ETSI Security Conference 2022

Post-quantum cryptography: the current state of play

Matthew Campagna

campagna@amazon.com

AWS Cryptography

Outline

How cryptographic engineering is done today

Quantum computing threat

Status of post-quantum cryptography standards

Impact to other international standards

ETSI TC CYBER; Quantum Safe Cryptography working group

Selecting the right tool

We select schemes that meet a few criteria:

Provides the security service we need

Secure for the lifetime of the intended use

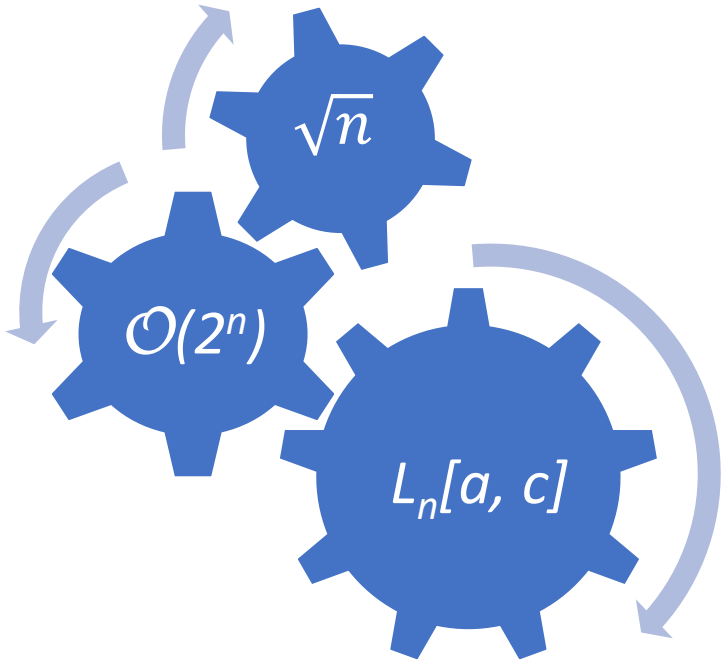
- Mechanism needs to protect data for x years
- It will take y years to upgrade the mechanism
- Lifetime of intended use = *x* + *y* years

Meets **performance** requirements

Simple, available and universally accepted

http://clipart-library.com/clipart/154494.htm

Security of an algorithm

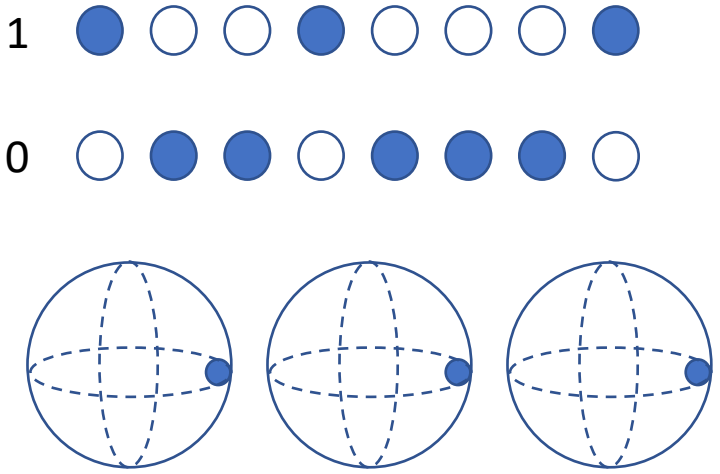


The computation complexity of the ***best known attacks***

How ***assured*** am I that better attacks are not coming?

Quantum computing

A qubit can be in both states $|0\rangle$ and $|1\rangle$ at the same time



- n bits can hold *1* of 2^n possible values at any given time
- n qubits can hold 2^n possible values at the same time

Quantum algorithms can be constructed to compute on 2^n possible values at the same time – but not all algorithms

Quantum computing

Shor's algorithm (1994): Can solve the discrete log problem (breaking Diffie-Hellman and Elliptic Curve Cryptography), and factor composite numbers (breaking RSA)

Grover's algorithm (1996): Can search an unsorted database of *N* items in $O(\sqrt{N})$ time (reducing the security of symmetric ciphers)

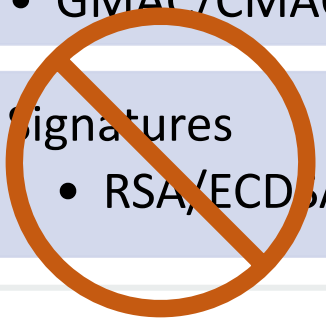
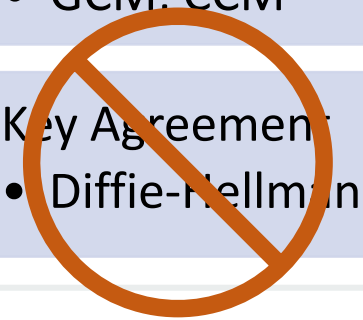
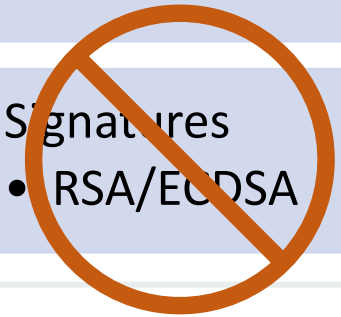
Classic Cryptography

Application or Protocol

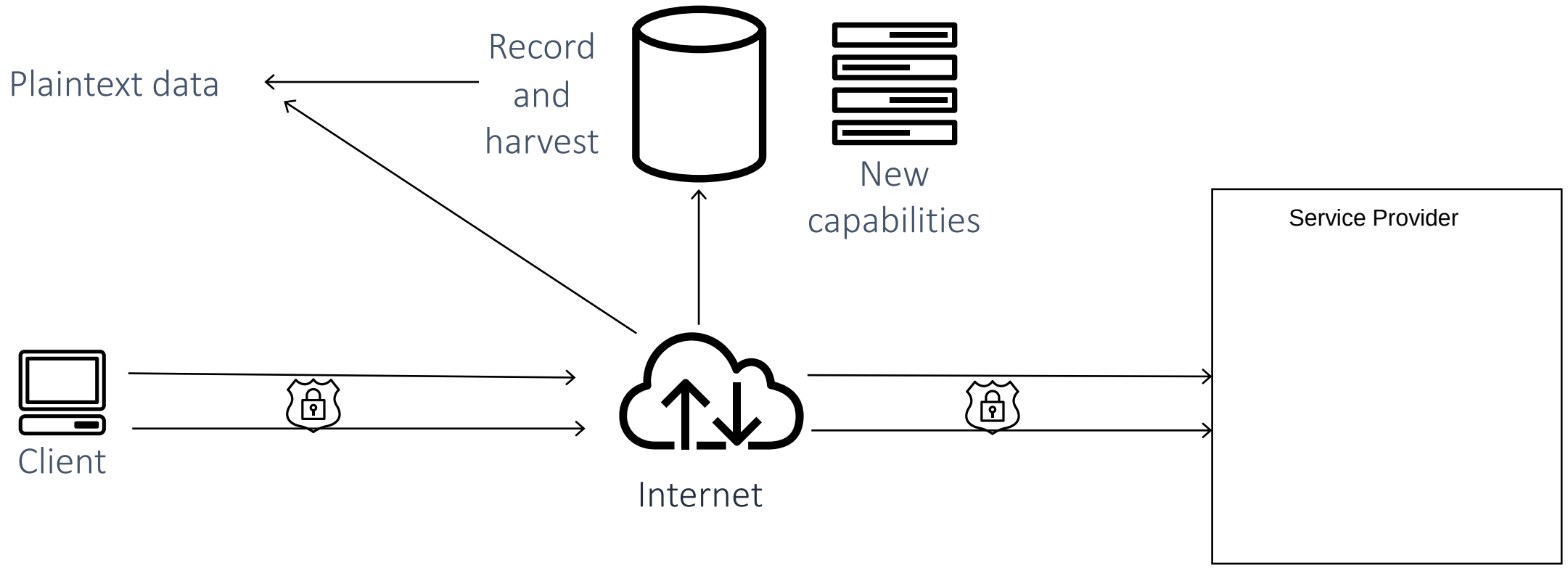
Data Integrity	Confidentiality	Authenticity	Non-repudiation

• Hash functions
  • SHA2, SHA3
  • SHAKE
• MACs
  • HMAC
  • GMAC/CMAC
	• Encryption
	  • AES
	• Modes
	  • CTR, CBC, XTS
	• AEAD Modes
	  • GCM, CCM
		• MACs
		  • HMAC
		  • GMAC/CMAC
		  • KMAC	

• Signatures
  • RSA/ECDSA
	• Key Agreement
	  • Diffie-Hellman
		• Signatures
		  • RSA/ECDSA
			• Signatures
			  • RSA/ECDSA

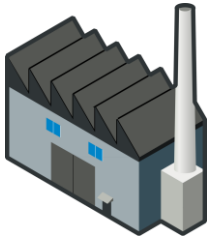





Long-term confidentiality (x)



Another problem (y)

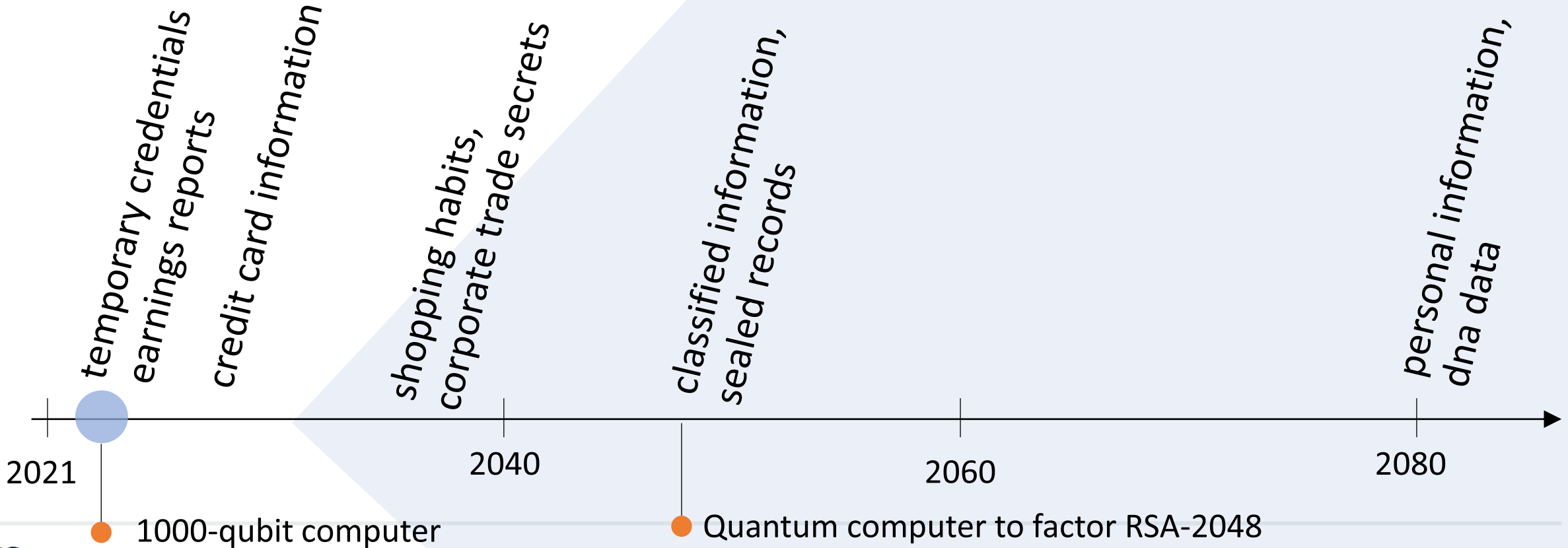




13 years

Cryptographic relevant quantum computer



What is the industry doing

Historic call for post-quantum/quantum-safe cryptography

2006 PQ Crypto Conference

2013 ETSI/IQC 1st Quantum Safe Cryptography Workshop

2015 ETSI's Quantum Safe Cryptography ISG (now a TC)

2016 NIST announces a Post-Quantum Cryptography Standardization Process

Update on NIST's PQC

2017 Round 1 NIST PQC standardization process (69 candidates)

2019: Round 2 NIST PQC standardization process (26 candidates)

2020: Round 3 NIST PQC standardization process (7/8 candidates)

2022: NIST Selection for PQ Standardization (1 KEM / 3 Signatures)

NIST PQC Candidates for Standardization

Key Encapsulation Mechanisms (KEM) – CRYSTALS-Kyber

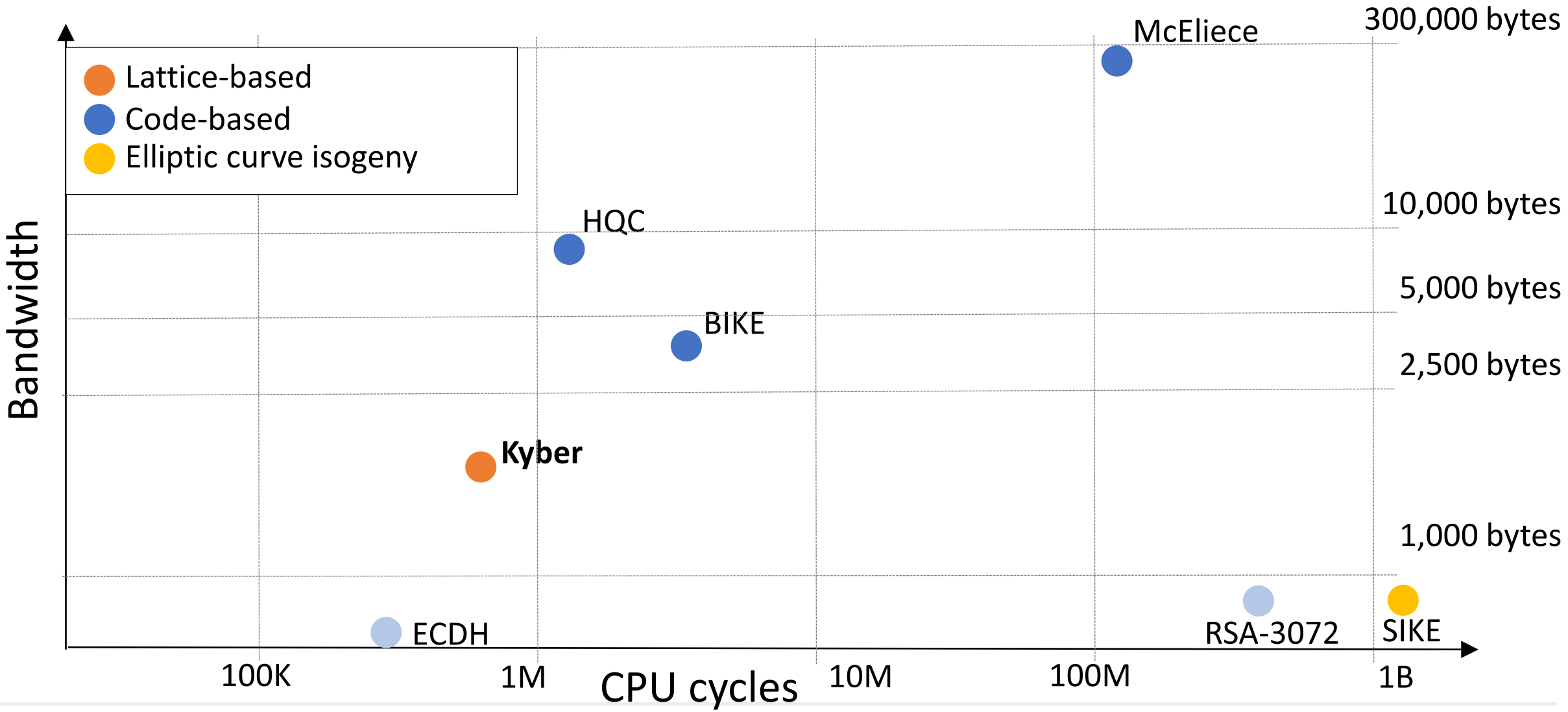
Signature Schemes – CRYSTALS-Dilithium, Falcon, SPHINCS+

KEM Schemes for future potential standards

BIKE/HQC/Classic McEliece/~~SIKE~~

New Call for Proposals: Digital Signature Algorithms with Short Signatures and Fast Verification

NIST Post-Quantum KEMs



NIST Post-Quantum Finalist for Standardization Signatures

Scheme	Private Key	Public Key	Signature
ECDSA (NIST P-256)	32	33	64
RSA-3072	384	387	384
Dilithium-II	**2528**	**1312**	**2420**
Falcon-512	1218	897	690
SPHINCS+Haraka-128f-robust	64	32	17088

https://openquantumsafe.org/liboqs/algorithms/

Hybrid key exchange in practice

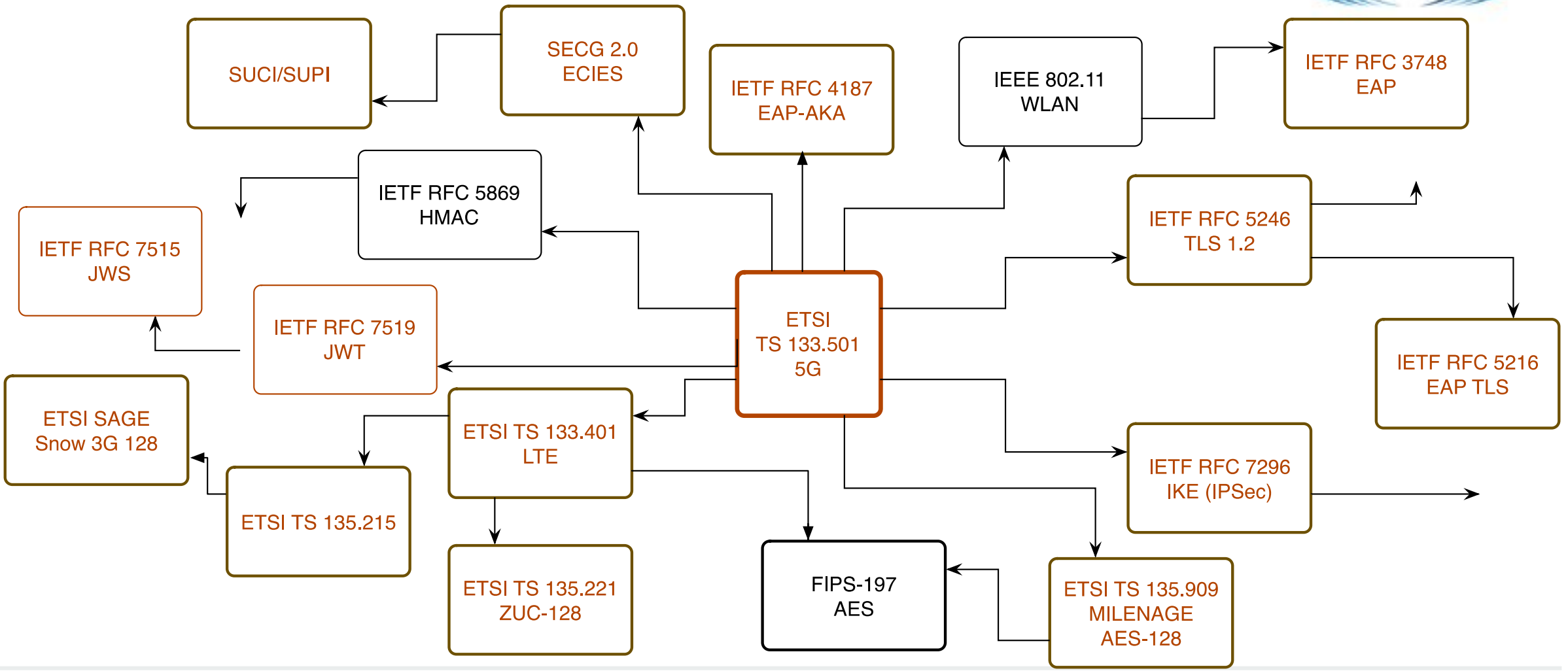
We have added ECDHE-with-Kyber ciphersuite to TLS 1.2 and 1.3 in s2n (our open-source TLS library).

These are deployed (but inactive) everywhere s2n is deployed.

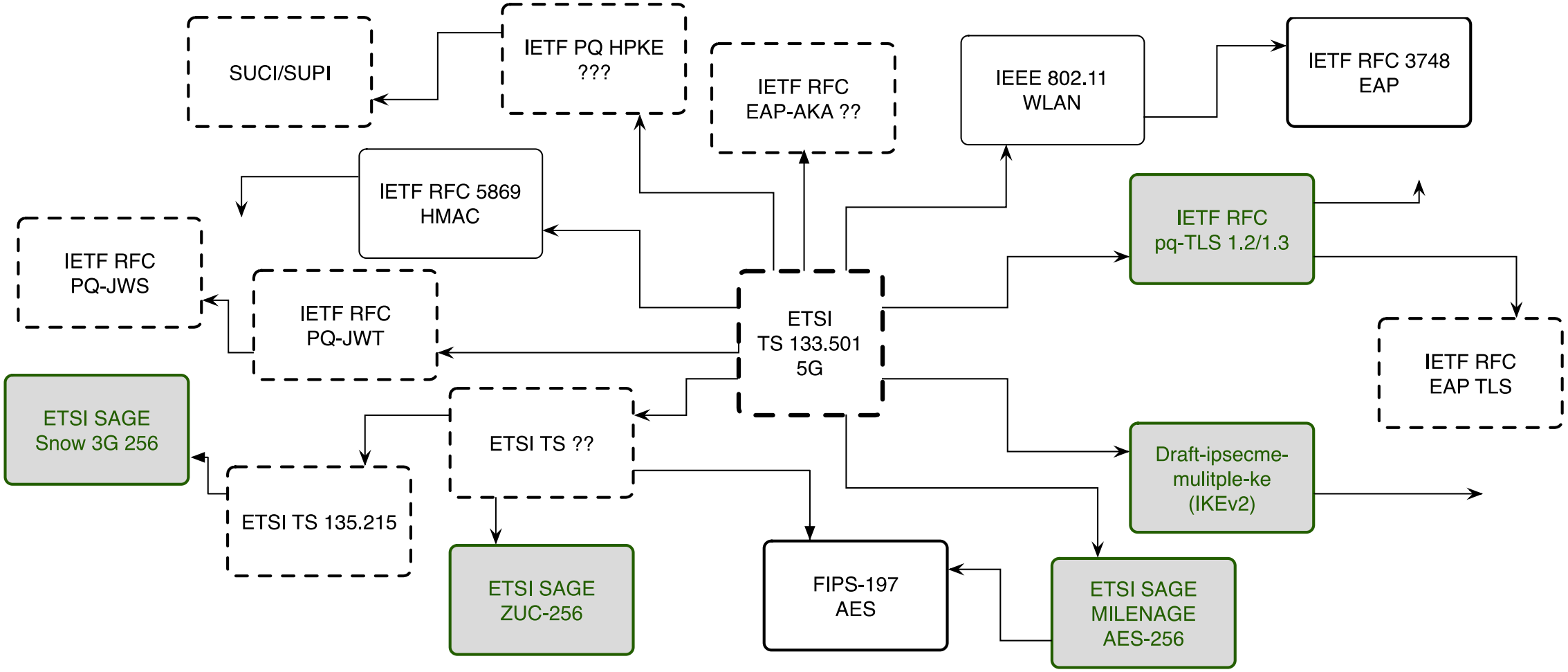
Active AWS Key Management Service, Secrets Manager, and AWS Certificate Manager.

	Bandwidth (bytes)	Total handshakes	Average (ms)	p0 (ms)	p50 (ms)	p90 (ms)	p99 (ms)
ECDHE (classic)	3,574	2,000	3.08	2.07	3.02	3.95	4.71
ECDHE + Kyber R3	5,898	2,000	3.36	2.38	3.17	4.28	5.35

How this space is being updated



How this space is being updated



ETSI CYBER QSC

Chair: Matthew Campagna (Amazon)

Vice chairs

- Philip Lafrance (ISARA)
- Dan Grundy (NCSC)

Secretary: Anthony Barnett (Thales)

Technical Officer: Sonia Compans (ETSI)

Healthy participation: 38 registered participants for most recent meeting – corporate/government/academia

Finished TR/TS

CYBER; Quantum-safe Hybrid Key Exchanges, ETSI TS 103 744 V1.1.1 (2020-12)

CYBER; Quantum-Safe Public Key Encryption and Key Encapsulation, ETSI TR 103 832 V1.1.2 (2021-09)

CYBER; Quantum-Safe Signatures, ETSI TR 103 616 V1.1.1 (2021-09)

CYBER; Migration strategies for Quantum Safe schemes, ETSI TR 103 619 V1.1.1 (2020-07)

CYBER; Quantum-Safe Identity-Based Encryption, ETSI TR 103 618 V1.1.1 (2019-12)

Quantum-Safe Virtual Private Networks, ETSI TR 103 617 V1.1.1 (2018-09)

Current Work Items

CYBER; Migration to QSC for ITS, DTR/CYBER-QSC-0018 (TR)

CYBER; Quantum-Safe Hybrid Key Exchanges, RTS/CYBER-QSC-0019 (TS 103 744)

CYBER; Impact of Quantum Computing on Cryptographic Security Proofs, DTR/CYBER-QSC-0020 (TR)

CYBER; Deployment Considerations for Hybrid Schemes, DTR/CYBER-QSC-0021 (TR)

CYBER;
Impact of Quantum Computing on Symmetric Cryptography, DTR/CYBER-QSC-0022 (TR)

How to participate

ETSI members can attend the meetings – etsi.org

27 – 28 September – CYBER QSC#27 (Sophia Antipolis, FR)

12 December – CYBER QSC#28 (Sophia Antipolis, FR)

9th ETSI-IQC Quantum-Safe Cryptography Workshop

Date:

13 – 15 February 2023

Call for participation:

16 September 2022 – 22 October 2022

Location:

ETSI Headquarters, Sofia-Antipolis, FR

Thank you!