Event summary and outcomes

Heung Youl YOUM,
ITU-T SG17 Chairman

9 May 2022

Opening and welcoming addresses

Master of Ceremony: **Reinhard Scholl**, Deputy Director, TSB, ITU and **Xiaoya Yang**, ITU-T Study Group 17 Counsellor

- **Houlin Zhao**, 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

- **SESSION 1: Overview of public key cryptography and public key infrastructure**
- Moderated by Professor Lia Molinari, Study Group 17 Vice-chair.
- Session 1 was focused on the creation, edition and evolution of ITU-T X.509.
- Mr. Jean-Paul Lemaire, Rapporteur of Q11/17 (Generic technologies to support secure applications) and ISO/IEC JTC1/SC 6/WG 10 Convenor, exposes about the history of X.509, the features and innovations in each edition.

Presentation summary – session 1 (Continuation)

- Mr. Erik Andersen has been the project editor for the ITU-T X.500 series, also on the ISO/IEC side.
  - His presentation was an overview of public key infrastructure.
  - Concepts such as public key cryptography, certification authority, digital signature, public key certificate, were presented relating entities, process and operation, and demonstrate the importance and relevance of the public key infrastructure

Session 1: Takeaways and suggestions

Takeaways and conclusions

- It was a very detailed roadmap about ITU-T X.509, and we can appreciate the firm intention of ITU and ISO to be attentive to the evolution of ICT and to update the standards.
- The work and effort of both panelists in the strengthening of ITU-T X.509 was highlighted.

Suggestions to ITU-T SG17

- It’s important to accompany the identity management methods and take it in account in the next proposals.
- The interoperability of the standards was one question in the of Q&A box session. It’s an interesting topic to consider.

Presentation summary – session 2

- **Historical and current use cases of ITU-T X.509**
- **Moderator**: **Kirsty Paine**, Strategic Advisor - Technology & Innovation, Splunk
- "Use cases of X.509 in internet protocols and applications" - **Russell Housley**, Founder of Vigil Security, LLC | Former IETF Chair (2007-2013)
- "ITU-T X.509 use case for V2X security credential management system" - **William Whyte**
- "Security Controls & Services" - **François Lorek**, Founder of TRAX, Digital Compliance Agency | Associate director | ISO/IEC JTC1 SC27 WG4 Vice convenor, France
- "How X.509 is used for building confidence in the use of ICTs" - **Jos Purvis**, Security Architect, Cisco Systems
- "X.509 application in power systems through IEC 62351" - **Steffen Fries**, Principal Engineer Security, Siemens AG, Germany

Session 2: Takeaways and suggestions

Takeaways and conclusions

- X.509 is a widely used standard with many applications in several verticals – we heard from automotive, internet, communication technologies and power systems
- Looking back and around at the extensive use cases can help us look forward
- The flexibility and usability of X.509 has led to its success
- IETF, ISO, IEEE and other organizations use X.509 as a basis for collaboration and industry use cases, making great use of, the ITU-T standard and technology.

Suggestions to ITU-T SG17

- Thank you for the standard on which we built our careers!
- Maintain the agility of X.509
  - Sometimes X.509 is not appropriate due to size - saving a few bytes and simpler encoding can be vital in some use cases
  - Consider the explosion of X.509 usage with IoT and zero-trust authentication needs
  - Think of crypto agility and ability to adapt to different lifetimes, use cases and revoke
- Communicate with other stakeholders to prevent innovation being held back
- Keep standards open

Session 3: Panel discussion – future directions for evolvement of ITU-T X.509

- Moderator: Phyllis Lee, Senior Director, Center for Internet Security
- Tony Rutkowski, CEO, Netmagic Associates LLC
- Douglas Steedman, CCITT Special Rapporteur of Question 35/ VII, Directory Systems (1985-1988)
- Hoyt L Kesterson II, Senior Security and Risk Architect, Avertium
- Russell Housley, Founder of Vigil Security, LLC | Former IETF Chair (2007-2013)
- Abbie Barbir, Question 10/17 Co-rapporteur | Senior Security Advisor, CVS Health, United States
- Carl Leitner, Technical Officer, Public Digital Health Technology, Digital Health and Innovation Department, WHO`
- Erik Andersen, Editor of ITU-T X.509 | Independent consultant, Andersen's L-Service, Denmark

Session 3 summary

- The panel focused on the future of X.509 as a two-part discussion:
  - Part 1: the evolution of where we are today – the “race to the bottom” and why/how this happened
    - history of X.509’s collaborative development and SG17’s role in it
    - the “race to the bottom” i.e., misfires in early deployment
    - the X.509 ecosystem use case and its evolution
  - Part 2: The future of X.509 and the role of standards in its evolution:
    - planning for post-quantum cryptography and X.509’s evolution to a crypto-agile future
    - next steps in X.509’s development including a decentralized PKI future and role of X.509 in building trust networks for digital COVID-19 certificates

Session 3: Takeaways (1)

- Collaboration has always been a core component of X.509’s rich history and development:
  - X.500 standards family were first joint publications from CCITT (ITU-T) and ISO
  - Initial use cases included in messaging handling, as network end-point and transport trust mechanisms
  - Development spanned academia, enterprise and legal, SDOs and national security communities, further evolution requires enhanced collaboration in the current standards ecosystem
- “Race to the bottom”: challenges in early deployment brought significant constraints on X.509’s use for trust purposes
  - X.509 was developed but implementation impeded because regulation was missing
  - Crypto-agility needs to be of focus for extensibility to tackle upcoming challenges i.e. smaller and more devices (IoT) and “faster” computing capabilities (post-quantum future)
  - Over the years, use cases expanded but significant efforts are still needed to ensure effective deployment for future applications incl. in zero trust implementations and COVID certificates

Session 3: Takeaways (2)

- Insights on directions for future developments:
  - 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)
  - Implementation of X.509 as basis for global trust networks to verify and validate vaccine certificates (WHO)
- Next stage for X.509:
  - Expansion of authorization and validation lists concepts to support IoT; refinement of certificate attributes and clear definition of the PKI-PMI relationship
  - Moving to “trust by consensus” with decentralized PKI
  - Development of complementary specifications:
    - X.510: protocol specifications with migration capabilities
    - X.507: PKI implementation and best practices with future extension into post-quantum

Session 3: Suggestions to ITU-T SG17

- Bolster collaboration within the X.509 standards ecosystem as it expands to new cases and continues to evolve
- Encourage the standards community to move towards an “open standard” policy (no paywalls)
- Focus on “crypto-agility” for future developments in X.509