Event summary and outcomes

Heung Youl YOUM, PhD

ITU-T SG17 Chairman

9 May 2023

Opening remarks

- **Masters of Ceremony:** Bilel Jamoussi, Chief of Study Groups, TSB, ITU & Xiaoya Yang, ITU-T Study Group 17 Counselor
- **Doreen Bogdan-Martin,** Secretary-General, ITU
- **Jin-Bae Hong,** Deputy Minister, Ministry of Science and ICT, Korea (Rep. of)
- **Heung Youl Youm,** Chairman, ITU-T Study Group 17, Security | Professor, Department of Information Security Engineering, Soonchunhyang University, Korea (Rep. of)

Presentation summary – session 1

Latest advances in X.509 from organizations across the world

- **Moderator:** Zhiyuan HU, vivo Mobile Communication Co. Ltd. , China | WP2/17 Vice-chair
- **Presentations**
  - **Russell Housley**, Former IETF Chair (2007-2013) | Founder of Vigil Security, LLC, United States
  - **Jean-Paul Lemaire**, Question 11/17 Rapporteur | ISO/IEC JTC1/SC 6/WG 10 Convenor
  - **Erik Andersen**, Editor of ITU-T X.509 | Independent consultant, Andersen's L-Service, Denmark
  - **Hyung-Soo (Hans) Kim**, Vice-chairman, ITU-T Study Group 13 | KT Corporation, Korea (Rep. of)
  - **Carl Leitner**, Technical Officer, Public Digital Health Technology, Digital Health and Innovation Department, WHO
  - **Dimitris Zacharopoulos**, Chair, CA/Browser Forum
  - **Steffen Fries**, Principal Engineer Security, Siemens AG, Germany

Session 1: Takeaways and suggestions

Takeaways and conclusions

- IETF LAMPS Working Group published some updates to X.509 certificate documents produced by IETF PKIX WG and is working on some work items, such as support for Post-Quantum Cryptography (PQC), and mechanisms for transition from traditional cryptography to PQC.
- ITU-T SG17 has the plan for three Recommendations X.508, X.509 and X.510 with some activities on PKI establishment and maintenance, ASN.1 modules, usage of quantum safe algorithms, usage of Authority and Validation lists for IoT devices which have limited capacity, etc.
- ITU-T SG13 is working on QKD network and published several relevant Recommendations. X.509 certificate is essential for QKD network and should take quantum safe algorithms into account in the future.

Suggestions to ITU-T SG17

- Consider reorganizing ITU-T X.509 to make attribute certificates part of PKI.

Session 1: Takeaways and suggestions

Takeaways and conclusions

- IEC 62351 supporting the security in power system automation bases on the application of X.509 certificates.
- Advances in quantum computing endangers specifically asymmetric cryptographic algorithms like RSA or Elliptic Curve Cryptography (ECC). It is proposed to specify some options in X.509 to allow using alternative cryptographic algorithms.
- Through the liaison with ITU-T SG17 enhancements to allow for a better application of attribute certificates are targeted.

Suggestions to ITU-T SG17

- Attribute certificates are an important mean for access control as discussed for power system automation. ITU-T SG17 is recommended to collaborate with IEC to enhance X.509 to allow for similar application options of attribute certificates as already available for public key certificates Attribute certificates is important for access control.

Session 1: Takeaways and suggestions

Takeaways and conclusions

- It’s suggested creating a world-wide federated PKI based on blockchain, in order to have world-wide trust using current PKI trust model.
- X.509 certificate is used in global health, for example, securing health information exchange (HIE) in African Union, securing communication endpoints in Australia, and global digital health certification network (e.g., COVID Certificates).
- CA/Browser forum produces guidelines covering X.509 certificates used for SSL/TLS, code signing, and S/MIME, to facilitate collaboration of certificate issuers and certificate consumers.
- There is a need to using a short-life certificate for some application.
- How attribute certificates fit into PKI, for example:
  - Attribute certificates important for access control
  - Identity assurance using public-key certificates also important for access control

Suggestions to ITU-T SG17

- The chain of trust with traditional PKI is too long. While the longer the chain of trust is, the more diluted trust becomes. ITU-T SG17 is recommended to study a world-wide decentralized PKI based on blockchain.
- Consider reorganizing ITU-T X.509 to make attribute certificates part of PKI.

Presentation summary – session 2

Panel discussion – future directions for evolvement of ITU-T X.509 focusing on impact from quantum risks

- **Moderator:** Afnan AlRomi, Communications, Space & Technology Commission (CST), Saudi Arabia | Vice-chair, ITU-T Study Group 17
- **Presentations**
  - Daniel Apon, Lead, MITRE, United States
  - Erik Andersen, Editor of ITU-T X.509 | Independent consultant, Andersen's L-Service, Denmark
  - Hoyt L Kesterson II, Security and Risk Architect, CNC Consulting, United States
  - Russell Housley, Former IETF Chair (2007-2013) | Founder of Vigil Security, LLC, United States
  - Stiepan Kovac, QRC Eurosmart SA, Luxembourg

Session 2: Takeaways and suggestions

Takeaways and conclusions

- As an outcome of the latest ISO/IEC JTC1 SC27 meeting, an amendment of 18033-2 to add support for quantum-resistant KEM has been started, taking into account the urgency to have the relevant options in PKI.
- Because of the need to “sign” electronic documents such as contracts, laws and regulations were amended to recognize such signatures.
  - Quantum computing breaks digital signature. There are challenges: How do we protect documents already signed?, How do we protect documents signed in the future?
- Some IOT devices use ECC rather than RSA because of smaller keys but key sizes of quantum-resistant algorithms are quite large.

Suggestions to ITU-T SG17

- Quantum computers will be a threat to asymmetric public key algorithms like RSA or ECC. ITU-T SG17 is recommended to study how to specify quantum-safe certificates with using quantum-safe encryption algorithms for the post-quantum transition.
- To help be ready for cryptographically relevant large scale quantum computers, it is recommended to:
  - Consider PQC algorithms that will be standardized by ISO/IEC SC 27, NIST or IETF to be used as normative reference.
  - Consider including PQC algorithms in protocol standards.
- Support collaboration within the X.509 standards ecosystem as it expands to new cases and continues to evolve.

Session 2: Takeaways and suggestions

Takeaways and conclusions

- Extensive following discussion were made on Quantum computers:
  - It is agreed that quantum computing will break asymmetric encryption and weaken symmetric encryption.
  - There is disagreement when a quantum computer that can effectively do that will appear.
  - Even if there is a low probability that it will happen in the next five years, the effect will be disastrous.
  - The NIST effort is not premature because it will take a long time to roll out implementations of the quantum resistant algorithms, software to manage them, and protocols supporting. Information technology changes slowly; the fact that we still have to discuss DES if proof of its resistance to evolution.
- A post-quantum cryptosystem (PQC) is secure against large-scale quantum computers.
- Adapting X.509 for PQC: post-quantum techniques for both one-certificate (mix of traditional and PQC public keys) and two-certificate (one traditional and one PQC) approaches (IETF).
- It is expected to use of hybrid method, i.e. concurrent use of classical and post quantum algorithms.

Suggestions to ITU-T SG17

- Focus on “crypto-agility” for future developments in X.509.
- Maintain the flexibility of X.509, as sometimes X.509 is not appropriate due to size - saving a few bytes and simpler encoding can be vital in some use cases

SG17 observation by SG17 chairman

- The 2nd ITU-T X.509 day event agreed to hold the 3rd ITU-T X.509 day on May 9, 2024.
- As a summary, SG17 is requested to authorize SG17 chairman to hold the 3rd ITU-T X.509 day on May 9, 2024, as it is well prepared to the 3rd event.

Thank you very much