IETF 123: Migrating Telecom to Quantum-Resistant Cryptography on a Global Scale

This Host Speaker Series session at 11:15 UTC on 24 July 2025 discussed these challenges the mobile industry faces in the transition to quantum-resistant cryptography and the industry's plans to overcome them.

This talk presented by John Preuß Mattsson, an expert in cryptographic algorithms and security protocols at Ericsson Research in Stockholm, Sweden, discussed challenges the mobile industry faces in the transition to quantum-resistant cryptography and the industry's plans to overcome them.

The mobile industry, with its unique characteristics, has been preparing for the transition to quantum-resistant cryptography for many years. As truly global standards, 4G and 5G require algorithms that are universally trusted and secure across all regions. Mobile networks are considered critical infrastructure, heavily regulated, and expected to adhere to government recommendations for migration timelines. However, performance and costs remain high priorities, which differs from national security systems. For many IoT applications, radio is the most limiting resource, making small sizes essential. Hardware like base stations has a long lifecycle, often remaining in service for decades.Mobile networks rely heavily on IETF standards for public-key cryptography, though they have a few unique protocols. 5G and 6G standards will introduce quantum-resistant algorithms in 2027–2028, and 6G will be quantum-resistant by design. Migrating public key infrastructure (PKI) and root-of-trust for firmware and software updates is a top priority.

IETF Live

IETF 123: Plenary

IETF 123: Migrating Telecom to Quantum-Resistant Cryptography on a Global Scale

IETF 123: IAB Open

IETF 123: IRTF Open

Previous IETF Live sessions