PQC Dialogue with Government Stakeholders

Meeting Organizers:
John Preuß Matsson, Ericsson
Alexander Engström, NDRE

March 17, 2025

PQC dialogue with government stakeholders

- This is a public side meeting. Open and free to attend for any IETF participant.

- **Subject to the IETF Note Well:**
  - By participating in the IETF, you agree to follow IETF processes and policies.
  - If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
  - As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
  - Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
  - As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

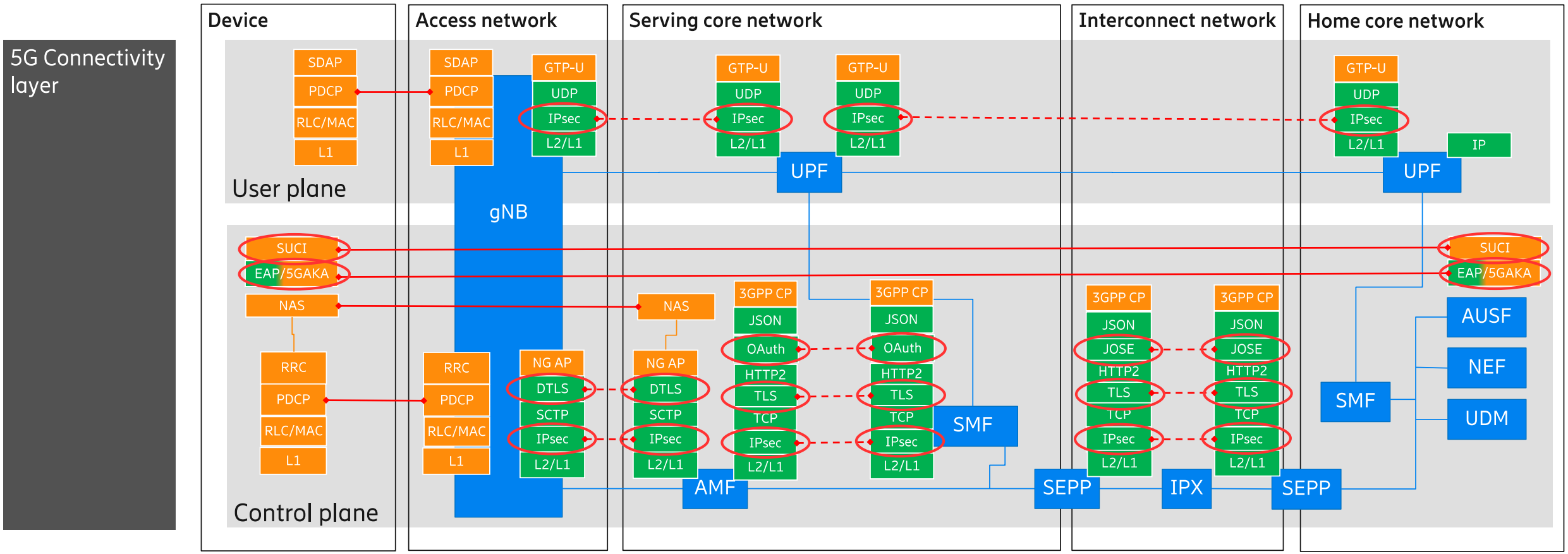
PQC dialogue with government stakeholders

- **Goals:**
  - Information sharing. There has been a lot of discussion and speculation in several groups on what different countries recommend and require.
  - Open dialogue and increased understanding between IETF people and government officials from all over the world.

- **Agenda:**
  - Introduction
  - Overview of PQC activities from governments
  - Dialogue and discussion

IETF protocols are essential for 5G (and 6G)

- 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. The amount of IETF protocols has increased for each generation.
  - IMSI encryption uses the SECG ECIES standard but augments it with X25519 (RFC 7748).
  - Important with global alignment on algorithms and hybridization.



EU Coordinated Roadmap for the transition to PQC

Alexander Engström, Swedish work group representative, pqc@fra.se

IETF 122, Bangkok

The Commission Recommendation of April 11, 2024

- The Commission Recommendation encourages Member States to develop a comprehensive strategy for the adoption of Post-Quantum Cryptography, to ensure a coordinated and synchronised transition among the different Member States for public administrations and critical infrastructures.
- The strategy should define clear goals, milestones, and timelines resulting in the definition of a joint Post-Quantum Cryptography Implementation Roadmap.

Work group: NIS CG WS PQC

- NIS2 Directive: new rules on cybersecurity of network and information systems.
- NIS Cooperation Group: The Group's overall mission is to achieve a high common level of security for network and information systems in the European Union. It supports and facilitates the strategic cooperation and the exchange of information among EU Member States.
- WS PQC: Work Stream PQC

Publication of roadmap

- Part one in mid-May 2025. Focus on timelines and first steps for member states. No technical recommendations.
- Part two in mid-May 2026. Technical recommendations.

From the roadmap draft

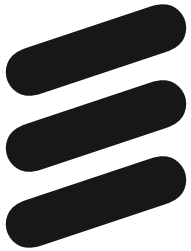
- In general, the transition should be done by the end of 2035.
- The transition for ”Harvest now, decrypt later” should be done by the end of 2030.

NIS CG publications

https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group

Potential discussion topics

- **Recommended PQC algorithms (KEMs and signatures)**
  - ML-KEM, ML-DSA, SLH-DSA, FN-DSA, Classic McEliece, FrodoKEM, BIKE/HQC, XMSS/LMS, …
  - Security category 1,2,3,4,5? Does it depend on algorithm and use case?
- **Timelines for PQC migration**
  - When should migration begin? When will it be required?
  - Does it depend on user, use case, protection lifetime, hardware vs software, migration complexity, value of the protected node and data, scheduled hardware replacement, etc.?
- **Hybridization or standalone PQC**
  - Difference between KEMs and Signatures
  - Differences between algorithms (e.g., lattice-based vs. hash-based)
  - Differences between use cases (e.g., confidentiality vs. authentication)
  - Is hybridization a short-term necessity or a long-term strategy?
- **Hybridization of PQC KEMs**
  - Single vs. multiple PQC algorithms? Role of symmetric keys?
  - KEM combiners: general-purpose vs. optimized designs
  - Which traditional curves? X25519/X448, NIST P-curves, Brainpool, …
- **Hybridization of signatures**
  - Role of symmetric keys?
  - Signature combiners, general or optimized?
  - Desired properties: SUF-CMA? Other security properties?
  - Which traditional signatures? EdDSA, ECDSA, RSA?
- **KDF and hash functions**
  - ML-KEM and ML-DSA mandate SHA-3.
  - Time to move away from SHA-2/HMAC/HKDF/MGF?



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