

Digital Vaccine Certificate Future Direction

August 11th, 2021

ITU Workshop on "Digital Vaccination Certificate"

Sanghwan Park (cowan@kisa.or.kr)

Director

Blockchain Technology Promotion Division

Korea Internet & Security Agency





| Table of Content



- 1** ▶ Korea's Case Study
- 2** ▶ Korea DID Promotion Policy
- 3** ▶ Future Works

1. Korea's Case Study (Digital Vaccination Certificate)

1. Technology Overview

- ✔️ KDCA issues digital vaccination certificate based on DID & blockchain technology
- Digital vaccination certificate contains COVID-19 vaccine name, vaccination date, vaccination venue, etc. in a mobile device to proof vaccination history

Issuance

A digital vaccination certificate is issued after the user identity is first verified

Usage

The user presents a QR code(Digital Vaccination Certificate link) to verifiers (restaurant, hospital, etc.). And they will verify the forgery/alteration of user's Digital Vaccination Certificate.



1. Korea's Case Study (KDCA's wallet COOV)

1-1. KDCA's COOV wallet use case (in-services, Issuing)

1) Identification of user



- DID
- Name
- Birth of date
- Gender
- Nationality
- Address

Identification Credential

2) KDCA issues digital vaccination certificate and it is stored on user's mobile application(Digital wallet)



- Vaccine Type
→ COVID-19
- Vaccine Brand
→ Pfizer
- Lot number
→ ER1919
- Sequence # of Doses
→ #1/2
- Vaccination Date
→ 2021.08.11
- Country
→ South Korea
- Clinic name
→ Korea Hospital
- Certificate status
→ Validate

Vaccination Verifiable Credential (Vaccination VC)

1. Korea's Case Study (KDCA's wallet COOV)

1-1. KDCA's COOV wallet use case (in services, Usage)

1) User presents vaccination certificate (QR code) to verifier

2) Verifiers Read user's QR code using their own COOV App

3) Verifier checks the validity of certificate online



(Including verification server information)

1. Korea's Case Study (Private DID Alliance's wallet)

1-2. Private DID Alliance wallet use case (Ways In discussion & to be developed, Issuing)

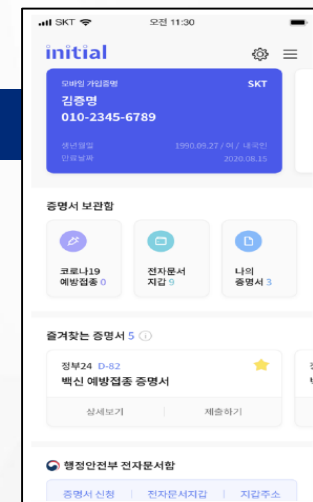
- Users can use their private digital wallet to get KDCA Digital Vaccination Certificate
- KDCA issues Digital Vaccination Certificate VC on Private DID alliance mobile apps

< Draft Implementation Outline (in discussion) >



Types of VCs (about 100) including Digital Vaccination Certificate

- Digital Vaccination Certificate (to be added)
- Resident Register
- Forest Land Register
- Certificate of Driver's License
- ...
- Student card
- University certificate of graduation
- Academic record
- ...



1. Korea's Case Study (Private DID Alliance's wallet)

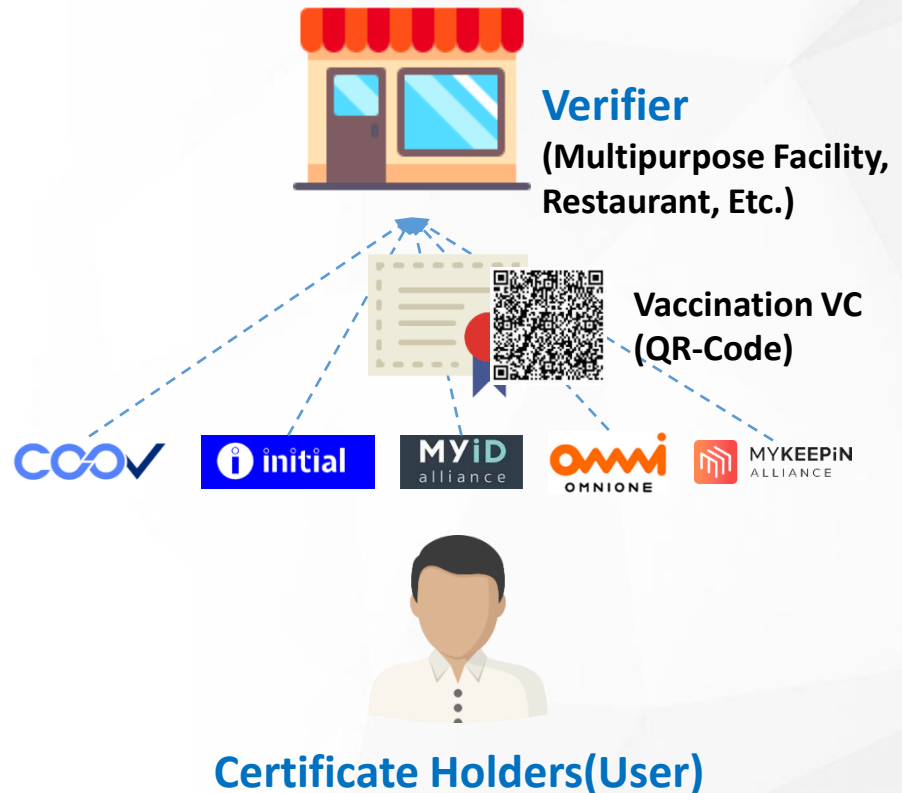
1-2. Private DID Alliance wallet use case (To be developed, Usage)

1) User presents vaccination certificate (QR code) to verifier



Creating QR-code (every 15 seconds)

2) Verifier verify the validity of user's Digital Vaccination Certificate VC and VP (using COOV app or DID alliance mobile app)



1. Korea's Case Study (Private QR Check-in services)

1-3. QR Check-in service usage (in services, Usage)

- KDCA adds electronic verification of COVID-19 vaccination function to QR Check-in services on popular mobile platform apps (NAVER, KakaoTalk)**
- Users can present their one-time QR codes upon entry to multipurpose facilities for use. And Verifiers can check both a electronic check-in authentication and vaccination certification together at a time**

NAVER



kakao



2. Korea DID Promotion Policy (MSIT, KISA)

2-1. Decentralized Identity Technology & Standardization Forum

Launched in September 2020 & 3 working groups (Policy, Tech, Service)

Policy WG

- The issuance of an identification policy per level of DID guarantee
- User guide per level of DID assurance
- Consulting for the designation of private DID business entity as an electronic signature service provider, Identification service provider.

Technology WG

- Develop VC profile standards for mobile driver's licenses, vaccination certificates, other DID documents, and credentials
- Review DID digital wallet security requirements and interoperable technologies

Service WG

- Develop an DID document lifecycle service model
- Identify areas that are potentially open to DID adoption along the lifecycle and analyze probable scenarios per area
- Develop a DID ecosystem strategy concerning digitally convertible DID documents and certificates

2. Korea DID Promotion Policy (MSIT, KISA)

2-2. Pilot Project & Policy Research

- **Driving Blockchain Pilot Projects in the public and private sectors**
 - Identify new blockchain-enabled services and demonstrate technological feasibility
 - 34 pilot projects executed from 2018 to 2020 (28 public, 6 private)
 - 19 pilot projects under way in 2021 including “Digital Vaccination Certificate” project based on DID with the KDCA
- **Doing Policy Research Study on Decentralized ID (DID) Service Adoption Plan**
 - Define DID Life-Cycle Service Model
 - Research into DID Policy in Foreign Countries
 - DID Service Global Expansion Strategy
 - Trust Anchor technology and operation guideline

3. Future Works

- ✓ **To broaden the use of digital vaccination certificates globally, the issues of security, trustworthiness, interoperability should be addressed**

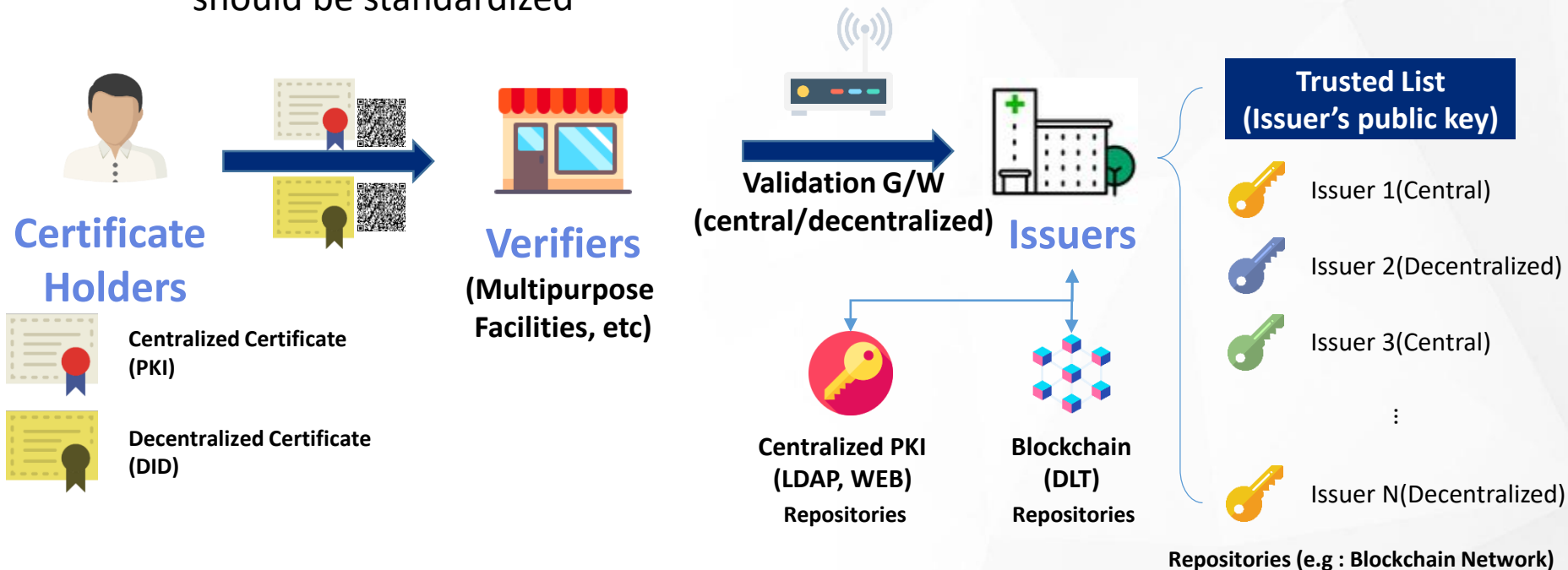
- ✓ **Digital Vaccination Certificate Security Consideration**
 - Digital Vaccination Certificate must be digitally signed by issuer
 - Issuer's private keys must be generated and used in HSM
 - Application code (smart contract) are developed in a secure coding
 - Subscriber(user)'s private key must be stored in secure elements
 - Screen capture preventive function recommended

- ✓ **Digital Vaccination Certificate Trustworthiness consideration**
 - Non-face to face subscriber(User) identification & authentication method be trustworthy(Assessing DID service Assurance Level)
 - Subscriber key and Certificate validity life cycle (Creation, Read, Update, Revocation, Etc.) should be implemented

3. Future Works

✔ Digital Vaccination Certificate Interoperability Consideration

- Two types of Vaccination Certificates can be used which have different technologies; one based on a central PKI Scheme, the other one based on a Distributed Ledger PKI scheme
- Trust Anchor needed to bridge trust and interoperability between different scheme of technologies and between a number of different issuers
- Vaccination QR Code payload profile & Digital Vaccination Certificate profile should be standardized



Thank You!

Sanghwan Park , Director of KISA
cowan@kisa.or.kr

Blockchain Technology Promotion Division
Korea Internet & Security Agency

