2nd joint ITU/WHO Workshop on Digital COVID-19 Certificates: Workshop Summary and Results

26 November 2021

Noah LUO, ITU-T SG16 chairman
Heung Youl YOUM, ITU-T SG17 chairman
Nasser Al MARZOUQI, ITU-T SG20 Chairman

Presentation summary – session 1 (1/2)

Session 1: Experience, best practices and solutions of digital COVID-19 certificates and certificate-based services

- WHO Technical Specifications, Implementation Guidance, Reference Implementations & Tooling for Digital Documentation of COVID-19 Certificates (DDCC)
  - Overview of WHO specifications for digital certificates: recommendations for minimum dataset, mapped to standards, ethics, national PKI infrastructure, options for ID binding, options about which trust network to map to, intended to ensure use across all countries for vaccines and test results without exacerbating health inequities
- EU Digital COVID Certificates: How it works – An explainer
  - EU overview of experiences of developing and deploying DCC gateway and guidance for EU member states, which respects the privacy policies of EU, signature validation done from EU gateway, uses PKI infrastructure, benefited from legal framework already in place, success due to flexibility of approach for operationalization by EU member states implementation, and minimum standards defined, with flexibility for interpretation by member states, and equivalency protocols for non-member states for adequacy

Presentation summary – session 1 (2/2)

Session 1 (continued):

- DID: A blockchain based solution to enable controllable and trustable data management
  - provided overview and foundational principles around digital identify, including an architectural approach for decentralized ID and verifiable credentials, within a blockchain; detailing the capabilities and use cases for such a service
- Trust network use case for Blockchain/DID based services; South Korea's Mobile Driver License
  - provided overview of Republic of Korea's experience with establishing trust network for identify for different use cases using decentralized ID, verifiable credentials, and blockchain

Session 1: Takeaways and Suggestions

Takeaways and Conclusions

1. Specifications and standards for digital certificates (with or without ID binding) need to accommodate all countries' constraints and maturity of digital adoption to ensure no one is left behind
2. There are a variety of countries and regions who have experience with implementing PKI based digital certificates in a way that are scalable, maintains privacy and security, are interoperable, and follows from established legal and MOUs to establish trust, and which function in a centralized or decentralized manner
3. Paper-based and QR code-based certificate should be considered for inclusiveness
4. Minimum standards are critical for common agreement between countries; flexibility in operationalizing them is important for countries
5. Centralized vs decentralized trust model
6. Single versus multi-credential verification
7. Common credential specifications, Interoperability
8. Trust about issuer and consumer of certificates
9. Countries have considerable experience with verifiable credentials and digital identity

Suggestions to ITU-T SGs

- ❑ Form Common processes, agreements and policies as basis of governance for trust architecture
- ❑ For those countries that want to bind identify to certificates, decentralized identity approaches can provide trust
- ❑ For adoption and interoperability within health, interoperability standards ICD and HL7 FHIR IPS are important
- ❑ Guidance on governance and standards related to linking certificates to identity should be considered by ITU
- ❑ Consider privacy respecting technologies when designing a digital vaccination certificate

Presentation summary – session 2 (1/2)

Session 2: Identity binding and trust networks for digital COVID-19 certificates and certificate-based services

- Three existing vaccination certificate systems
  - COOV, a blockchain-based COVID-19 vaccination certificate system
  - EU Digital COVID Certificate : Implementation and practice – experience after five months' experience
  - Experiences in the implementation of Digital COVID-19 certificates in Latin American
- COOV, a blockchain-based COVID-19 vaccination certificate system
  - Blockchain based
  - A fast and efficient way to certificate the vaccination
  - Prevent forgery, ensure privacy and enhance efficiency
  - Selectively disclose information
  - International compatibility
  - Decentralized identity
  - Static QR for Interoperability
  - Follows EU DCC data set version 1.3.0

Presentation summary – session 2 (2/2)

Session 2 (continued):

- EU Digital COVID Certificate: Implementation and practice – experience after five months' experience
  - PKI based DCC requiring PKI gateway to extend trust
  - Selectively disclose information
  - Component's interoperability
  - Decentralized identity
  - Documents available at https://ec.europa.eu/health/ehealth/covid-19_en
- Experiences in the implementation of Digital COVID-19 certificates in Latin America
  - Accredits vaccination against COVID -19 for people who need to travel between countries
  - Seeking fast and efficient transnational responses
  - QR authentication
  - Agreement with the European Union (EU's COVID digital certificate system)

Session 2: Takeaways and suggestions

Takeaways and Conclusions

1. Zone based three different systems for vaccination certificates (COOV, ED DCC, Mi Argentina)
2. EU DCC documents: requirements
3. Consider a fast and efficient way to certificate the vaccination
4. Consider to prevent forgery, ensure privacy and enhance efficiency
5. Selectively disclose information
6. Decentralized identity

Suggestions to ITU-T SGs

- ❑ Invite stakeholders to develop the requirements for interoperability of Vaccination certificate and submit their specifications to ITU-T.
- ❑ Work on decentralized identity at ITU.
- ❑ Work on common and expandable credential for selectively disclosing information.

Presentation summary – session 3 (1/2)

Session 3: Key standards to support implementation of COVID-19 certificates and services

- Standards from 3 SDOs, ITU-T SG17, ISO/IEC JTC 1, SC17 and SC31 were presented:
  - QR Code standards overview
    - Advantages and Disadvantages of QR code
      - QR Code has become ubiquitous, recognized by people
      - Decoding software is available by default on numerous devices
      - Requires a phone with a camera
      - Malicious QR codes combined with a permissive reader can put a computer's contents and user's privacy at risk
  - Trust and identity by decentralized PKI and by data protection
    - ITU-T SG17 is working on decentralized PKI
    - It has the following:
      - Access control – Rec. ITU-T X.1080.0
      - Cybersecurity – Rec. ITU-T X.510 | ISO/IEC 9594-11

Presentation summary – session 3 (2/2)

Session 3 (continued):

- Introduction to ISO/IEC 18013-5
  - ISO Mobile driving license (mDL) (ISO/IEC 18013-5) is expected to support
  - a protocol for two devices to establish a secure wireless communication
  - channel and exchange structured request and response messages
  - identification of the mDL holder (user binding)
  - selective release of data elements by the mDL holder (data minimization)
  - a protocol to retrieve mDL data directly from the mobile device of the mDL
  - holder, purely offline, facilitating availability and non-traceability
  - an optional protocol to retrieve mDL data from the issuing authority
  - a mechanism to establish integrity and authenticity of the mDL data
  - a mechanism to confirm device binding (signing at transaction time)
  - global level challenges

Session 3: Suggestions

Suggestions to ITU-T SGs

- Invite ISO/IEC and others to work with ITU-T SGs 16, 17, and 20
- Clear demands from member states are essential
- Work jointly to identify ways to harmonize standards that can provide trust and interoperability, e.g., ITU-T X.1080.0 and ITU-T X.510 and Distributed PKI
- Develop ways to extend existing established standards, e.g., QR Code, to be more robust and secure
- ITU-T JCA-DCC under TSAG will be a good platform for assessing needs and demands, etc.

Session summary – session 4 (1/2)

Session 4: Round table – Gaps and directions for future standardization

- WHO representative's discussion points
  - Digital Documentation of Covid Certificates, or DDCC, for Vaccination Status, a companion DDCC document for Test Results Challenges faced by governments
  - Successful implementation of interoperable covid certificates
  - JCA's role
- SC27 representative's discussion points
  - Work items for DCC or supporting implementation of DCC
  - Difference between identity and identification
  - The most important next step in the area of identity management

Session summary – session 4 (2/2)

Session 4 (continued):

- SG17 representative's discussion points
  - Potential new work items for SG17, Support JCA-DCC, Collaboration platform
  - Equal representatives between regions, countries such as Latin-American, or African countries
- SC16 representative's discussion points
  - SG16 work items identified to support WHO's DCC in terms of two aspects (continuity of care scenario, proof of vaccination scenario)
- SC20 representative's discussion points
  - Work items for DCC or supporting implementation of DCC
  - Standardization tasks with relevance for SG20

Session 4: Takeaways and suggestions (1/3)

Takeaways and Conclusions

1. No work items under way for DCC by SG16, SG17, SG20 and SC27 were identified, however, some documents were identified to support implementation of WHO's DCC
2. WHO's two specifications could be submitted for adoption of ITU-T standards
3. X.509, X.1403, X.672, X.srdidm, etc. in SG17, H.810-819, F751.0, - F751.2, etc. in SG16, Y.4811, Y.4464, Y.445, etc. in SG20, ISO 29100, ISO 24760, ISO 29134, ISO27551, ISO 20889, ISO 27559, ISO 29115, ISO 29003, etc. in SC27 and other existing Recommendations could be used to supplement DCC
4. Privacy principles in ISO/IEC 29100 should be applied to DCC from the initial point DCC. New work items should be analyzed from a privacy perspective to check which data and which data flows are really needed

Suggestions to ITU-T SGs & TSAG

- ❑ Reconfirm invitation to WHO to submit their current and future specifications to ITU-T
- ❑ Invite SGs especially for SG17 to conduct gap analysis and consider study on new topics, such as (1) normative health content, (2) establishment of trust network for interoperability among existing certificates, (3) DCC based Decentralized identity, (4) PII protection guideline for DCC, (5) Identity binding issues including late and early binding, (6) using zero knowledge technology to provide anonymous certificate if there is a gap
- ❑ Invite three SGs (SG16, SG17, SG20) to join JCA-DCC to conduct future coordination activities especially with other organizations and groups
- ❑ Invite SG16, SG17 and SG20 to consider starting work in this area within the remit of each SGs, if necessary, in a harmonized way and to minimize overlaps, maximize interoperability, and focus on missing parts

Session 4: Takeaways and suggestions (2/3)

Takeaways and Conclusions

5. Decentralized PKI based DCC could be used as an interim solution toward Decentralized identity-based DCC
6. Gaps such as establishing efficient trust network for providing interoperability among existing and future DCCs, identity binding issues to provide anonymous DCC
7. Gap analysis is pre-requisite for each SGs to identify new work topics within their remits
8. Trust network for interoperability and identity binding issues and DCC using PET technology could be a gap for future standardization work

Suggestions to ITU-T SGs & TSAG

- ❑ Invite JCA-DCC to form JCA-DCC members by inviting all SGs to nominate representative to JCA-DCC and start coordination work within ITU-T SGs, including coordination work with other relevant groups (WHO, EU) and focus on developing standardization roadmap that will help TSAG and ITU-T SGs understand the landscape
- ❑ Invite JCA to consolidate the number of approaches in the market for trust networks and identity binding
- ❑ Invite TSAG to approve ToR of JCA-DCC reflecting input from members at January 2022 TSAG meeting
- ❑ Invite TSB to support this JCA-DCC focusing on standardization coordination activities and to consider supporting establishment of Collaboration platform on DCC like CITS, to conduct coordination activities for the DCC promotion activities except standardization activities

Session 4: Takeaways and suggestions (3/3)

Takeaways and Conclusions

9. Three pillars for successful implementation of DCC identified: normative health content, the establishment of trust networks, and the binding of identity to digital covid certificates
10. SG16 work items such as H.812.5 should be considered for supporting WHO's DCC in terms of two aspects (continuity of care scenario, proof of vaccination scenario)

Suggestions to ITU-T SGs & TSAG

- Invite SG20 to start work with relevance for SG20 to support DCC based services, if necessary

Thank you!