Report on ITU Workshop on "Future of Verifiable Health Credentials Beyond COVID-19"

11 September 2023

Carl Leitner, Heung Youl Youm
Co-Chairman, JCA-DCC

Presentation summary – session 1 (1/2)

- **Topic:** Various implementation use cases for verifiable health credentials including digital COVID-19 certificates from different countries/regions/organizations across the world
- **Moderator:** Sungchae Park, Soonchunhyang University, Korea (Republic of)
- **Presentations (7):**

(1) Edem Adzogenu, Senior Advisor, Innovation & Digitalization, Africa CDC & African Union: The journey so far and the road ahead

(2) Ciaran Carolan, Program Manager (PKD), ICAO: Verifiable Health Credentials for International Travel - A use case with unique considerations

(3) Hyunjoon Kim, Senior Researcher, KISA: Korea DID use cases and Blockchain promotion policy

(4) Kazue Sako, Editor, ISO 29191 | Professor, Department of Computer Science and Engineering, Waseda University, Japan: Selective disclosure for privacy

Presentation summary – session 1 (2/2)

- **Topic:** Various implementation use cases for verifiable health credentials including digital COVID-19 certificates from different countries/regions/organizations across the world
- **Moderator:** Sungchae Park, Soonchunhyang University, Korea (Republic of)
- **Presentations (7):**

(5) Woojin Jung, Director for Information and Statistics, Korea Disease Control and Prevention Agency: Experiment about COVID-19 Verifiable Credential for Vaccination in ROK

(6) Young-jin Kim, Interoperability of DLT Systems, Managing Director, Dreamsecurity Co. Ltd.: Introduction on Interoperability of DLT systems - Focus on Technological Developments and Standardization Trends

(7) Pradipta Kundu, Director, Health Mission, eGov Foundation: Power of Digital Public Infrastructure (DIVOC) to deliver national scale health programs

Session 1: Takeaways and suggestions

Takeaways and conclusions

- Looked into various COVID-19 certificate use cases implemented by some countries and related organizations.
- New technology using new digital signatures allows us selective disclosure and predicate proofs to achieve minimum disclosure for privacy.
- Consideration of interoperability for building trust-cross global collaboration in response to COVID-19 and beyond and Blockchain-based technological implementations with interoperability in mind.
- The adoption of the hybrid approach is expected to lead to a of use cases for COVID-19 and beyond.

Suggestions to ITU-T TSAG and JCA-DCC

- Collaborate with ICAO, other SDOs in the development of a common standard to standardize the format and enhance security features/functions of COVID-19 and beyond certificates.
- Consider incorporate into verifiable health credential the concept of Selective disclosure for privacy presented in ISO/IEC 29191, Requirements for partially anonymous, partially unlinkable authentication.
- Consider block chain technologies to build trust framework in addition to PKI trust framework.
- Consider developing standards for ensuring interoperability between various types of verifiable health credentials.

Presentation Summary – Session 2: Underlying technologies and security and privacy interests of certificate holders for supporting implementation of Verifiable Health Credentials including Digital COVID-19 certificates

- **Topic:** Underlying technologies and security and privacy interests of certificate holders for supporting implementation of Verifiable Health Credentials including Digital COVID-19 certificates
- **Moderator:** Changoh Kim, Q4/17 Associate Rapporteur, Q3/Q4/Q7/Q13/Q14 Editor in ITU-T SG 17 | CISO, Yanolja, Korea (Rep. of) .
- **Presenters**
  - **Konstantin Hyppönen**, Policy Officer (SNE) DG Health and Food Safety (SANTE), European Commission and **Michiel Sweerts**, Head of Sector, eHealth, Well-being and Ageing, DG CNECT, European Commission: Future of Verifiable Health Credentials Beyond COVID-19 - EU Digital COVID Certificate (EU DCC)
  - **Josh Mandel**, Chief Architect, Microsoft Healthcare | Chief Architect, SMART Health IT | Lecturer, Department of Biomedical Informatics, Harvard Medical School: SMART health cards framework
  - **Eugene Lee**, Global President, RaonSecure Co. Ltd, Korea (Rep. of): Ways to secure & manage verifiable heath credentials
  - **Bingsheng Zhang**, Editor of ISO/IEC 27565 I Professor, College of Computer Science and Technology, Zhejiang University, China: Introduction to ISO 27565, Information security, cybersecurity and privacy protection — Guidelines on Privacy Preservation based on Zero Knowledge Proofs

Session 2: Takeaways and suggestions (1/2)

Takeaways and conclusions

- Analyzing the EU-DCC trust framework and equivalence decision process designed with GDPR in mind and considering the Future of Verifiable Health Credentials beyond COVID-19.
- Overview of a smart health card with verifiable credentials for sharing, privacy, and transparency, and technical design for connectivity with emerging technologies.
- Introducing the Guidelines on Privacy Preservation based on Zero-Knowledge Proofs (ISO/IEC 27565), which includes privacy and security considerations.
- Analyzing use cases of identity verification technology with Trusted Framework and considering the direction of continuous development of identity verification technology using blockchain such as DID

Suggestions to ITU-T TSAG and JCA-DCC

- Consider ongoing work items in Q10/17 or Q14/17 to implement verifiable health credential
- Consider trust framework based on Blockchain technologies.
- Consider the guidelines for implementing zero-knowledge proof-based personal information protection technology. (relate to ISO/IEC 27565)
- Consider X.sup.uc-dcc document through analysis of EU trust framework

Session 2: Takeaways and suggestions (2/2)

Takeaways and conclusions

- **Identify fundamental underlying technologies for the implementation of verifiable health credentials**
  - Framework for building trust networks
  - Verifiable health credentials from security and privacy issues
  - Identify potential controls to address security and privacy issues
- **EU Digital COVID Certificate**
  - A framework for the common issuance, verification and acceptance of interoperable vaccination, test and recovery certificates
  - **Verifiability**: ensure authenticity, integrity and validity
- **SMART Health Cards Framework**
  - Trust and privacy to keep a copy of your important health records on hand and share
  - Verifiable Clinic Information in FHIR and Model used by Issuer, Holder and Verifier
- **Ways to Secure & Manage Verifiable Health Credentials**
  - Expanding verifiable Credential Use Cases of Korea COOV Mobile App and Korea Mobile Driver's License system on Decentralized Identity based on Blockchain
- **Introduction to ISO 27565**
  - Information security, cybersecurity and privacy protection — Guidelines on Privacy Preservation based on Zero Knowledge Proofs

Suggestions to ITU-T TSAG and JCA-DCC

- **Consider establishing trusted Framework**

  - A global trust framework for future verifiable health credentials that enhances healthcare efficiency and enables secure sharing of health information while respecting privacy could be envisioned.

- **Consider obtaining user Consent for Security and Privacy**

  - User is in control of their information and can decide what to share and with whom without fear that their interactions will be monitored.

- **Continue Global Standardization on**

  - multiple verification capabilities, need rule engine with different requirements by countries, and seamless international verification capability.

Presentation Summary – Session 3

- **Topic:** Building trust frameworks for Verifiable Health Credentials including digital COVID-19 certificates
- **Moderator: Kyeong Hee Oh**, Q14/17 Co-rapporteur | TCA services, Korea (Rep. of)
- **Presenters**
  - **Erik Andersen, Editor of ITU-T X.509 | Independent consultant, Andersen's L-Service, Denmark**
  - **Carl Leitner, Technical Officer, World Health Organization I Co-chairman of JCA-DCC**
  - **Marcos Allende López, Technical Leader I Coordinator, LACChain Global Alliance (please confirm your presence – remote or onsite)**
  - **Hwa-Jeong Hwang, Consultant & Blockchain Business Development, LG CNS, Blockchain Business Enhancement Group, Korea (Rep. of)**
  - **Christophe Stenuit, Founder, ViewConcept, Belgium (remote)**

Session 3: Takeaways and suggestions

Takeaways and conclusions

– **Decentralized Public-Key Infrastructure (DPKI) as it relates to Verifiable Health Credentials**
  - Trust by consensus - PKI domains federated using blockchain technology
  - Standards support - Rec. ITU-T X.50x| ISO/IEC 9594-13 etc.,

– **Global Digital Health Strategy: Actions for the WHO secretariat – Mandate for Trust Architecture**
  - Digital personal health record: Leveraging the SMART Guidelines methodology to digitize and scale provider-side and client-side solutions
  - **WHO as a trust anchor - Global Digital Health Certification Network (GDHCN)**

– **Pioneer work of LACChain and LACPass in LATAM**
  - What failed with COVID19 certificates
  - Alternatives to address current interoperability issues

– **DID SaaS for enterprises**
  - Forming a DID-based ecosystem
  - Onboarding onto the DID SaaS

– **Standardization viewpoint on Identity & Access Management**
  - ISO/IEC 24760, A framework for identity management
  - ISO/IEC 29146, A framework for access management

Suggestions to ITU-T TSAG and JCA-DCC

- **Consider using decentralized PKI Framework**

  - Need of federated PKI domains using blockchain technology

  - It seems problematic to create a world-wide federated PKI having world-wide trust using current PKI trust model

- **Develop technical framework and standardization to support global digital health strategy**

  - WHO and EU worked closely on technical guidance on COVID-19 Certificates.

  - There are different approaches to implement the trust

- **Address issue for providing interoperability**

  - A national interoperable digital health ecosystem should be set up in such a way that the information technology health infrastructures are both interoperable among each other and, allowing for differences in national legislation and policies, capable of sharing health data with infrastructures of other countries.

Presentation Summary – Session 4: Panel discussion – Directions for future Verifiable Health Credentials and the future of JCA-DCC

- **Moderator:** Heung Youl Youm, Co-chairman of JCA-DCC | Professor, Department of Information Security Engineering, Soonchunhyang University, Korea (Rep. of) .
- **Panelists**
  - Erik Andersen, Editor of ITU-T X.509 | Independent consultant, Andersen's L-Service, Denmark
  - Carl Leitner, Technical Officer, World Health Organization I Co-chairman of JCA-DCC
  - Kai Rannenberg, Convenor, ISO/IEC JTC 1/SC 27/WG 5 "Identity management and privacy technologies" | Chair of Mobile Business & Multilateral Security, Goethe University Frankfurt, Germany
  - Wojciech Wiewiorowski, European Data Protection Supervisor
  - Keundug Park, Q10/17 Associate Rapporteur | Professor, Seoul University of Foreign Studies (SUFS), Korea (Rep. of)

Session 4: Takeaways and suggestions(1/4)

Takeaways and conclusions

– Verifiable Health Credentials carry important and sensitive personal information.

– Therefore, essential elements for the development of the credentials and the related protocols are:

  - Careful handling of personal data
  - Careful analysis of the related data flows with regard to the principle of need-to-know
  - A privacy and data protection impact analysis following e.g. ISO/IEC 29134
  - Check of the processes against e.g. ISO/IEC 29151, 27701, 29184, 27560
  - Avoiding over-identfication when health credentials are checked.
  - Use of partial identities as a concept to enable credential holders to only show the attributes necessary for the respective application
  - Design of credentials and protocols considering e.g. ISO/IEC 24760, 29146, 27551, 27556 and 27565

Suggestions to ITU-T TSAG and JCA-DCC

- Check the processes for issuance and verification of Verifiable Health Credentials and the formats of the related certificates using standards and projects such as
  - ISO/IEC 24760, ISO/IEC 27551, ISO/IEC 27560, ISO/IEC 27565
  - ISO/IEC 27701, ISO/IEC 29134, ISO/IEC 29146, ISO/IEC 29151
  - ISO/IEC 29184
- Check whether health-specific interpretation are needed and if needed develop them.

Session 4: Takeaways and suggestions(2/4)

Takeaways and conclusions

- It is expected that future verifiable digital health credentials will take up new use cases such as those in the International Patient Summary as health worker credentials.
- There is also a need to ensure that utilization of credentials are not able to be monitored by the issuers.
- WHO launched the Global Digital Health Certification Network (GDHCN) in June 2023 which provides a Public Key Infrastructure that can be used for verification of the digital signatures of health credentials.
- The GDHCN is utilizing a transitive trust relationship with the European Union's Digital COVID Certificate (EU DCC) network to enable the existing EU DCC participants to rapidly join.

Suggestions to ITU-T TSAG and JCA-DCC

- Define verifiable health credential and identify associated underlying technologies.
- Develop standards around privacy preserving authorization.
- Consider current case, Global Digital Health Certification Network (GDHCN) in WHO, for building trust framework.

Session 4: Takeaways and suggestions(3/4)

Takeaways and conclusions

- It is necessary to migrate from DCC systems to VHC systems, a kind of expansion of the DCC systems, as the future of verifiable health credentials (VHCs).
- SDOs would continue to standardize work for VHC beyond DCC, in terms of security, privacy, interoperability, etc.
- Access control using attribute certificate is necessary for the VHC.
- The use of the distributed PKI scheme has some advantage for establishing trust network for verifiable health credential.
- Defining a data format for verifiable health credential is essential for its interoperability.

Suggestions to ITU-T TSAG and JCA-DCC

- Consider further working for access control using attribute certificates, based on privacy protection domain model and cross domain privileges.
- Consider migration strategies to post-quantum cryptographies for verifiable health credential.
- Consider use of DPKI for establishing the trust network for verifiable health credential.
- Consider the legal/regulatory requirements to ensure a minimum data collection for the verifiable health credential.
- **Consider use of open-source software and develop open standards.**
- **Develop specification for DPKI.**
- Consider privacy policy limitation, such as privacy issue, to use DPKI.
- **Consider developing privacy friendly verifiable health credential, based on privacy by design.**

Session 4: Takeaways and suggestions(4/4)

Takeaways and conclusions

– It is needed to consider several legal/regulatory requirements from laws/regulation, e.g., EU GDPR and other local data protection laws.

– The main role of EU GDPR is to regulate across EU.

– Standardization is critical for balancing identification and privacy requirement for implementing VHC.

Suggestions to ITU-T TSAG and JCA-DCC

- **Consider migrating from current JCA-DCC to JCA-VHC (Joint coordination activity for verifiable health credentials).**
- **Implement the migration to JCA on verifiable health credential from the next study period (2025-2028).**