comply

SERVICE OFFERING
OCTOBER 2026

TELECOM OPERATORS · QUANTUM-SAFE CRYPTOGRAPHY

Quantum-safe assessment for telecom operators

One assessment across your IT, your mobile network and your satellite links. Every quantum-vulnerable key and certificate found, ranked by what it protects, and turned into a dated plan your vendors and regulators can work with.

3 layers	End-2030[1]	2035[2]	PQ.03[3]
IT · RAN, core and OSS/BSS · satellite, in one CBOM	EU recommended date for high-risk use cases, critical infrastructure included	RSA and elliptic curves disallowed in NIST's draft transition plan	GSMA telecom guidance every finding maps to, with PQ.05 and PQ.07

Sources: 1 NIS Cooperation Group, coordinated PQC roadmap, June 2025. 2 NIST IR 8547, initial public draft, November 2024. 3 GSMA Post-Quantum Telco Network Taskforce. Full source list on page 5.

BUSINESS AND RISK

Your network carries secrets that outlive its cryptography

Traffic recorded today can be decrypted once a quantum computer of sufficient size exists. An operator is exposed three ways: the data it carries, the equipment it cannot change quickly and the partners it cannot migrate without.

Risk

Harvest now, decrypt later
Subscriber identities, signalling, enterprise and government traffic

Long-lived equipment
RAN and core change on vendor cycles; satellites keep their hardware for life

Trust anchors
eSIM PKI, SIM OTA keys, code signing: one forged signature reaches the fleet

Interconnect
Roaming partners, IPX, SEPP: neither side migrates alone[3]

No cryptography at all
SS7/MAP, GTP-C and legacy management rely on the perimeter

Regulation

NIS2 Art. 21(2)(h)
A cryptography policy for public networks and services, as transposed nationally[4]

EU coordinated roadmap
National roadmaps end-2026 · high-risk end-2030 · the rest by 2035, as far as feasible[1]

UK Telecommunications (Security) Act
Security duties and a code of practice for public networks[5]

NIST IR 8547
112-bit RSA and ECC deprecated after 2030; all RSA and ECC disallowed after 2035 (draft)[2]

GSMA and 3GPP
PQ.03 · PQ.05 · PQ.07 · TR 33.938 · TR 33.703 · Rel-20[3, 6]

Business

Board and supervisors
A dated plan in place of an estimate

Procurement
PQC requirements in RAN, core and satellite tenders before the next refresh

Vendor leverage
Readiness evidence per vendor, per release

Enterprise and public sector
Customers asking what protects their traffic; quantum-safe connectivity as an offer

Cost control
Migration timed to planned refresh cycles, not emergency swaps

What a quantum computer breaks, and where it sits in your network

CRYPTOGRAPHY	WHERE IN A TELECOM NETWORK	EFFECT	REPLACEMENT
Public key: RSA, DH, ECDH, ECDSA, X25519	TLS, IKE, SSH, SUCI, eSIM PKI, certificates, code signing	BROKEN	ML-KEM, ML-DSA, SLH-DSA, LMS; hybrid with classical first[7]
Symmetric, 128-bit: AES-128, MILENAGE/TUAK keys	Radio and SIM authentication, SDLS, data at rest	WEAKENED	256-bit keys and algorithms (3GPP Rel-20)[6]
Hashes: SHA-256 and up	Signatures, key derivation	HOLDS	No change at current sizes[7]

SCOPE

One inventory across IT, the mobile network and space

Every layer ends in the same CycloneDX CBOM, scored the same way, so a SEPP certificate and a VPN gateway are ranked on one scale.

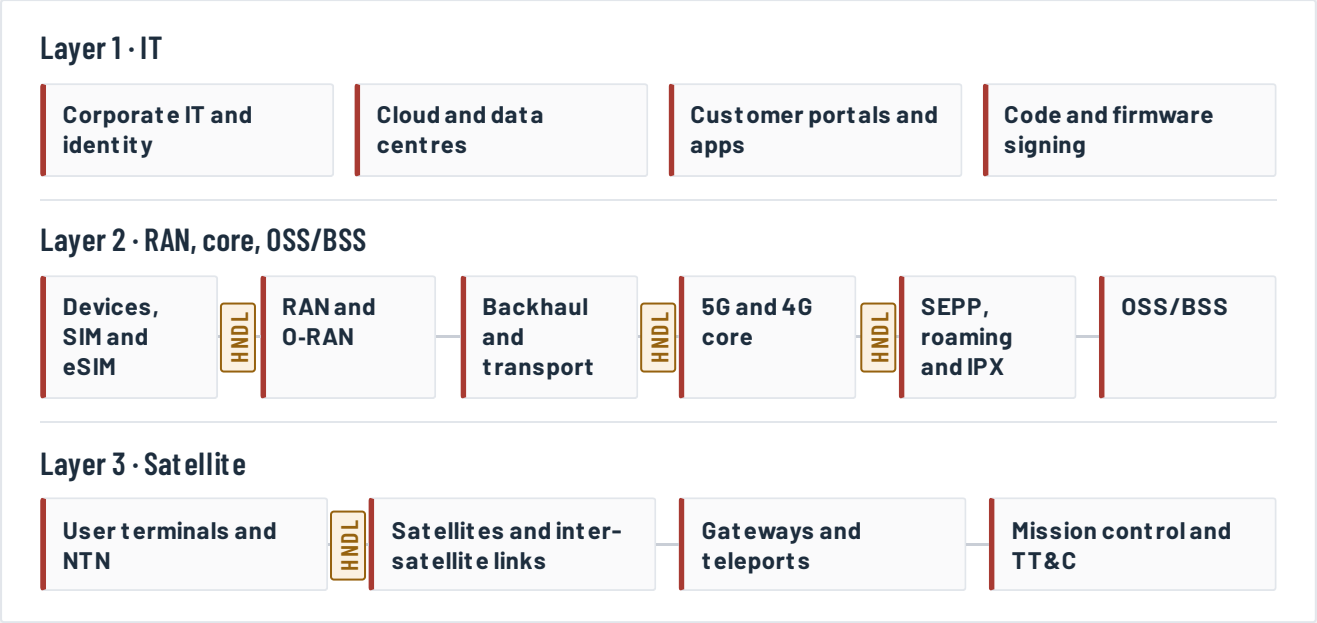

Figure 1. The domains we assess in each layer of a typical operator. Red edge: public-key cryptography a quantum computer breaks. HNDL: links worth recording today to read later.

Layer 1 · IT

DOMAIN	PROTOCOLS AND ARTEFACTS	QUANTUM-VULNERABLE
Web, APIs and portals	TLS 1.0–1.3 · mTLS · HTTPS/REST · gRPC	RSA/ECDHE key exchange · RSA/ECDSA certificates · legacy suites
Remote access	SSH · IPsec/IKEv2 · TLS VPN	(EC)DH groups · host and user keys
Identity and PKI	X.509 CAs · OCSP/CRL · ACME · Kerberos/AD · LDAPS · SAML/OIDC	CA keys and lifetimes · token signing (RS256, ES256)
Email and DNS	S/MIME · SMTP STARTTLS · DKIM · DNSSEC	RSA/ECDSA signatures · zone-signing keys
Keys and data at rest	HSM/KMS · database TDE · backup encryption	RSA key wrapping · 128-bit keys on long-lived data
Cloud and containers	Kubernetes and service-mesh mTLS · ingress TLS · cloud KMS	Certificate rotation · algorithm agility
Code and firmware signing	RSA/ECDSA signing keys · CI/CD release signing	Trust anchors that devices verify for years

PROTOCOL COVERAGE

We read the network the way 3GPP and GSMA describe it

Layer 2 · RAN, core and OSS/BSS

DOMAIN	INTERFACES AND PROTOCOLS	REFERENCE	QUANTUM-VULNERABLE
RAN and backhaul	IPsec/IKEv2 on NG, Xn, F1, E1(S1, X2 in 4G)· CMPv2 enrolment	TS 33.210 · 33.310 · 33.501	IKE(EC)DH · RSA/ECDSA certificates
Open RAN	Open Fronthaul M-Plane (NETCONF over SSH or TLS)· O1· A1· E2	O-RAN WG11	SSH/TLS key exchange · SMO and xApp certificates
5G core (SBA)	HTTP/2 over TLS · OAuth 2.0 tokens (JWS)· NF certificates	TS 33.501	ECDHE · RSA/ECDSA certificates and tokens
Roaming and interconnect	SEPP N32-c TLS, N32-f PRINS · Diameter (TLS/DTLS/IPsec)· GTP over IPX · SS7/MAP	TS 33.501· GSMA PQ.05	Partner-facing keys · links with no cryptography
Voice and IMS	SIP over TLS · IMS IPsec (Gm)· SRTP · MIKEY-SAKKE (mission-critical)	TS 33.203 · 33.180	Key agreement · SAKKE keys
Subscriber identity	SUCI: ECIES profile A (X25519), B (P-256)· 5G AKA · MILENAGE/TUAK	TS 33.501· 35.206 · 35.231	ECIES home-network keys · 128-bit K
SIM, eSIM and OTA	eSIM remote provisioning PKI (ECDSA)· SIM OTA SCP80/SCP81	SGP.22 · SGP.32 · TS 102 225	GSMA CI and EUM certificates · OTA key sets
Lawful interception	X1, X2 and X3 handover over TLS	ETSI TS 103 221	TLS key exchange · certificates
OSS/BSS and management	NETCONF/SSH · SNMPv3 · REST/TLS · Kafka/AMQP TLS · RADIUS/TACACS+ · OAuth APIs	—	Management-plane keys · legacy SNMP and RADIUS
Transport	MACsec (MKA)· IPsec · SD-WAN · MPLS/SR · optical-layer encryption	IEEE 802.1AE	Key exchange behind link encryption

Layer 3 · Satellite networks

DOMAIN	INTERFACES AND PROTOCOLS	REFERENCE	QUANTUM-VULNERABLE
Ground segment	Gateway and teleport IPsec · NOC/MOC TLS · SSH/SNMP	—	As in layers 1 and 2
TT&C and space link	CCSDS SDLS · SDLS Extended Procedures (key management, OTAR)	CCSDS 355.0 · 355.1	Symmetric key lengths · ground key management
User links and terminals	DVB-S2X/RCS2 security · VSAT management (TLS/SSH)· firmware signing	EN 302 307 · EN 301 545	Terminal certificates · firmware trust anchors
Non-terrestrial networks	5G over satellite, reusing the 5G security of layer 2	3GPP NTN · GSMA PQ.07	As layer 2, on the NTN path
Dependencies	GNSS authentication: Galileo OSNMA (ECDSA)	Galileo OSNMA	RAN and core timing

HOW WE ASSESS

From evidence to findings with a next step

How we collect the evidence

Active probing – TLS, DTLS, SSH and IKE endpoints: versions, groups, suites, certificate chains

Passive analysis – Mirrored traffic or captures (SPAN/TAP): handshakes only, never payload

Agents – Servers, VNFs/CNFs, Kubernetes nodes: libraries, keystores, configuration

Configuration and vendor exports – NETCONF/YANG, CA and HSM inventories, vendor PQC statements

What you receive

CBOM per layer and domain – CycloneDX 1.7

Risk-ranked findings – HNDL flag, owner and fix

Vendor and partner matrix – Per vendor, per release

Dated roadmap – Owned, mapped to GSMA PQ.03 and 3GPP

Evidence pack – For the board, NIS2 and TSA reviews

FINDING	LAYER	EXPOSURE	HNDL	NEXT STEP
SEPP N32-c TLS to roaming partners: ECDHE P-256 only	2 · Roaming	HIGH	Yes	Hybrid TLS on the SEPP; partner plan per GSMA PQ.05
Backhaul IPsec on IKEv2 DH group 14 (2048-bit MODP)	2 · RAN	HIGH	Yes	Hybrid IKEv2 (RFC 9370, ML-KEM) in the next release
RAN software signed with an RSA-2048 key valid 15 years	1 · Signing	HIGH	No	ML-DSA or LMS signing agreed with the vendor
eSIM profile download PKI on ECDSA P-256 certificates	2 · SIM, eSIM	HIGH	No	Plan the certificate rollover with your eUICC vendors
TT&C link on AES-128, ground keys distributed under RSA	3 · Satellite	MEDIUM	Yes	AES-256; quantum-safe key distribution on the ground

Figure 2. Example findings, in the format of the report.

For more information: contact@qcomply.tech

Sources

1. NIS Cooperation Group, *Coordinated PQC Implementation Roadmap*, June 2025. digital-strategy.ec.europa.eu
2. NIST, *IR 8547, Transition to Post-Quantum Cryptography Standards*, initial public draft, Nov 2024. csrc.nist.gov
3. GSMA PQTN, *PQ.03 v2* (telecom use cases), Oct 2024; *PQ.05* (roaming), Jul 2025; *PQ.07* (NTN), Feb 2026. gsma.com
4. *Directive (EU) 2022/2555 (NIS2)*, Article 21(2)(h). eur-lex.europa.eu
5. *Telecommunications (Security) Act 2021* and Telecommunications Security Code of Practice. legislation.gov.uk
6. 3GPP SA3, TR 33.938, TR 33.703 and the Release 20 256-bit algorithms (TS 35.240–35.248). 3gpp.org
7. NIST, *FIPS 203, 204 and 205* (ML-KEM, ML-DSA, SLH-DSA), August 2024. csrc.nist.gov