

Current Use Cases



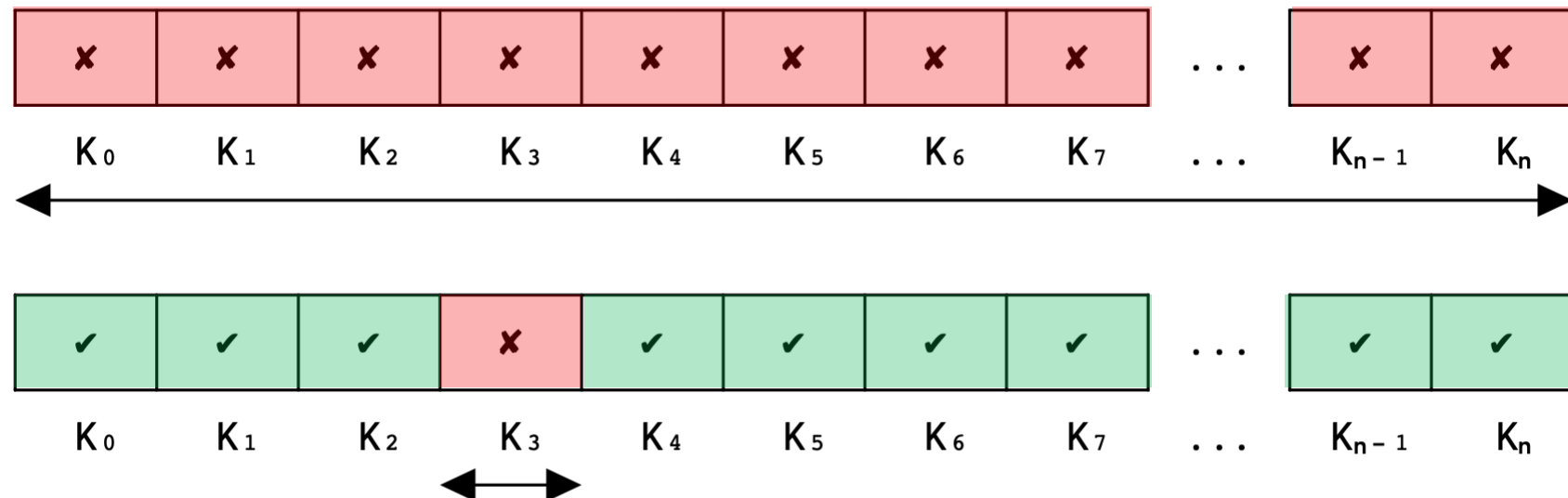
John Preuß Mattsson
Expert Cryptographic Algorithms and Security Protocols, Ericsson

CURRENT, IETF 126, Vienna, 21 July 2026

FS and PCS have been best practice for decades



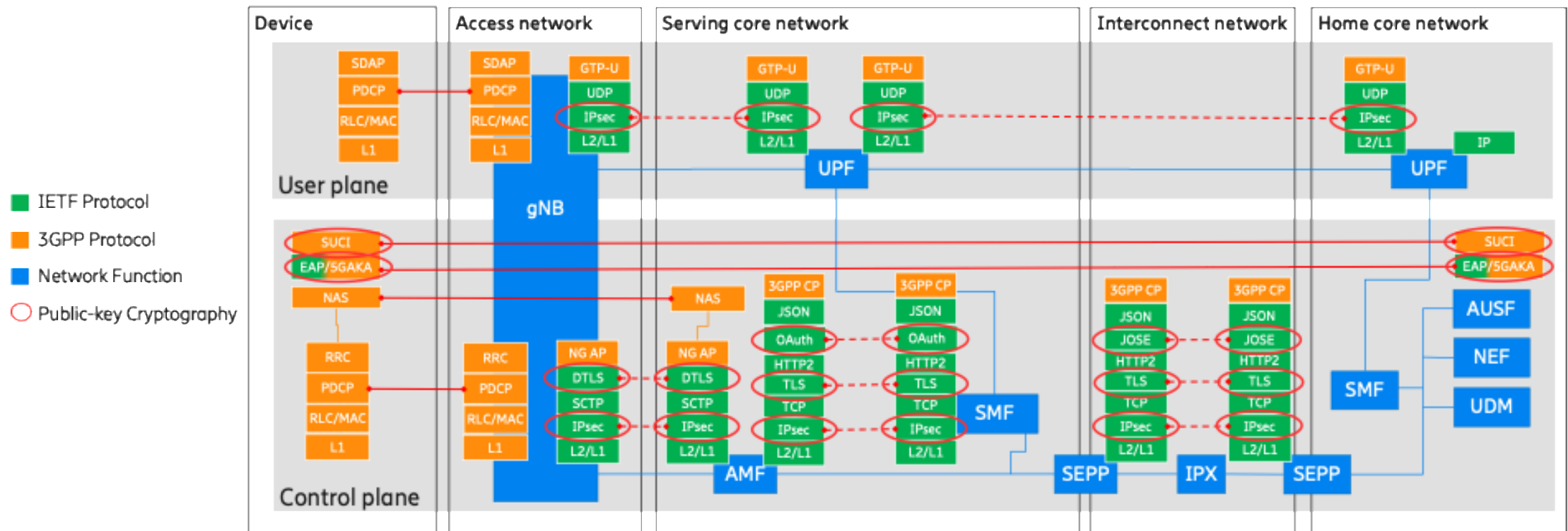
- Frequent rekeying using ephemeral key exchange is recommended every hour or 1–100 GB to provide Forward Secrecy (FS) and Post-Compromise Security (PCS), limiting the impact of key compromise [RFC 4253][ANSSI DAT-NT-003].
- RFC 7624 highlighted the need for IETF protocols to mitigate static key exfiltration in an era of pervasive surveillance, increasing the attacker's cost and risk of detection.
- Reauthentication is essential for confidentiality: it provides PCS against active attackers that have not compromised the long-term authentication key.



Long-lived connection and requirements in 5G/6G



- Telecom systems have many long-lived connections. FS, PCS, PQC, and reauthentication are requirements.
- PCS/reuthentication can be done at the protocol (MLS), library (IPsec), or application layer (QUIC/TLS).
 - Changes to existing application layer may not be possible
 - Application should not be responsible for lower layer rekeying and reauthentication.



MIKEY-SAKKE replacement for mission critical



- 3GPP has specified the use of MIKEY-SAKKE, which is based on pairing-based cryptography, for mission-critical application-layer group communication [RFC 6509].
- The most straightforward quantum-resistant replacement today is MIKEY+MLS.



Unidirectionality as a privacy requirement in radio



- Radio transmission (TX) inherently reveals the sender's location.
- For use cases where location privacy is highly sensitive, unidirectional communication (RX only) is therefore a fundamental requirement.
- Even in unidirectional operation, the strongest possible rekeying mechanisms should be used.

