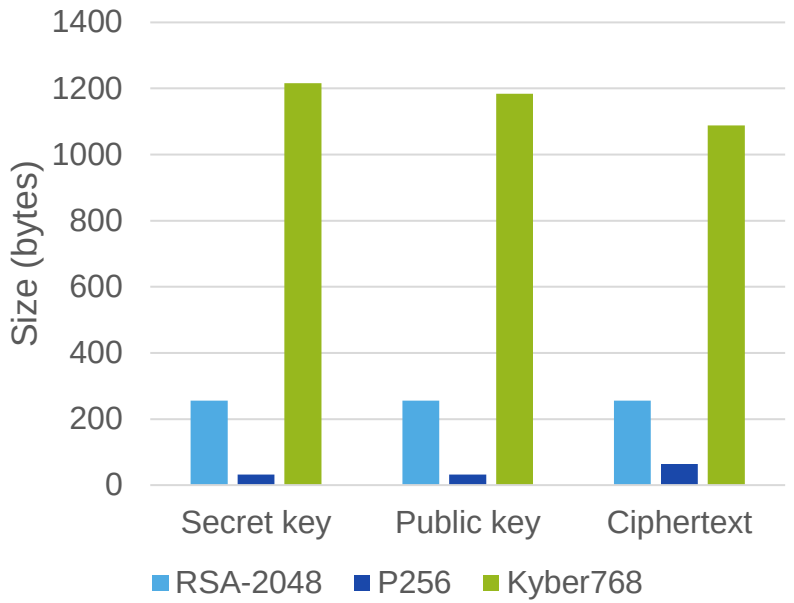
No Silver Bullet
If a crypto scheme was better, we would have standardized this already

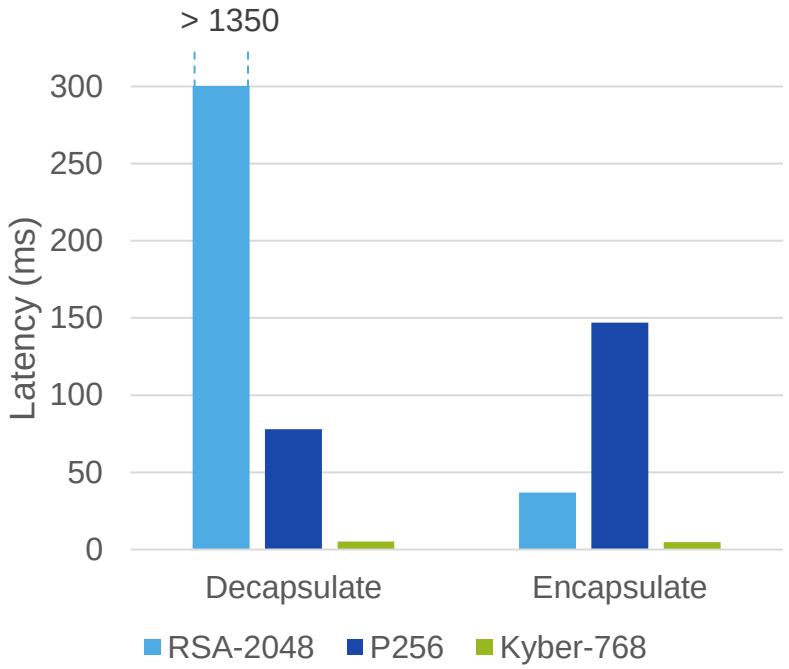
Cryptographic Keys
Orders of magnitude larger.
In the final: up to 1.3MB
Winners: up to 4.8KB
(ECC: 32 bytes, RSA: 384 bytes)

Performance
Varies: some faster some significantly slower.
SHA-3 is a dominating component (~80%)

Memory
Orders of magnitude more: up 100KB memory of RAM when executing

Bandwidth & Power
Larger signatures (up to 4.6KB) → more bandwidth required → increase in power usage



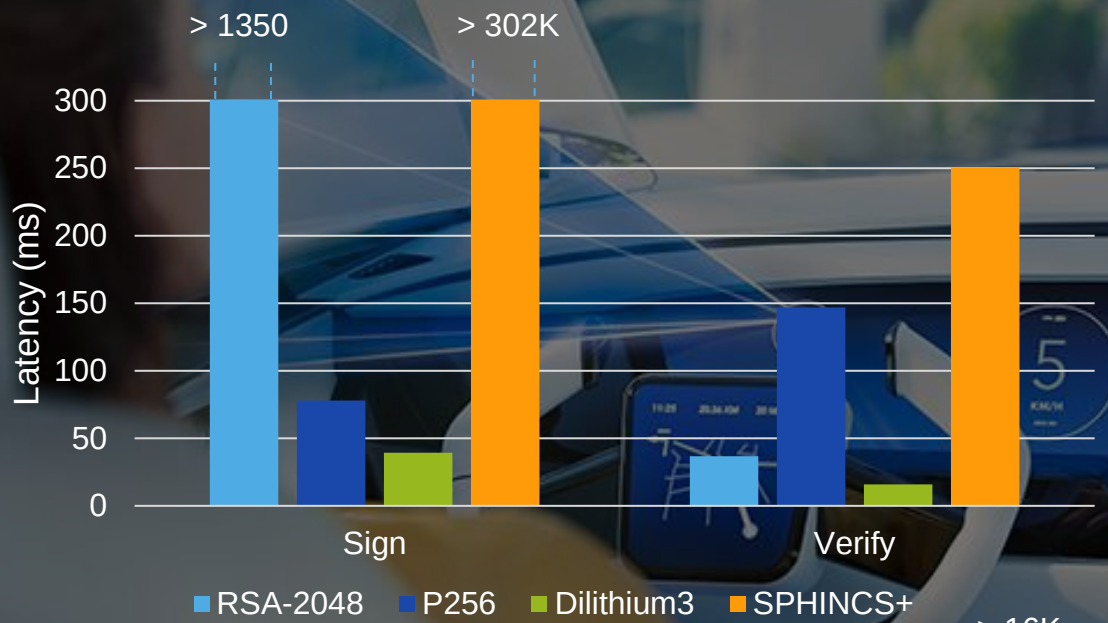


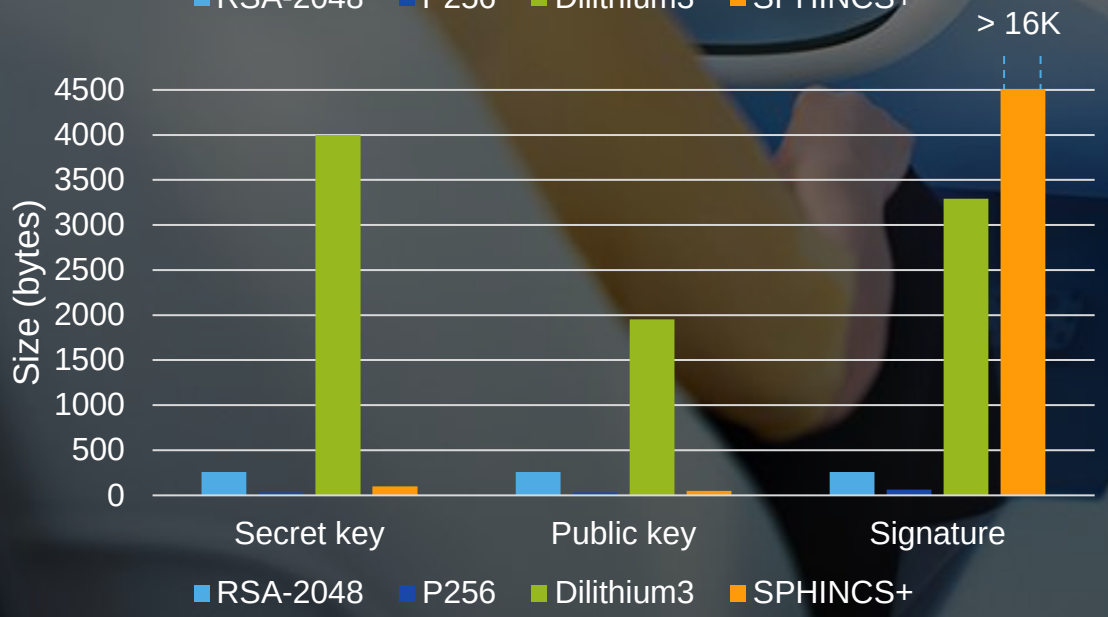
KEY-EXCHANGE IMPACT

Kyber **co-designed by NXP** with IBM, ARM and academic partners

- Measurements on Cortex-M4 @ 168MHz from pqm4 framework
- Functional implementation only (not hardened)
- **70 ~ 80 percent** of run-time in SHA-3

DIGITAL SIGNATURE IMPACT





USE CASE STUDY
IMPACT ASSESSMENT: S32G

S32G2 VEHICLE NETWORK PROCESSOR – A NEW TYPE OF AUTOMOTIVE PROCESSOR

OUR TARGET PLATFORM: S32G274A

3 Lockstep Arm® Cortex®-M7 Microcontrollers

4 Cluster Lockstep Cortex-A53 Microprocessors

8 MB of system RAM

POST-QUANTUM CRYPTO

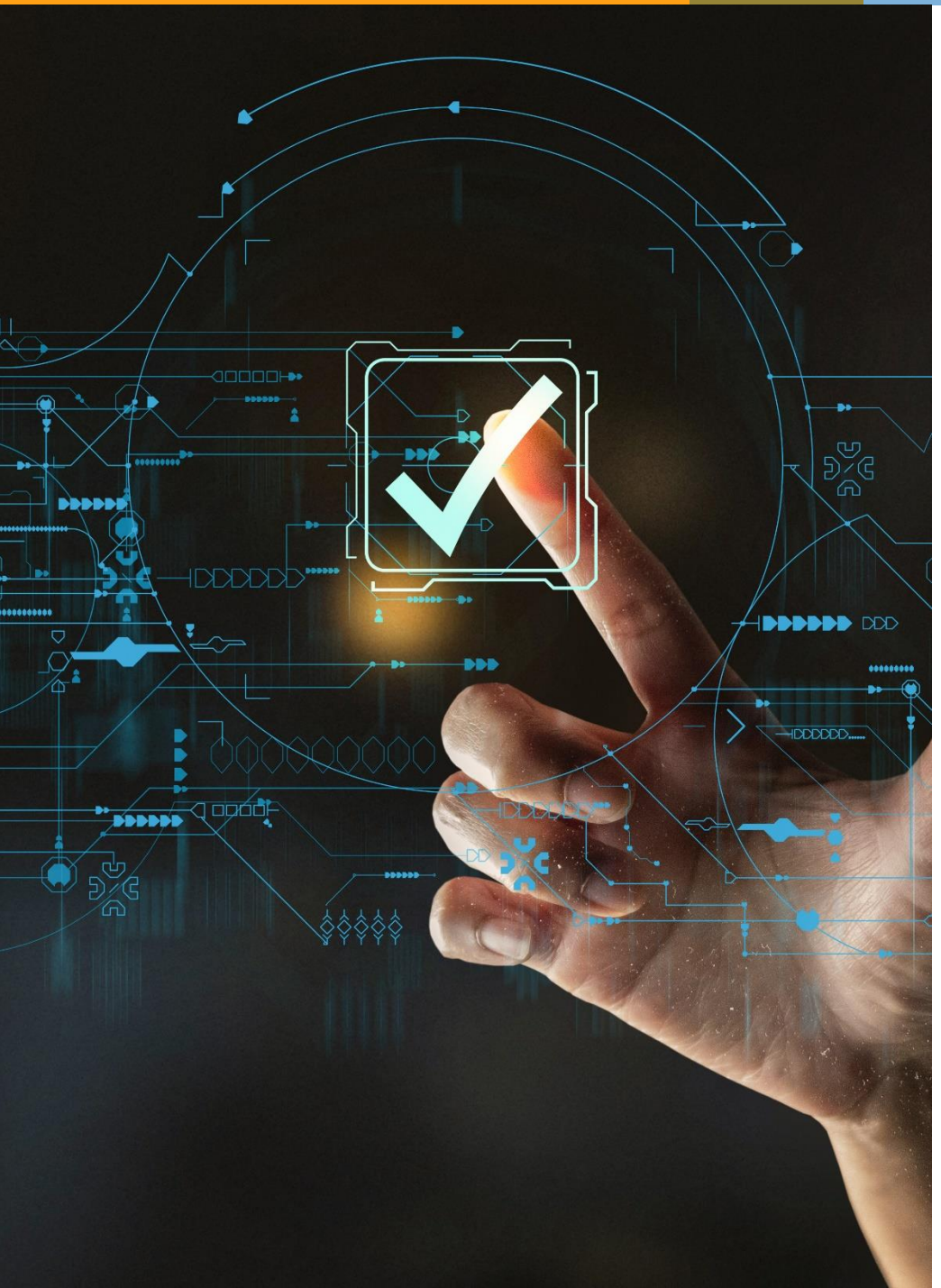
Can we enable PQC secure boot?

Integrate PQC secure signature verification

SAFE ASSURE™ by NXP

www.nxp.com/S32G2

EDGELOCK™ ASSURANCE by NXP



BENCHMARKS FOR AUTHENTICATION OF FW SIGNATURE ON THE S32G2

Alg.	Size		Performance (ms)			
			1 KB		128 KB	
	PK	Sig.	Inst.	Boot	Inst.	Boot
RSA 4K	512	512	2.6	0.0	2.7	0.2
ECDSA-p256	64	64	6.2	0.0	6.4	0.2
Dilithium-3	**1952**	**3293**	**16.7**	**0.0**	**16.9**	**0.2**

- Demonstrator only, further optimizations are possible (such as hardware accelerated SHA-3)
- Signature verification only required once for installation!
- During boot the signature verification can be replaced with a check of the Reference Proof of Authenticity

CUSTOMER-FIRST APPROACH FOR POST-QUANTUM CRYPTOGRAPHY

- Customer support for migration
- Continued innovation for high-assurance implementations (resistance against side-channel and fault attacks) and dedicated PQC hardware
- Crypto agility with seamless upgradability of our existing devices

For more details check out [nxp.com/pqc](nxp.com/pqc)

SECURE CONNECTIONS
FOR A SMARTER WORLD