

# PQC @ ETSI

Matthew Campagna

2023-03-03



# Outline



A brief history of the TC CYBER WG QSC

Basic information about the working group today

Completed Technical Recommendations and Specifications

Concatenate & Cascade Hybrid Key Exchanges

Current Work Items

How to participate in ETSI TC CYBER WG QSC

AWS's perspective on PQ migration

# ETSI



## European Telecommunication Standards Institute

- Regionalized standards body focused on ITS
  - 29 Technical Committees, 17 Industry Specification Groups, 2 Open Source Groups
- Special role in Europe to produce Harmonized European Standards (CEN, CENELEC, ETSI)
- Partners in 3GPP and oneM2M
- Funded through membership and EC, Europe Free Trade Association (EFTA)
- Director-General: Luis Jorge Romero

# ETSI TC CYBER WG QSC



2013 1<sup>st</sup> ETSI-IQC Quantum Safe Cryptography Workshop

2015 ETSI published the Quantum Safe Cryptography and Security Paper

2015 ETSI Industry Specification Group (ISG) on QSC

2017 QSC becomes a working group of TC CYBER

Meetings are coordinated with CYBER, meet 4 times a year in Sophia-Antipolis

# ETSI TC CYBER WG QSC



Chair: Matthew Campagna (Amazon)

Vice chairs:

Philip Lafrance (ISARA)

Dan Grundy (NCSC)

Secretary: Anthony Barnett (Thales)

Technical Officer: Sonia Compans (ETSI)

Healthy participation: 30 – 40 registered participants from corporate/government/academia

# Finished TR/TS



CYBER; Quantum-Safe Key Exchanges, [ETSI TR 103 507 V1.1.1 \(2017-10\)](#)

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; Quantum-Safe Virtual Private Networks, [ETSI TR 103 617 V1.1.1 \(2018-09\)](#)

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

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

State Management for stateful authentication mechanisms, [ETSI TR 103 692 V1.1.1 \(2021-11\)](#)

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

# Concatenate hybrid key exchange

Alice

$(d, P) = \text{Generate}()$   
 $(sk, R) = \text{Generate}()$

Form  $M_A = (P, R, \dots)$

Bob

# Concatenate hybrid key exchange

Alice

$(d, P) = \text{Generate}()$   
 $(sk, R) = \text{Generate}()$

Form  $M_A = (P, R, \dots)$

$M_A$



Bob

$(k, Q) = \text{Generate}()$   
 $ss, CT = \text{Encaps}(R)$

Form  $M_B = (Q, CT, \dots)$



# Concatenate hybrid key exchange

Alice

$(d, P) = \text{Generate}()$   
 $(sk, R) = \text{Generate}()$

Form  $M_A = (P, R, \dots)$

$ss = \text{Decaps}(sk, CT)$

$\text{secret} = dQ \parallel ss$

$\text{key} = \text{KDF}(\text{secret}, M_A \parallel M_B)$

$M_A$

$M_B$

Bob

$(k, Q) = \text{Generate}()$   
 $ss, CT = \text{Encaps}(R)$

Form  $M_B = (Q, CT, \dots)$

$\text{secret} = kP \parallel ss$

$\text{key} = \text{KDF}(\text{secret}, M_A \parallel M_B)$

# Concatenate hybrid key exchange

Alice

$(d, P) = \text{Generate}()$   
 $(sk, R) = \text{Generate}()$

Form  $M_A = (P, R, \dots)$

$ss = \text{Decaps}(sk, CT)$

$\text{secret} = dQ \parallel ss$

$\text{key} = \text{KDF}(\text{secret}, M_A \parallel M_B)$

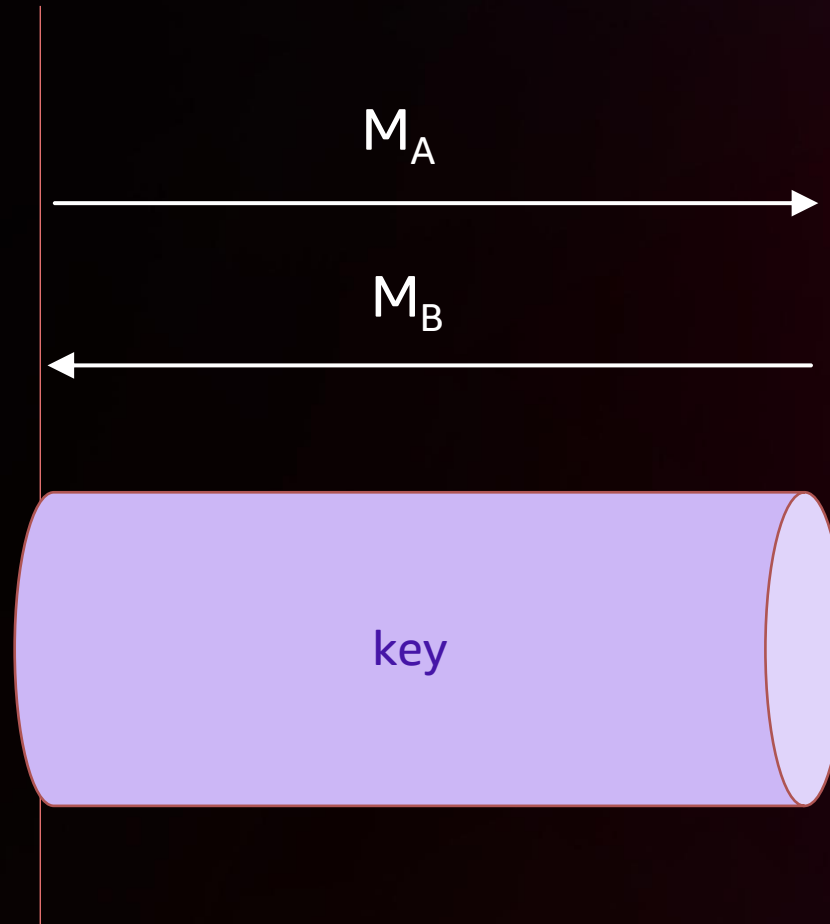
Bob

$(k, Q) = \text{Generate}()$   
 $ss, CT = \text{Encaps}(R)$

Form  $M_B = (Q, CT, \dots)$

$\text{secret} = kP \parallel ss$

$\text{key} = \text{KDF}(\text{secret}, M_A \parallel M_B)$



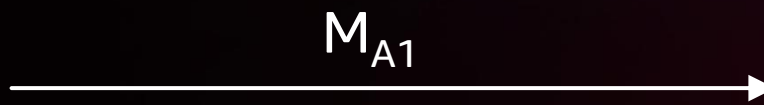
# Cascade hybrid key exchange

Alice

$(d, P) = \text{Generate}()$   
Form  $M_{A1} = (P, \dots)$

$M_{A1}$

Bob



# Cascade hybrid key exchange

Alice

$(d, P) = \text{Generate}()$   
Form  $M_{A1} = (P, \dots)$

$M_{A1}$

$M_{B1}$

Bob

$(k, Q) = \text{Generate}()$   
Form  $M_{B1} = (Q, \dots)$

# Cascade hybrid key exchange

Alice

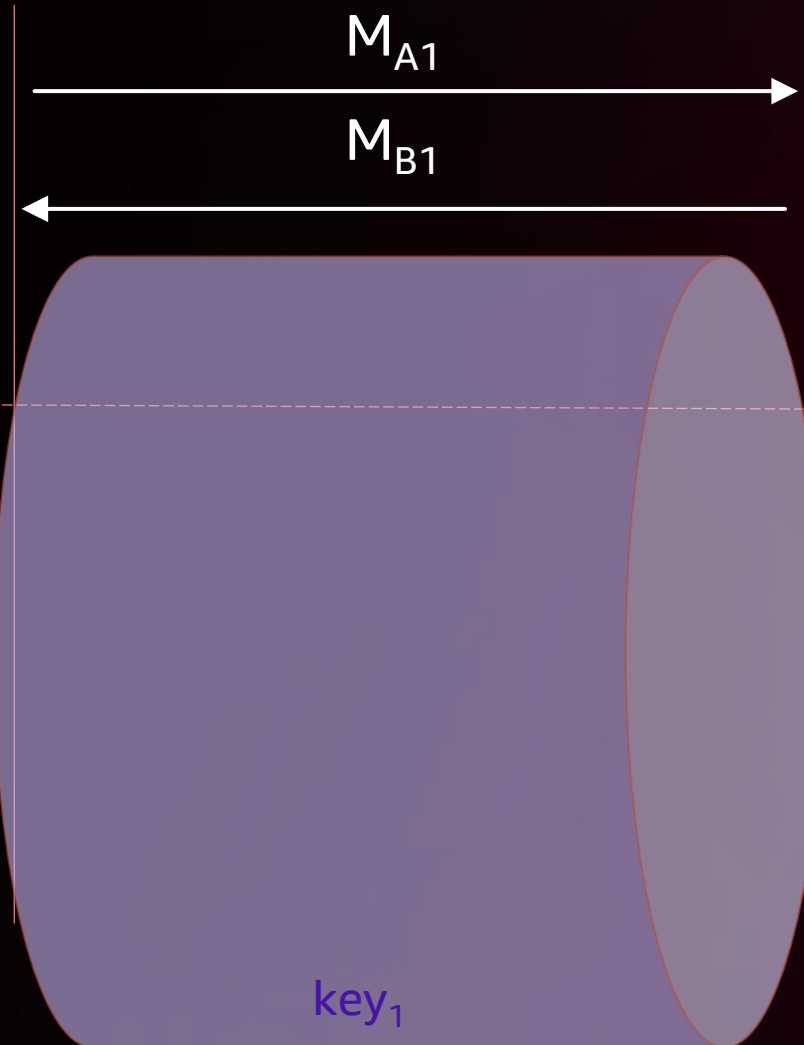
$(d, P) = \text{Generate}()$   
Form  $M_{A1} = (P, \dots)$

$\text{secret} = \text{PRF}(cs, dQ, M_{A1}, M_{B1})$   
 $cs \parallel \text{key}_1 = \text{KDF}(\text{secret}, \dots)$

Bob

$(k, Q) = \text{Generate}()$   
Form  $M_{B1} = (Q, \dots)$

$\text{secret} = \text{PRF}(cs, kP, M_{A1}, M_{B1})$   
 $cs \parallel \text{key}_1 = \text{KDF}(\text{secret}, \dots)$



# Cascade hybrid key exchange

Alice

$(d, P) = \text{Generate}()$   
Form  $M_{A1} = (P, \dots)$

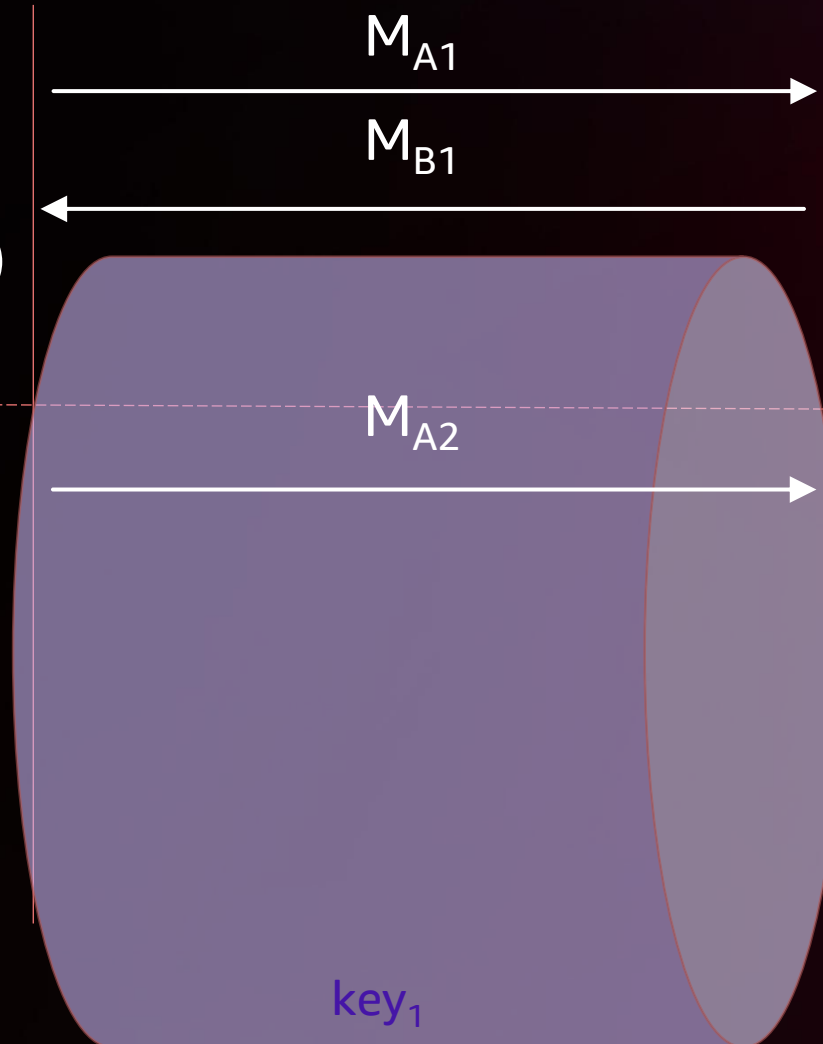
$\text{secret} = \text{PRF}(cs, dQ, M_{A1}, M_{B1})$   
 $cs \parallel \text{key}_1 = \text{KDF}(\text{secret}, \dots)$

$(sk, R) = \text{Generate}()$   
Form  $M_{A2} = (R, \dots)$

Bob

$(k, Q) = \text{Generate}()$   
Form  $M_{B1} = (Q, \dots)$

$\text{secret} = \text{PRF}(cs, kP, M_{A1}, M_{B1})$   
 $cs \parallel \text{key}_1 = \text{KDF}(\text{secret}, \dots)$



# Cascade hybrid key exchange

Alice

$(d, P) = \text{Generate}()$   
Form  $M_{A1} = (P, \dots)$

$\text{secret} = \text{PRF}(cs, dQ, M_{A1}, M_{B1})$   
 $cs \parallel \text{key}_1 = \text{KDF}(\text{secret}, \dots)$

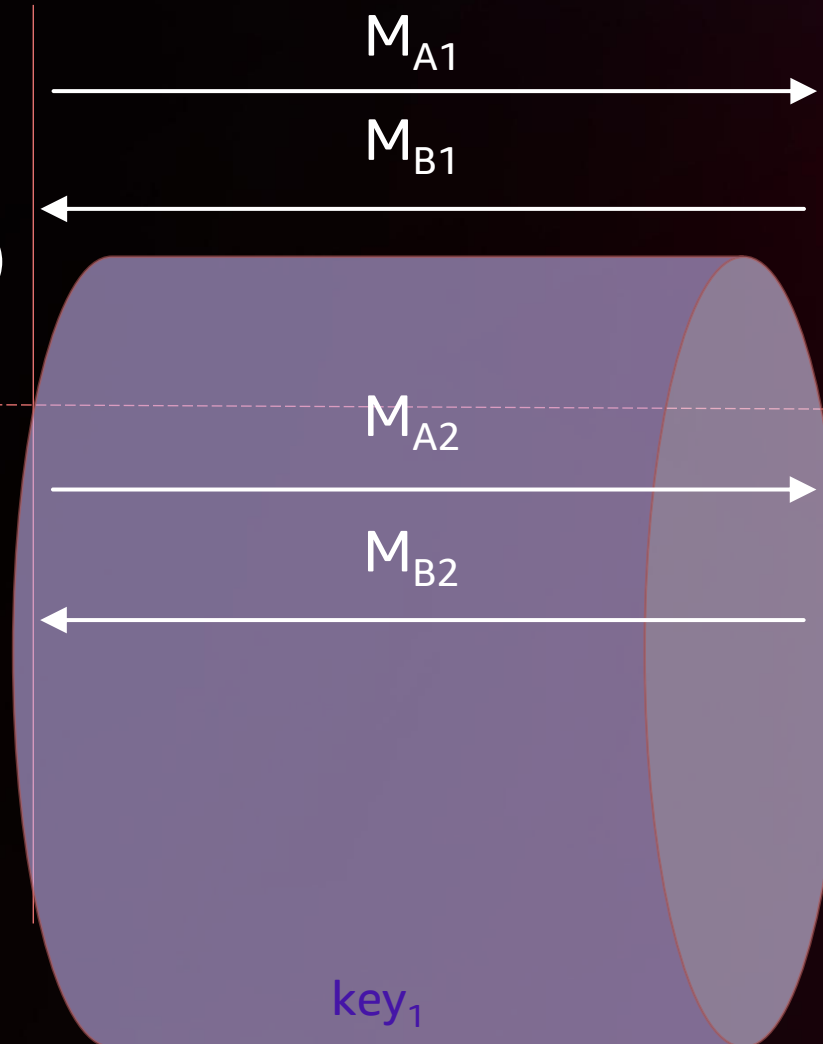
$(sk, R) = \text{Generate}()$   
Form  $M_{A2} = (R, \dots)$

Bob

$(k, Q) = \text{Generate}()$   
Form  $M_{B1} = (Q, \dots)$

$\text{secret} = \text{PRF}(cs, kP, M_{A1}, M_{B1})$   
 $cs \parallel \text{key}_1 = \text{KDF}(\text{secret}, \dots)$

$(ss, CT) = \text{Encaps}(R)$   
Form  $M_{B2} = (CT, \dots)$



# Cascade hybrid key exchange

Alice

$(d, P) = \text{Generate}()$   
Form  $M_{A1} = (P, \dots)$

$\text{secret} = \text{PRF}(cs, dQ, M_{A1}, M_{B1})$   
 $cs \parallel \text{key}_1 = \text{KDF}(\text{secret}, \dots)$

$(sk, R) = \text{Generate}()$   
Form  $M_{A2} = (R, \dots)$

$ss = \text{Decaps}(sk, CT)$   
 $\text{secret} = \text{PRF}(cs, ss, M_{A2}, M_{B2})$   
 $cs \parallel \text{key}_2 = \text{KDF}(\text{secret}, \dots)$

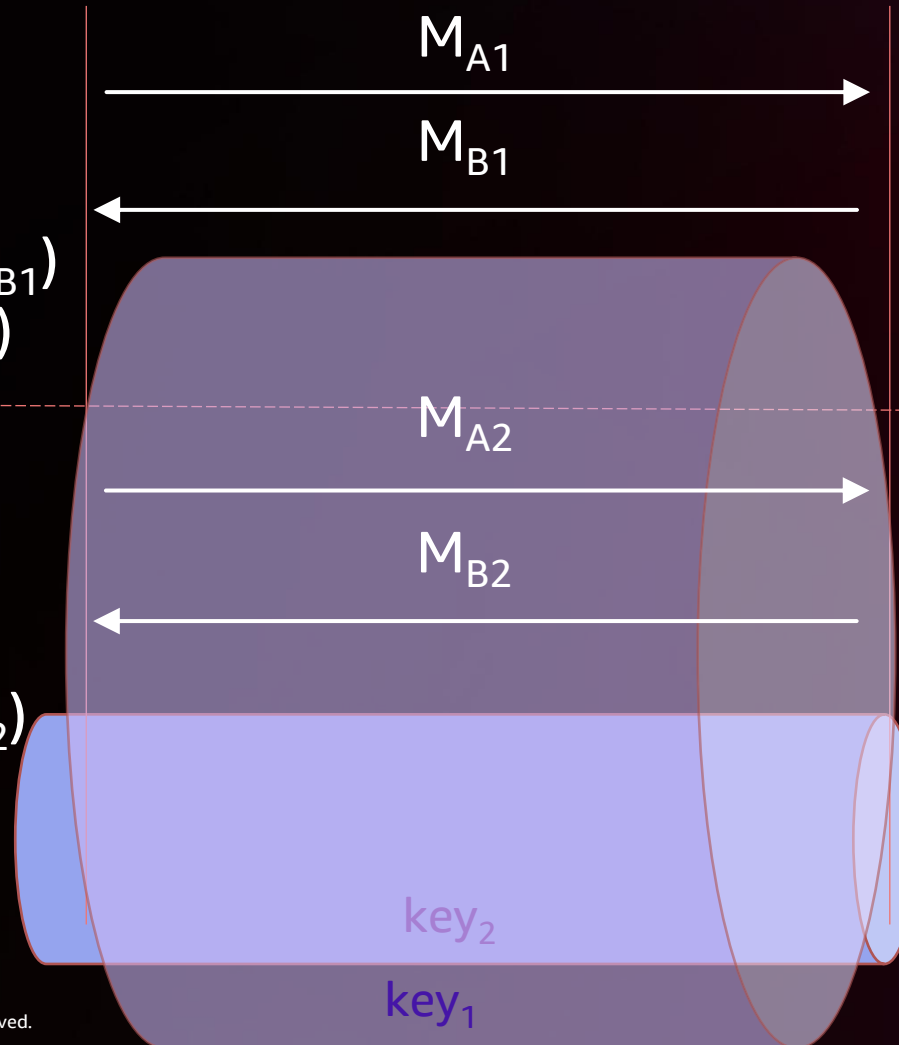
Bob

$(k, Q) = \text{Generate}()$   
Form  $M_{B1} = (Q, \dots)$

$\text{secret} = \text{PRF}(cs, kP, M_{A1}, M_{B1})$   
 $cs \parallel \text{key}_1 = \text{KDF}(\text{secret}, \dots)$

$(ss, CT) = \text{Encaps}(R)$   
Form  $M_{B2} = (Q, \dots)$

$\text{secret} = \text{PRF}(cs, ss, M_{A2}, M_{B2})$   
 $cs \parallel \text{key}_2 = \text{KDF}(\text{secret}, \dots)$





# Current Work Items



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

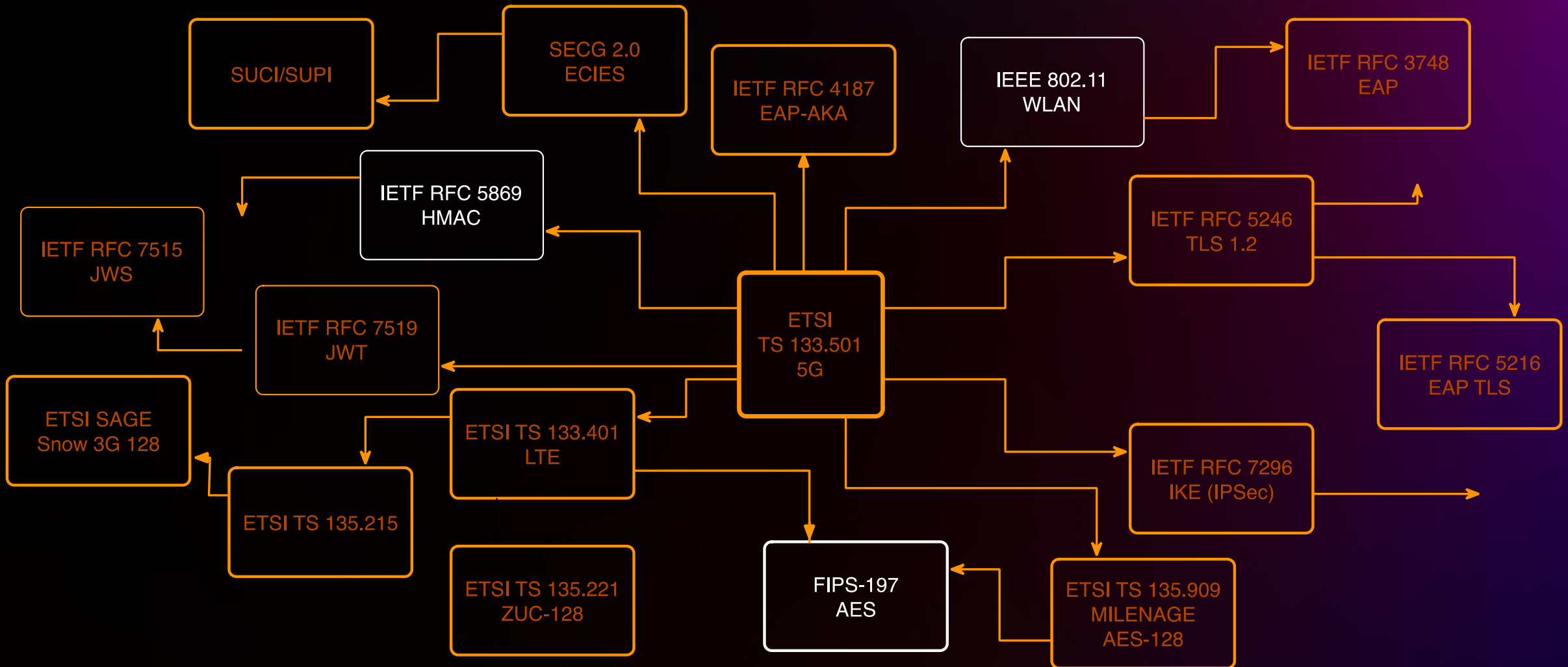
CYBER; Deployment Considerations for Hybrid Schemes, DTR/CYBER-QSC-0021(TR)

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

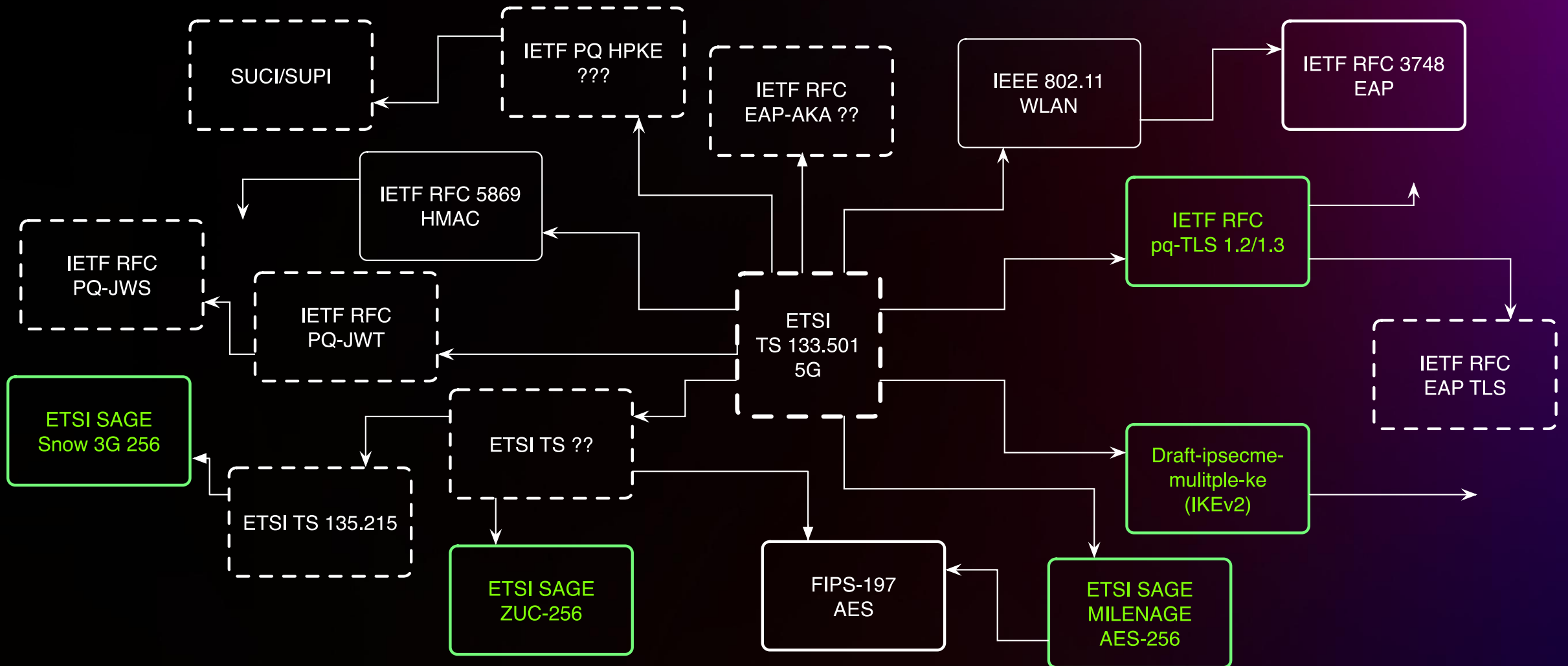
Impact of Quantum Computing on Cryptographic Security Proofs, DTR/CYBER-QSC-0020(TR)

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

# 5G Standards map



# 5G PQ Standards Map



# How to participate



9 Feb 2023 - 1:40:39 AM (GMT+1)  
Sophia Antipolis - France

Home | Resources | People | Services | Manage | IPR | Search | Events | Help | WEBstore

	BOARD	E3MAG	FC	GA	IPR	OCG	3GPP	oneM2M
<b>CYBER</b> Show/Hide groups	CABLE	CYBER	DECT	EE	eHEALTH	EMTEL	ERM	ESI
	LI	MSG	MTS	RRS	RT	SAFETY	SAGE	SES
	STQ	TCCE	TSA	USER	ARF	CDM	CIM	ENI
	mWT	NFV	NIN	OEU	PDL	QKD	RIS	SAI
	TFS	C_Letter	NSO	STF	WORKSHOP			

All of these → CYBER CYBER QSC

Home Meetings Contributions Work Programme Drafts Remote Consensus Actions

## General information - CYBER QSC

### Cyber Security

- [CYBER Terms of Reference](#)
- [CYBER Activity Report](#)
- [CYBER Related Agreements](#)
- [CYBER Published Deliverables](#)
- [CYBER overview presentation](#)
- [CYBER roadmap](#)
- [CYBER Consumer IoT roadmap](#)
- [Templates for Consumer IoT Derivative work](#)
- [QSC White Paper: Quantum Safe](#)
- [QSC Published Deliverables](#)
- [CYBER public wiki](#)
- [CYBER Open Area \(public drafts\)](#)



# How to participate



23 May – CYBER QSC#30 (Sophia Antipolis, FR)

19 September – CYBER QSC#31 (Sophia Antipolis, FR)

5 December – CYBER QSC#32 (Sophia Antipolis, FR)

# AWS Cryptography



CloudHSM



Key Management Service



Secrets Manager



Certificate Manager



Signer



AWS Encryption SDK and LibCrypto Libraries



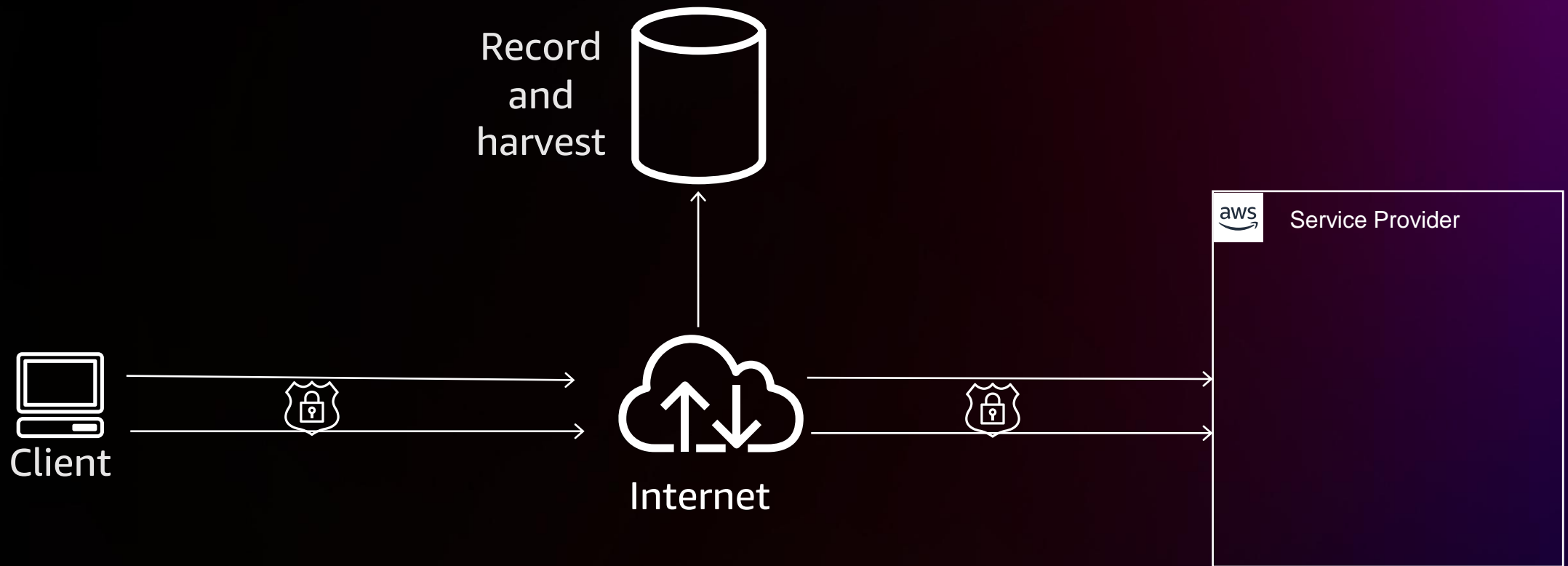
AWS OpenSource TLS and QUIC protocols

AWS Crypto Bar Raisers

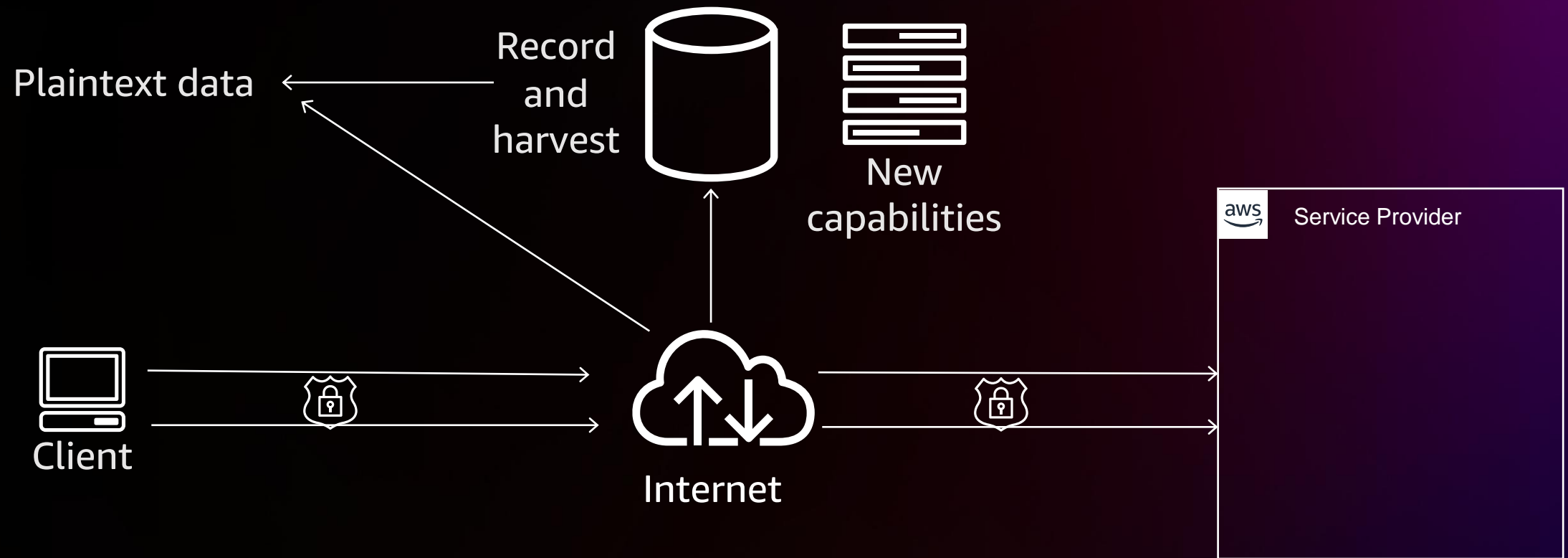
Post-quantum cryptography

Cryptographic computing

# Long-term confidentiality

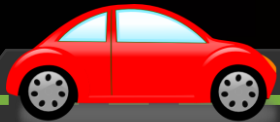
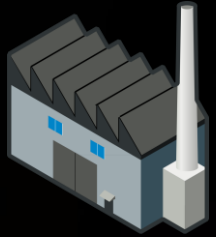


# Long-term confidentiality



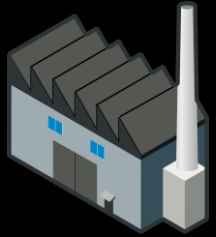


# Long-term roots of trust



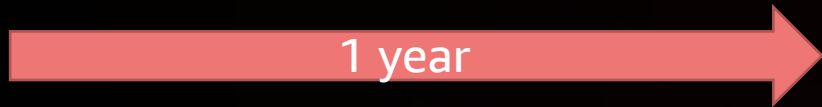
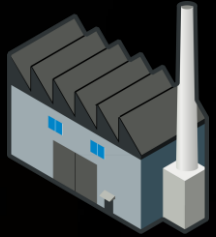
<http://clipart-library.com/clipart/cars-clipart-2.htm>

# Long-term roots of trust



<http://clipart-library.com/clipart/cars-clipart-2.htm>

# Long-term roots of trust



<http://clipart-library.com/clipart/cars-clipart-2.htm>

# Long-term roots of trust



13 years

<http://clipart-library.com/clipart/cars-clipart-2.htm>

# Recent US Government News

## 2022-05-04 National Security Memorandum on mitigating risks due to QC

- 90 days, Establish Migration to Post-Quantum Cryptography Project at NIST.
- 180 days, Establish Requirements for inventorying all currently deployed cryptographic systems (with NIST, CISA and NSA)

## 2022-09 CNSA 2.0 - Commercial National Security Algorithm Suite 2.0

- 2033 - Forecast transition to quantum-resistant cryptography
- 2025 – Suggested transition to QR firmware and software signing

## 2022-11-18 OMB Memo Migrating to Post-Quantum Cryptography

- 2023-05-04 date for Agencies to provide initial inventory for high impact or High Value Assets systems

## H.R.7535 - Quantum Computing Cybersecurity Preparedness Act

- 180 days - Director of OMB (with CISA) issue guidance on inventory and migration to PQC.
- 1 year – Agencies shall provide OMB with inventory and develop a plan for migration.

# How is AWS Preparing?



## CORE STANDARDS

---

### NIST

- PQC Standards

### ETSI – Quantum Safe Cryptography

- PQ Hybrid Standards
- PQ Migration



## PROTOCOLS

---

### IETF

- PQ-TLS 1.2 and 1.3
- PQ SSH
- PQ Signatures in X.509
- PQ KEMs in X.509
- PQ QUIC



## LIBRARIES

---

### s2n-TLS

- PQ Hybrid TLS 1.3 in s2n
- Available in AWS KMS, ACM, Secrets Manager

### AWS-LC

- PQ key exchange and Signature schemes

### AWS Java SDK w/ CRT



## COLLABORATIONS

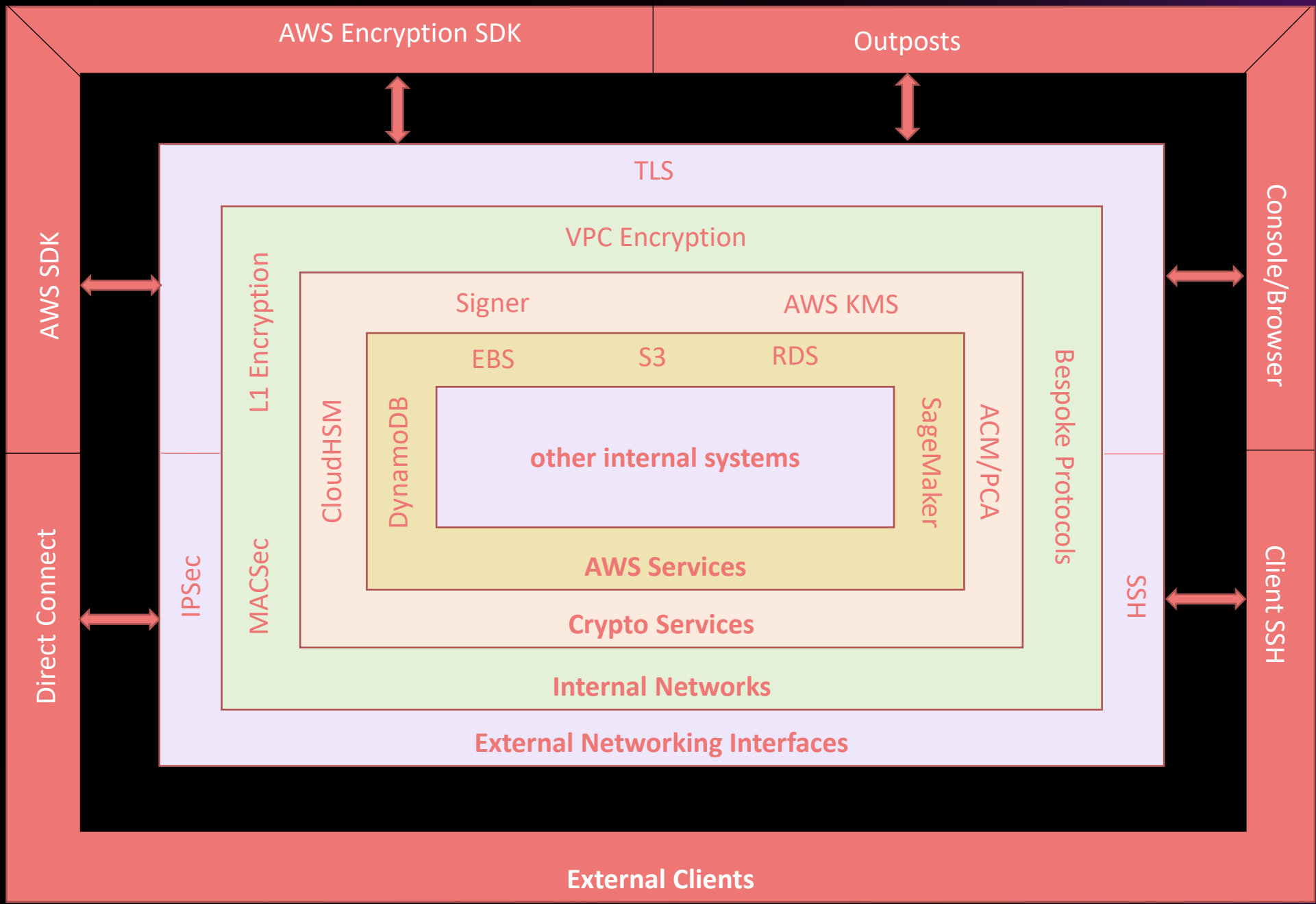
---

### NCCoE

- Industry PQ-migration experiments

### University of Waterloo

- Open Quantum Safe libOQS



# Migration (as fast as possible)

Phase 0 (+2 years): Inventory of existing systems, identification & development of new standards, testing, migration plans.

Phase 1 (0 – 5 years): Deployment of PQ-KEMs for long-term confidentiality

(opportunistic with agile systems now, and less agile systems after standardization)

Phase 2: (2 – 5 years): Deployment of new PQ long-lived roots of trust

(smaller, specialized or closed systems moving to use)

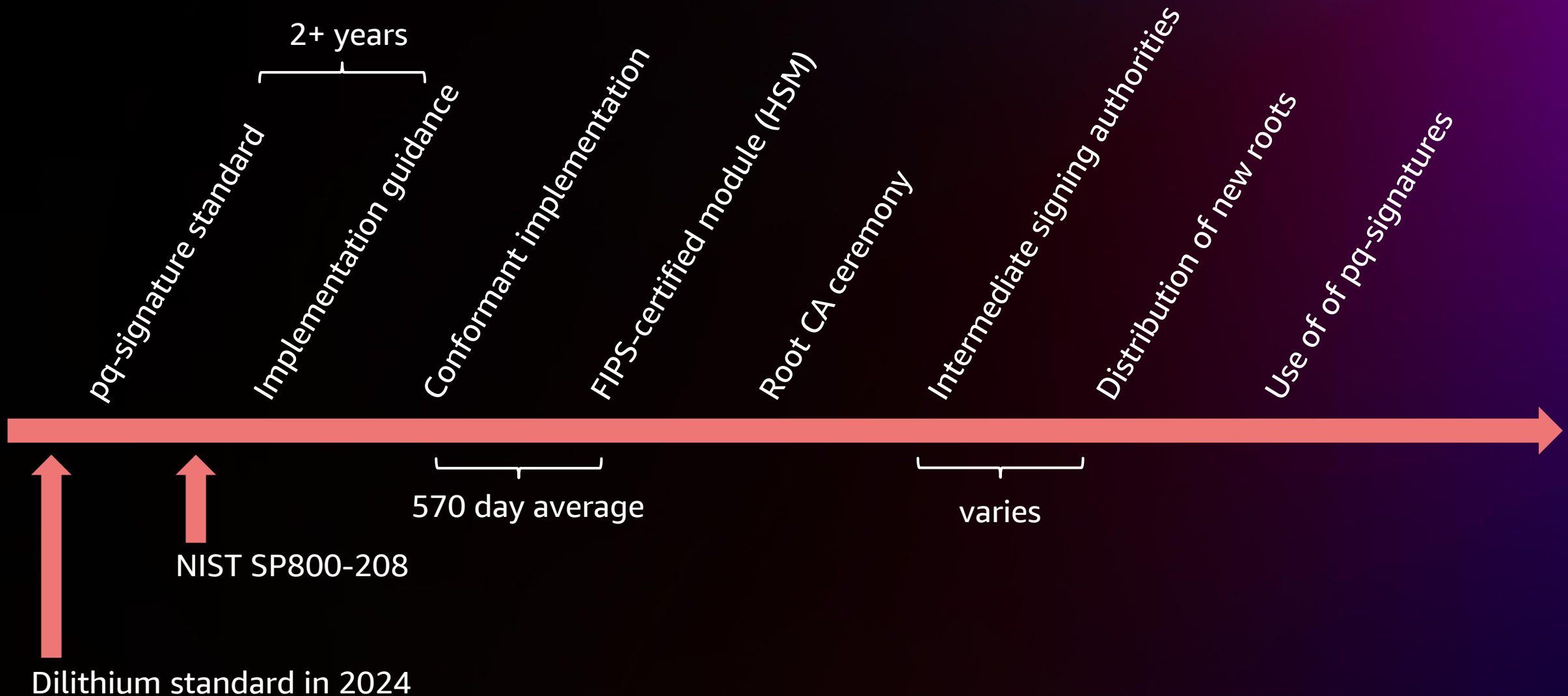
Phase 3: (T – 5 years): Wide-scale use of PQ signatures



NOTE: This slide does not represent AWS's pq migration timeline – rather it states an opinion that this is the fastest an entity could prudently move to pqc.



# Timeline for stateful-HBS signing authority



# Question

## Background:

- NIST has published NIST SP800-208 on Stateful Hash-Based Signatures (sHBS), a quantum resistant scheme.
- NSA has updated CNSA 2.0 to recommend that government systems begin transitioning to this by 2025 for firmware and software authentication.

## Question:

How urgent are your needs for sHBS?

# References

<https://aws.amazon.com/security/post-quantum-cryptography/>

<https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/>

[https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA\\_CNSA\\_2.0\\_ALGORITHMS\\_.PDF](https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF)

<https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf>

<https://www.congress.gov/bill/117th-congress/house-bill/7535/text>



# Thank you!

