INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2017-2020

SG17-LS68

Original: English

Question(s): 11/17 Geneva, 29 August - 6 September 2017

Ref.: SG17-TD787-R1

Source: ITU-T Study Group 17

Title: LS on ITU-T SG17 work on quantum-safe PKI

LIAISON STATEMENT

For action to: -

For comment to: -

For information to: IETF LAMPS, IETF IPSECME, ETSI TC Cyber WG QSC

Approval: ITU-T SG17 meeting (Geneva, 6 September 2017)

Deadline: N/A

Contact: Jean-Paul Lemaire
Rapporteur Q11/17
Tel: +33618473756
E-mail: jean-paul.lemaire@univ-paris-diderot.fr

ITU-T Study Group 17 is pleased to inform you that in our August/September 2017 meeting we agreed to start work on the inclusion of a proposal to include optional support for multiple public-key algorithms in Recommendation ITU-T X509 | ISO/IEC 9594-8.

The industry is preparing ICT systems to be resistant to attacks by large-scale quantum computers in addition to more sophisticated attacks by conventional computing resources. Proposed was an optional feature to the X.509 certificate that provides a seamless migration capability to existing PKI systems, and is completely backwardly compatible with existing systems.

While public-key key establishment algorithms are typically negotiated between peers and are generally fairly simple to update, the authentication systems typically rely on a single digital signature algorithm which are more difficult to update. This is because of the circular dependency between PKI-based identity systems and the dependent communication protocols. In order to update a PKI system, one would typically need to create a duplicate PKI system that utilizes a new digital signature algorithm and then migrate all the dependent systems one by one.

This proposal eliminates the need to create such duplicate PKI systems by adding optional extensions to contain alternate public key and alternate signature, and a method for the CA to sign certificates using a layered approach to ensure that every attribute is authenticated by both signatures. The resulting certificate, while containing new quantum safe public key and signature, can still be used by existing systems relying on the classic public key and signature.

_____