



Post Quantum Cryptography for Non-Terrestrial Networks

Version 1.0

04 February 2026

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Copyright © 2026 GSM Association

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Compliance Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Table of Contents

1	Introduction	3
1.3	Definitions	3
1.4	Abbreviations	3
1.5	References	4
2	NTN Use-cases	6
2.1	Satellite to Ground	7
2.1.1	Satellite Connections as Transport Network	7
2.1.2	Satellite Connections as Transport Network for LTE Backhaul	10
2.2.1	Direct-to-Phone	10
2.2.2	Satellite IoT Connection	11
3	System Context	12
3.1	Sensitive Data Discovery	14
3.2	Cryptographic Inventory	15
3.3	Migration Strategy Analysis and Dependencies	16
3.4	Stakeholders	16
3.5	PKI Implications	17
3.6	Legacy Impact	18
3.7	Potential Actions / Dependencies	18
3.8	Dependencies	19
3.8.1	Standards	19
3.8.2	National Guidelines	19
3.8.3	Vendors	19
3.8.4	3rd-parties	20
3.8.5	Performance	20
3.9	Gantt Chart for PQC Migration	22
3.10	PQC Migration Process Description	22
3.11	Synergy with Internal Programs	23
3.12	Synergy with External Programs	23
Annex A	Document Management	24
A.1	Document History	24

1 Introduction

As the telecommunications landscape expands beyond traditional ground-based infrastructure, non-terrestrial networks (NTNs) are poised to play a pivotal role in global connectivity. This document explores the implications of PQC implementation in NTN, providing insight into system context, technical challenges, standards implications and migration considerations. This document adds to the use cases covered in PQ.03 Post Quantum Cryptography – Guidelines for Telecom Use Cases v2.0 [03]

1.3 Definitions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “NOT RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in BCP 14 [5] [6] when, and only when, they appear in all capitals, as shown here.

1.4 Abbreviations

Term	Description
AES	Advanced Encryption Standard
CCSDS	Consultative Committee for Space Data Systems
DTLS	Datagram Transport Layer Security
E2EE	End-to-end Encryption
ENISA	European Network and Information Security Agency
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute
FTP	File Transfer Protocol
GDPR	General Data Protection Regulation
GEO	Geostationary Earth Orbit
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IPsec	Internet Protocol Security
ISL	Inter-Satellite Link
ISSLs	Inter Satellite Laser Links
LEO	Low Earth Orbit
LI	Lawful Intercept
LTE	Long Term Evolution
MACsec	Media Access Control Security
MITM	Man in the Middle

MNO	Mobile Network Operator
NIST	National Institute of Standards and Technology
NTN	Non-Terrestrial Network
OEM	Original Equipment Manufacturer
OISLs	Optical Inter-satellite Links
PKI	Public Key Infrastructure
PQC	Post Quantum Cryptography
QKD	Quantum Key Distribution
QSC	Quantum Safe Cryptography
RF	Radio Frequency
SecGW	Security Gateway
SNO	Satellite Network Operator
SSH	Secure Shell
TCP	Transmission Control Protocol
TLS	Transport Layer Security
USIM	Universal Subscriber Identity Module
VPLMN	Visited Public Land Mobile Network
VPN	Virtual Private Network

Table 1: Abbreviations

1.5 References

Ref	Doc Number	Title
01	Void	
02	PQ.01	GSMAPQ.01 – Post Quantum Telco Network Impact Assessment Whitepaper, Version 1.0, 17 Feb 2023
03	PQ.03	GSMA PQ.03 – Post Quantum Cryptography – Guidelines for Telecom Use Cases, Version 2, Sept 2024
04	-	Satellite Spoofing from A to Z: On the Requirements of Satellite Downlink Overshadowing Attacks, Salkield, Edd and Szakály, Marcell and Smailes, Joshua and Birnbach, Simon and Köhler, Sebastian and Strohmeier, Martin and Martinovic, Ivan. in Proceedings of the 16th Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), 2023 https://ora.ox.ac.uk/objects/uuid:e9d5d85f-b77f-4f11-8006-17dd88660467/download_file?file_format=application%2Fpdf&sa

		fe_filename=Salkield_et_al_2023_satellite_spoofing_from.pdf&type_of_work=Conference+item
05	350.1-G-3	CCSDS Security Threats Against Space Missions, Informational Report, Issue 3, CCSDS 350.1-G-3, The Green Book, February 2022. Consultative Committee for Space Data Systems, Washington DC https://public.ccsds.org/Pubs/350x1g3.pdf
06	357.1-O-1	CCSDS Intergovernmental Certification Authority Experimental Specification CCSDS 357.1-O-1 ORANGE BOOK December 2024. Consultative Committee for Space Data Systems, Washington DC https://public.ccsds.org/Pubs/357x1o1.pdf
07	355.0-B-2	CCSDS Space Data Link Security Protocol, Recommended Standard CCSDS 355.0-B-2 (Blue Book), July 2022. Consultative Committee for Space Data Systems, Washington DC https://public.ccsds.org/Pubs/355x0b2.pdf
08	Void	
09a	350.7-G-2	CCSDS Security Guide for Mission Planners, Informational Report, CCSDS 350.7-G-2 (Green Book), April 2019. Consultative Committee for Space Data Systems, Washington DC. https://public.ccsds.org/Pubs/350x7g2.pdf
09b	TR 33.700-29	Study on security aspects of 5G satellite access in the 5G architecture, Release 19
10	TR 38.821	Solutions for NR to support non-terrestrial networks (NTN), Release 16
11	TR 22.865	Study on satellite access Phase 3, Release 19
12	TR 33.938	3GPP Cryptographic Inventory
13	SP800-56C	Recommendation for Key-Derivation Methods in Key-Establishment Schemes
14	10.3390	S. Plastras, D. Tsoumatidis, D.N. Skoutas, A. Rouskas, G. Kormentzas, C. Skianis, "Non-Terrestrial Networks for Energy-Efficient Connectivity of Remote IoT Devices in the 6G Era: A Survey". Sensors 2024, 24, 1227. https://doi.org/10.3390/s24041227
15	10.69978	Lee, J. Kim, "Survey on Security for Non-Terrestrial Networks", Research Briefs on Information and Communication Technology Evolution, 10, 111–123, 2024, https://doi.org/10.69978/rebict.e.v10i.196
16		GSMA PQC Government Guidelines

		https://www.gsma.com/newsroom/post-quantum-government-initiatives-by-country-and-region/
17		Latency in Communications Networks, EMEA Satellite Operators Association, April 2017 https://gsoasatellite.com/wp-content/uploads/2017-04-Latency-in-Communications-Networks.pdf (Accessed 2025-09-30)
18	doi.org/10.1109/I CEIB61477.2024 .10602698	Insights into Low Earth Orbit Satellite Communication Dynamics: Quality of Service Analysis of Connection Behavior, Latency, and Doppler Shift, Zoltan Gal et. al. https://ieeexplore.ieee.org/document/10602698 (Accessed 2025-09-30)
19		Security Engineering, Third Edition 2020, Ross Anderson. ISBN: 978-1-119-64278-7
20	33.703	3GPP 33.703. Title: Study on transitioning to Post Quantum Cryptography (PQC) in 3GPP (draft)

Table 2: References

2 NTN Use-cases

Non-Terrestrial Networks (NTNs), particularly satellite-based systems, present unique security challenges that require a distinct approach compared to traditional 5G security measures. [5] NTNs operate in dynamic and resource-constrained environments, with satellites and ground components from diverse manufacturers, leading to incongruent security practices and vulnerabilities [8]. The lack of maturity of on-orbit reprogramming technologies and limited onboard processing capabilities make NTNs susceptible to sophisticated attacks, including jamming, eavesdropping, and unauthorized access to satellite control systems [4]. The wide geographic coverage of NTNs exacerbates challenges such as managing secure handovers, routing in dynamic topologies, and key distribution.

The 3GPP architecture for NTN describes two implementation scenarios: transparent payload and regenerative payload. There are then six more detailed scenarios depending on the satellite orbit. [10]

- *"A transparent payload: Radio Frequency filtering, Frequency conversion and amplification. Hence, the waveform signal repeated by the payload is un-changed;*
- *-A regenerative payload: Radio Frequency filtering, Frequency conversion and amplification as well as demodulation/decoding, switch and/or routing, coding/modulation.*

This is effectively equivalent to having all or part of base station functions (e.g. gNB) on board the satellite (or UAS platform)." [10]

Many commercial NTN implementations such as those focused on end-user connectivity such as broadband services continue to rely on traditional application-layer protocols like TCP/IP for data delivery given that early and large-scale NTN investments were driven by the goal of providing global internet access.

Satellite constraints such as high latency and bit error rates impact the performance of communications protocols, requiring adaptive and lightweight security mechanisms to protect user plane traffic without degrading service quality. Some OEMs use lightweight cryptography, which should be assessed in PQC planning.

A defence-in-depth approach is imperative, where compensating controls, such as physical layer security techniques, play a key role in mitigating risks, especially given the extended satellite maintenance cycles, exceeding six months.

In mobile backhaul use cases, particularly over satellite links, both protocol and computational overhead introduced by security mechanisms must be considered carefully [14, 15]. While encryption does not typically increase packet size, integrity protection mechanisms — such as the addition message authentication codes (MAC) — do add overhead to control and user plane messages.

When security protocols such as IPsec or DTLS are used over satellite backhaul links, this may result in increased packet sizes and latency due to encapsulation and processing.

The management plane remains a high-value target for attackers seeking to compromise the system's availability, its protection must remain a top priority. As NTNs become critical enablers for maritime operations, rural connectivity, and IoT deployments — especially in underserved regions — it is essential to deploy robust, interoperable, and context-aware security frameworks optimized for NTN-specific constraints.

Finally, the security of the satellite infrastructure itself is important.

- Satellites use specialised communications protocols.
- Securing the satellite command-link is a high priority [7].
- Securing the satellite technology supply chain is important [6].
- Securing the ground segment.

2.1 Satellite to Ground

2.1.1 Satellite Connections as Transport Network

The satellite provides a transport network to connect different parts of an operator's network, e.g. to provide backhaul in remote regions.

Non-3GPP architecture:

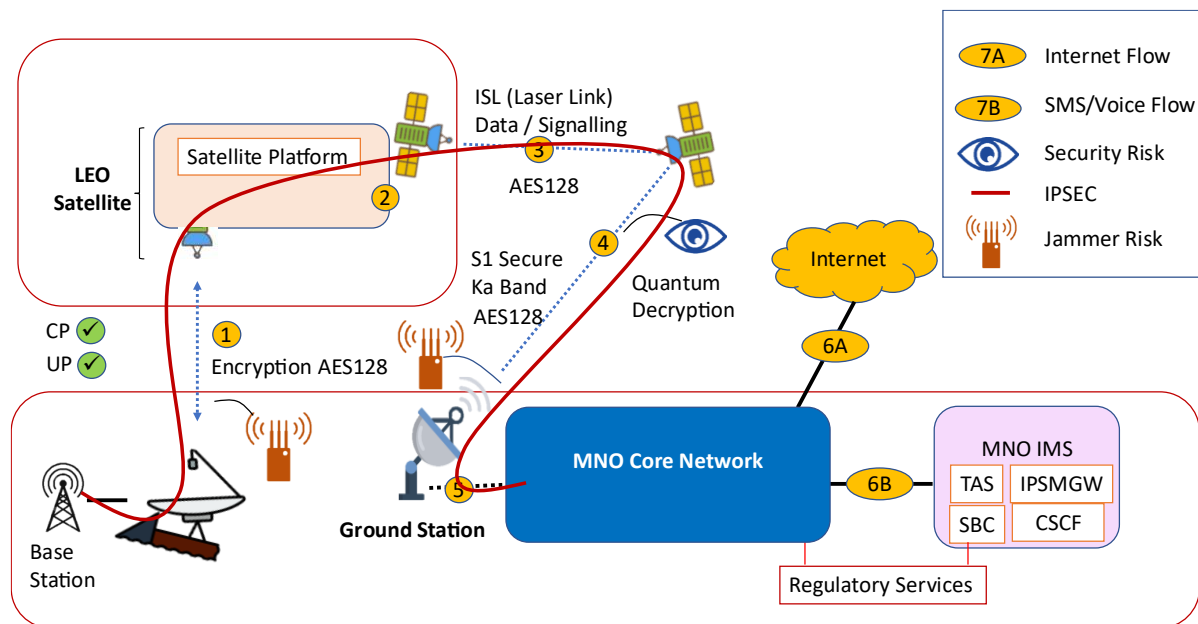


Figure 1: Backhaul Connection System Architecture

3GPP architecture:

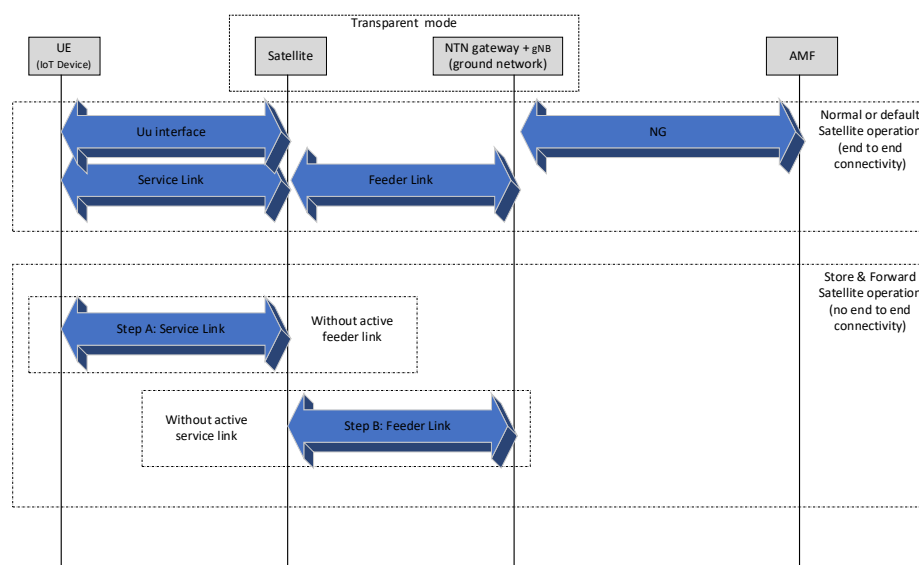


Figure 2: Non-terrestrial network typical scenario based on transparent payload

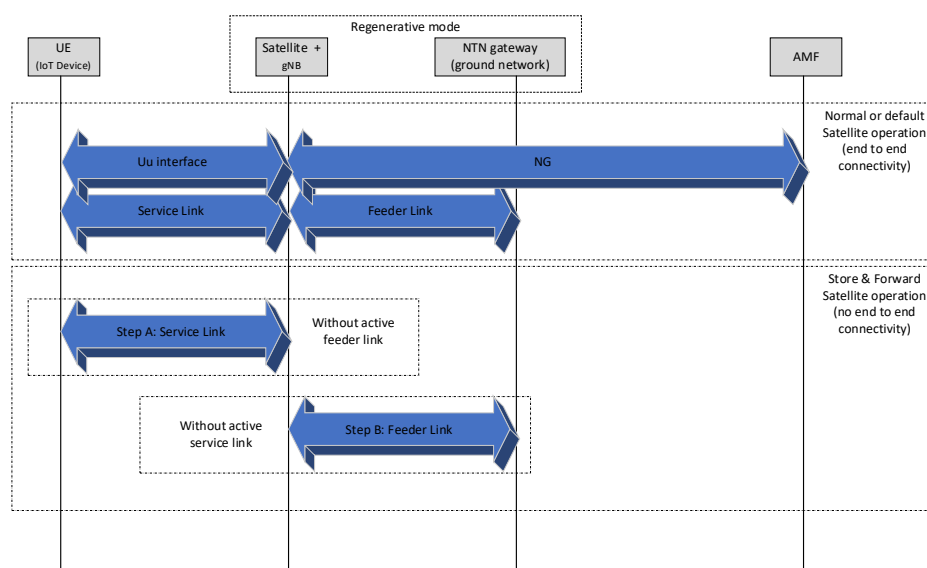


Figure 3: Non-terrestrial network typical scenario based on regenerative payload

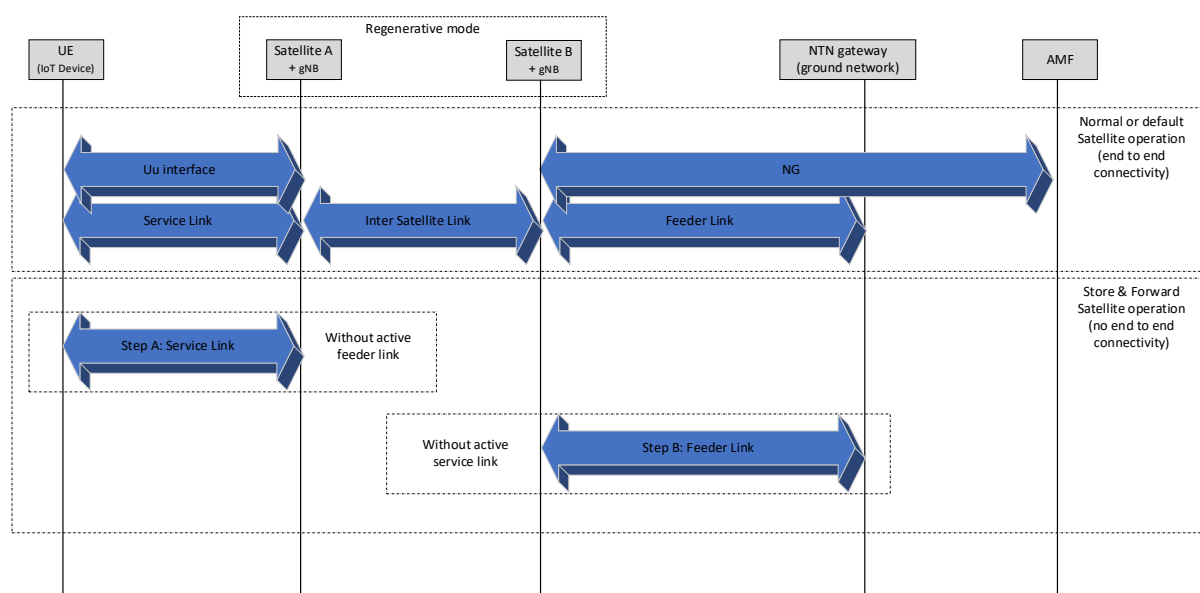


Figure 4: Non-terrestrial network typical scenario based on regenerative payload inter satellite communication

In 3GPP NTN configurations, the satellite is connected towards core network via the feeder link and is providing the service link for the user equipment. In the transparent payload, the gNB is connected to the satellite via the feeder link. The gNB itself is then connected to the core network via transport network.

As per 3GPP architecture the transport network between gNB and core network, more specifically the N2 and N3 interfaces, is protected by IPsec. The IPsec security associations between gNB and core network provide confidentiality, integrity protection, and replay protection.

The segment between the ground station and the satellite — including uplink and downlink RF transmissions — may implement additional link-layer encryption. (E.g. AES-128, a proprietary modem protocol or physical layer encryption standard.) These encryptions are not defined in 3GPP, but serve to protect traffic while it is within the satellite operator's domain.

Jamming threats, particularly in the Ku-band (or Ka-band, depending on deployment), remain a concern, especially in the terminal-to-satellite and satellite-to-ground station segments. Localized jamming attacks can disrupt connectivity and are a known risk in commercial LEO deployments [4].

Satellite orbits affect round trip times from the ground. GEO satellites have typical latency of 500 msec, MEO satellites around 125 msec; LEO satellites between 2 and 20 msec [17,18]. Longer latency has three effects. It increases latency for user plane traffic. It slows down IPsec-based connection establishment and slows IPsec key re-establishment.

In latency-sensitive scenarios, other transport security mechanisms (e.g., DTLS) may be preferred.

Best-practice in security is to implement a defence-in-depth approach [19]. IPsec provides network-layer protection, other mechanisms such as TLS (application layer) and MACsec (link layer), may be used depending on the threat model and operational constraints.

2.1.2 Satellite Connections as Transport Network for LTE Backhaul

Use of a satellite connection to implement a backhaul network for LTE, most likely to base stations in remote areas.

This setup includes standard LTE signalling, where the control plane over the air interface is both encrypted and integrity protected, as defined in 3GPP TS 33.401. Mutual authentication mechanisms prevent Man-in-the-Middle (MITM) attacks.

Like terrestrial wireless networks, RF-based NTN links remain susceptible to jamming threats, particularly in S-band, Ku-band, or Ka-band deployments where adversaries can emit high-power interference signals. Optical satellite links — such as Inter-Satellite Laser Links (ISLLs) also known as optical inter-satellite links (OISLs) or Free-Space Optical Communication — are resistant to jamming due to the cost of mounting an attack. This is due to the narrow beam divergence, high directivity, and physical propagation properties of optical links. While jamming is a significant problem for RF-based NTN communication architectures and air interfaces, optical links may give some protection.

2.2 Satellite to Users

This scenario is where the satellite provides service direct to the subscriber's device.

2.2.1 Direct-to-Phone

Direct-to-phone satellite communication employs a multi-layered security architecture to ensure robust protection for both control and user plane traffic. The first step in securing the air interface is the implementation of standard encryption and integrity mechanisms. In the

control plane, encrypted signalling and integrity verification should be used, preventing potential MITM (Man-In-The-Middle) attacks due to mutual authentication protocols.

For the user plane, 4G standards already employ encryption, and 5G enhances this with optional user plane integrity protection mechanisms.

Inter-Satellite Laser Links (ISLLs) utilize traditional encryption and authentication algorithms, such as AES-128, to secure data transmission [XX]. Using insecure connections or insecure key distribution practices creates a risk of eavesdropping by an external spacecraft.

Satellite platforms also present potential vulnerabilities, particularly in the ground segment or data relay infrastructure. In some operational environments — especially those involving legacy systems or commercial downstream services — application-layer protocols such as HTTP or FTP may be used to transmit telemetry data, software updates, or bulk payload data. If these protocols are not secured (i.e., don't use TLS or SSH), they may expose sensitive information to interception or tampering.

To mitigate this risk, secure communication channels should be enforced across the entire satellite communication chain. For instance, AES-128 encryption is often applied at the Ka-band physical layer for uplink and downlink transmission via vendor-specific implementations. While sophisticated adversaries may attempt to intercept signals near ground stations using advanced RF receivers, successful decryption remains highly impractical without access to the appropriate encryption keys and system-level context.

Transmission links between the ground station and the Satellite Network Operator EPC (Evolved Packet Core) pose an additional risk if left unencrypted, as these could potentially be intercepted. While the proximity of these links within the same building reduces the likelihood of such attacks, the use of IPSEC for these connections should be used by the SNO to ensure robust security.

On the Satellite Network Operator EPC side, lawful interception (LI) functions may be used for monitoring without the primary network operator's consent. This risk aligns with standard roaming practices, as inbound roamers are subject to regulatory requirements for lawful interception in visited networks (VPLMN).

For securing voice and SMS services over NTN, end-to-end encryption and integrity protection should follow the 3GPP IMS security model, as defined in **TS 33.203**. While IPsec may be used to secure intermediate network segments (e.g., between IMS nodes or over satellite backhaul), it does not provide end-to-end protection for voice or SMS from the terminal. Therefore, specialized high-assurance use cases (e.g., government or defense-grade communications) may implement additional application-layer encryption or use dedicated secure voice applications on top of standard IMS-based VoIP.

In the case of data traffic, no such IPSEC tunnel exists. To safeguard sensitive data from interception, end-to-end encryption starting from the terminal should be employed. VPN solutions or similar mechanisms can ensure communication security for data services.

2.2.2 Satellite IoT Connection

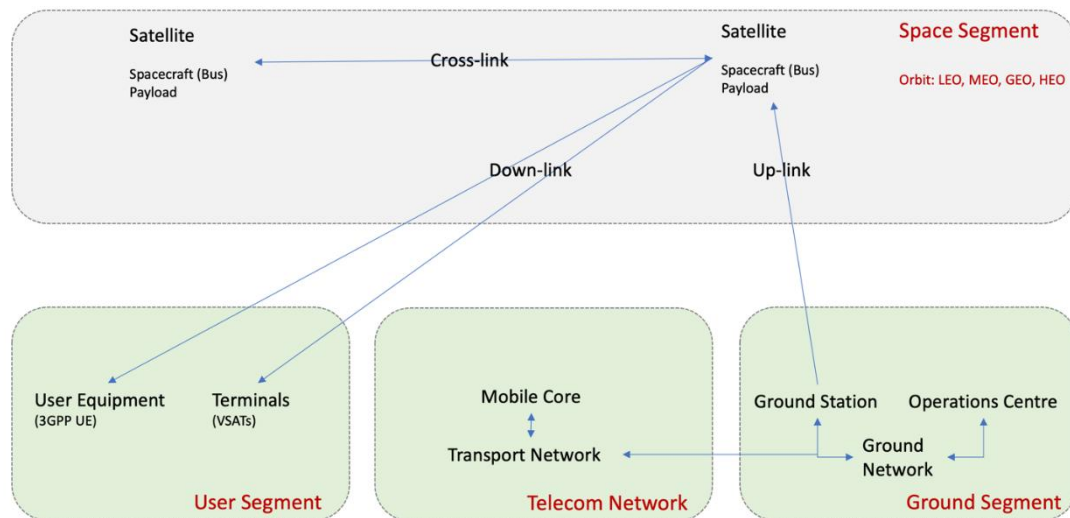
Satellite-based IoT connections introduce unique challenges and vulnerabilities, particularly as quantum computing threatens existing cryptographic systems. As IoT devices often operate with limited computational resources and are deployed in resource-constrained environments, integrating PQC mechanisms into satellite-based IoT networks requires careful consideration of both security and performance.

IoT devices connect to satellites via the air interface, where control plane signalling and user plane traffic are secured using encryption and integrity protection mechanisms. In a PQC context, hybrid cryptographic solutions that combine classical algorithms (e.g., DH, RSA) with quantum-safe algorithms are recommended. This approach ensures backward compatibility while transitioning to PQC standards. Lightweight PQC key-encapsulation algorithms optimized for IoT environments, such as NTRU or ML-KEM, can be utilized to address the computational limitations of IoT devices. Satellite platforms handling IoT traffic face significant risks if legacy cryptographic systems are not replaced with quantum-safe alternatives. Signals transmitted via uplink and downlink should be encrypted using PQC-enhanced protocols to protect against potential quantum computing attacks. Secure Ka-band transmission with PQC algorithms ensures the confidentiality of IoT data during transit. Additionally, hybrid cryptographic approaches can provide protection while migrating to fully quantum-safe solutions. The link between ground stations and IoT platforms should employ PQC algorithms to ensure secure data transmission. IPSEC tunnels and Datagram Transport Layer Security (DTLS) should be updated to integrate quantum resistant capabilities, such as ML-KEM, for key exchange. This ensures that sensitive IoT data remains secure even against quantum adversaries. Certificate management for these connections should incorporate post-quantum digital signatures to mitigate risks associated with quantum-based key compromise.

IoT devices often rely on pre-distributed keys, which may be vulnerable to quantum attacks. Implementing quantum resistant key exchange mechanisms is essential for protecting IoT communications. Periodic key rotation ensures that session keys remain secure over time. End-to-end encryption (E2EE) incorporating quantum-safe protocols can prevent eavesdropping and unauthorized access to IoT data. The integration of post-quantum cryptography into satellite IoT connections is critical to future-proofing these systems against quantum computing threats. By adopting PQC algorithms, robust key management practices and hybrid cryptographic approaches, satellite-based IoT networks can ensure security and resilience while maintaining performance in resource-constrained environments.

3 System Context

The system context provides a high-level view of the system, so we can focus on the areas where encryption is used, abstracted from implementation details.



GMSA PQ.nn Satellite Context

Figure 5: Satellite Context

Satellite, consists of:

- spacecraft (or bus) with power, manoeuvring, command and control
- payload (transponders or transceivers for a communications satellites)

Up-link. Ground-to-space communications link carrying :

- satellite command and control (manoeuvring and station keeping, maintenance, telemetry)
- network data for onward transmission to terminals and user equipment

Down-link. Space-to-ground communications link, carrying:

- network data for terminals and user equipment
- telemetry

Cross-link

- Communications link between two (or more) satellites in orbit. There are multiple technologies. Not all satellite systems use cross-links.

Ground Segment. The systems that operate the Space Segment, including

- (Satellite) Operations Centre, manages all satellites and payloads
- Ground Stations, manage the up-links to a fleet of satellites, multiplex satellite command and control with network traffic
- Ground Network, links Operations Centre to Ground Stations

User Segment. The people or devices using the satellite service.

- User Equipment, devices that implement 3GPP air interfaces
- Terminals, devices that implement ITU-T or proprietary air interfaces

Telecom Network. The operator network, which connects to the Ground Segment

- Mobile Core
- Transport Network

3.1 Sensitive Data Discovery

Sensitive data transmitted over the satellite interfaces in NTN systems must be identified and adequately protected to ensure confidentiality, integrity, and authenticity. These attributes are essential in preventing unauthorized access, eavesdropping, and data breaches. The protection requirements may vary depending on the interface and the specific type of information exchanged.

Sensitive Data	Description
IMSI	International Mobile Subscriber Identity; uniquely identifies a user in the network.
Session Encryption Keys	Keys used for air interface encryption and authentication.
Long Term Keys	USIM Key K (for instance)
Location Information	Real-time location data of the user or terminal.
User Data	User-generated or transmitted data, such as voice, SMS, or internet packets.
Control Plane/Network Signalling	Signalling traffic between UE and Core includes identity, auth, registration details
Session Metadata	Information about session duration, start and end times, and associated services.
Management Plane Sensitive Data	Information about Admin users, passwords, keys, PAM tokens, remote management protocols traffic.
Telemetry Data	Information collected by the sensors
Interconnect & Roaming Sensitive Data	Information that exchanged cross trust boundaries such as IPX/GRX transport security data, 5G Roaming Interconnect (SEPP / N32 traffic).
Satellite signing keys	Firmware signing key(s) for payload updates

Command up-link data	Satellite command and control from Satellite Operations Centre
Command up-link keys	Keys for satellite command and control authentication and encryption
Satellite payload updates	Signed firmware from Satellite Operations Centre

Figure 6: List of Possible Sensitive Data

3.2 Cryptographic Inventory

The cryptographic inventory identifies and catalogues the encryption, authentication, and integrity algorithms currently deployed across the NTN system. This includes both traditional and quantum-resistant algorithms used in satellite-to-ground, satellite-to-user, and inter-satellite communication interfaces. The inventory aims to assess the cryptographic mechanisms' effectiveness, identify potential vulnerabilities, and prioritize updates to ensure compliance with evolving security standards.

Algorithm/Protocol	Usage Context	Security Features	Type of Cryptography
AES-128	Satellite-to-ground link	Confidentiality and Integrity Protection	Symmetric
IPSEC ESP	gNB/ng-eNB to MNO Security Gateway	Confidentiality and Integrity Protection	Symmetric
IKEv2	AuthN and IPsec SA setup	Confidentiality and Integrity Protection	Symmetric
		Digital Signature and Key Agreement	Asymmetric, Symmetric
SHA-256	Key-Derivation	Hash/Digest Computation	Symmetric
HMAC-SHA-256	Keyed Hashing	Key Derivation	Symmetric
TLS 1.3	Management plane communication	Encryption, session security,	Symmetric
		digital signature	Asymmetric
EAP-TLS	M-plane	Key Agreement	Asymmetric, Symmetric
		Key Derivation	Symmetric

Table 3: Cryptographic Inventory

For the 3GPP cryptographic inventory please refer to TR 33.938 [12].

3.3 Migration Strategy Analysis and Dependencies

The migration strategy analysis evaluates the transition from legacy cryptographic algorithms to PQC algorithms. This process includes assessing current systems, prioritizing critical assets, and identifying technical, operational, and regulatory dependencies. Effective planning and coordination with the broader ecosystem, including OEMs, SNOs, and MNOs, are essential to ensure a seamless transition while minimizing disruptions.

One option is a phased transition strategy. Start with Hybrid key-exchange and Hybrid signature schemes:

“In addition to the currently approved techniques for the generation of the shared secret Z ... this Recommendation permits the use of a “hybrid” shared secret of the form $Z' = Z || T$, a concatenation consisting of a “standard” shared secret Z that was generated during the execution of a key-establishment scheme (as currently specified in [SP 800-56A] or [SP 800-56B]) followed by an auxiliary shared secret T that has been generated using some other method.” [13]

The transition will end with pure PQ scheme.

The start of the migration process is dependent on several factors, including the readiness of OEMs to support post-quantum cryptographic standards and the availability of compatible hardware and software modules. Coordination with regulatory bodies to ensure compliance with emerging standards is essential, particularly in regions where cryptographic legislation is evolving:

Dependency	Description	Mitigation Plan
Standardization Timelines	PQC algorithm standardization (e.g., NIST PQC) and protocol standardization (e.g., IETF)	Migration options include: - Interim use of hybrid cryptographic schemes - Pure PQC schemes
Hardware Compatibility	Existing satellites lack support for resource-intensive PQC algorithms	Incremental hardware upgrades or optimizations
Regulatory Compliance	Alignment with international and local cryptographic regulations	Early engagement with regulatory bodies
Supply Chain Readiness	Lack of PQC modules from OEMs	Develop joint roadmaps with suppliers

Table 4: Migration process dependencies

The transition to post-quantum cryptography necessitates a holistic approach that balances technical readiness, regulatory compliance, and ecosystem coordination. Establishing a governance framework and fostering collaboration with stakeholders are crucial to overcoming migration challenges and ensuring long-term security resilience.

3.4 Stakeholders

The successful transition to PQC in NTN systems requires the active involvement of various stakeholders across the ecosystem. Each stakeholder plays a critical role in ensuring secure,

seamless, and efficient migration while addressing technical, operational, and regulatory challenges. Effective collaboration and communication among these entities are vital to achieving shared security objectives:

- **Satellite Network Operators (SNOs):** Ensure the implementation of PQC-compatible hardware and software across satellite platforms and ground stations.
- **Mobile Network Operators (MNOs):** Deploy PQC mechanisms in network infrastructure, particularly in backhaul and core network elements.
- **Equipment Manufacturers (OEMs):** Develop and certify hardware and software solutions that support PQC standards and interoperability.
- **Regulatory Bodies:** Define and enforce compliance with emerging PQC standards and security regulations.
- **Standardization Organizations:** Establish globally accepted PQC standards and protocols (e.g., NIST, ETSI, 3GPP, IETF, CCSDS).
- **National and Regional Space Agencies:** Develop technology and standards for space systems
- **Roaming Partners / IPX Providers:** To support PQC/hybrid key since roaming depends on: Interconnect security mechanisms (IPsec, TLS, certificates), Trust relationships between PLMNs, Roaming hubs and intermediaries in the middle. So, the IPX provider becomes a “crypto translator / bottleneck”, and should support the same PQ/hybrid cryptographic posture across many operators simultaneously.

Collaboration between SNOs, MNOs, and OEMs is essential to ensure compatibility and interoperability of PQC technologies. Regulatory bodies and standardization organizations must provide clear guidelines and timelines to facilitate alignment across the ecosystem.

3.5 PKI Implications

In NTN systems, the distribution and validation of certificates in satellite-to-ground communication are particularly challenging due to high latency and potential packet loss. Resource-constrained satellite platforms may struggle to efficiently process larger certificates, necessitating lightweight PKI implementations optimized for such environments. [8]

To ensure the robustness of PKI systems in the post-quantum era, NTN operators could adopt hybrid certificate solutions, quantum-safe key distribution methods, and optimize validation processes for latency-prone and resource-constrained environments. Collaborative efforts with standardization bodies and OEMs are essential to address these challenges effectively.

IETF and NIST provides a mapping of PQC algorithms. For example, ML-KEM-512 has a comparable security level as AES128:

PQ Security Level	AES/SHA(2/3) hardness	PQC Algorithm
1	AES-128 (exhaustive key recovery)	ML-KEM-512, FN-DSA-512, SLH-DSA-SHA2/SHAKE-128f/s
2	SHA-256/SHA3-256 (collision search)	ML-DSA-44
3	AES-192 (exhaustive key recovery)	ML-KEM-768, ML-DSA-65, SLH-DSA-SHA2/SHAKE-192f/s

4	SHA-384/SHA3-384 (collision search)	No algorithm tested at this level
5	AES-256 (exhaustive key recovery)	ML-KEM-1024, FN-DSA-1024, ML-DSA-87, SLH- DSA-SHA2/SHAKE-256f/s

Table 5: Mapping of PQC algorithms

3.6 Legacy Impact

The adoption of PQC in NTN poses significant challenges for legacy systems. These systems, often designed with limited computational capabilities and constrained resources, may struggle to support the increased complexity and larger key sizes associated with PQC algorithms. Understanding the impact on legacy components is essential to ensure a seamless and secure transition without compromising network functionality.

Legacy satellite systems may face significant performance bottlenecks when migrating to Post-Quantum Cryptography (PQC), especially due to the increased computational demands and larger key sizes associated with lattice-based or hash-based algorithms. Protocols such as IPsec and TLS can support PQC; early versions rely on cryptographic algorithms (e.g., RSA, DH, ECDH) that are not quantum-safe. Adopting PQC requires updating these protocols to use new, standardized quantum-resistant key exchange and signature schemes.

In practice, this needs protocol-level extensions (e.g., PQ-TLS 1.3, Post-Quantum IKEv2), which require firmware and software updates in both satellite terminals and ground infrastructure. For resource-constrained legacy systems, particularly those relying on fixed-function hardware or older chipsets, these upgrades may pose performance and integration challenges — making PQC migration a non-trivial task.

To address these challenges, a phased approach to migration is recommended, starting with hybrid cryptographic solutions that combine legacy and PQC keys. This ensures backward compatibility and minimizes disruptions during the transition. Additionally, resource optimization techniques can be employed to extend the lifespan of legacy hardware while maintaining security. Legacy systems pose unique challenges to the adoption of PQC. Strategic planning and phased upgrades can mitigate risks and ensure a smooth transition. Collaboration with OEMs and standardization bodies is essential to developing backward-compatible solutions and optimizing existing infrastructure for post-quantum security.

3.7 Potential Actions / Dependencies

Successful adoption of PQC in NTN requires a well-defined set of actions and an understanding of the dependencies. These actions must address technical, operational, and regulatory challenges, while considering the ecosystem-wide coordination required to implement quantum-safe mechanisms effectively.

One of the critical actions is the selection and implementation of PQC algorithms recommended by recognised standardization bodies such as NIST and ETSI into protocols defined by IETF (e.g. TLS, IPsec). This requires rigorous testing to ensure interoperability with existing systems and protocols, particularly in NTN environments characterized by high latency and resource constraints.

3.8 Dependencies

3.8.1 Standards

Standards play a critical role in ensuring the successful adoption of PQC in NTN systems. They provide a framework for interoperability, security compliance, and performance optimization across diverse stakeholders, including satellite operators, mobile network operators, and equipment vendors. Alignment with established standards is essential to mitigate risks and accelerate deployment.

The NIST PQC initiative has defined a set of quantum-safe algorithms that serve as the foundation for secure communication in the post-quantum era. Additionally, ETSI's Quantum-Safe Cryptography (QSC) group provides guidelines for the implementation and standardization of PQC in telecommunication networks, including NTNs. Collaboration with standardization bodies such as 3GPP, IETF and ISO is crucial to ensure global alignment.

The Consultative Committee for Space Data Systems (CCSDS) is a voluntary organisation of national and international space agencies. As stated, the CCSDS *“addresses data systems problems that are common to all participants, and to formulate sound technical solutions to these problems. Inasmuch as participation in the CCSDS is completely voluntary, the results of Committee actions are termed Recommended Standards and are not considered binding on any Agency.”* [8] These CCSDS Recommended Standards cover a wide range of domains, including security and cryptographic topics. Organisations should maintain awareness of CCSDS activity, in case PQC-related recommendations emerge.

Adhering to standards ensures that PQC implementations are interoperable and secure. The evolving nature of PQC standards presents challenges, such as the need for frequent updates to hardware and software. Early engagement with standardization bodies can help organizations stay ahead of compliance requirements.

3.8.2 National Guidelines

National guidelines are critical in shaping the adoption and implementation of PQC in NTN systems. These guidelines provide a regulatory framework that aligns with national security priorities, data protection laws, and international standards, ensuring a cohesive approach to securing sensitive communications in the post-quantum era.

The United States National Institute of Standards and Technology (NIST) has led global efforts in PQC standardization, and also provides guidelines that emphasize the importance of transitioning to quantum-safe algorithms. The European Union Agency for Cybersecurity (ENISA) has published documents outlining best practices for quantum-safe cryptography in critical infrastructure, including NTNs.

Compliance with national guidelines may require significant changes to existing systems, particularly in regions with strict data protection regulations such as GDPR in the EU. Additionally, variations in national policies could complicate cross-border interoperability, necessitating alignment efforts between global and national standards.

3.8.3 Vendors

Vendors provide the hardware, software, and tools required to implement quantum-safe mechanisms and enable PQC adoption. Vendors' ability to innovate and align with emerging

standards directly impacts the success of PQC integration in NTN systems, particularly in resource-constrained environments like satellites and ground stations.

Vendors must focus on developing PQC-compatible hardware, such as quantum-resistant cryptographic accelerators, to support secure communications in NTN environments. Additionally, software solutions must be adapted to ensure that existing security protocols can seamlessly integrate with quantum-resistant algorithms without compromising performance.

The success of PQC deployment heavily depends on the readiness of vendors to deliver certified solutions that meet international standards. Delays in hardware production or a lack of alignment with standards like those from NIST, ETSI and IETF could slow down the transition process.

Vendor Role	Dependency	Proposed Solution
Hardware Development	Availability of PQC-compatible chips and accelerators.	Collaborate with chip manufacturers for early development.
Protocol Implementation	Adapting security protocols (e.g., IPSEC, TLS) to support PQC.	Develop protocol extensions for seamless integration.
Supply Chain	Timely delivery of certified cryptographic modules.	Establish partnerships to secure supply chains.
Certification and Testing	Alignment with emerging PQC standards from NIST and ETSI.	Participate in standardization, testing and certification programs.

Table 6: Vendor dependencies

3.8.4 3rd-parties

Third-party entities play a crucial role in the adoption of PQC by providing complementary services such as software solutions, security assessments, and system integration. Their expertise and tools are essential in ensuring a smooth transition to quantum-safe mechanisms, particularly in highly complex ecosystems like NTN systems.

Third-party integration services are vital in enabling NTN operators to adapt their systems to support PQC. These entities also provide critical security audits to identify vulnerabilities and ensure compliance with emerging standards. However, reliance on third-party solutions must be managed carefully to avoid vendor lock-in risks that could limit flexibility in future upgrades.

The successful deployment of PQC often depends on third-party providers for specialized services, such as security assessments and cryptographic key management solutions. Delays or inconsistencies in service delivery could create bottlenecks in the transition timeline, necessitating careful selection and oversight of third-party vendors.

3.8.5 Performance

Performance considerations are critical when integrating PQC into NTNs. The computational complexity and larger key sizes of PQC algorithms can introduce latency, increase processing overhead, and impact bandwidth efficiency, particularly in resource-constrained environments such as satellite systems.

The adoption of Post-Quantum Cryptography (PQC) in NTN systems primarily impacts asymmetric cryptographic operations, such as key exchange and digital signatures, which are essential for initial session setup and authentication. PQC algorithms like Kyber or Dilithium involve significantly larger key sizes and signatures compared to classical counterparts (e.g., RSA, ECDH), potentially increasing bandwidth consumption during handshakes as well as computational and memory demands on terminals, satellites, and ground stations.

However, these operations occur infrequently — typically once per session or during key agreement events — meaning the overall impact on transmission latency and bandwidth usage is bounded. In contrast, symmetric cryptographic algorithms (e.g., AES, HMAC), which are used for ongoing encryption and integrity protection of data traffic, are not substantially affected by PQC migration, except in scenarios requiring long-term quantum resilience, where moving from AES-128 to AES-256 may be advisable.

Therefore, while asymmetric PQC integration may require hardware upgrades or software optimizations, especially in legacy or constrained NTN nodes, the performance impact is event-based and can be mitigated through architectural planning and protocol design.

To mitigate the performance impacts of PQC, NTN systems can implement hardware accelerators to handle the increased computational demands. Additionally, algorithm optimization and hybrid cryptographic frameworks can reduce latency and ensure seamless integration with existing systems.

Performance Metric	Impact	Proposed Solution
Latency	Increased delay in control and user plane communications.	Use latency-efficient PQC algorithms.
Computational Load	Higher processing requirements on satellites and ground stations.	Deploy hardware accelerators (e.g., FPGA, ASIC).
Bandwidth Utilization	Increased bandwidth usage due to larger key sizes.	Optimize transmission protocols and compression.
Power Consumption	Higher energy demands for cryptographic operations.	Optimize power management and implement efficient hardware.
Memory Consumption	Larger keys/certificates + crypto libraries increase memory use, risky in embedded environments	Minimize on-space cryptographic stack; gateway termination; implement compact certificate chains; remove unused algorithms.

Table 7: Performance Metric

3.9 Gantt Chart for PQC Migration

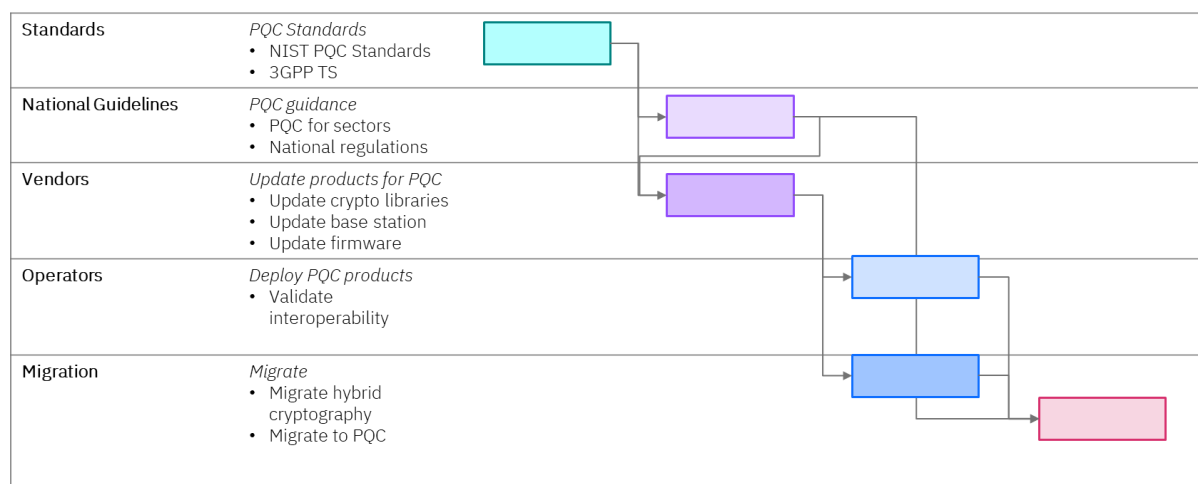


Figure 7: Gantt Chart for PQC Migration

3.10 PQC Migration Process Description

The migration to PQC involves a phased and multi-stakeholder approach, balancing operational readiness, emerging technical standards, and sector-specific guidance. This process is anchored by a coordinated effort among key standards bodies, each with distinct but interdependent roles:

- The **National Institute of Standards and Technology (NIST)** is leading the selection and standardization of quantum-safe algorithms (e.g., **FML-KEM**, **ML-DSA**, **SLH-DSA** etc.) through its ongoing PQC project.
- The **Internet Engineering Task Force (IETF)** is actively developing new RFCs to integrate these algorithms into existing protocols, such as **TLS 1.3**, **IPsec/IKEv2**, and **DNSSEC** — not by merely updating, but by **extending protocols and defining hybrid or replacement cryptographic mechanisms**.
- **3GPP**, through internal studies like **TR 33.703 [20]**, is assessing how to incorporate PQC algorithms into mobile network security architecture, particularly for control and user plane protection.
- Organizations like **ETSI** and industry consortia such as the **GSMA** contribute sectoral guidance and coordinate industry alignment on best practices for quantum-safe migration.

In parallel, **national regulatory authorities** are developing frameworks and endorsing **sovereign cryptographic standards** for PQC, which may influence algorithm choices or mandate national approval processes. PQC migration must also account for **interoperability, regulatory alignment, and implementation feasibility** across diverse systems and international jurisdictions.

This phase ensures that the migration strategy aligns with local regulations and data protection laws while fostering collaboration between public and private entities.

- Equipment vendors play a crucial role in updating products to support PQC mechanisms. Upgrading base and ground stations, cryptographic inventory, and PKI systems to meet the computational and security demands of post-quantum cryptography. Collaboration

with standards bodies and operators is essential to maintain compatibility and performance.

- Operators focus on testing and deploying PQC-enabled solutions. Interoperability testing ensures seamless integration with existing infrastructure, deploying updated RAN components, and securely implementing updated hardware. Operators also coordinate with vendors to validate hardware and software upgrades.
- The final phase is the system-wide migration to PQC. Replacing legacy cryptographic systems with quantum-safe algorithms in critical components such as management and control planes. The migration must minimize disruptions while maintaining backward compatibility with existing systems during the transition period.

3.11 Synergy with Internal Programs

Operators can streamline migration, optimize resource allocation, and enhance overall system security by leveraging ongoing efforts. Internal programs focused on legacy cryptographic management, such as PKI operations and key lifecycle management, can be extended to include PQC mechanisms. Existing cybersecurity initiatives, including penetration testing, vulnerability management, and incident response, provide a foundation for testing and validating PQC-enabled NTN systems.

3.12 Synergy with External Programs

Synergy with vendors and satellite network operators about the operator migration plan, which will affect the product development of vendors and deployment in the satellite in advance.

Annex A Document Management

A.1 Document History

Version	Date	Approval Authority	Editor / Company
1.0	04 February 2026	PQTN/TF	PQTN TF

Other Information

Type	Description
Document Owner	GSMA PQTN
Editor / Company	Yolanda Sanz, GSMA

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.