Event summary and outcomes

Heung Youl YOUM, PhD

ITU-T SG17 Chairman

20 February 2023

Opening remarks

- **Master of Ceremony:** Xiaoya Yang, ITU-T Study Group 17 Counsellor
- **Opening remark,** Seizo Onoe**,** Director, Telecommunication Standardization Bureau, ITU
- **Welcome remark(I),** Heung Youl Youm, Chairman, ITU-T Study Group 17, Security | Professor, Department of Information Security Engineering, Soonchunhyang University, Korea (Rep. of)
- **Welcome Remark(II),** Julien Bringer, ISO TC 307/JWG 4 Co-Convenor

Session 1: Generic introduction to scope, work methodology and overall work items

- **Moderator:** Kwadwo Osafo-Maafo, WP5/17 Vice-Chairman | NCA, Ghana
- **Presentations**
  - Youki Kadobayashi, Question 14/17 Co-Rapporteur | NICT, Japan: "Overview of ITU-T SG17"
  - Julien Bringer, ISO TC 307/JWG 4 Co-Convenor: "Overview of ISO TC 307/JWG 4"
  - Olivier Dubuisson, ITU-T TSAG Rapporteur I Orange, France: "Collaboration mechanisms between an ITU-T Study Group and ISO TC"

Presentation Summary – Session 1

- ISO/TC 307 works on international standards, technical specifications, and technical reports (ISO/TR 23244:2022 on privacy and PII protection, ISO/TR 23249 on overview of existing DLT systems for identify management, etc.)
- Both SG 17 and ISO/TC 307 have processes to collaborate and work on DLT. Procedures in place include
  - WTSA Resolution 7 “Collaboration with ISO and IEC”
  - ITU-T A.23 and ISO/IEC JTC 1 standing document 3
  - Category A liaison maintained by JTC 1 with ITU-T
  - Supplement 5 of ITU-T Series A Recommendations
  - Common Patent Policy for ITU-T/ITU-R/ISO/IEC)

Session 1: Takeaways and suggestions

Takeaways and conclusions

- Both organizations have similar approaches and find relevant the contributions made to BC & DLT
- More work can be done to bring ISO and ITU work in DLT to countries and organizations

Suggestions to ITU-T SG17

- Countries have different levels of participation and engagement in ISO/TC 307/JWG 4 and ITU-T SG 17, and it is important to have regular programs or sessions for countries to access, use and contribute to both.
- Experts and users inside and outside ITU and ISO may need further guidance on the procedures for collaboration.
- Some work items may be added to questions such as Q7 on topics related to globally significant foundational activities in Financial Services.

Session 1: Takeaways and suggestions

Suggestions to ITU-T SG17

- Between ITU-T SG17 and ISO/TC 307, specify the terms of reference of the cooperation according to clause 8.2 of Supplement 5 to the A-series of ITU-T Recommendations for approval by both plenaries.
- Cooperation to be in the form of a common team (of experts from both ITU-T SG17 and ISO/TC 307) working on a common text (i.e. same standard published by ITU-T and ISO).
- ITU-T SG17 should ramp up its "marketing" by being more creative -- for instance by creating infographic or one-page brochure of the key Recommendations (some technology such as AI may be used, and translations for different languages as well).

Presentation summary – session 2

- **Moderator:** Sungchae Park, Soonchunhyang University, Korea (Republic of)
- **Presentations:**
  - Julien Bringer, ISO TC 307/JWG 4 Co-Convenor: "Completed projects in ISO TC 307/JWG 4"
  - Ke Wang, Question 14/17 Associate-Rapporteur | China Mobile Communications Corporation: "Deep dive on the current and completed work items in Study Group 17, focusing on Q14/17"
  - Jörn Erbguth, University of Geneva: "European Data Protection Regulation"
  - Kepeng Li, Senior Standard Expert, TenCent: "Smart contract security"
  - Rapolas Lakavičius, Policy Officer, Directorate-General for Communications Networks, Content and Technology, European Commission

Session 2: Takeaways and suggestions

Takeaways and conclusions

- Completed projects on security, privacy and identity for blockchain and DLT in ISO TC 307/JWG 4 were presented, such as ISO/TR 23244:2020, ISO/TR 23576:2020
- The work items on DLT security have been developed under Q14/17, and they are classified as follows:
  - Security protection of DLT: X.1401, X.1402, TR.qs-dlt, etc.
  - Security protection of DLT based on applications: X.1405, X.1408, etc.
  - Using DLT for security: X.1403. X.1409
- Two main issues between GDPR & DLT were addressed such as,
  - Right to be forgotten & immutability of DLT
  - Accountability & decentralization;

  In addition, solutions are provided: explaining the European blockchain regulatory sandbox initiative.

Suggestions to ITU-T SG17

- In the spirit of harmonization and to enrich the content of Recommendations developed by SG17, SG17 is recommended to consider, as much as possible, relevant ISO TRs during development of its work items (e.g., some considerations on digital asset custodians from ISO/TR 23576 may be relevant to Rec. X.1405)
- Consider whether security and privacy issues are unique to DLTs and require their own set of security requirements or, if already published work addressing security and privacy aspects can be adapted for the context of DLTs.

Session 2: Takeaways and suggestions

Takeaways and conclusions

- Six challenges for smart contract security and security considerations according to the lifecycle management were presented: smart contract design and development, compilation and deployment, invocation and execution, and maintenance and management. Related standards work items were also shared.
- EU regulation activities and proposals were presented such as, Data Act Regulation - incl. Smart Contracts, EUDI/eIDAS2 Regulation - incl. E-Ledgers, Markets In Crypto Asset Regulation (MiCA), Crypto Resilience Act; including Smart contracts for data sharing.

Suggestions to ITU-T SG17

- Consider meeting requirements such as Right to be forgotten vs. Immutability of DLT & Accountability vs. Decentralization from the roles and regulation, and develop recommendations for DLT security, privacy and management taking these requirements into account.
- Consider establishing liaison with ISO TC 68 to address security, privacy and identity management for financial sector.
- Consider using a hybrid model to meet the requirements from GDPR.

Session 3: DLT identity management

- **Moderator:** Heung Ryong Oh, ITU-T Study Group 17 Q2 Co-rapporteur | Chief Researcher, Standardization Division, TTA , Korea (Republic of)
- **Presentations**
  - Paolo Campegiani, Head of Innovation, Bit4id, Italy: “JWG4 Activities on Identity Management”
  - Abbie Barbir, Question 10/17 Co-Rapporteur | Senior Security Advisor, CVS Health, United States: “Decentralized Identity Management”
  - Kanghyo Lee, Senior Researcher, Korea Internet & Security Agency (KISA): "NFT Usage and Future Direction”
  - Radhilufti Madehi, FNSValue, Korea (Rep. of): “Next-Generation Passwordless Blockchain Secure authentication”
  - Paolo Campegiani, Bit4id, Italy: “Electronic Ledgers in the eIDAS Regulation Revision”

Session 3: Takeaways and suggestions

Takeaways and conclusions

- ISO/TC307 JWG4 addressed ISO/TR 23249(existing DLT systems), ISO/TR 23644(trust anchors) and ISO/AWI 7603(decentralized identity) for DLT identity management.
- ITU-T SG17 Q10 addressed several identity managements such as Federated Identity, Decentralized Identity, Bootstrapping Identity and Verifiable Credentials.
- NFT(Non-Fungible Token) using DLT technologies was presented concept, use cases, security issues and future directions in Korea.
- Passwordless technology using blockchain was presented several advantages for secure authentication.
- The eIDAS regulation covers two relevant areas of intervention in The European Union; Cross-border recognition of nationally issued electronic identities and Cross-border validity of trust services provided by private parties.

Suggestions to ITU-T SG17

- Continue collaboration and cooperation for DLT-based identity management between ITU-T SG17 and ISO/TC307.
- Study to mitigate security issues such as the link between NFT and digital content, copyright infringement and NFT fake image.
- Consider establishing a new work item for emerging technology such as passwordless blockchain secure authentication, based on Contribution from membership.
- Consider to establish new work item for gaps identified and interoperation such as heterogeneous DLT-based identity systems.
- Consider to promote a global interconnection for the qualified trust service providers using DLT systems.

Session 4: Panel discussion – sharing future work items from Study Group 17's point of view

- **Moderator:** Zhiyuan Hu, WP2/17 Vice-chair | vivo Mobile Communication Co., Ltd., China
- **Panelists:**
  - Julien Bringer, ISO TC 307/JWG 4 Co-Convenor
  - Kyeong Hee Oh, Question 14/17 Co-Rapporteur | TCA Services, Korea (Rep. of)
  - Abbie Barbir, Question 10/17 Co-Rapporteur | Senior Security Advisor, CVS Health, United States
- **Questions to panelists:**
  - *Security and privacy of DLT:* Some studies on security and privacy of DLT have been done in ISO TC 307/JWG 4 and ITU-T SG17. Are there any other security and privacy issues not covered by these studies but very important? For example, is it necessary to consider quantum resistant signature schemes for long-term ledgers, or security issues of DLT interoperability?
  - *To improve security and privacy for identity management based on DLT:* What issues/aspects are essential to build DLT-based identity management system? | What kind of issues/aspects should be standardized in SG17 for identity management based on DLT?

Two aspects of DLT security and privacy

A. Security and privacy of DLT
   - Threats and risks
   - Vulnerabilities and mitigation methods
   - ……

B. To improve security and privacy by DLT
   - Identity management
   - Smart contracts
   - Cross-border payments
   - Original content creation
   - Supply chain management
   - ……

Work items in ITU-T SG17

A) Security of DLT:

1. X.1400: Terms and definitions for distributed ledger technology
2. X.1401: Security threats of distributed ledger technology
3. X.1402: Security framework for distributed ledger technology
4. X.1404: Security assurance for distributed ledger technology
5. TR.qs-dlt: Technical Report: Guidelines for quantum-safe DLT system
6. X.sc-dlt: Security controls for distributed ledger technology

B) To improve security by DLT:

1. X.1403: Security guidelines for using DLT for decentralized identity management
2. X.1405: Security threats and requirements for digital payment services based on distributed ledger technology
3. X.1406: Security threats to online voting system using distributed ledger technology
4. X.1407: Security requirements for digital integrity proofing service based on distributed ledger technology
5. X.1408: Security threats and requirements for data access and sharing based on the distributed ledger technology
6. X.1409: Security services based on distributed ledger technology
7. X.1410: Security architecture of data sharing management based on the distributed ledger technology
8. X.srscm-dlt: Security Requirements for Smart Contract Management based on the distributed ledger technology

Work items in ISO TC 307/JWG 4

Published:

1. ISO/TR 23244:2020 Privacy and personally identifiable information protection considerations
2. ISO/TR 23249:2022 Overview of existing DLT systems for identity management
3. ISO/TR 23576:2020 Security management of digital asset custodians [from WG2]

On-going:

1. ISO/WD TR 23642 Overview of smart contract security good practice and issues
2. ISO/DTR 23644 Overview of trust anchors for DLT-based identity management
3. ISO/WD 7603 Decentralized Identity standard for the identification of subjects and objects
4. PWI 12833 - Re-identification and privacy vulnerabilities and mitigation methods in blockchain and distributed ledger technologies

Session 4: Takeaways and suggestions

Takeaways and conclusions

- There are too many use cases with different platform, different architecture and different implementation. Interoperability of DLT is very important, especially for identity management across the ecosystem.
- It is necessary to study DLT security, especially security assessment, security assurance, interoperability security, quantum safe evaluation, etc.
- It is necessary to study DLT privacy, especially personal business information protection, open access personal information, personal information traceability, etc.
- Although unified DID data format has already been specified in W3C, it is very difficult to be adopted by the applications. How to find a way to monetize is also a big challenge.

Suggestions to ITU-T SG17

- Security assessment of DLT is a potential topic to be studied in SG17. SG17 should inform SG16 to look for cooperation and coordination once any work item on this topic is established in SG17.
- Interoperability security of DLT should be studied in SG17.
- SG17 should study the whole picture or new concept for DLT-based Identity management system.
- PII protection of DLT-based identity management is also a potential topic to be studied in SG17.

Thank you very much