Quantum Safe 5G Core

PQTN Compliant 5G Core NF PQC Migration

PQTN (Post Quantum Telco Network) is a task force initiated by GSMA focused on addressing the challenges of post-quantum cryptography in the telecommunications industry.

Note: *The **Status** column indicates NgKore's progress in the migration process.*

AMF (Access and Mobility Management Function)

Interface / Properties	Protocol	Current Algorithms	PQTN Specified Algorithms	Status
N2	NGAP over SCTP	IPSec (Classical)	IPSec with ML-KEM-768	Completed
SBI (Namf): N8, N12, N22, etc	HTTP/2 + mTLS 1.3	Classical: ECDHE + ECDSA, RSA, etc	ML-KEM-768 + ML-DSA-65 or Hybrid PQC	Completed
SBI (Authorization)	OAuth 2.0	RS256 or ES256	ML-DSA or Hybrid ML-DSA	Completed

SMF (Session Management Function)

Interface / Properties	Protocol	Current Algorithms	PQTN Specified Algorithms	Status

N4	PFCP over UDP	IPSec (Classical)	IPSec with ML-KEM-768	Completed
SBI (Nsmf): N7, N10, N11, etc	HTTP/2 + mTLS 1.3	Classical: ECDHE + ECDSA, RSA, etc	ML-KEM-768 + ML-DSA-65 or Hybrid PQC	Completed
SBI (Authorization)	OAuth 2.0	RS256 or ES256	ML-DSA or Hybrid ML-DSA	Completed

UDM (Unified Data Management)

Interface / Properties	Protocol	Current Algorithms	PQTN Specified Algorithms	Status
SIDF Function	ECIES	ECC: X25519 & secp256	ML-KEM-768 or X25519MLKEM768 with AES-256	Completed
SBI (Nudm): N8, N10, N13, etc	HTTP/2 + mTLS 1.3	Classical: ECDHE + ECDSA, RSA, etc	ML-KEM-768 + ML-DSA-65 or Hybrid PQC	Completed
SBI (Authorization)	OAuth 2.0	RS256 or ES256	ML-DSA or Hybrid ML-DSA	Completed

NRF (Network Repository Function)

Interface / Properties	Protocol	Current Algorithms	PQTN Specified Algorithms	Status

SBI (Nnrf)	HTTP/2 + mTLS 1.3	Classical: ECDHE + ECDSA, RSA, etc	ML-KEM-768 + ML-DSA-65 or Hybrid PQC	Completed
OAuth (Authorization Server)	JWT/JWS	RS256 or ES256	ML-DSA or Hybrid ML-DSA	Completed

UPF (User Plane Function)

Interface / Properties	Protocol	Current Algorithms	PQTN Specified Algorithms	Status
N3	GTP-U over UDP	IPSec (Classical)	IPSec with ML-KEM-768	Completed
N4	PFCP over UDP	IPSec (Classical)	IPSec with ML-KEM-768	Completed
N6	Various	Depends on deployment	IPSec with ML-KEM-768	Completed

AUSF (Authentication Server Function)

Interface / Properties	Protocol	Current Algorithms	PQTN Specified Algorithms	Status
SBI (Nausf): N12, N13, etc	HTTP/2 + mTLS 1.3	Classical: ECDHE + ECDSA, RSA, etc	ML-KEM-768 + ML-DSA-65 or Hybrid PQC	Completed

SBI (Authorization)	OAuth 2.0	RS256 or ES256	ML-DSA or Hybrid ML-DSA	Completed

PCF (Policy Control Function)

Interface / Properties	Protocol	Current Algorithms	PQTN Specified Algorithms	Status
SBI (Npcf): N5, N7, N15, etc	HTTP/2 + mTLS 1.3	Classical: ECDHE + ECDSA, RSA, etc	ML-KEM-768 + ML-DSA-65 or Hybrid PQC	Completed
SBI (Authorization)	OAuth 2.0	RS256 or ES256	ML-DSA or Hybrid ML-DSA	Completed

NSSF (Network Slice Selection Function)

Interface / Properties	Protocol	Current Algorithms	PQTN Specified Algorithms	Status
SBI (Nnssf): N22	HTTP/2 + mTLS 1.3	Classical: ECDHE + ECDSA, RSA, etc	ML-KEM-768 + ML-DSA-65 or Hybrid PQC	Completed
SBI (Authorization)	OAuth 2.0	RS256 or ES256	ML-DSA or Hybrid ML-DSA	Completed

Inter-PLMN and Roaming Interfaces

Interface	Function	Protocol	Current Algorithms	PQTN Specified Algorithms	Status
N32-c (Control Plane)	SEPP–SEPP	TLS 1.3	Classical: ECDHE + ECDSA, RSA, etc	ML-KEM-768 + ML-DSA-65 or Hybrid PQC	Ongoing
N32-f (Forwarding)	SEPP–SEPP	HTTP/2 TLS 1.3	Classical: ECDHE + ECDSA, RSA, etc	ML-KEM-768 + ML-DSA-65 or Hybrid PQC	Ongoing

Management and Support Interfaces

System	Interface	Protocol	Current Algorithms	PQTN Specified Algorithms	Notes	Status
Element Management	HTTPS	TLS 1.2/1.3	RSA/ECDSA	ML-DSA or Hybrid ML-DSA	Admin access security	Completed
SSH Management	SSH	SSH 2.0	RSA/ECDSA	ML-DSA or Hybrid ML-DSA	Remote shell access	Completed

Database and Storage Migration

Component	Interface	Current Algorithms	PQTN Specified Protection	Data Sensitivity
UDM Database	Internal API	AES-128 + RSA key wrap	AES-256 + ML-KEM-768 key wrap	Subscriber data, SUPI
Configuration DB	Internal API	AES-128 + RSA	AES-256 + ML-DSA-65	Network configuration

Certificate and Key Management

PKI Component	Current Algorithms	PQTN Specified Algorithms	Transition Method	Dependencies
Root CA	RSA-4096	ML-DSA-87	New root deployment	HSM upgrade
Intermediate CA	RSA-2048	ML-DSA-65	Cross-signed transition	Root CA ready
NF Certificates	ECDSA P-256	ML-DSA-65	Parallel issuance	Intermediate CA
TLS Server Certs	ECDSA P-256	ML-DSA-65	Rolling replacement	Per NF schedule
Client Certificates	ECDSA P-256	ML-DSA-44	On-demand issuance	Service requests

Acknowledgements

The NgKore Community would like to thank the following people who contributed to this solution brief: Aditya Koranga and Shubham Kumar.