Quantum-resistant cryptography in PKI

Enabling the transition through cross-SDO collaboration

Stiepan A. Kovac, QRC Eurosmart SA (LU)

The basics

- ITU-T SG17 Q11 jointly with ISO/IEC JTC1 SC6 standardize PKI, and refer to ISO/IEC JTC1 SC27 WG2 as the primary source for approved cryptographic mechanisms.
- ISO/IEC SC27 WG2 has traditionally had a very rigid process (understandably so) for the uptake of new algorithms in its 18033 series. However:
- Quantum is a special case as per the US and other governments' recognition of it being a topic to be dealt with without delay as its IT applications will break PKI and crypto(graphy) as it stands.

Latest news from global standardization

- As an outcome of the latest ISO/IEC JTC1 SC27 meeting, an amendment of 18033-2 to add support for quantum-resistant KEM (to replace RSA or ECC in that capacity) has been started, taking into account the urgency to have the relevant options in PKI
- Of crucial importance for that to happen was the presence of two SG17/SC6 delegates to the meeting in question, aside NIST's and other key players' such as the German BSI, now leading the amendment in collaboration with NIST and us notably.
- European standardization is taking the matter very seriously likewise as some EU directives might require specific types of cryptography to attain the level of security and particular properties required by laws; the main work occurs in CEN/CENELEC.
- Your servant in SF right after the SC27 plenary on the job to replace RSA :-)