QRAN: QUANTUMIZED O-RAN

O-RAN SOLUTION ENHANCED WITH POST QUANTUM CRYPTOGRAPHY AND QRNG

Cloud Native Security India

CLOUD NATIVE
COMMUNITY GROUPS

CORAN LABS

WHO ARE WE?

Vipin Rathi

Assistant Professor @DU

- Chair Hyperledger Telecom SIG
- Board Member of OpenInfra Foundation Asia

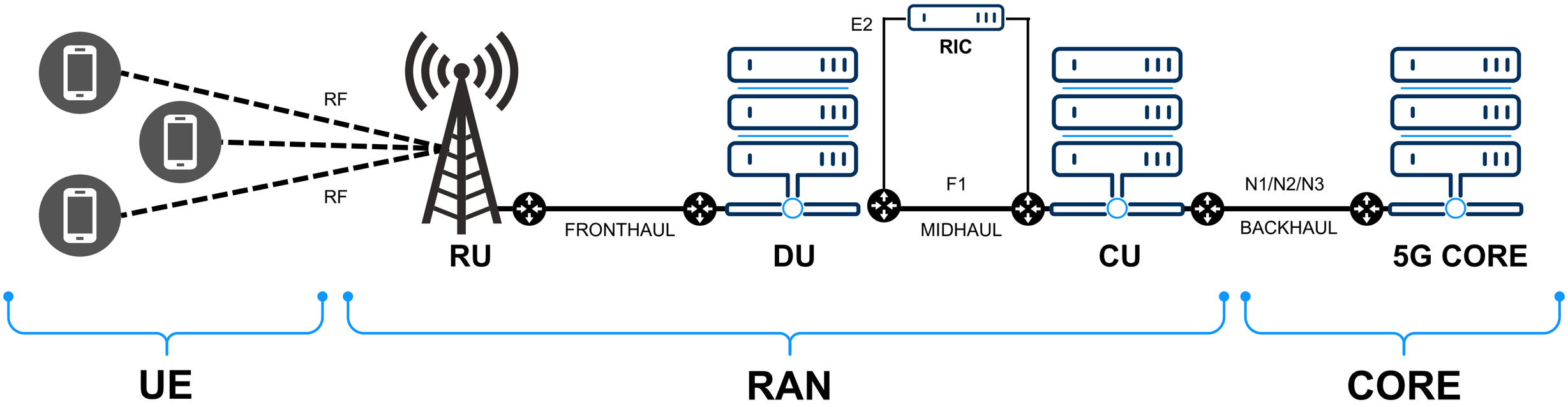
LinkedIn

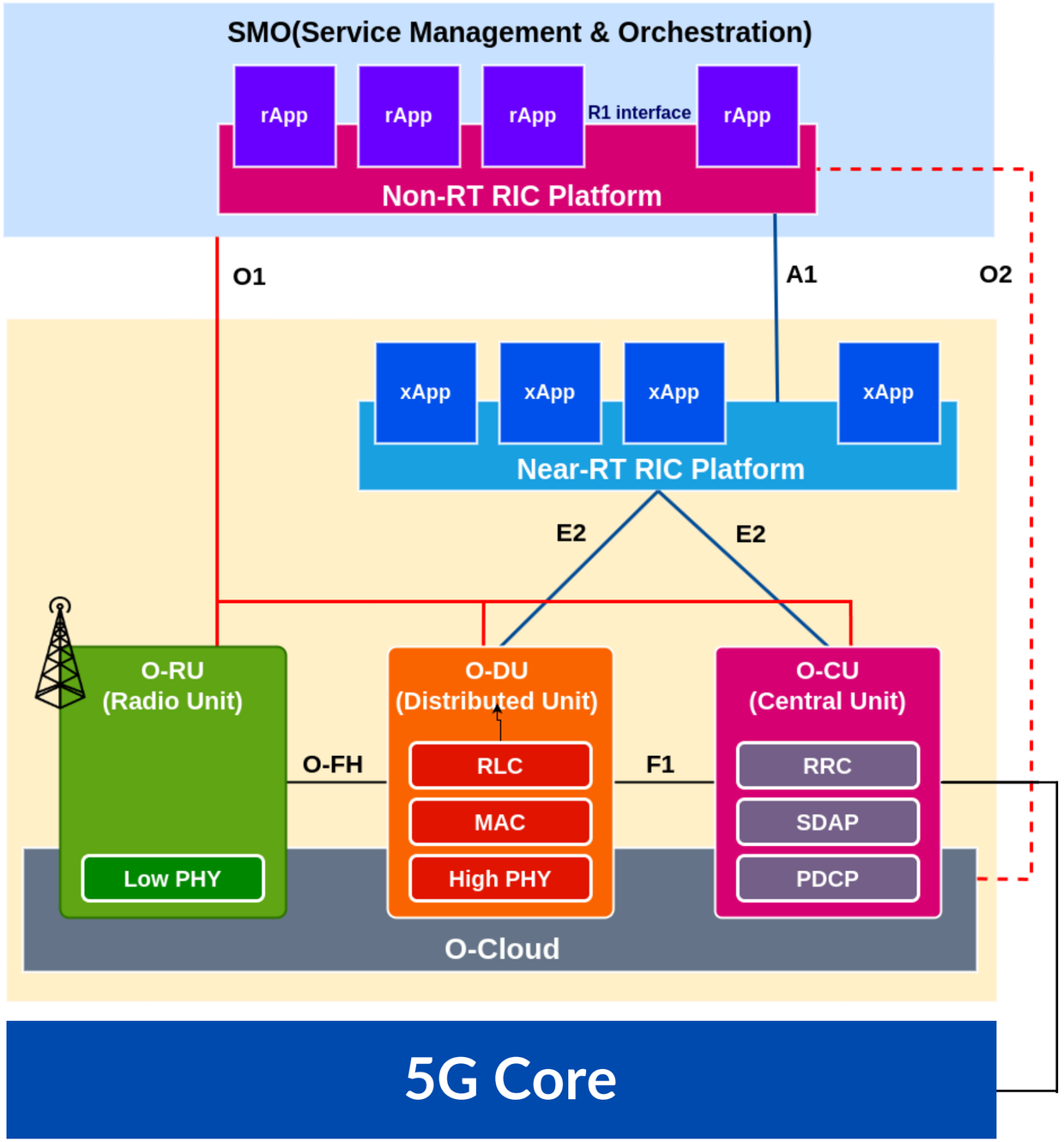
Aditya Koranga

Post-Quantum
Cryptography Researcher

LinkedIn

E2E CONNECTION: FROM DEVICES TO THE INTERNET





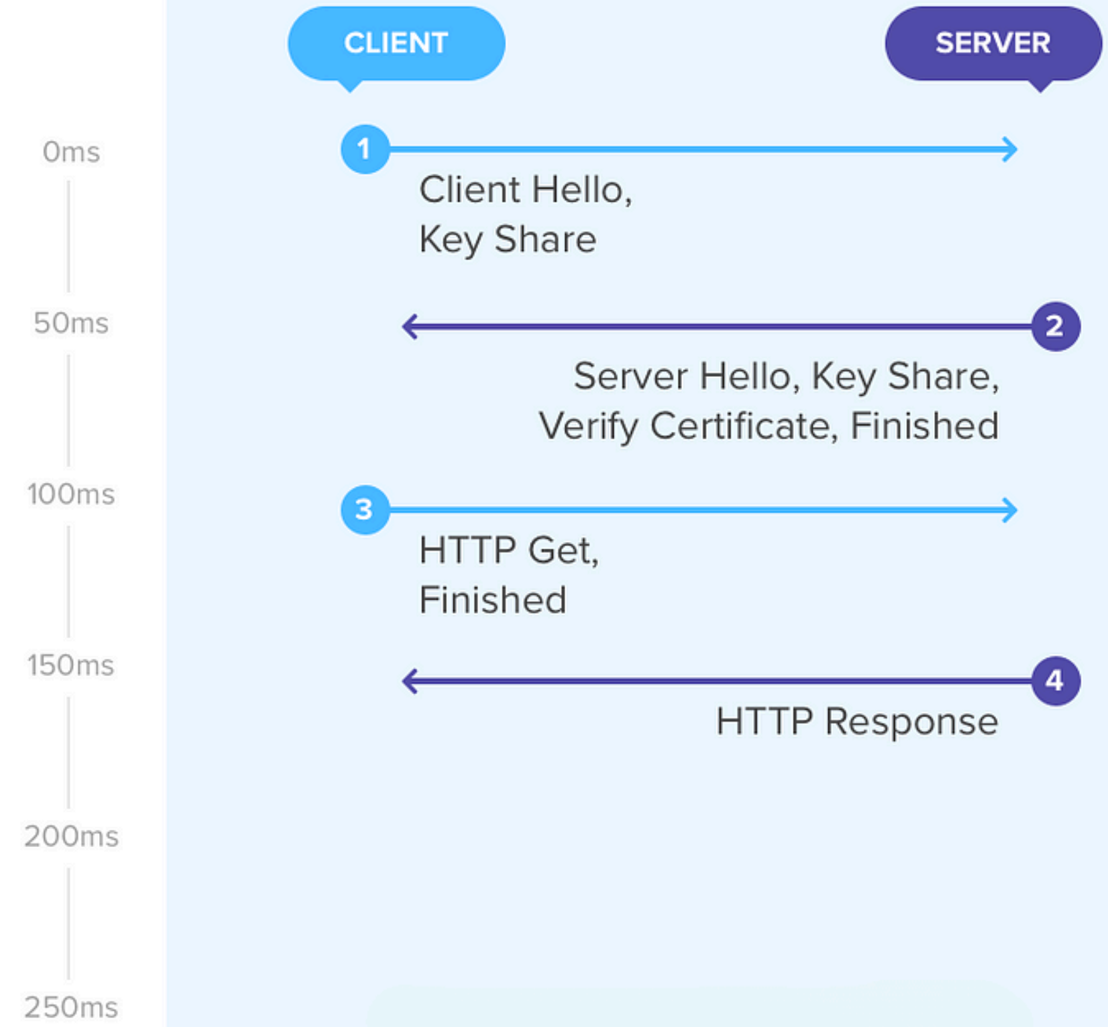
SECURITY IN O-RAN

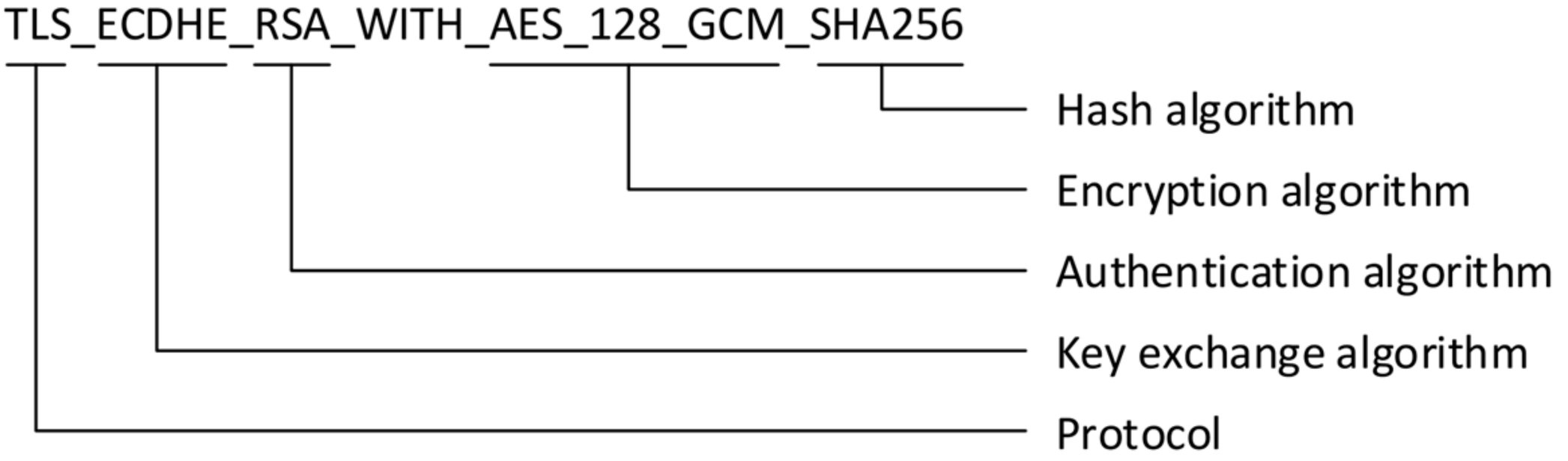
Open RAN architecture offers a pathway to more secure networks and open interfaces compared to proprietary architecture. The open interfaces specified in the O-RAN technical guidelines enhance independent visibility, creating opportunities for an overall improved and more secure network infrastructure.

CLASSICAL CRYPTOGRAPHY IN O-RAN

- ECC/ RSA
- mTLS
- DTLS
- IPSec
- PRNG
- 128-bit symmetric key
- IKEv2
- etc.

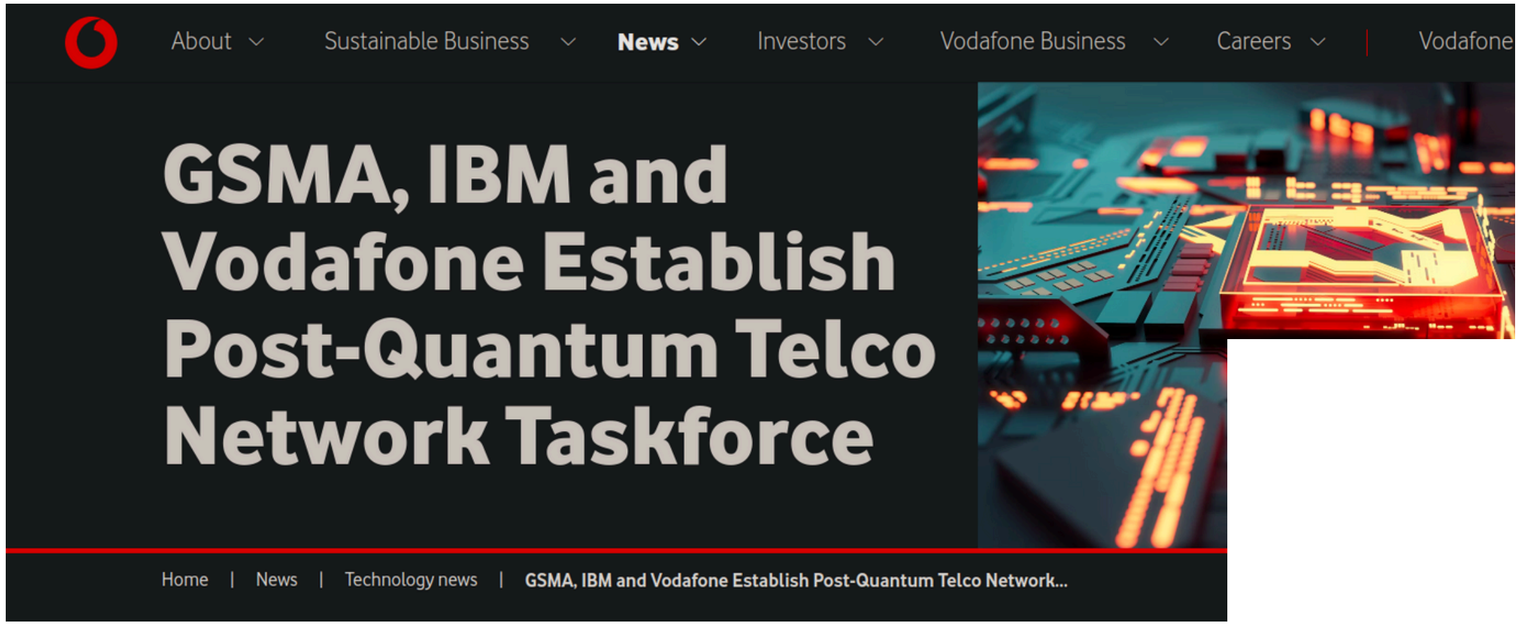
TLS


CLIENT
SERVER
0ms
50ms
100ms
150ms
200ms
250ms
1
Client Hello,
Key Share
2
Server Hello, Key Share,
Verify Certificate, Finished
3
HTTP Get,
Finished
4
HTTP Response


TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
Hash algorithm
Encryption algorithm
Authentication algorithm
Key exchange algorithm
Protocol

NEED FOR:

Post-Quantum Cryptography & Quantum Random Number Generator



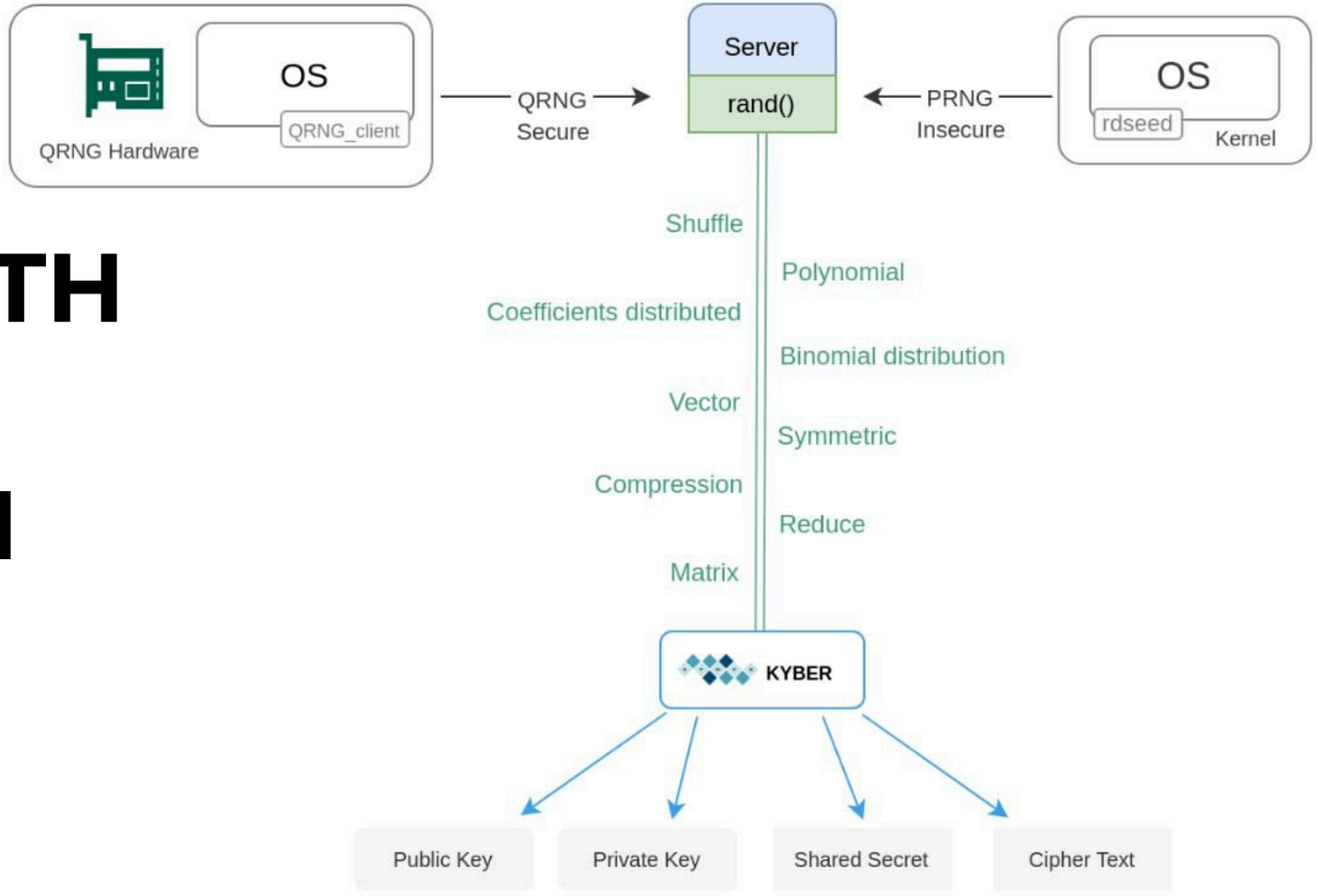
GSMA™

Post Quantum Cryptography – Guidelines for Telecom Use Cases

Version 1.0

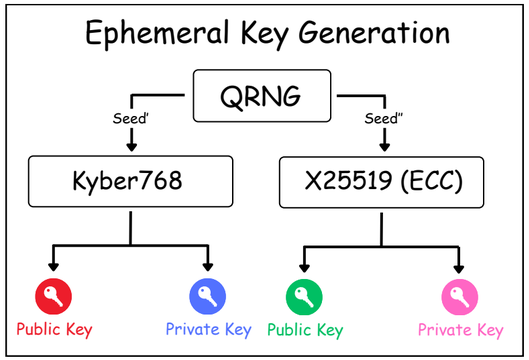
22 February 2024

ENHANCING TELECOM SECURITY WITH QRNG INTEGRATION



CLIENT

SERVER

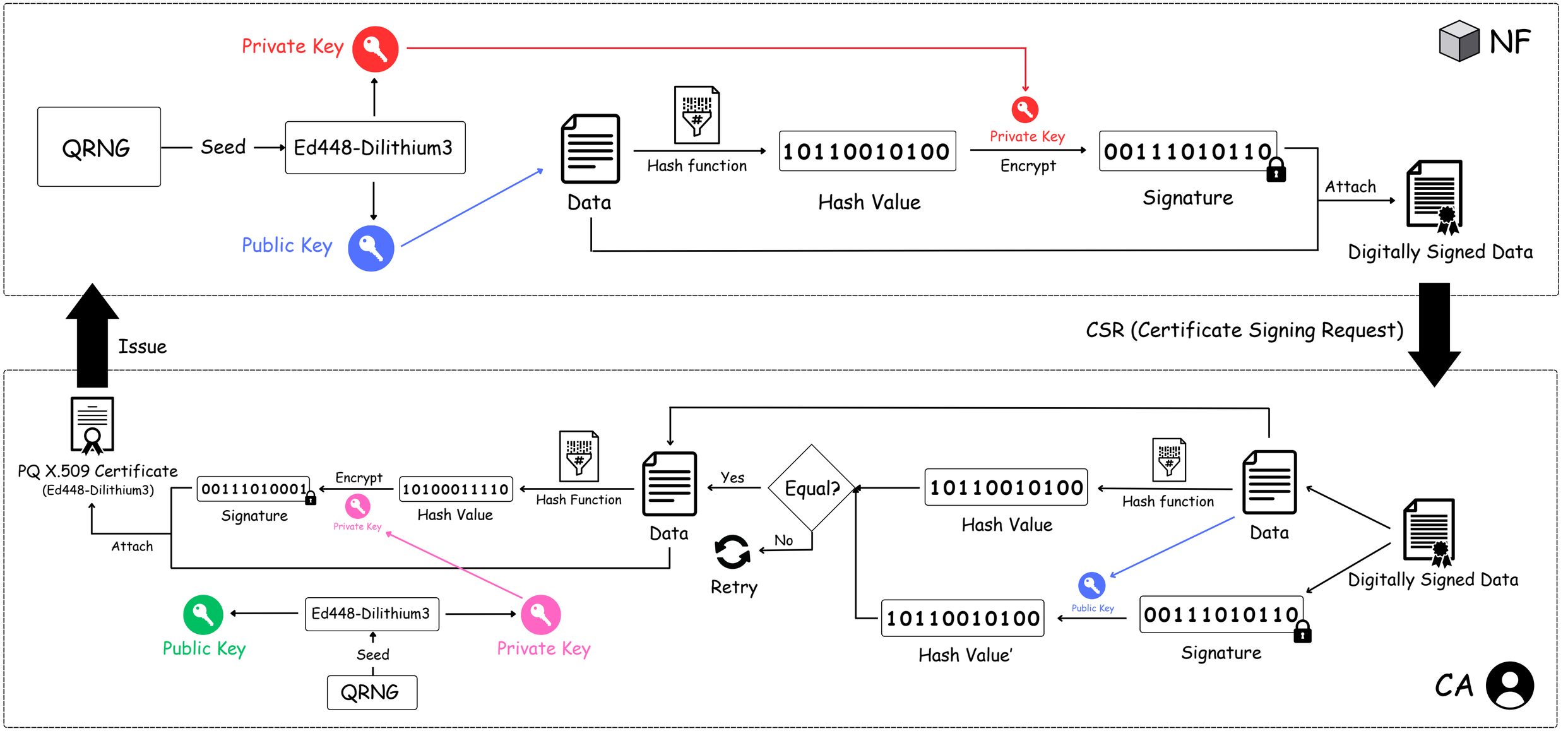


PQ TLS 1.3 ClientHello (Plaintext)

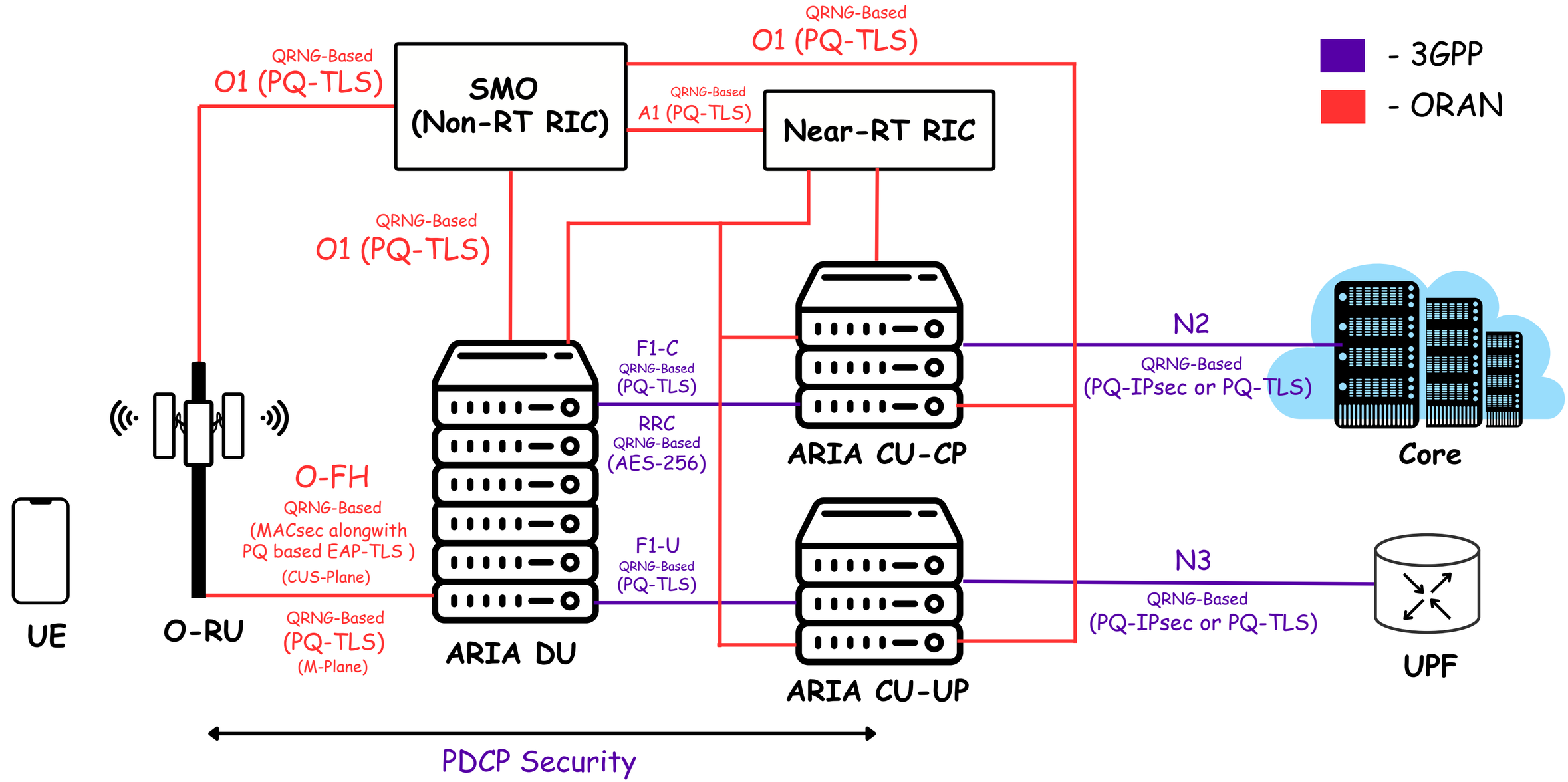
+ supported_group
  - PQ KEM list
    - PQ Hybrid KEMs: X25519Kyber, NTRU
    - Fallback Classical Methods: X25519, CurveP256
+ signature_algorithms
  - PQ Authentication Algorithm list
    - Hybrid PQ Schemes: Ed448-Dilithium3
    - Fallback Classical Algorithms: ECDSA, EdDSA, RSA
+ signature_algorithms_cert
+ key_share
  - Ephemeral Public Key
    - Kyber(KEM)
    - X25519(ECC)

TLS Handshake Starts

PQ-TLS Generation



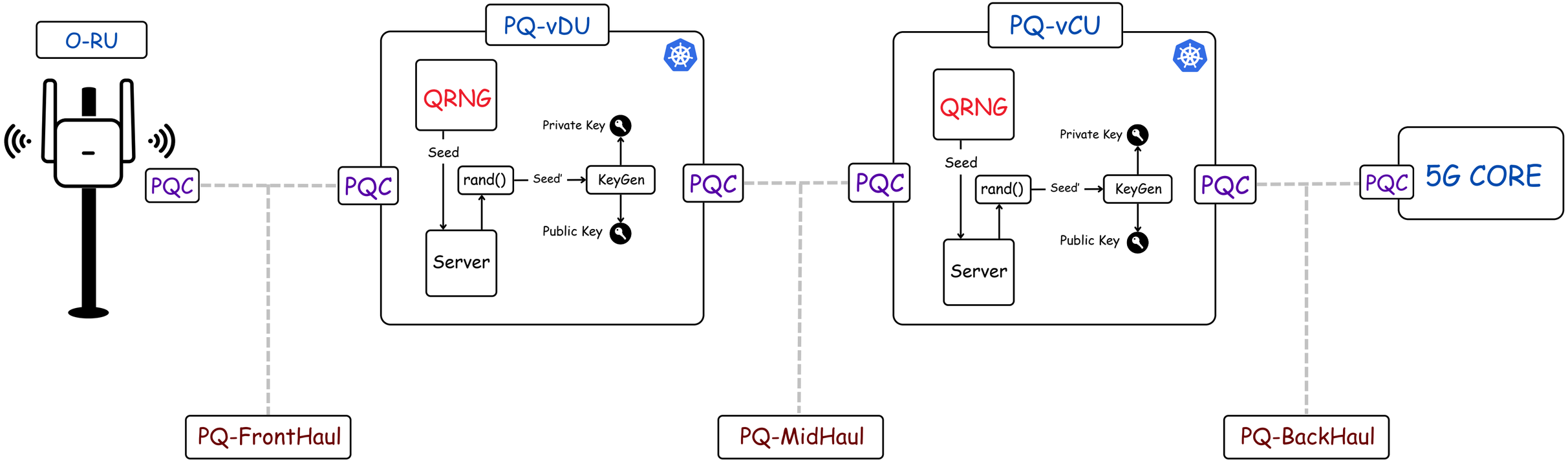
Q-RAN: Quantumized O-RAN



MIGRATION FROM O-RAN TO Q-RAN

Interfaces/ Protocols	Between Nodes	Existing Security Mechanisms	Post Quantum Security Mechanisms	Specified By
RRC	UE & gNB	128-NEA/128-NIA (AES-128)	256-NEA/256-NIA (AES-256) (QRNG Based Key Generation)	3GPP
F1AP	O-CU-CP & O-DU (F1-C) O-CU-UP & O-DU (F1-U)	NDS/IP (IPsec ESP & IKEv2) or DTLS	PQ-IPsec or PQ-TLS (QRNG Based Key Generation)	3GPP
E1AP	O-CU-CP & O-CU-UP			3GPP
BackHual (N2 & N3)	O-CU-CP & 5GC (N2) O-CU-UP & 5GC (N3)			3GPP
Xn	Source gNB & Target gNB			ORAN WG11
E2	Near-RT RIC(xAPPs) & O-CU-CP			ORAN WG11
O-FH (CUS-Plane)	O-DU & O-RU	IEEE 802.1x with EAP-TLS	MACsec alongwith PQ based EAP-TLS (QRNG Based Key Generation)	ORAN WG11
O-FH (M-Plane)	O-RU & O-DU/SMO	mTLS, SSHv2	PQ-TLS (QRNG Based Key Generation)	ORAN WG4
O1	SMO & O-RAN Managed Elements	mTLS		ORAN WG11
A1	Near-RT RIC & Non-RT RIC	mTLS		ORAN WG11

VIRTUALISED Q-RAN



QORE: QUANTUMIZED CORE SOLUTION

BEYOND 5G CORE SOLUTION INTEGRATED WITH POST QUANTUM CRYPTOGRAPHY AND QRNG

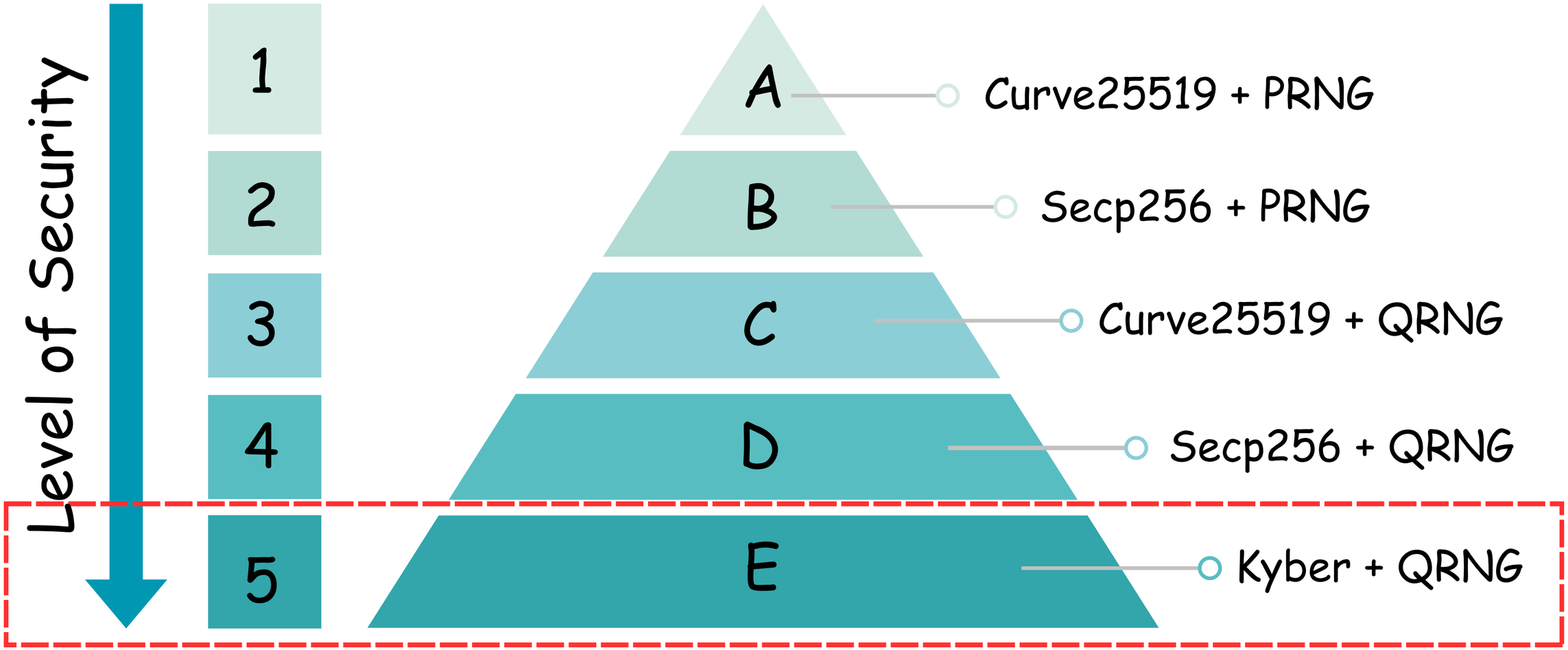
CORE WITH POST QUANTUM CRYPTOGRAPHY

- Qore operates in **Two Modes** for SUPI Concealment: Hybrid and Homogeneous Post-Quantum Encryption
  - **(I) Hybrid Post-Quantum Encryption**: Combines the post-quantum algorithm Crystal-Kyber with classical algorithms such as Curve25519 and Secp256r1
  - **(II) Homogeneous Post-Quantum Encryption**: Utilizes Crystal-Kyber solely, providing a robust and secure encryption method
- It also supports multiple Encryption Profiles, each offering an increasing level of security, AES-256 for stronger encryption, and incorporates Quantum Random Number Generator (QRNG) for Key Generation
- Communication between NFs is done via Service Based Interfaces (SBI) supplemented by Service Communication Proxy (SCP). This communication is secured by PQ-mTLS, utilizing Hybrid PQ Signature schemes (Ed448-Dilithium3) for signatures and certificates and Hybrid PQ KEMs (x25519Kyber768) for the key exchange.

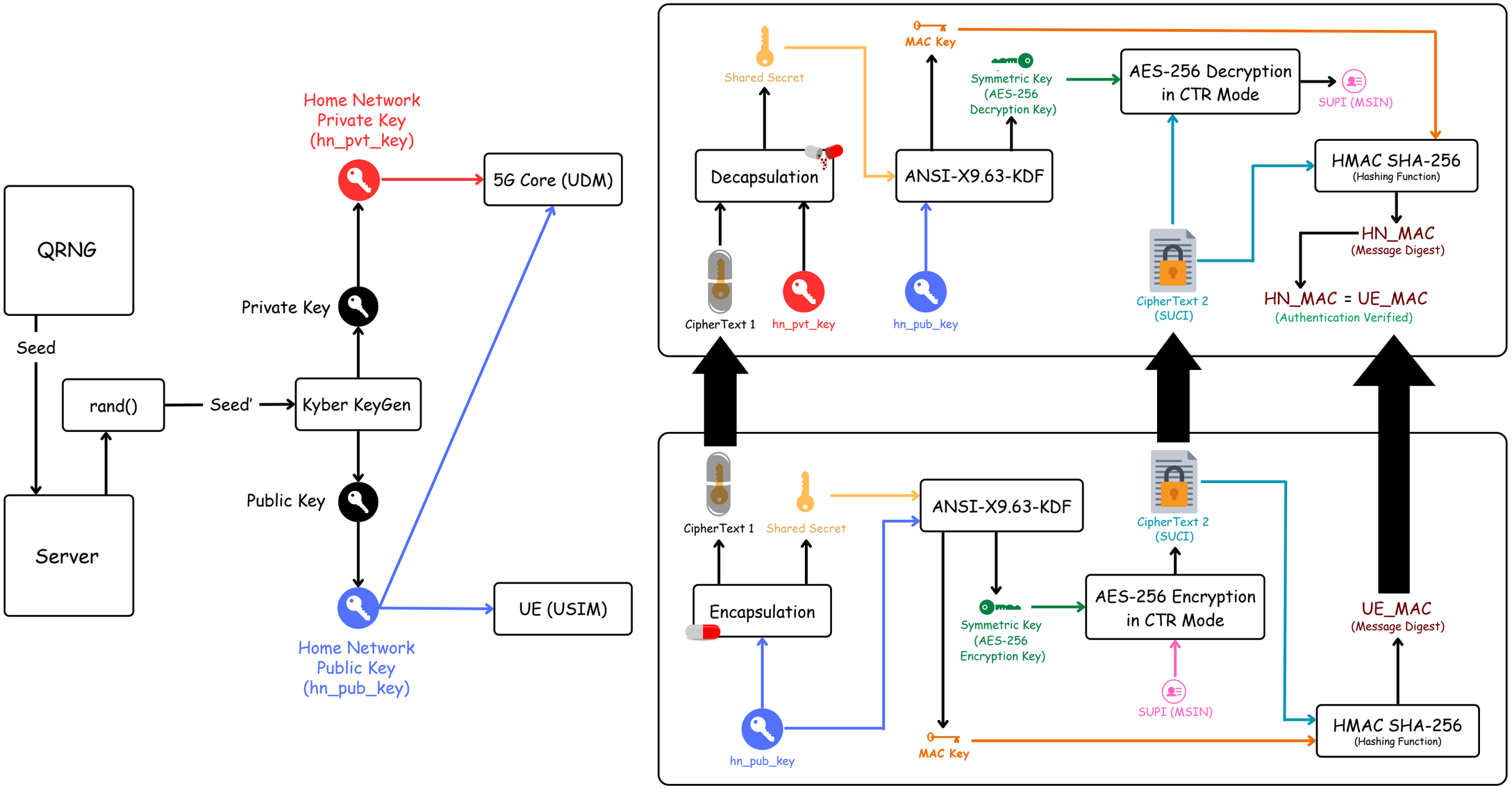
MIGRATION FROM CORE TO QORE

Functionality	Classical Encryption	Post Quantum Encryption	Status
SUPI to SUCI	ECIES(Elliptic Curve Integrated Encryption Scheme)	Crystals-Kyber (Key Encapsulation Mechanism)	✅ Done
		Hybrid Post Quantum Mechanism	✅ Done
Random Number	PRNG(Pseudo Random Number Generator)	QRNG(Quantum Random Number Generator)	✅ Done
SBI Communication	mTLS	PQ-TLS	✅ Done
Digital Certificates	Classical cryptographic algorithm	Dilithium	✅ Done
Symmetric Key	AES128	AES256	✅ Done
N3 User Data	IPSec	PQ-IPSec	🟡 Ongoing
N3 User Data	DTLS	PQ-DTLS	🟡 Ongoing

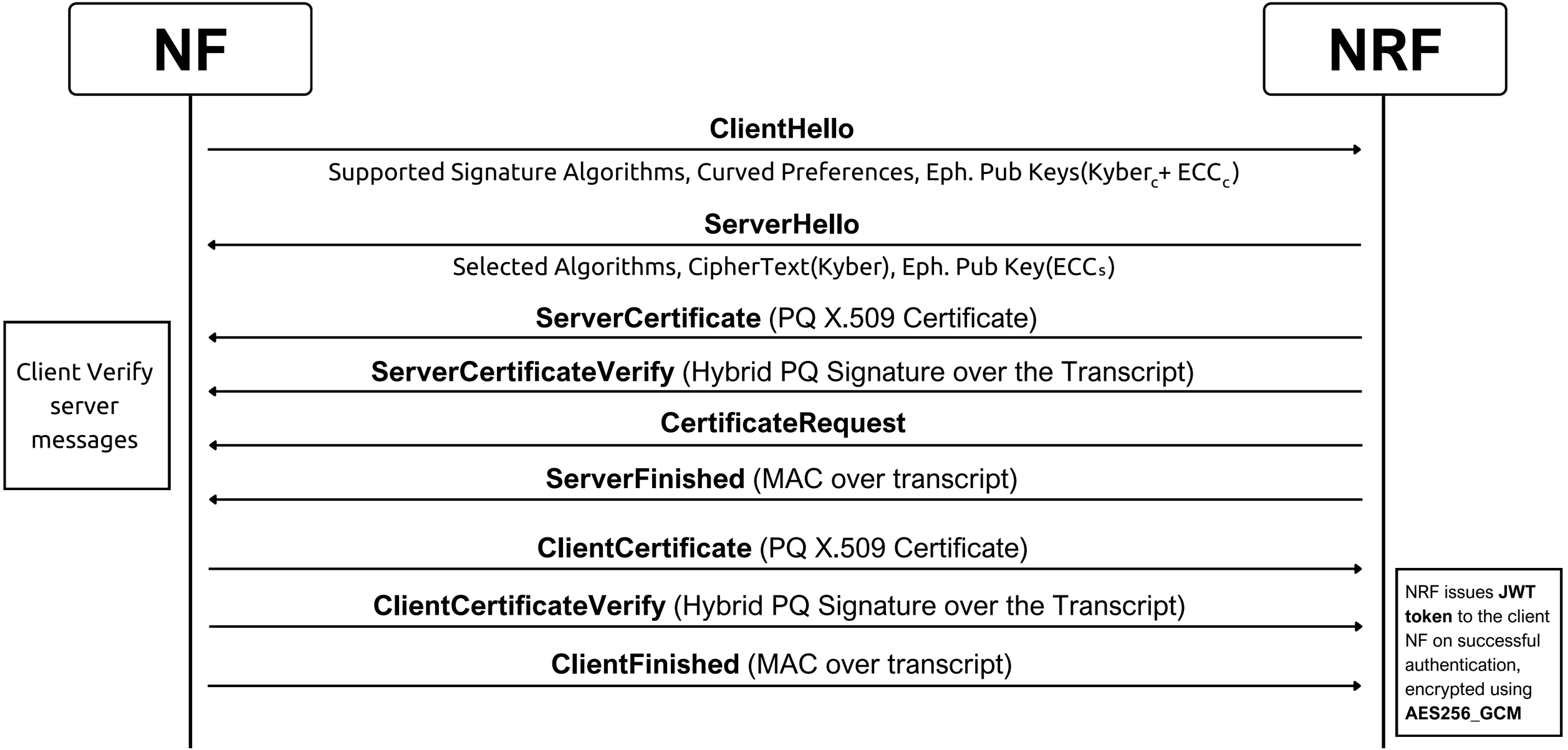
QORE(II) ENCRYPTION PROFILE



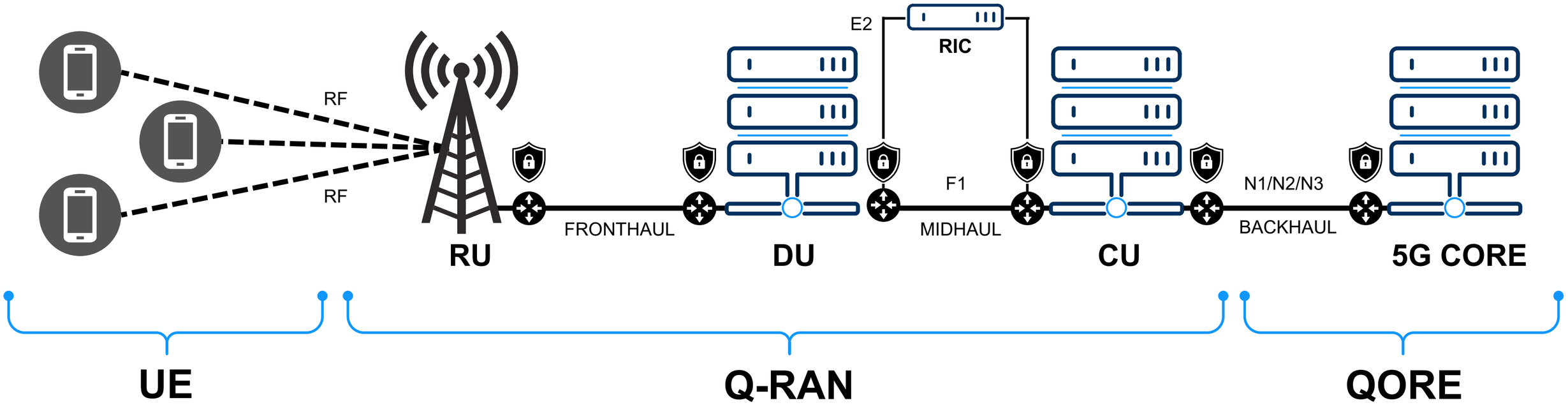
QORE(II): SUPI CONCEALMENT



QORE: PQ-TLS BASED SBI COMMUNICATION



E2E QUANTUM SECURE CONNECTION: FROM DEVICES TO THE INTERNET



THANK YOU

@coranlabs