

# Migrating Telecom to Quantum-Resistant Cryptography on a Global Scale

**John Preuß Mattsson**

Expert Cryptographic Algorithms and Security Protocols, Ericsson  
MSc Engineering Physics/Theoretical Computer Science  
MSc Business Administration and Economy

April 9, 2025



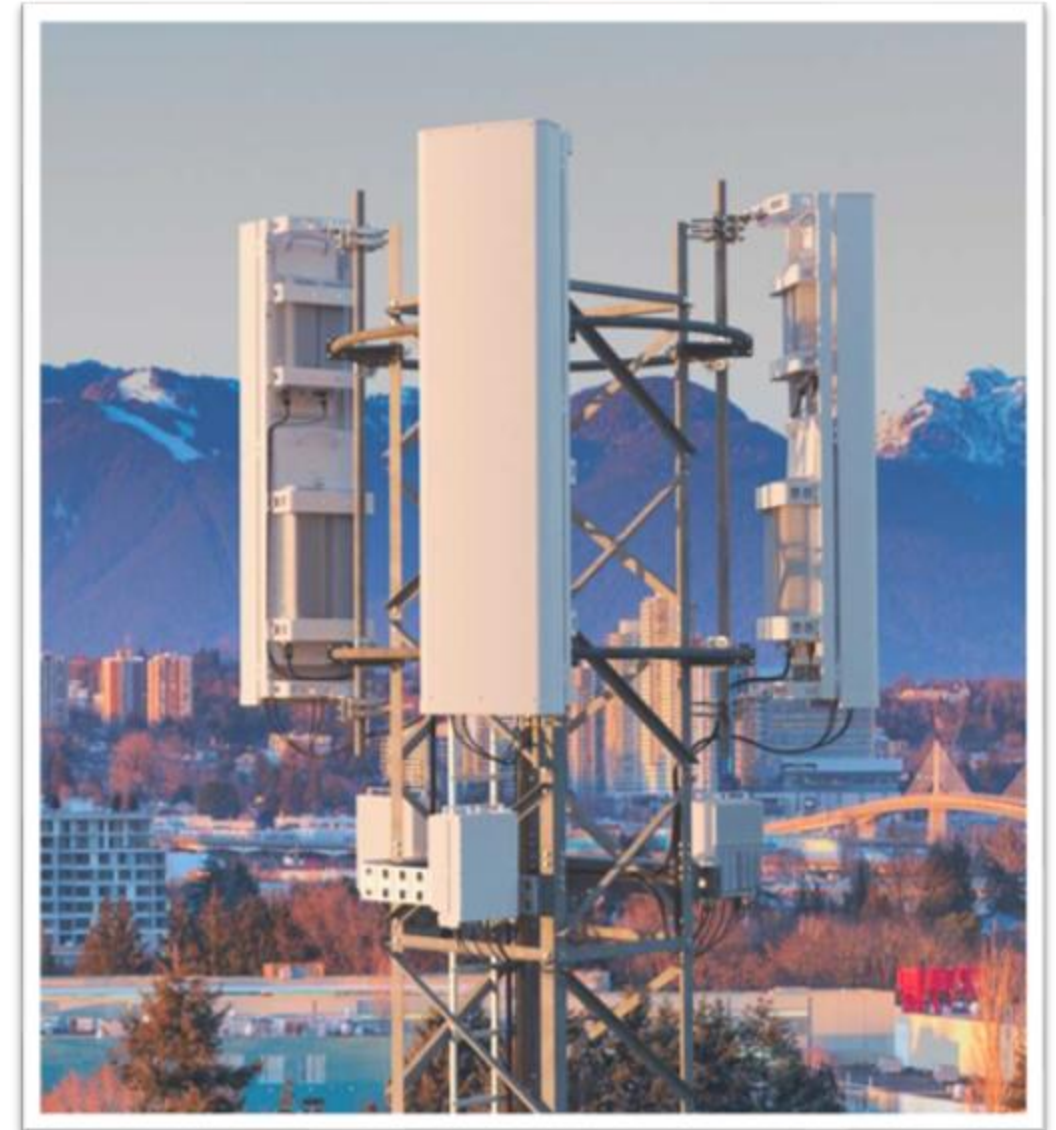
# 4G, 5G, and 6G – truly global standards




# Characteristics of the telecom industry



- Highly regulated
- Mostly licenced spectrum
- High reliance on standardization (3GPP, ORAN, GSMA, etc.)
- Critical infrastructure
- Increased use for public safety and industry
- High security and privacy requirements
- Rapid technological evolution
- High competition & consolidation
- Operators, infrastructure, smartphone, and chipset vendors



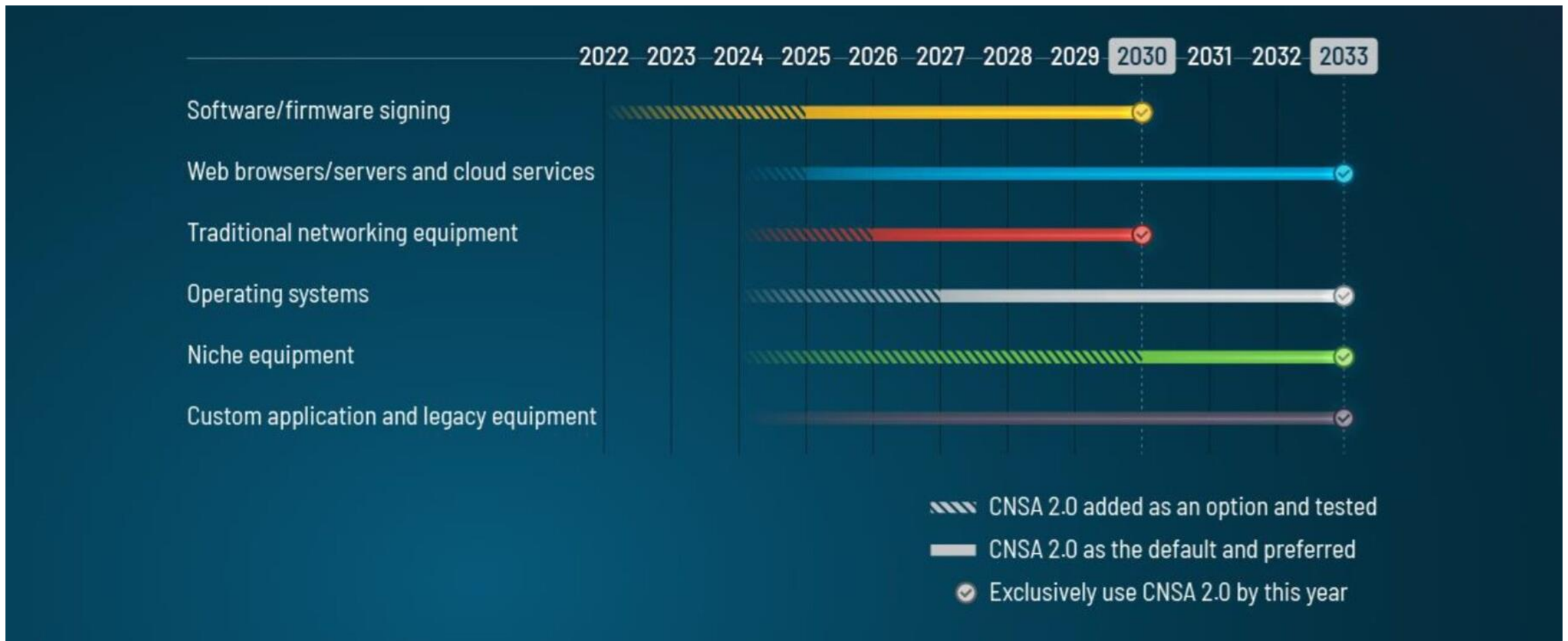
A large billboard with a black background and white text, set against a clear blue sky. The billboard is supported by two black poles and has a metal frame. The text is written in a clean, sans-serif font and is centered on the billboard. The billboard is tilted slightly to the right.

The transition to quantum-resistant  
cryptography presents an excellent  
opportunity to reassess out-dated  
algorithms and practices that no longer  
meet acceptable security standards

# Migration timelines for telecom



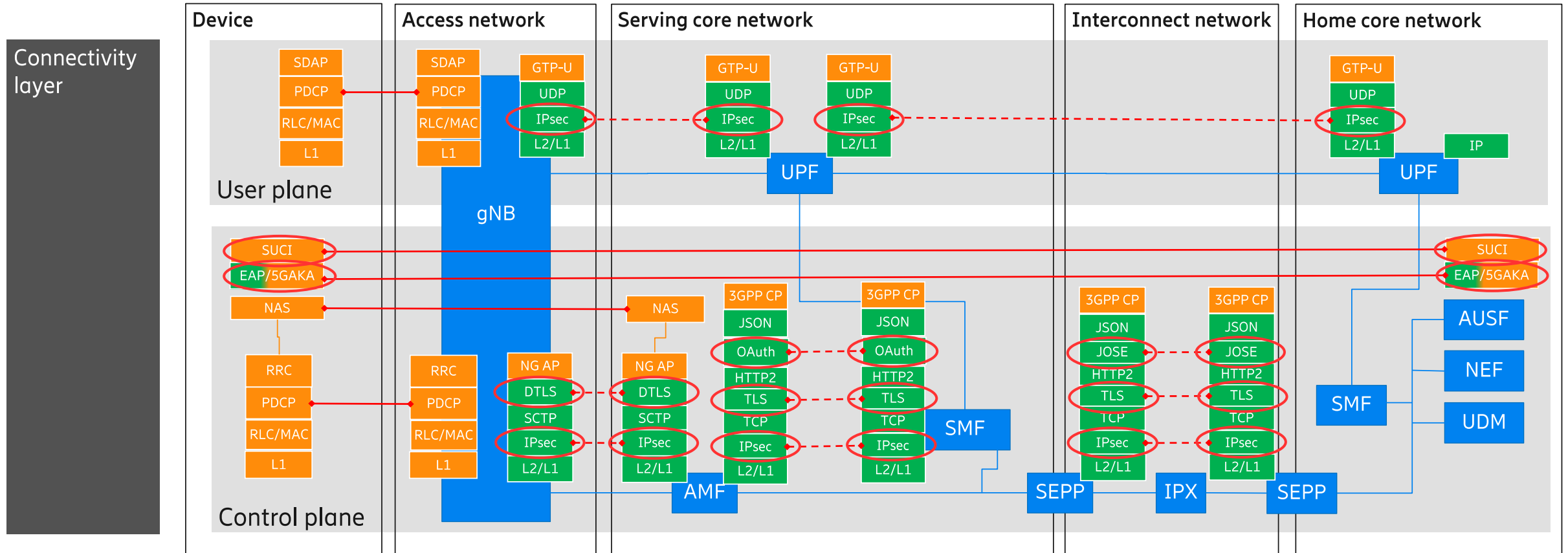
- Countries and agencies globally generally align on migration timelines.
  - Migrate as soon as possible, prioritized systems by 2030, and all systems by 2035
  - Only use standardized algorithms and protocols.



# Public-key crypto in the 3GPP 5G connectivity layer



- 5G relies on IETF protocols like IKEv2, TLS 1.3, DTLS, JOSE, Internet X.509 profile, CMP, CRL, OCSP, EAP-TLS, and EAP-AKA-FS for almost all uses of public-key cryptography.
- IMSI encryption uses the SECG ECIES standard but augments it with X25519 (RFC 7748).
- **Conclusion: IETF is essential for PQC migration in 5G and 6G.**

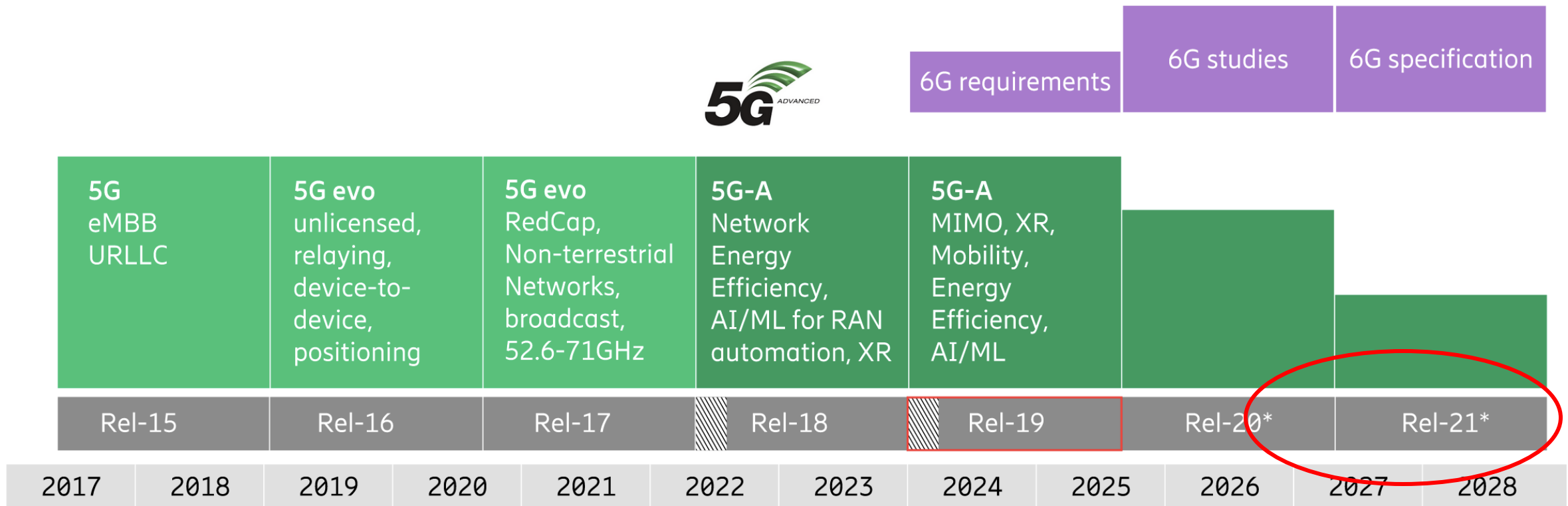




# 3GPP 5G and 6G timelines

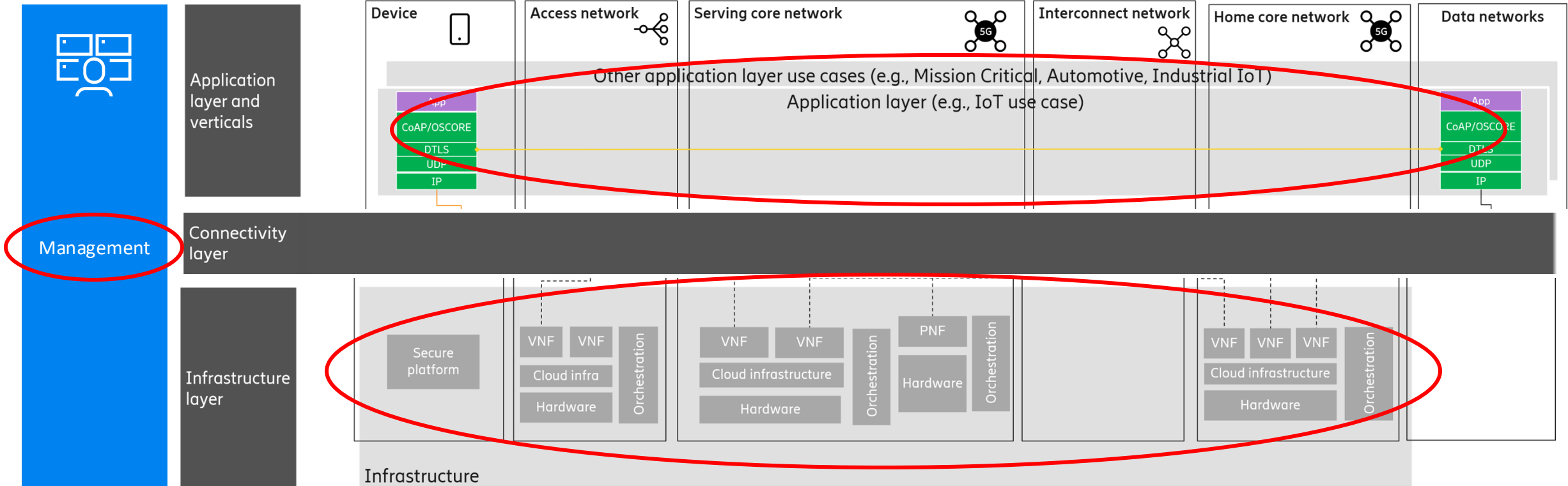


- 5G and 6G will both migrate to PQC. 6G will be fully quantum-resistant from the start.
- Focus on ML-KEM (FIPS 203), ML-DSA (FIPS 204), and SLH-DSA (FIPS 205).
- Need hardened (sometimes certified) software and hardware implementations of final NIST and IETF standards.



\*Indicative timeline

# Application, infrastructure, and management layers



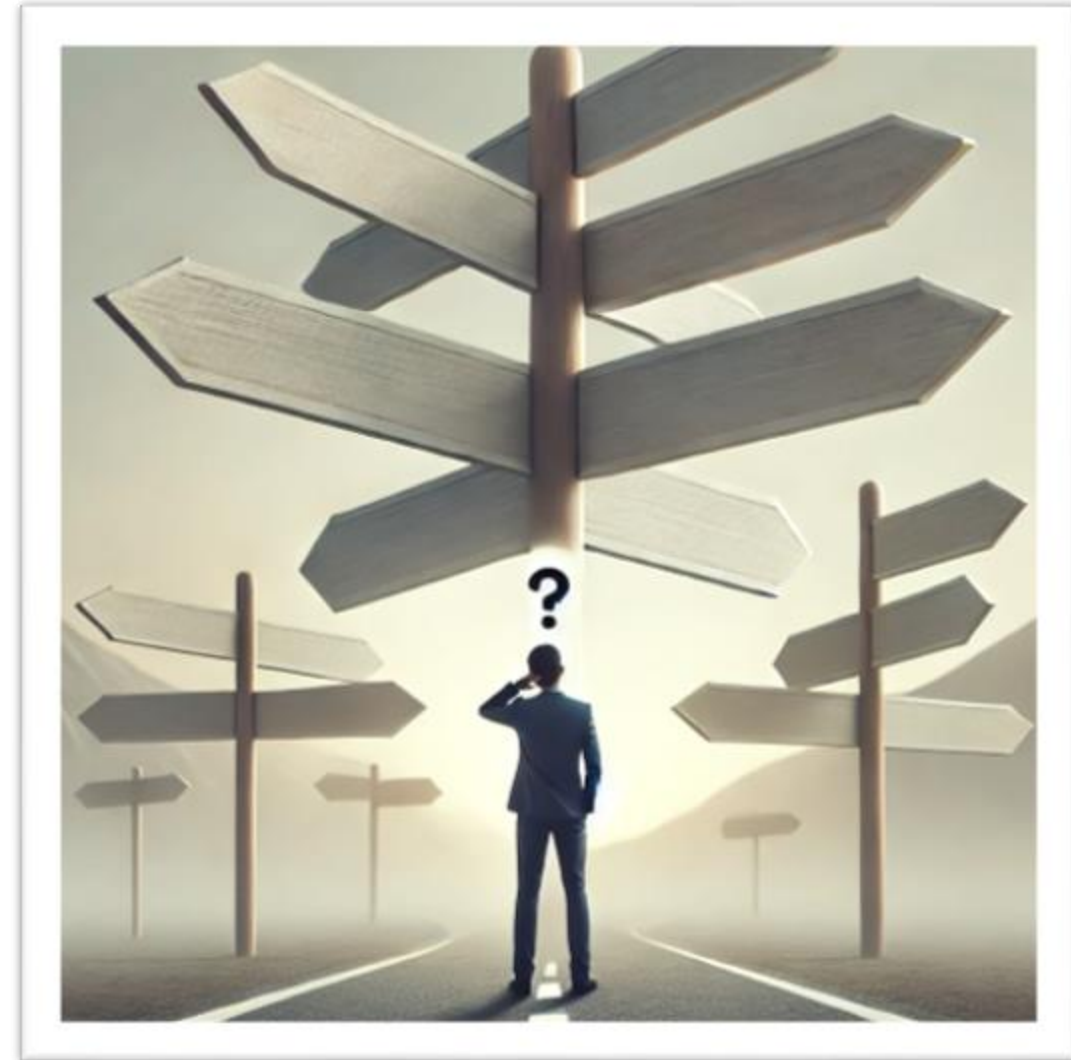
- In addition to the protocols in the connectivity layer application, management, and infrastructure layer also use public-key cryptography in DTLS-SRTP, MIKEY-SAKKE, ACE, COSE, SSH.
- Signatures for secure boot, remote attestation, firmware updates, software signing, etc., not standardized by 3GPP.
  - Firmware update for 5G nodes is a high-value target and migration needs to be prioritized.
  - Ericsson plans to support SLH-DSA-SHAKE-256s, ML-DSA-87 in hybrid with Ed448, and standalone ML-DSA-87.



# PQC requirements from various national bodies



- Most government agencies are now recommending ML-KEM, ML-DSA, and SLH-DSA. However:
  - Some require hybridization of ML-KEM and ML-DSA, while other forbid hybridization.
  - Some allow all security levels, some recommend level 3, and some require level 5.
  - Some recommend SLH-DSA, while other forbid SLH-DSA.
  - Some require LMS/XMSS single-tree, while other recommend multi-tree.
  - P-256, P-384, and Brainpool curves are increasingly seen as regional algorithms with Curve25519/448 being the globally preferred curves with superior security and performance.
  - Some recommend SHA-3 (ML-KEM, ML-DSA, and Ed448 use SHA-3 internally) while other require SHA-2.



# IETF and 3GPP statements on symmetric cryptography



## IETF Statement:

- “The idea that symmetric cryptography will be practically affected by CRQCs is now seen as a misconception. The “bits of security” concept does not work with algorithms that are not parallelizable and NIST is therefore transitioning to quantum-resistant security levels based on symmetric algorithms where level 1 is equivalent with AES-128, level 2 is SHA-256, etc. UK government assesses that “symmetric algorithms with at least 128-bit keys (such as AES) can continue to be used”. **While classical supercomputers might be able to brute force AES-128 around the year 2090**, a huge cluster of one billion CRQCs (according to one estimate costing one billion USD each) would take a million years of uninterrupted calculation to find a single AES-128 key. **Algorithms with quadratic ( $n^2$ ) speedup like Grover’s algorithm (which is proven to be optimal) will not provide any practical quantum advantage for breaking symmetric cryptography and likely not for any other problems.”**

## 3GPP Statement:

- “A very good summary of the impact of Cryptographically Relevant Quantum Computers (CRQCs) on symmetric cryptography was recently given in a statement by the Internet Engineering Task Force (IETF). The IETF statement refers to UK NCSC whitepaper that says symmetric algorithms with at least 128-bit keys (such as AES) can continue to be used. **SA3 agrees with IETF’s analysis.** Most other 128-bit algorithms such as SNOW 3G, ZUC, TUAK, KMAC128, Ascon, etc. are likely to have similar quantum overhead for Grover’s algorithm which is known to be optimal. Even if an algorithm has slightly lower quantum overhead than AES-128, SA3 believes the algorithm would still fulfill the requirement (comparable to key search on AES-128) for quantum resistance category 1”

(but 6G will likely use high-performance 256-bit algorithms)

**Sam Jaques keynote at CHES 2024:** “Qubits would cover the moon”

**NIST 2024:** “All NIST-approved symmetric primitives that provide at least 128 bits of classical security are believed to meet the requirements of at least Category 1 security”

# 3GPP/ETSI/GSMA Algorithms



Algorithms for authentication and key generation:

Cipher	Proprietary	Proprietary	Proprietary	AES/Rijndael-256	Keccak
Input key size	128	128	128	128, 256	128, 256
Output key size	54	54	64	128, 256	128, 256
Name	COMP-128-1	COMP-128-2	COMP-128-3	MILENAGE(-256)	Tuak

Algorithms for encryption and integrity: (\*A5/2 and GEA1 are export ciphers with no more than 40 bits effective security):

Cipher	Proprietary	Proprietary	KASUMI	KASUMI	KASUMI	SNOW 3G	SNOW 3G	AES	AES	ZUC	ZUC
Key size	64*	64	64	128	128	128	128	128	128	128	128
Mode	XOR	XOR	f8-mode	f8-mode	CBC-MAC	XOR	CW-MAC1	CTR	CMAC	XOR	CW-MAC2
Type	ENC	ENC	ENC	ENC	INT	ENC	INT	ENC	INT	ENC	INT
Tag size					32		32		32		32
GSM	A5/2	A5/1	A5/3	A5/4							
GPRS	GEA1	GEA2	GEA3	GEA4	GIA4	GEA5	GIA5				
UMTS				UEA1	UIA1	UEA2	UIA2				
LTE						128-EEA1	128-EIA1	128-EEA2	128-EIA2	128-EEA3	128-EIA3
NR						128-NEA1	128-NIA1	128-NEA2	128-NIA2	128-NEA3	128-NIA3



# 6G will likely use 256-bit algorithms



- Work initiated (in 2017), partly because of worries regarding quantum attacks now seen as a misconception.
- ETSI SAGE has specified AES-256, SNOW 5G, and ZUC-256 in GCM-SST mode. Many benefits:
  - Much faster in both software and hardware
  - Longer authentication tags that behaves like ideal MACs
  - Compliance with government requirement
  - Improved security against multi-key attacks

Name	Tag length (bytes)	Forgery probability before first forgery	Forgery probability after first forgery	Expected number of forgeries
GCM_SST_14	14	$1 / 2^{112}$	$1 / 2^{112}$	$v / 2^{112}$
GCM_SST_12	12	$1 / 2^{96}$	$1 / 2^{96}$	$v / 2^{96}$
POLY1305	16	$1 / 2^{91}$	$1 / 2^{91}$	$v / 2^{91}$
GCM	16	$1 / 2^{116}$	1	$\delta \cdot v^2 / 2^{117}$

*Table 1: Comparison between AES-GCM-SST, ChaCha20-Poly1305, and AES-GCM in unicast QUIC where the maximum packet size is  $2^{16}$  bytes.  $v$  is the number of decryption queries and  $\delta$  is the Bernstein bound factor.*

# Backup algorithms and hybrids



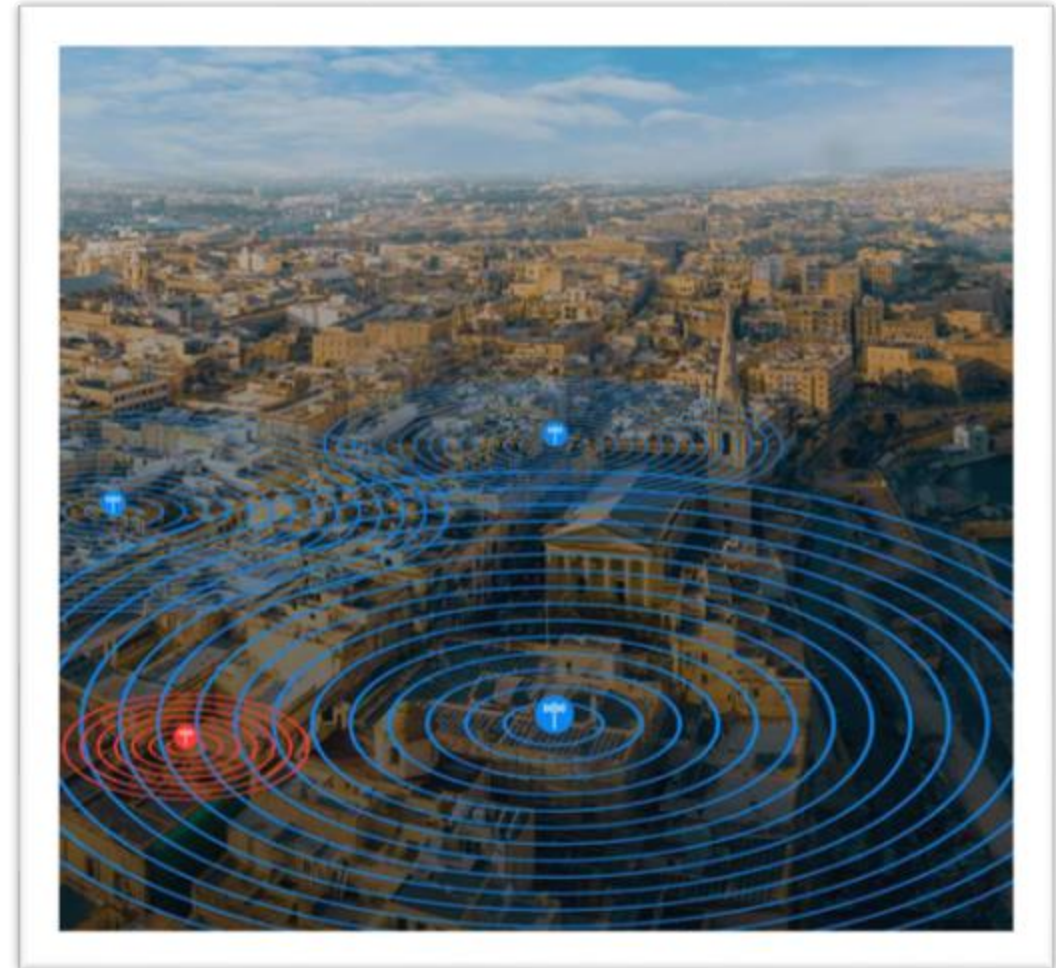
- To meet time requirements, telecom will need to pick the first available PQC implementations and use them in production systems.
- Many early implementation have bugs and side-channels. Hybrids are a cheap defense-in-depth.
- HQC and Classic McEliece are good backup algorithms to ML-KEM.
- Standards for backup algorithms might not be available until later.



# Key conclusions



- Regulators agree on migration timelines and algorithms (ML-KEM, ML-DSA, SLH-DSA).
- Regulators recommend different parameters.
- Telecom will likely use conservative options (high security level, hash-based or lattice in hybrid, stateless, SHA-3, Curve25519/Curve448).
- IETF is essential for PQC migration in 5G and 6G.
- Quantum computer attacks will have no general practical effect on symmetric crypto (like AES-128).
- **Mobile networks standards and products will support PQC algorithms soon for both 5G and 6G.**





# Further reading



- Ericsson Technology Review, “Quantum technology and its impact on security in mobile networks”  
<https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/ensuring-security-in-mobile-networks-post-quantum>
- Constrained Radio Networks, Small Ciphertexts, Signatures, and Non-Interactive Key Exchange  
<https://csrc.nist.gov/csrc/media/Events/2022/fourth-pqc-standardization-conference/documents/papers/constrained-radio-networks-pqc2022.pdf>
- New Scientist, “Cryptographers bet cash on when quantum computers will beat encryption”  
<https://www.newscientist.com/article/2370022-cryptographers-bet-cash-on-when-quantum-computers-will-beat-encryption/>
- NSA, “Announcing the Commercial National Security Algorithm Suite 2.0”  
[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)
- BSI, ANSSI, Dutch and Swedish NCSA, “Position Paper on Quantum Key Distribution”  
[https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum\\_Positionspapier.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.pdf)
- Ericsson Blog, “Migration to quantum-resistant algorithms in mobile networks”  
<https://www.ericsson.com/en/blog/2023/2/quantum-resistant-algorithms-mobile-networks>
- arXiv, “Quantum-Resistant Cryptography”  
<https://arxiv.org/abs/2112.00399>
- NISTIR 8547, “Transition to Post-Quantum Cryptography Standards”  
<https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf>
- ANSSI, “Guide des Mécanismes cryptographiques”  
[https://cyber.gouv.fr/sites/default/files/2021/03/anssi-guide-mecanismes\\_crypto-2.04.pdf](https://cyber.gouv.fr/sites/default/files/2021/03/anssi-guide-mecanismes_crypto-2.04.pdf)
- Galois Counter Mode with Strong Secure Tags (GCM-SST)  
<https://datatracker.ietf.org/doc/html/draft-mattsson-cfrg-aes-gcm-sst>



# Further reading



- Status of quantum computer development  
[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/Entwicklungstand\\_QC\\_V\\_2\\_0.html?nn=916616](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/Entwicklungstand_QC_V_2_0.html?nn=916616)
- ANSSI plan for post-quantum transition  
[https://pkic.org/events/2023/pqc-conference-amsterdam-nl/pkic-pqcc\\_jerome-plut\\_anssi\\_anssi-plan-for-post-quantum-transition.pdf](https://pkic.org/events/2023/pqc-conference-amsterdam-nl/pkic-pqcc_jerome-plut_anssi_anssi-plan-for-post-quantum-transition.pdf)
- Landscape of Quantum Computing in 2024  
[https://sam-jaques.appspot.com/quantum\\_landscape\\_2024](https://sam-jaques.appspot.com/quantum_landscape_2024)
- On factoring integers, and computing discrete logarithms and orders, quantumly  
<http://kth.diva-portal.org/smash/get/diva2:1902626/FULLTEXT01.pdf>
- IETF Statement on Quantum Safe Cryptographic Protocol Inventory  
<https://datatracker.ietf.org/liaison/1942/>
- 3GPP Statement on PQC Migration  
[https://www.3gpp.org/ftp/tsg\\_sa/WG3\\_Security/TSGS3\\_118\\_Hyderabad/docs/S3-244307.zip](https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_118_Hyderabad/docs/S3-244307.zip)
- Sam Jaques, “Quantum Attacks on AES”  
<https://www.youtube.com/watch?v=eB4po9Br1YY&t=3227s>
- FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA) approved  
<https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved>
- ML-KEM is Great. What’s Missing?  
<https://emanjon.github.io/Publications/ML-KEM%20is%20Great!%20What's%20Missing.pdf>





<https://www.ericsson.com/en/security>