

Design and implementation of digital student ID system based on verifiable credentials

Ito, Eisuke
Research Institute for IT, Kyushu University

Yamaguchi, Takashi
Grad School of ISEE, Kyushu University

Itokawa, Ryo
Grad School of ISEE, Kyushu University

<https://hdl.handle.net/2324/7342414>

出版情報 : pp.12-15, 2024. IEEE

バージョン :

権利関係 : © 2024 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.



Design and implementation of digital student ID system based on verifiable credentials

Eisuke Ito
Research Institute for IT
Kyushu University
Fukuoka, Japan

ito.eisuke.523@m.kyushu-u.ac.jp

Takashi Yamaguchi
Grad. school of ISEE
Kyushu University
Fukuoka, Japan

yamaguchi.takashi.228@s.kyushu-u.ac.jp

Ryo Itokawa
Grad. school of ISEE
Kyushu University
Fukuoka, Japan

itokawa.ryo.975@s.kyushu-u.ac.jp

Abstract—With the rise of smartphone usage, digital credentials are gaining feasibility, and several are already in use. For instance, digital vaccination certificates have been issued by government health authorities in various countries, including Japan, where the Digital Agency and Ministry of Health, Labour and Welfare provide them. The mobile driver’s license, with ISO specifications set in 2021, is anticipated to be particularly transformative.

Our study investigates the development of digital student and staff IDs on smartphones. Using the World Wide Web Consortium’s (W3C) Verifiable Credentials (VC) specification, digital student IDs can be securely issued with built-in electronic identity verification. This enables functionality like building access, library borrowing, and lecture attendance verification. This paper details the design and verification processes, along with a prototype system for digital student IDs.

Index Terms—Digital student ID, Verifiable Credentials (VC), user authentication system, Digital Certificate, Digital Signature

I. INTRODUCTION

With the increasing adoption of smartphones, digital credentials are becoming more feasible. Some digital credentials have already been implemented. In certain countries, digital vaccination certificates were issued by government healthcare authorities[1]. In Japan, the Digital Agency and the Ministry of Health, Labour and Welfare issued digital vaccination certificates[2]. The mobile driver’s license, standardized by ISO in 2021[3], represents one of the most significant advancements in digital credentialing.

As part of the ongoing digitalization trend, we are considering implementing digital student and staff IDs on smartphones. The W3C (World Wide Web Consortium) has defined a specification for Verifiable Credentials (VC)[4]. By utilizing VC technology, digital student IDs can be issued. The VC specifications include electronic identity verification capabilities. Through verifying the authenticity of a student VC (digital credential), it becomes possible to enable features such as building access, authentication for library book borrowing, and lecture attendance verification.

For simplicity, we focus only on student IDs in this paper. However, the same approach is applicable to staff

ID cards as well. In this paper, we describe the design of issuance and verification processes and also present a prototype system for digital student IDs.

This paper is organized as follows. In Section II, we explain the trend of VC and related technologies. Section III describes printed/internal information on present IC student ID card. Section IV describes the policy and design of the digital student ID card we considered. Section V shows the development status of the prototype system, and also describes remaining lessons learned and challenges. Finally, we conclude in Section VI.

II. TRENDS IN VERIFIABLE CREDENTIALS (VC)

Verifiable credentials (VC) has been considered as digital personal identification documents on devices like smartphones.

A. W3C VC (Verifiable Credentials)

The W3C defines Verifiable Credentials (VC) specifications[4], including Issuer, Holder, Verifier, and Verifiable Data Registry. Figure 1 illustrates the relationships among these entities. The Issuer provides credentials stored by the Holder and validated by the Verifier using cryptography. VC data is in JSON format, converted to JWT (JSON Web Token), and displayed as QR codes, known as Verifiable Presentations (VPs). These VPs use cryptographic methods for authentication.

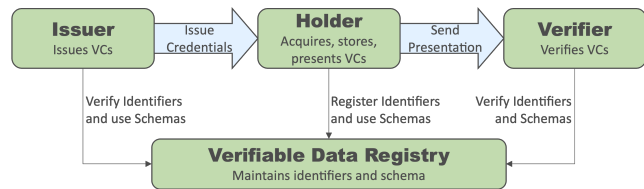


Fig. 1. VC overview diagram by W3C.

B. Digital vaccination certificate

During the COVID-19 pandemic, digital vaccination certificates were issued globally, including in Japan[1][2]. Japan’s system uses My Number IC cards for authentication and displays certificates in JWT format as QR codes. Verification is enabled through public key cryptography.

C. mDL

The digitization of driving licenses is also being considered. The standard for mobile driving licenses (mDL) was released by ISO in 2021[3]. Several countries and states are conducting pilot projects for mobile driving licenses. Using the mDL data format, it is possible to verify the authenticity of the data within the mDL. The data is not limited to driving licenses. Therefore, the mDL format is currently being considered for use as document data.

III. IC STUDENT ID CARD

To understand the requirements for a digital student ID system, it is essential to first examine the current physical IC student ID cards issued by Japanese universities, including Kyushu University. So, we first examine the existing physical IC student ID cards.

A. Printed Information

Table I shows printed details include university name, affiliation, student ID number, name, date of birth, enrollment year, photo, and issuer details (e.g., university president). The reverse side contains login ID, unique card number, barcode, and cooperative money seal.

B. Internal Information

Internally, the IC card stores a unique number and data for the VRICS system, developed at Kyushu University, to enable services like building access, library usage, and e-money for the campus cooperative. Table II shows internal information.

TABLE I
PRINTED INFORMATION ON STUDENT CARD

Front	University name Affiliation (faculty/department) Student ID number Name Date of birth Year of enrollment Headshot photo Issuer (president of Univ.)
Back	Contact details of the affiliated university Login ID Uniq card number Barcode of student ID number Seal information for cooperative money

TABLE II
IC STUDENT CARD STRUCTURE

Internal	Unique card number VRICS system app and PID (Personal ID)
----------	--

IV. DESIGN OF STUDENT ID SYSTEM

A. Guideline

Before designing the digital student ID system, we established guidelines as follows:

- Retain the information and functions of existing IC student ID cards.
- Use a simple structure for ease of implementation.
- Utilize existing authentication infrastructure where possible.

Based on these guidelines, we chose SAML-based distributed authentication, specifically Shibboleth[5], widely used in universities for electronic journal access. Shibboleth's IdP authenticates users and provides attribute data to the SP (Service Provider) in SAML format[6]. By integrating this system, we minimize time and cost while maintaining secure authentication for digital student ID issuance.

As shown in Figure 2, when issuing a digital student ID card, we can reduce the time and cost of constructing a new authentication system by designing it. So that the existing authentication infrastructure can be used to verify the identity and provide student

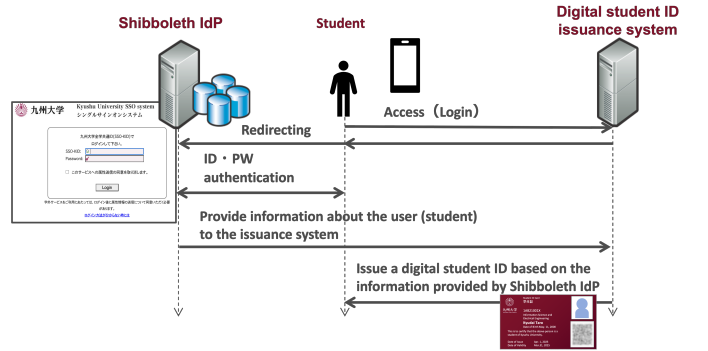


Fig. 2. Digital student ID issuance process

B. Data structure of digital student ID

The digital student ID retains the features of existing IC student ID card, incorporating VC data and a headshot photo. The VC is formatted in JSON and includes a digital signature to ensure data integrity. Table III shows key attributes of VC (digital student ID).

TABLE III
DATA STRUCTURE OF VC DIGITAL STUDENT ID

Data (Item)	Description
Issuer	Name of university, name of president (official seal image)
Affiliation	Department and Discipline
Name	Kanji name, Kana name, Romanized name
Date of Birth	Date of birth
Expiry Date	Expiry date
Student ID	String
Login ID	Included if necessary
Digital Signature	Signature algorithm and signature data
Public Key URL	Public key corresponding to the private key for signing

To verify the digital student ID's authenticity, the holder's identity must be confirmed by matching their face

with the headshot on the ID. The headshot is stored only within the app, ensuring privacy, and is excluded from the VC data. Figure 3 illustrates the concept.



Fig. 3. Conceptual image of digital student ID

C. VC issuance process

Using SAML-based authentication, like Shibboleth IdP, the IdP sends SAML data to the SP (Service Provider) upon successful authentication. Here, the VC issuer acts as the SP, creating VCs in JWT[7] format with digital signatures using SAML data. The issued VC is returned to the holder (student) and stored on their device.

- The student launches the ID app.
- (If available, identity is verified using own national IC cards.)
- The student requests a VC from the university.
- The issuer redirects to the IdP for authentication.
- The IdP returns SAML data upon success.
- The issuer creates the signed VC.
- The student receives and stores the VC in the app.

As of October 2024, Kyushu University's IdP supports only ID/password authentication. Multi-factor authentication should be adopted for enhanced security.

D. VC verification process

The digital student ID verification procedure involves presenting a secure, time-sensitive QR code, generated through two time-based one-time passwords (TOTPs)[8] to prevent potential spoofing. The procedure, shown in Figures 4 and 5, proceeds as follows:

- 1) QR Code Generation: The student's app generates a QR code containing the student ID, TOTP1, TOTP1 confirmation URL, and an AES-encrypted string of the VC using TOTP2.
- 2) QR Code Presentation: The student presents the generated QR code to the verifier.
- 3) Verification Request: The verifier scans the QR code and queries the issuing authority to verify TOTP1 using the provided confirmation URL.
- 4) TOTP2 Retrieval: Upon successful verification, TOTP2 is generated and sent to the verifier.
- 5) VC Decryption and Signature Verification: The verifier decrypts the VC using TOTP2 and verifies its authenticity using the digital signature.

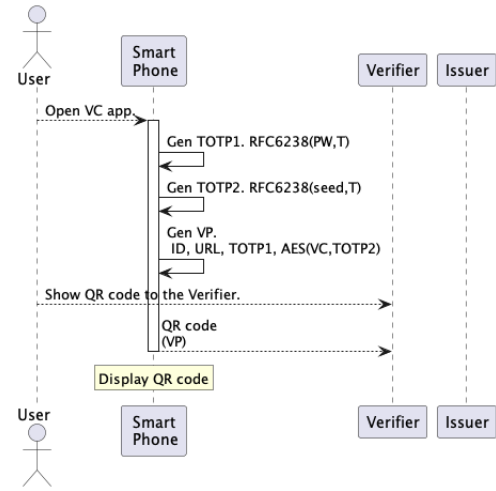


Fig. 4. VP(Verifiable Presentation) of student ID

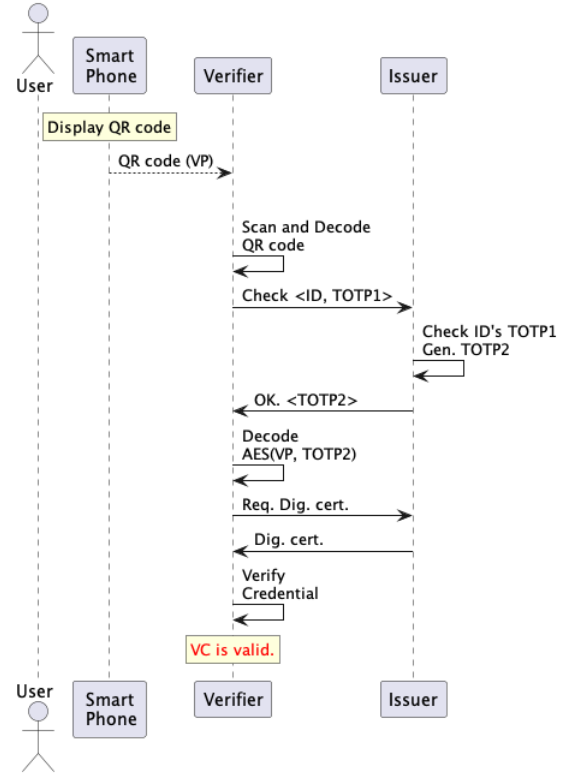


Fig. 5. VC verification process

This process provides a secure, dynamic verification method that ensures the student ID is valid and has not been tampered with. The QR code's encryption and frequent renewal with TOTPs minimize the risk of spoofing, maintaining a high level of security in real-world applications.

V. IMPLEMENTATION

We implemented a prototype digital student ID system using two PCs and Android smartphones. The system

TABLE IV
HARDWARE AND SOFTWARE OF THE PROTOTYPE SYSTEM

	Issuer	IdP	Smartphone
Machine	Beelink MINI-S12 N95		Sony Xperia ACE-2 SO-41B
OS	Ubuntu 24.04		Android
Middle ware	Flask 3.0.3 Python 3.12 Ubuntu 24.04	Open LDAP 2.6.7 Keycloak 25.0.4	Flutter App -

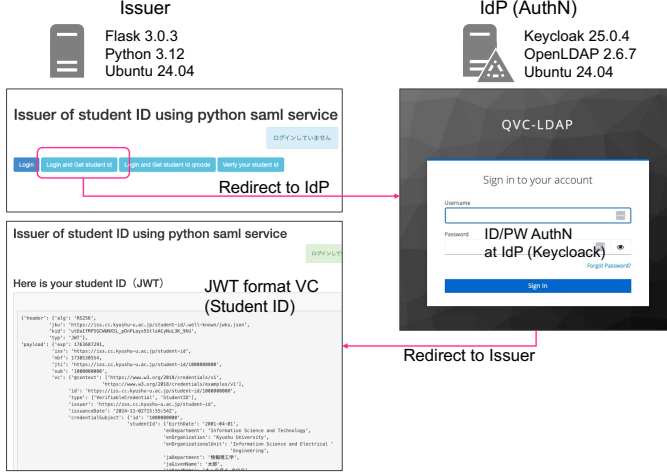


Fig. 6. screen transitions of the prototype

uses Keycloak instead of Shibboleth IdP, enabling ID/PW authentication via LDAP or AD integration, as well as MFA. Keycloak supports SAML 2.0 for SSO and OpenID Connect for ID token-based authentication and access control. Table IV shows details of hardwares and softwares, and Figure 6 illustrates the screen transitions of the prototype system.

In the prototype issuer, a digital student ID is issued via password authentication. Since password authentication is weak, there is a risk that other people can issue student IDs. In the future, we plan to introduce a more secure user authentication process.

A. Lessons learned and challenges

We discuss the lessons learned from implementing the prototype system and the future expansion of its functions.

- 1) **TOTP based periodical change:** The prototype system does not implement periodically changing Verifiable Presentations (VP) using TOTP. To prevent spoofing through VC screenshots, we aim to introduce a mechanism for periodic changes using TOTP.
- 2) **Weakness of authentication:** As described in subsection IV.C, both Kyushu University's IdP and the current prototype system rely solely on password authentication. Since password authentication is inherently weak, we plan to adopt more robust authentication mechanisms in the future.
- 3) **Headshot photo:** The prototype system lacks a headshot photo. To display the headshot on the

digital student ID, we need to utilize face image storage in LDAP or AD, or alternatively, construct a dedicated database for headshots.

- 4) **Lifecycle of student ID:** Attribute data on the student ID may change due to events such as name changes from marriage, faculty transitions, or advancement to graduate school. We aim to support modifications aligned with the lifecycle of students.
- 5) **Selective disclosure:** To prevent the display or sharing of private information, selective disclosure[9] mechanism should be implemented our system.
- 6) **Multilingual support:** Unlike IC cards, digital student IDs can easily switch display languages. Multilingual support is also under consideration.

VI. CONCLUSION

This paper presents a digital student ID system using verifiable credentials (VCs). We designed the issuance and verification processes for VCs and implemented a prototype of the digital student ID system. The issuing authority and authentication authority are deployed on two Linux PC servers. We use Keycloak for the authentication authority. Additionally, we developed a student ID application for Android smartphones. The prototype system is not yet fully functional. Future work will focus on further development to achieve complete functionality.

REFERENCES

- [1] T.-C. Yu, I.-M. Parng, J.-S. Yeh, G.-W. Cao, and F.-C. Wang, "A digital certificate system that complies with international standards: Taiwan digital covid-19 certificate," *Standards*, vol. 3, no. 4, 2023, pp. 341–355.
- [2] The Ministry of Health, Labour and Welfare of Japan, "Shingata Korona Uirusu Kansenshō Yobō Sesshu Shōmei-sho (Sesshu Shōmei-sho) ni tsuite (About novel coronavirus vaccination certificate(vaccination certificate)),," https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/vaccine_certificate.html, accessed on 24.06.2024.
- [3] "ISO/IEC 18013-5:2021, Personal identification ISO-compliant driving licence, 2021-10-4," <https://www.iso.org/standard/69084.html>, accessed on 24.06.2024.
- [4] W3C. Verifiable Credentials Data Model v1.1, 2022. <https://www.w3.org/TR/vc-data-model/>. Accessed on 24.06.2024.
- [5] Shibboleth, "Shibboleth Consortium - Shaping the future of Shibboleth Software," <https://www.shibboleth.net/>, accessed on 24.06.2024.
- [6] OASIS, "Security Assertion Markup Language (SAML) V2.0 Technical Overview," <https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html>, accessed on 24.06.2024.
- [7] M. Jones and J. Bradley and N. Sakimura, "JSON Web Token (JWT)," <https://www.rfc-editor.org/rfc/rfc7519>, accessed on 24.06.2024.
- [8] D. M'Raihi, J. Rydell, M. Pei, and S. Machani, "TOTP: Time-Based One-Time Password Algorithm," RFC 6238, May 2011, accessed on 24.06.2024.
- [9] D. Fett, K. Yasuda, and B. Campbell, "Selective Disclosure for JWTs (SD-JWT)," *sd-jwt*, Internet-Draft draft-ietf-oauth-selective-disclosure-jwt-10, Jul. 2024, work in Progress, <https://datatracker.ietf.org/doc/draft-ietf-oauth-selective-disclosure-jwt/10/>, Accessed on 07.08.2024.