Government–Industry Dialogue Side Meeting

Meeting Organizers:
John Preuß Mattsson, Ericsson
Alexander Engström, Swedish NCSC
July 23, 2026

Government–Industry Dialogue

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

- **Subject to the IETF Note Well -** A reminder of IETF policies:
  - IETF participants are expected to **behave in a professional manner and extend respect and courtesy to their colleagues at all times** (see RFC 7154: IETF Guidelines for Conduct and IETF Anti-Harassment Policy). If you have any concerns about behavior, please contact the Ombudsteam who have a duty of confidentiality and extensive powers to act, as set out in RFC 7776: IETF Anti-Harassment Procedures.
  - If you are aware that any IETF contribution (as defined in RFC 5378: Rights Contributors Provide to the IETF Trust) is covered by patents or patent applications that are owned or controlled by you, your employer or your sponsor, you must disclose that fact, or not participate in the discussion (see RFC 8179: Intellectual Property Rights in IETF Technology).
  - For detailed process information consult RFC 2026: Internet Standards Process and RFC 2418: IETF Working Group Guidelines and Procedures and updates to those.
  - The IETF routinely makes public written, audio, video, and photographic records of IETF activities, including your personal information as set out in the IETF Privacy Statement.

Government–Industry Dialogue

- **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.

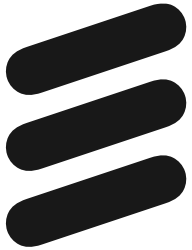
- **Agenda:**
  - Introduction
  - Overview of PQC activities from governments
    - Europe, North America, Asia, …
  - Industry challenges and perspectives
  - Dialogue and discussion
  - Next side-meeting

Some developments since the last side-meeting

- EU, UK, Canada, and many others published roadmaps and timelines for the for the transition to PQC
- NIST SP 800-27 and progress on FIPS 206 (FN-DSA), FIPS 207 (HQC-KEM), and additional SLH-DSA
- IETF progress on integrating PQC into Internet protocols
- 3GPP/GSMA starting normative work item on PQC for 5G/6G
- Significant improvements in quantum algorithms
- White house memorandum accelerating PQC migration
- More organizations aiming for full migration 2030
- Pentagon memorandum on PQC migration
- ISO standardized FrodoKEM and Classic McEliece
- Progress on CNSA 2.0 profiles for Internet protocols
- Increased use of SHA-3, (Turbo)SHAKE and XOFs
- Large-scale deployments: X25519MLKEM768 in over 70% of HTTP requests
- Increased support of PQC in libraries and hardware
- NIST round 3 signatures with MPCitH, Isogeny, and MQ
- Academic research on e.g., composite signatures, lightweight KEMs and NIKEs such as DAWN and MIKE
- China Next-Generation Cryptography program
- Russia developing national cryptographic standards

Potential discussion topics

- **Challenges, and approaches for PQC migration**
  - **When should migration begin?** When will it become mandatory? Will there be exceptions?
  - **How should migration priorities be determined?** Should they depend on the user, use case, protection lifetime, hardware vs. software, migration complexity, value of the protected system and data, or planned hardware replacement cycles?
  - **How should legacy hardware that cannot be fully migrated be handled?** Replacing deployed systems may be prohibitively expensive. Should organizations adopt a risk-based approach? Is it acceptable to use compensating controls, such as local IPsec security gateways (perimeter protection), to protect legacy devices?
- **Quantum-resistant advanced cryptography**
  - Homomorphic encryption, Private information retrieval, Multiparty computation, Zero-knowledge proofs, Private set intersection, Anonymous Credentials, Selective disclosure, Identity- and Attribute-based cryptography.
- **Hybridization**
  - While there is agreement that SLH-DSA does not require hybridization, recommendations for ML-KEM and ML-DSA differ. Some profiles require standalone, while some governments recommend hybrids.
  - The Web is planning to deploy hybrid ML-KEM together with standalone ML-DSA. Are any governments planning to update their recommendations?
  - Is hybridization a short-term transition mechanism or a long-term strategy? When can standalone PQC be expected to become the default recommendation? Can constrained IoT migrate directly from ECC to standalone PQC?
  - What are the desired security and operational properties of composite signatures?



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

The Swedish NCSC recommendations on PQC

with some notes on the EU transition and PQC for PETs

Alexander Engström at IETF 126, July 23, 2026

The Swedish national recommendations for the transition to quantum safe cryptography

- Published by the National Cybersecurity Center in May 2026

The Swedish PQC recommendations

- Everything sensitive to harvest-now-decrypt-later should be transitioned by 2030, and everything else by 2035.
- An important backdrop to the recommendations is the new Cybersecurity law, implementing the NIS2-directive.
- Immediate actions recommended for governmental agencies and companies:
  - Engage the management level to work strategically.
  - Create an inventory of crypto used today.
  - Cooperate with other actors in your sector.

Algorithms and protocols

- The cryptographic algorithms employed must be standardized in open transparent processes and already used at global scale by companies and governmental agencies.

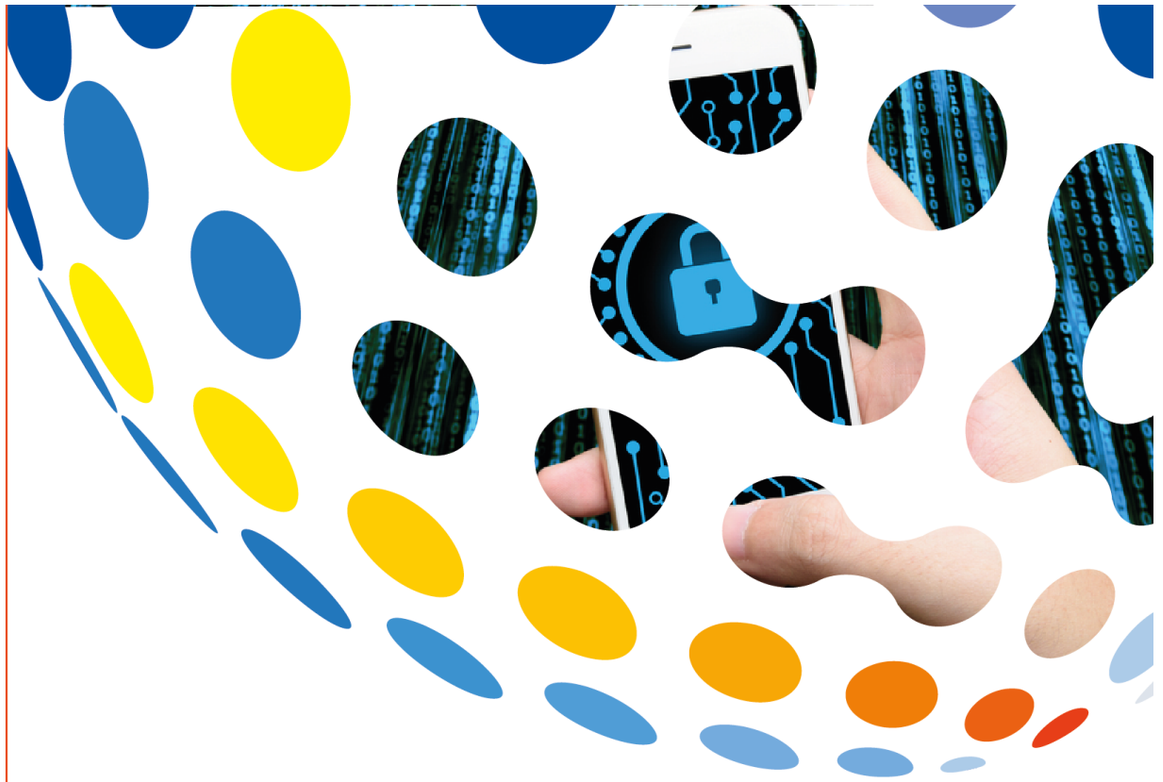
  Currently the only examples are from NIST.

- Protocols should also be standardized. Main venues are IETF, ETSI and 3GPP.

Rekommenderad	Inte längre rekommenderad
ML-KEM[1]	ECDH[2] RSA[3]
ML-DSA[4] SLH-DSA[5]	ECDSA EdDSA RSA[6]
LMS XMSS[7]	

The EU recommendation to member states

- Published in June 2025
- Written by NIS CG WS PQC, a workgroup consisting of member state representatives.
- Its target audience is the member states.



A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography

Part 1, Version: 1.1, EU PQC Workstream

11.06.2025

NIS COOPERATION GROUP

The EU roadmap timeline

1. By **31.12.2026**:
   - At least the *First Steps* have been implemented by all Member States.
   - Initial national PQC transition roadmaps have been established by all Member States.
   - PQC transition planning and pilots for high- and medium-risk use cases have been initiated.
2. By **31.12.2030**:
   - The *Next Steps* have been implemented by all Member States.
   - The PQC transition for high-risk use cases has been completed.
   - PQC transition planning and pilots for medium-risk use cases have been completed.
   - Quantum-safe software and firmware upgrades are enabled by default.
3. By **31.12.2035**:
   - The PQC transition for medium-risk use cases has been completed.
   - The PQC transition for low-risk use cases has been completed as much as feasible.

The EU roadmap — Milestone 1: End of 2026

- First Steps:
  - Identify and involve stakeholders.
  - Support mature cryptographic asset management.
  - Create dependency maps.
  - Perform quantum risk analysis.
  - Include the supply chain.
  - Create a national awareness and communication program.
  - Share knowledge and get involved with the NIS CG work stream on PQC.
  - Develop a timeline and an implementation plan.
- **Main achievements**:
  - PQC transition planning and pilots for high- and medium-risk use cases have been initiated.
  - Initial national PQC transition roadmaps have been established by all Member States.

Enhanced capacity for modern data sharing – privacy-enhancing technology in public administration

A 400 pages report from a governmental commission of inquiry. Published in June 2026.

- The step before a new law is proposed in Sweden
- En stärkt förmåga till modern datadelning – integritetsfrämjande teknik i offentlig förvaltning (SOU 2026:44)

The Swedish PET inquiry

PQC considerations

- The inquiry found that the there are good reasons to increase the adaptation of PETs within the public administration.

- Cryptographic PETs include: Homomorphic encryption, Private information retrieval, Multiparty computation, Zero-knowledge proofs, Private set intersection, and Attribute-based encryption.

- They are differently mature, but there are already some relevant use cases.

- The inquiry found that the adaptation of PETs would benefit a lot from standardization work in for example IETF. There are use cases from public administration and software companies are competent in developing solutions — but standards are still missing.

- It is important to look forward and standardize quantum safe solutions to further use cases of cryptology.