

検証可能な資格情報によるデジタル学生証・職員証 の検討

伊東, 栄典
九州大学情報基盤研究開発センター

<https://hdl.handle.net/2324/7183341>

出版情報 : 2024-03-08. Saga University Computer and Network Center
バージョン :
権利関係 :



2024年3月8日
佐賀大学総合情報基盤センター
統合認証シンポジウム



検証可能な資格情報による デジタル学生証・職員証の検討

伊東 栄典

九州大学 情報基盤研究開発センター

ito.eisuke.532@m.kyushu-u.ac.jp

まえおき

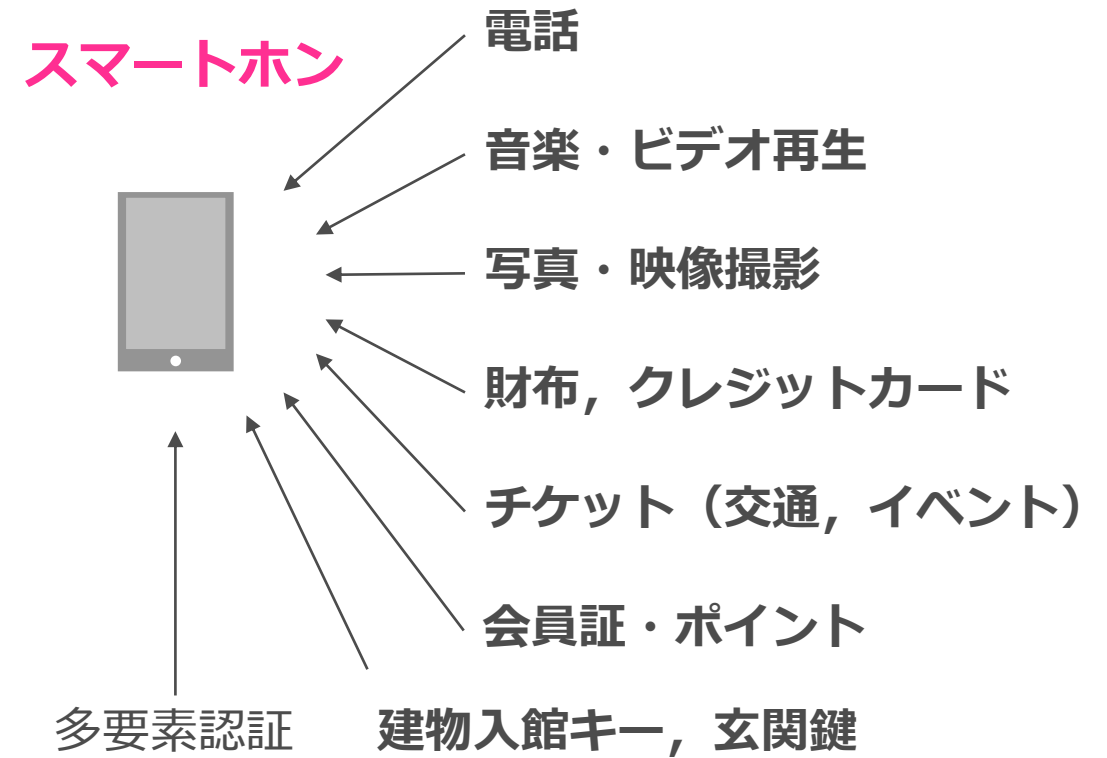
- 本研究は伊東栄典とジェイズ・コミュニケーション社が共同研究として開発中です。
- 九州大学における「デジタル学生証導入」は、まだ話も出ていない段階です。
- まだまだ穴だらけなので、ご指摘いただけると助かります。

1. はじめに

1. はじめに
2. 関連技術と先行事例
3. デジタル学生証の要求要件
4. 方針と設計
5. 試作システム
6. スマホログイン
7. おわりに

1. はじめに

- 様々なサービス・機能がスマートフォンに集約
- 資格情報の格納も開始
 - ワクチン接種証明（2021年10月）
 - デジタル庁+厚生労働省
- 本研究
 - **学生証・職員証をデジタル化して，スマートフォンで使いたい。**
 - その際，外部組織でも資格情報を確認できるようにしたい。



※以降「学生証」のみ言及。説明は「職員証」でも概ね適用可能。

本発表の内容

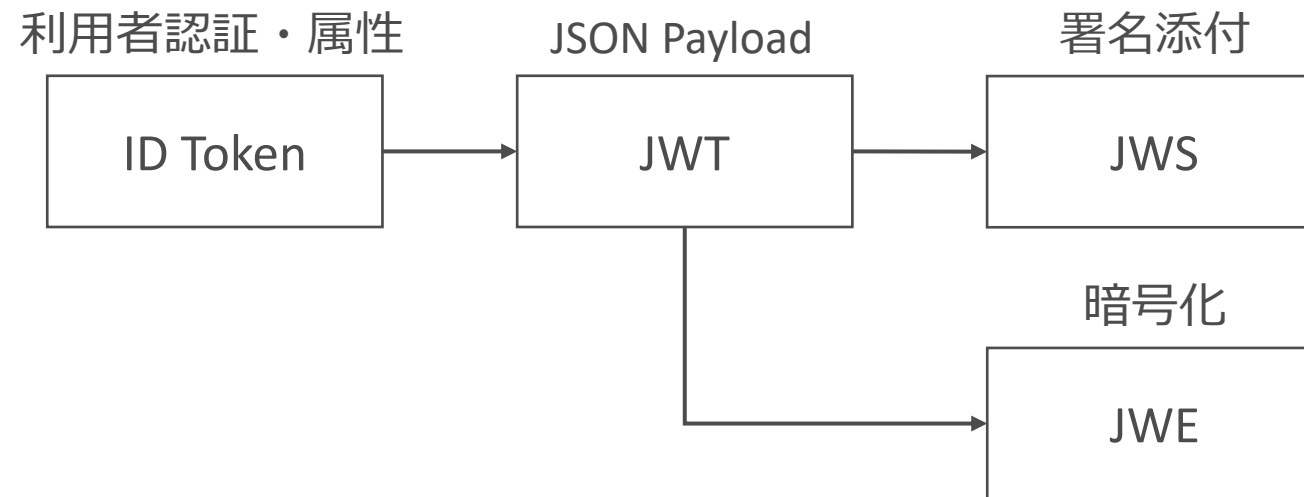
- 目標：デジタル化した学生証をしてスマートフォンで実現
 - ICカード学生証が，色々と面倒
 - 携帯するのが面倒（交通系IC等とかぶる）
 - スマホ学生証ができれば楽。
- 本発表の内容
 - 関連技術や先行事例の調査
 - デジタル学生証の要求要件の明確化
 - 実現方針と発行・検証機構の設計
 - システムの試作（途中）

2. 関連技術と先行事例

1. はじめに
2. 関連技術と先行事例
3. デジタル学生証の要求要件
4. 方針と設計
5. 試作システム
6. スマホログイン
7. おわりに

2.1 JSON Web Token/Signature/Encryption (JWT, JWS, JWE)

- Web系サービスにおける利用者認証処理の効率化のために導入
- 利用者認証, 認可処理の結果を保持するもの → Token
- Token情報をJSONで記述
- JSONを Base64 URL Encoding



2.2 Verifiable Credentials (VC) by W3C.

- **Verifiable Credentials** = 「内容を検証可能な自己主権型のデジタル証明書」
 - VCデータは, JSON, JWT, JWS, JWE 形式での記述を想定
- **【発行者】 (Issuer)** が **【保持者】 (Holder)** に対して発行した**証明書 (Credentials)** を, **【検証者】 (Verifier)** が検証できる仕組み。
- **Verifiable Data Registry** : 識別子や鍵, その他関連データの作成や検証を仲介。

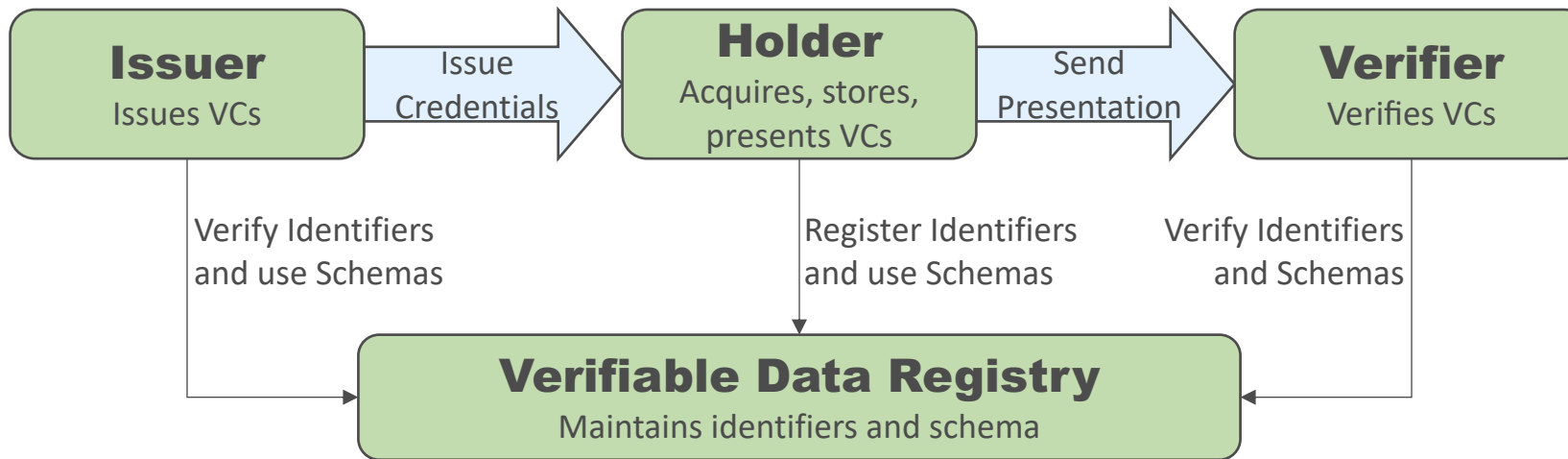


Figure 1 The roles and information flows forming the basis for this specification.

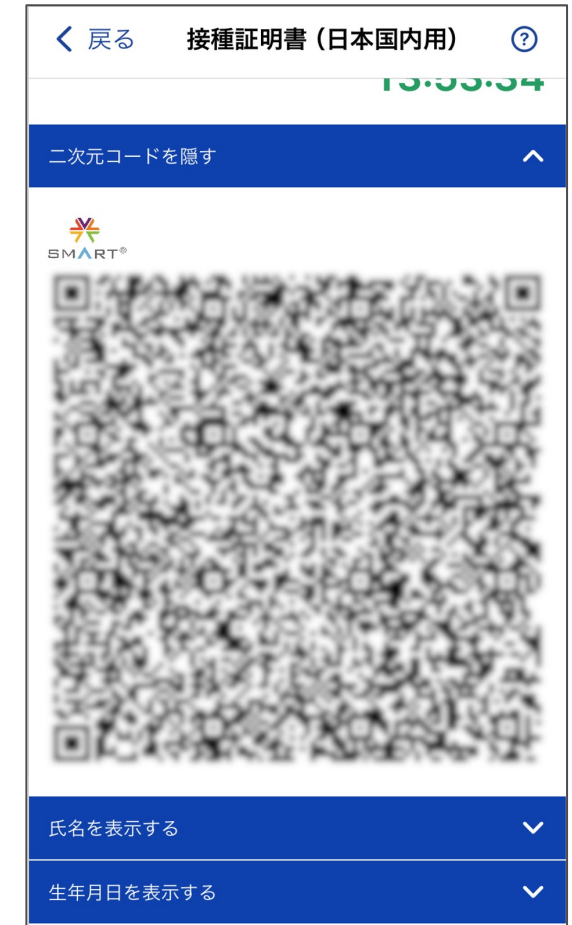
出典 : [Verifiable Credentials Data Model v1.1 \(W3C\)](https://www.w3.org/TR/vc-data-model/)

VC事例：ワクチン接種証明



- デジタル庁・厚生労働省 (2021年12月20日)
- ワクチン接種証明がVCとして発行される。
 - マイナカードによる本人確認後
- QRコードで接種証明情報を提供 → 署名で真正性を検証可能
 - SHC (SMART Health Cards) 規格
 - VDS-NC (Visible Digital Seal for Non-Constrained environment)
- SHC型 QRコード
 - デコードで数値列
 - 数値列のデコードで, JSONデータ
 - 発行者, 資格情報の種類, 署名方式や署名, また署名の検証に必要な公開鍵のURL
 - URLが示す公開鍵で署名を検証可能

ワクチン接種証明書 SHC形式QRコード

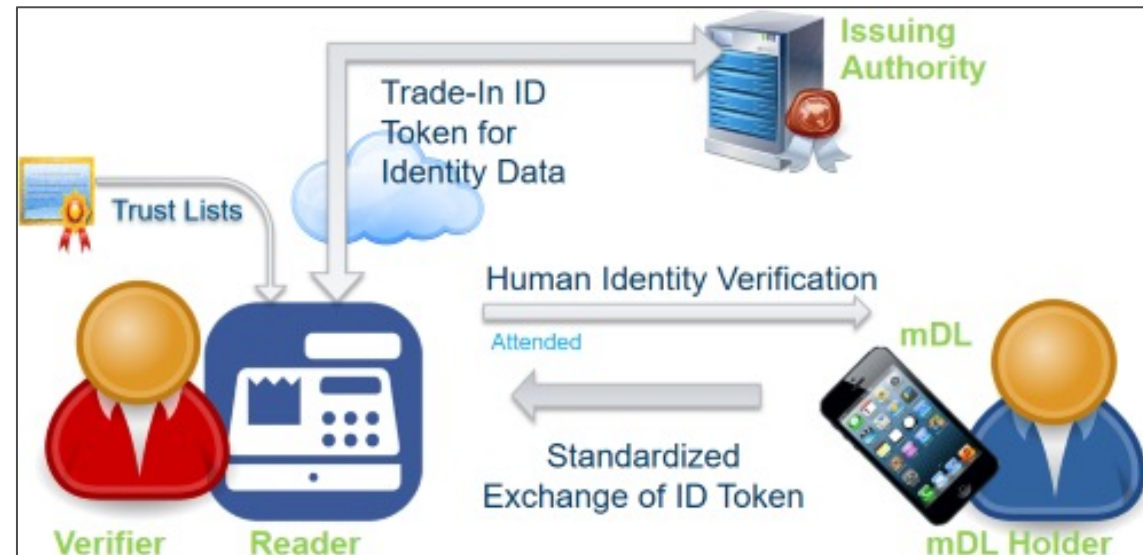
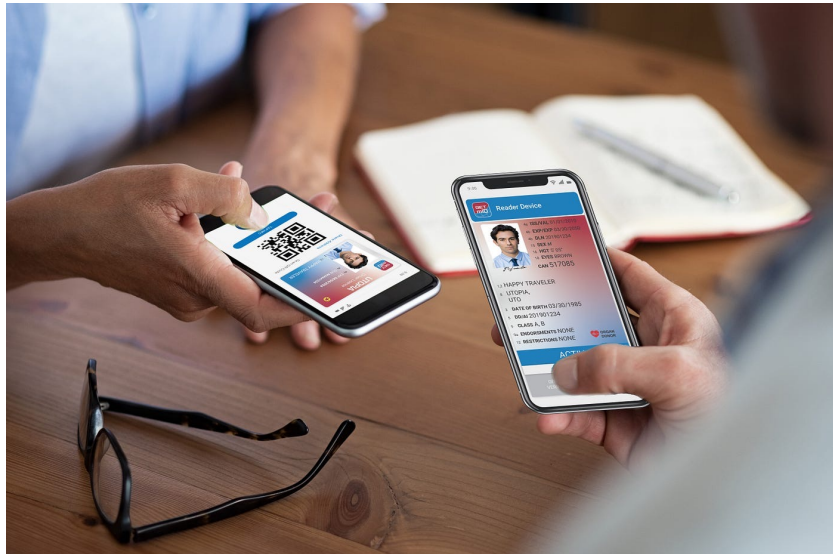


2.3 モバイル運転免許証

- **ISO/IEC 18013-5:2021**

Personal identification — ISO-compliant driving licence — Part 5: **Mobile driving licence (mDL)** application

– <https://www.iso.org/standard/69084.html>



David Kelts, The New Mobile Driver Licenses — How to Use ISO 18013–5, Apr 24, 2019.

<https://medium.com/@dkelts.id/mobile-driver-licenses-mdl-how-to-use-iso-18013-5-5a1bbc1a37a3>

モバイル運転免許証

- オーストラリア Queensland Digital Licence app
 - <https://www.qld.gov.au/transport/projects/digital-licence>
 - 2022年から開始。パスポート, Driver license, Birth Certificate (出生証明)
- EU、域内全域で利用可能なデジタルID発行で政治合意
 - <https://www.jetro.go.jp/biznews/2023/07/66bc431cbb8dc76a.html>
 - 加盟国発行のデジタルIDに基づき、EU共通規格に準拠した欧州デジタルIDウォレットを提供
 - 身分証明書, **デジタル運転免許証** (審議中), 処方箋などの医療データ, 教育や職業に関する資格などを保存・管理でき、電子署名にも対応。
- 世界で進むデジタル運転免許証 中国は2022年に全面普及へ
 - <https://ascii.jp/limit/group/ida/elem/000/004/067/4067464/>

金沢大学身分証アプリ

- <https://note.w3.kanazawa-u.ac.jp/contents/615>
- 令和3年10月1日から試行運用



MyID (マイディ) JSS社

- <https://myid.co.jp/>
- すべての身分証をスマホアプリで。
- 運用費：学生数（社員、会員）×1200円（年額）



主な機能

コミュニケーション機能



アプリを通じて、学生・生徒と大学・学校とがメッセージをやりとりすることができます。Push通知で直接端末にメッセージを送るため、メールを読まない学生・生徒でもメッセージの確認率が上がります。

出席登録



ビーコンを使用することで手作業・口頭での出欠確認が必要なくなります。学生・生徒が教室でアプリにアクセスするだけで、出席登録が完了します。

安否確認



災害時等には速やかに安否確認を行うことができます。学生・生徒がどこにいても、電話回線が繋がらなくても影響を受けません。



スケジュール帳の
確認



QRコード・
バーコードの表示



学生手帳の閲覧



通学証明書の発行
&more...

詳しくは
こちらをチェック!

がアプリ!
紹介動画



導入学校
インタビュー



https://www.soumu.go.jp/main_sosiki/joho_tsusin/top/local_support/ict/jirei/2020_004.html

デジ学

- デジ学アプリ <https://www.digigaku.jp/>
- 2024/01/31で新規受付終了



3. デジタル学生証の要求要件

1. はじめに
2. 関連技術と先行事例
3. デジタル学生証の要求要件
4. 方針と設計
5. 試作システム
6. スマホログイン
7. おわりに

学生証とは？

媒体	内容	特徴
学生手帳＋写真貼り付け	文字による身分情報 顔写真による本人確認 学生のルール	雨や摩擦に弱い。 携帯する小冊子は文字が読みにくい。
紙カード＋写真貼り付け	文字による身分情報 顔写真による本人確認	雨や摩擦に弱い→ラミネート加工 コピー機の普及後、偽造が簡単に。
プラスチックカード (身分情報と顔写真を印字)	文字による身分情報 顔写真による本人確認	耐久性向上 偽造が難しい
icカード (身分情報と顔写真を印字)	文字による身分情報 顔写真による本人確認 NFCによる情報交換	偽造がかなり難しい 耐タンパ性（内部情報取得困難） NFCで内部保存情報にアクセス可能。
デジタル学生証 (スマホアプリ)	文字による身分情報 顔写真による本人確認 検証可能情報	常時携帯 外部通信と内部での処理が可能 アプリ更新による機能更新可能 NFCも利用可能（かもしれない）

ICカード学生証

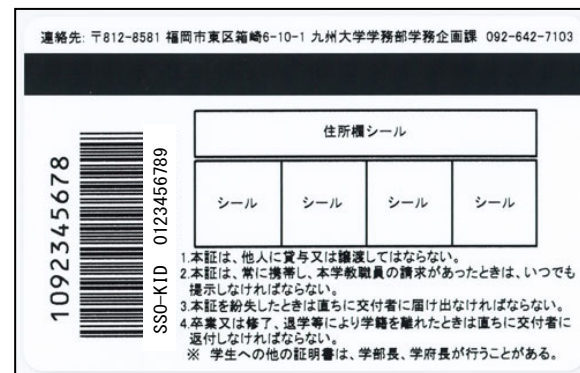
身分証（券面情報）

おもて



大学名，学部学科，顔写真
学生番号，氏名，生年月日
発行日，有効期限，印鑑
登録コード

うら



連絡先 (住所・Tel), SSO-KID
カード番号 (バーコード)
住所，シール (生協マネー)

ICカード

・ 内部情報

- カード番号
- VRICSシステム
 - ・ PIDシステム
- 生協電子マネー

・ 用途

- 建物の入館
- 図書館：入退室，図書貸出
- 授業の出席管理
- 生協電子マネー

デジタル学生証の要求要件

- 身分証に必要情報は残す
 - （大学の印鑑画像は必要か？）
- ICカード機能の継続
 - 建物ドア・部屋ドアを開ける
 - 図書貸出
 - 生協ICカードマネー
- 追加機能
 - 学生への通知（全体通知，個別通知）
 - 安否確認
- カード型の学生証は残す。
 - 学外の身分証としてカード型学生証が有効
 - 配布したい情報
 - アカウントの**初期登録コード**
 - 学生証アプリへ誘導するQRコード印刷
 - 学則

学生証・職員証のライフサイクル

- 発行
- 失効
- 有効期限
- 紛失処理
- 内容変更（氏名変更，転学部，組織改編）

4. 方針と設計

1. はじめに
2. 関連技術と先行事例
3. デジタル学生証の要求要件
4. 方針と設計
5. 試作システム
6. スマホログイン
7. おわりに

4.1 デジタル学生証の実現方針

- 既存学生証と同様に，大学で管理したい。
 - 発行，有効化，失効などの管理作業。
- なるべく安く簡易に実現したい。
- ICカード学生証が持つ機能をなるべく継承
 - 券面情報（身元情報）
 - バーコード
 - ドアの鍵
 - 信頼できる相手に身元情報提示
- できれば多言語化

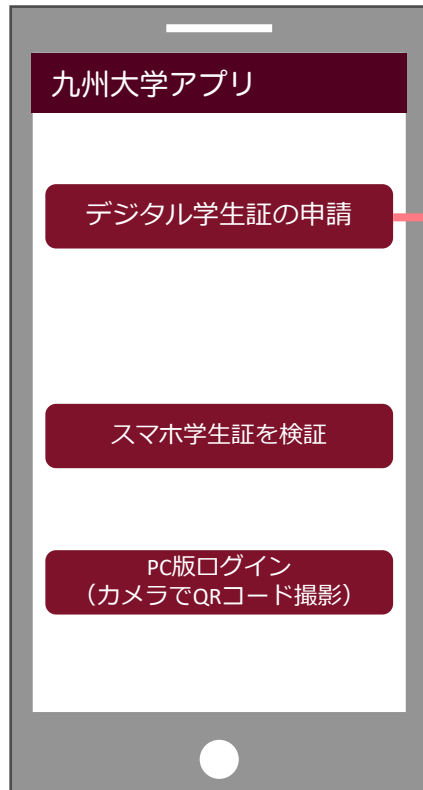
→ 中央集権型システム

→ 既存の認証基盤を利用

4.2 デジタル学生証アプリの画面

デジタル学生証画面（想定図）

初期画面



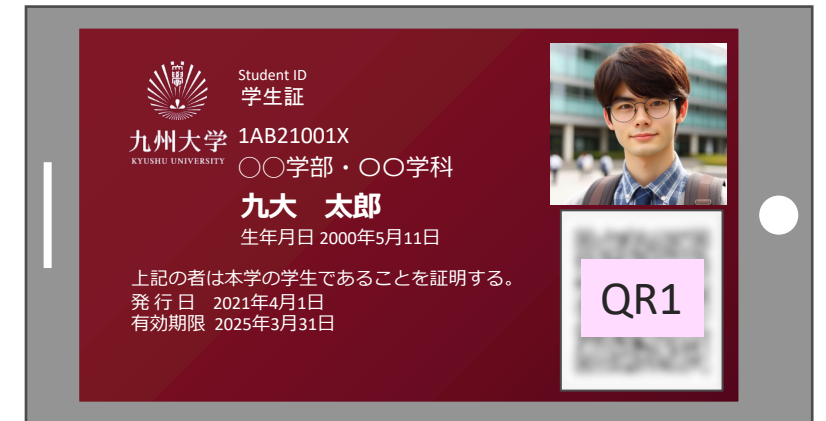
学生証VC 発行



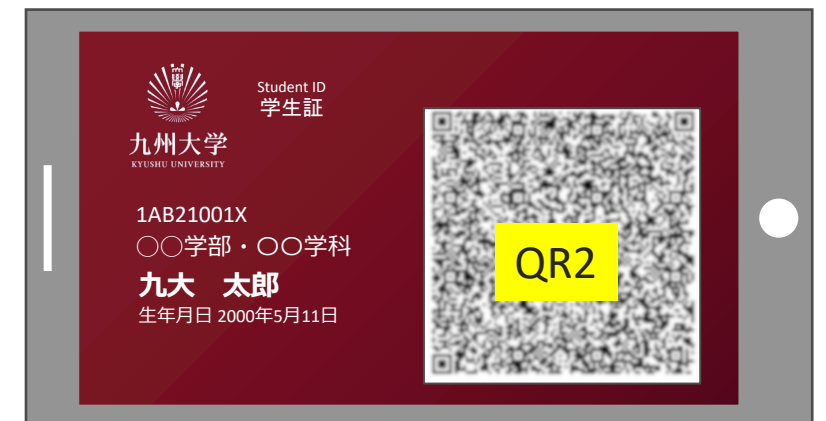
自分で利用



他者に提示（１）

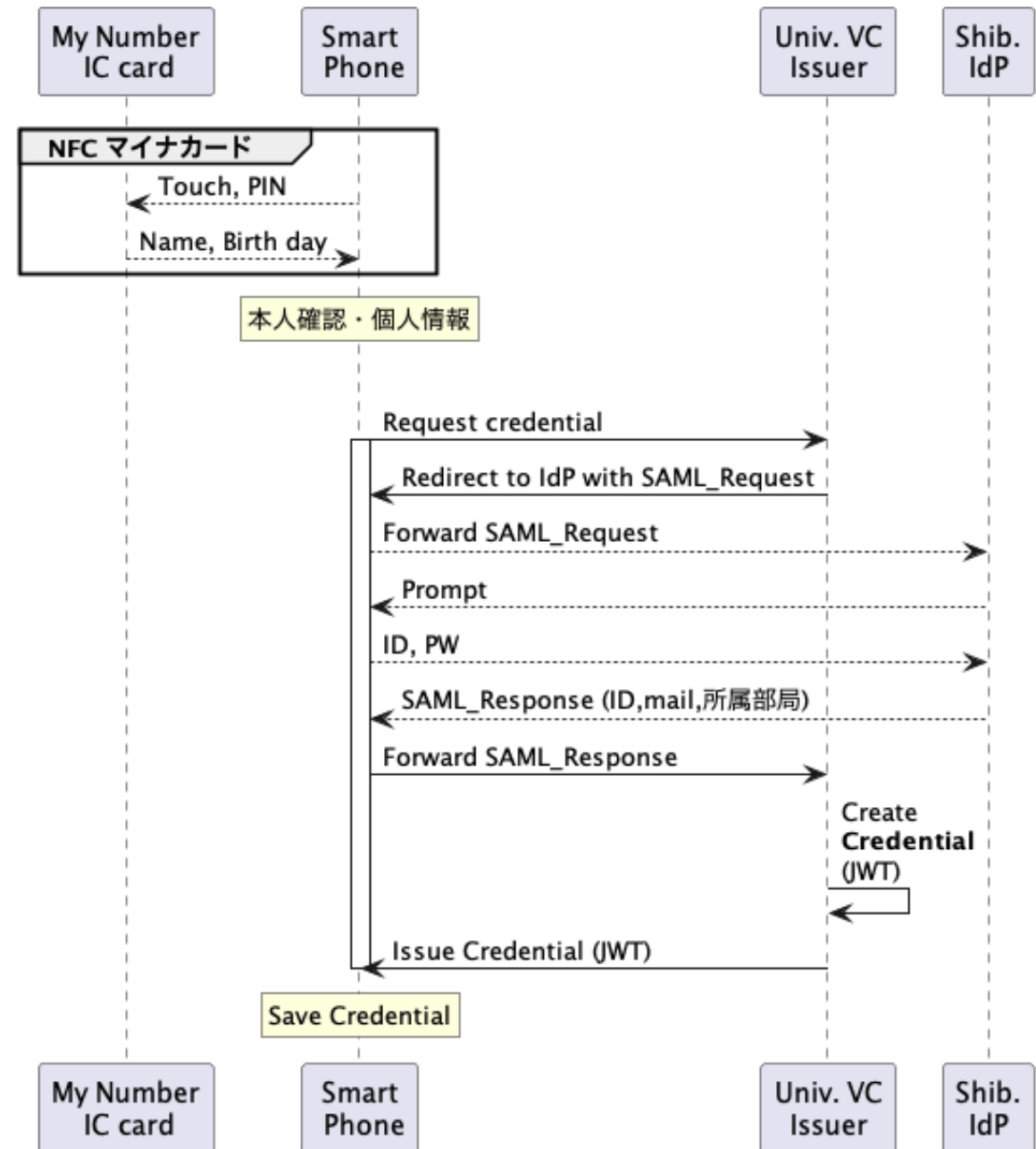


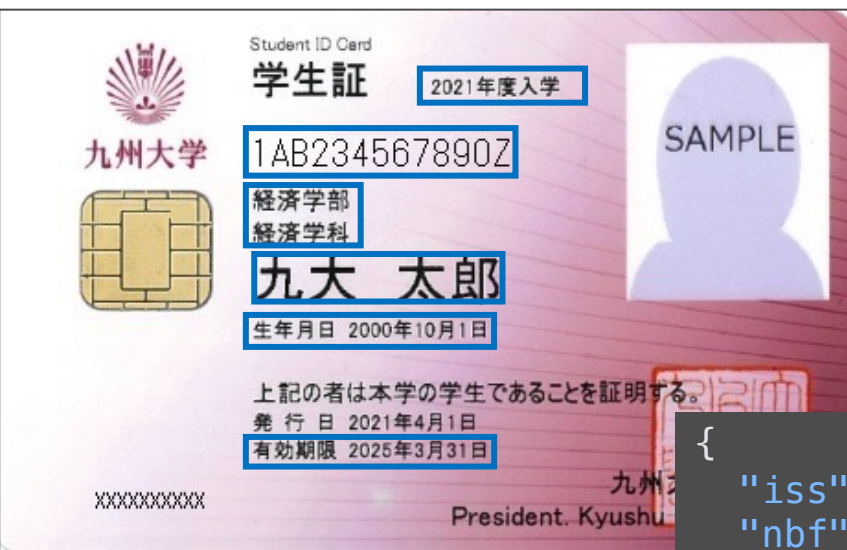
他者に提示（２）



4.3 デジタル学生証：発行手順（案）

- 保有者（学生）は専用アプリを起動
- （可能ならマイナカードで本人確認）
 - ID/PW認証だけでは弱いため。
- 大学へ学生証VC発行を要求
- Shibboleth IdPで，ID/PW認証
- SAML Responseで返る属性情報から，発行局でVC作成，利用者へ応答
 - 学生証のJWT作成
 - 電子署名JWSを付与
- 利用者は，発行されたVCを格納





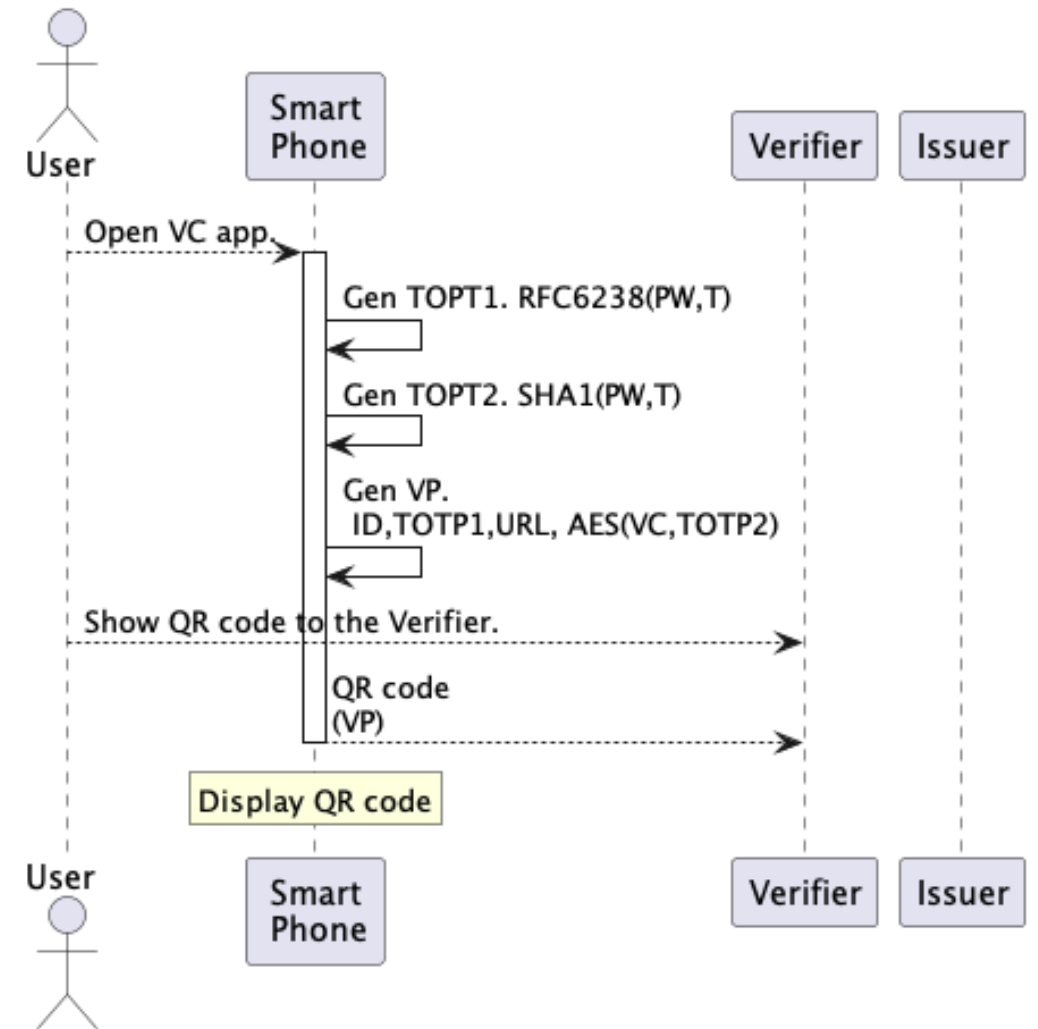
- 入学年度
- 学籍番号
- 学部学科
- 氏名
- 生年月日
- 有効期限

学生証VCの案 (JSON形式, Payload部分)

```
{
  "iss": "https://iss.kyushu-u.ac.jp/issuer",
  "nbf": 1522508400,
  "exp": 1711897199,
  "iat": 1694659887,
  "vc": {
    "type": ["https://studentid.cards"],
    "credentialSubject": {
      "sidVersion": "0.1",
      "name": [{"use": "usual", "family": "Kyudai", "given": "Taro"}],
      "nameKanji": [{"use": "usual", "family": "九大", "given": "太郎"}],
      "nameKana": [{"use": "usual", "family": "キュウダイ", "given": "タロウ"}],
      "birthDate": "2000-10-01",
      "studentID": "1EC18001X",
      "loginID": "1234567890",
      "admissionYear": "2021年",
      "expirationDate": "2024年3月31日まで"
    }
  }
}
```

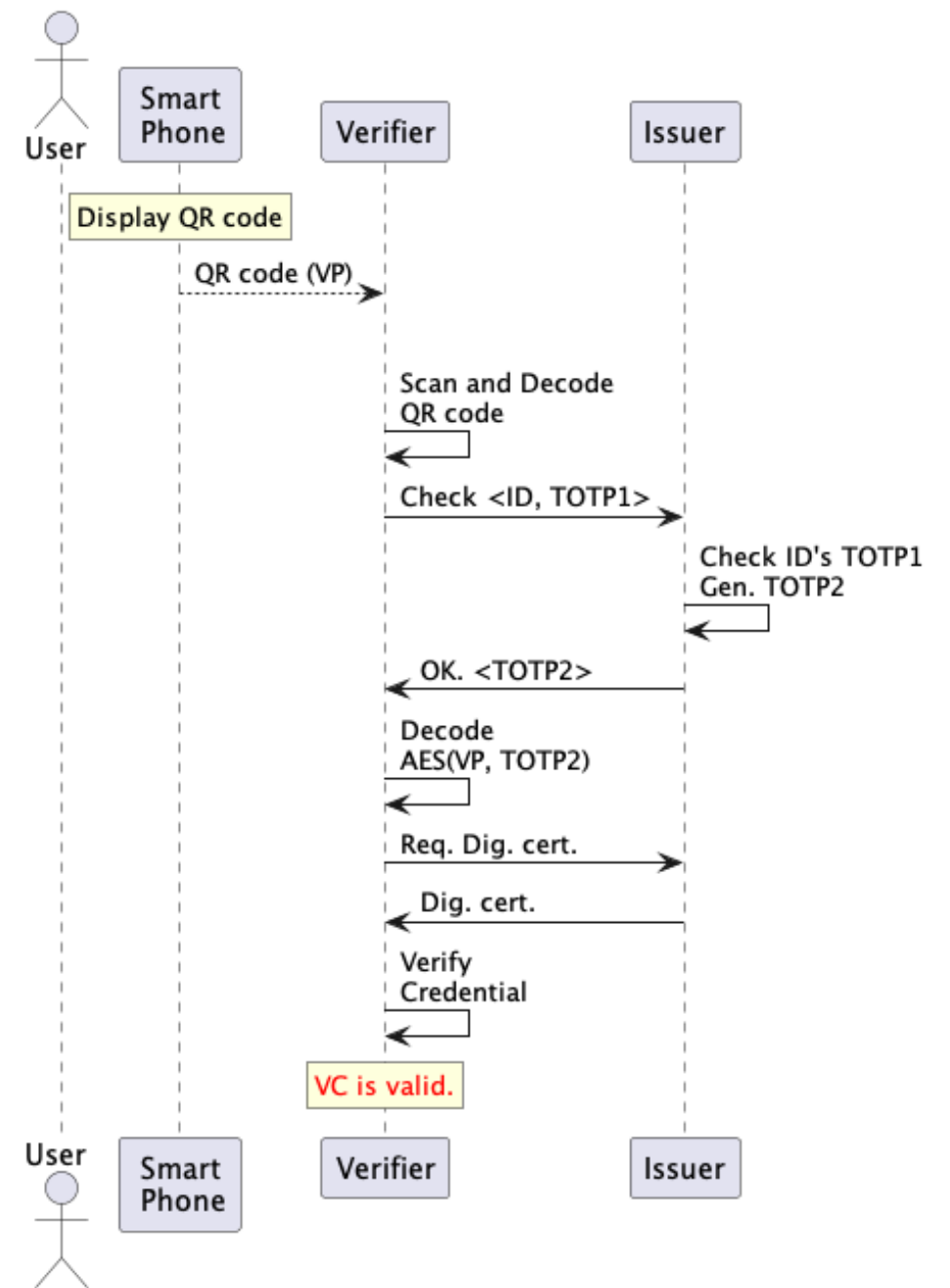
4.4 デジタル学生証：検証手順（案）

- オンラインでの検証手続きを想定
（発行局に情報確認）
- 所有者
 - 発行局も確認可能なTOPTを2つ作成。
 - 以下の4つ組をQRコード化
 - 利用者ID, TOPT1, 確認先（発行局）, VC(JSON)をTOTP2でAES暗号化
- 検証者
 - QRコードから内部情報を抽出
 - 発行局に, IDとTOPT1が正しいか問い合わせ
 - 正しい場合, TOTP2が返る
 - TOTP2でVCをデコード
 - VCの電子署名を検証
 - 発行局の公開鍵を取得して計算
 - 検証が正しいならばOK



4.4 デジタル学生証：検証手順（案）

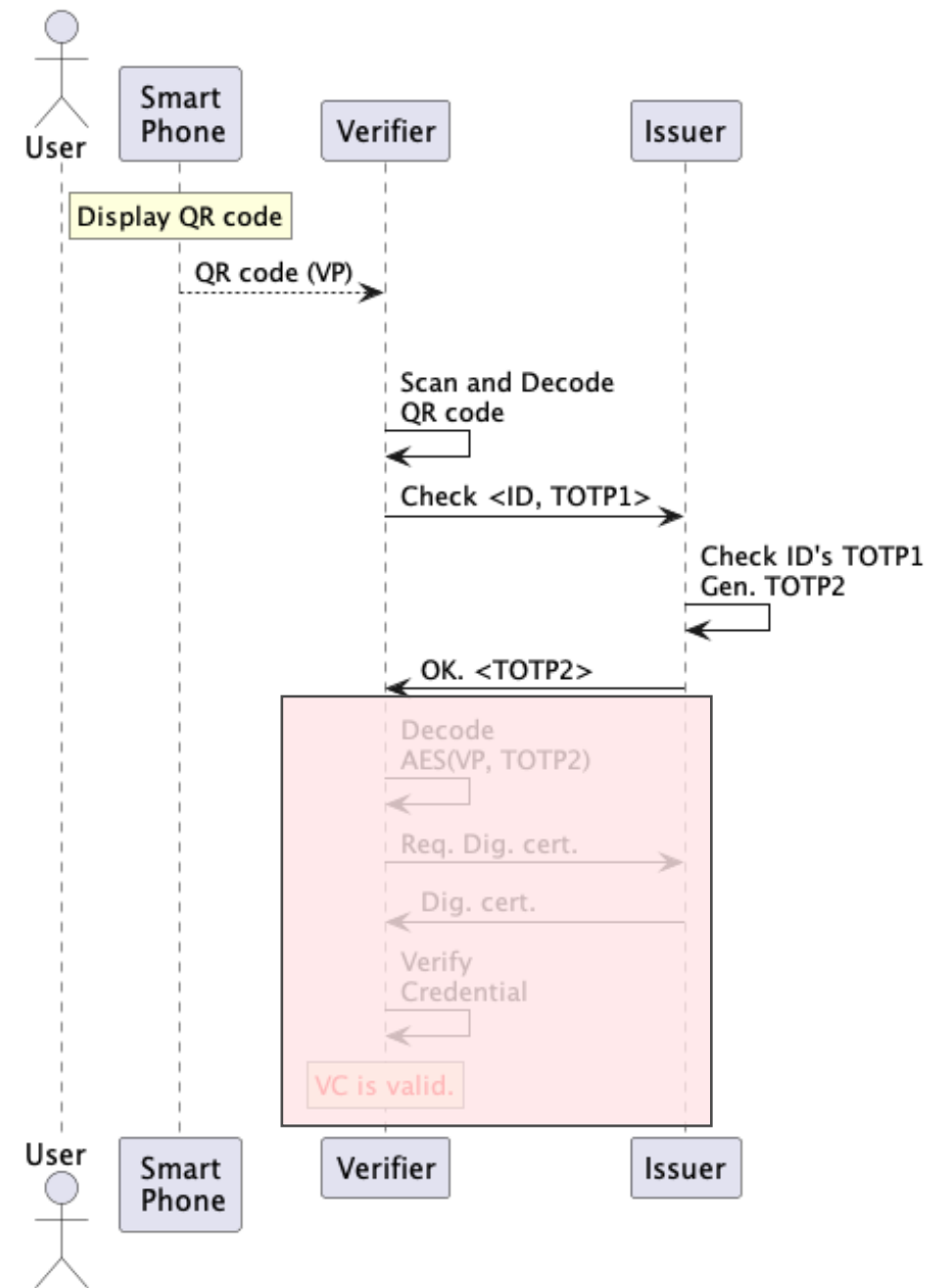
- オンラインでの検証手続きを想定
（発行局に情報確認）
- 所有者
 - 発行局も確認可能なTOPTを2つ作成。
 - 以下の4つ組でVP作成 → QRコード化
 - 利用者ID, TOPT1, 確認先（発行局）, VC(JSON)をTOTP2でAES暗号化
- 検証者
 - QRコードから内部情報を抽出
 - 発行局に, IDとTOPT1が正しいか問い合わせ
 - 正しい場合, TOTP2が返る
 - TOTP2でVPをデコード
 - VCの電子署名を検証
 - 発行局の公開鍵を取得して計算
 - 検証が正しいならばOK



4.5 デジタル学生証の利用

- 先の検証手続きでは，全情報を検証者に渡してしまう。
- デジタル学生証の使い方を分けてみる
 - 他者に見せて身元情報提示
 - 1. バーコードで学生IDの提示
 - 2. **ドアの鍵**
 - 3. **表示情報の正しさだけを検証**
 - 4. 学生証の個人情報を提供
- 全情報を渡す場合は少ない
 - どんな場合に渡すのか？
 - 渡す相手を信頼する方法は？

ICカードキーや
スマートキーの
手続きを模倣したい



自分で利用

ドアの鍵



他者に提示 (1)

定期券や学割購入時の確認



表示内容の真正性だけを検証

他者に提示 (2)

文科省やNIIへの入館?

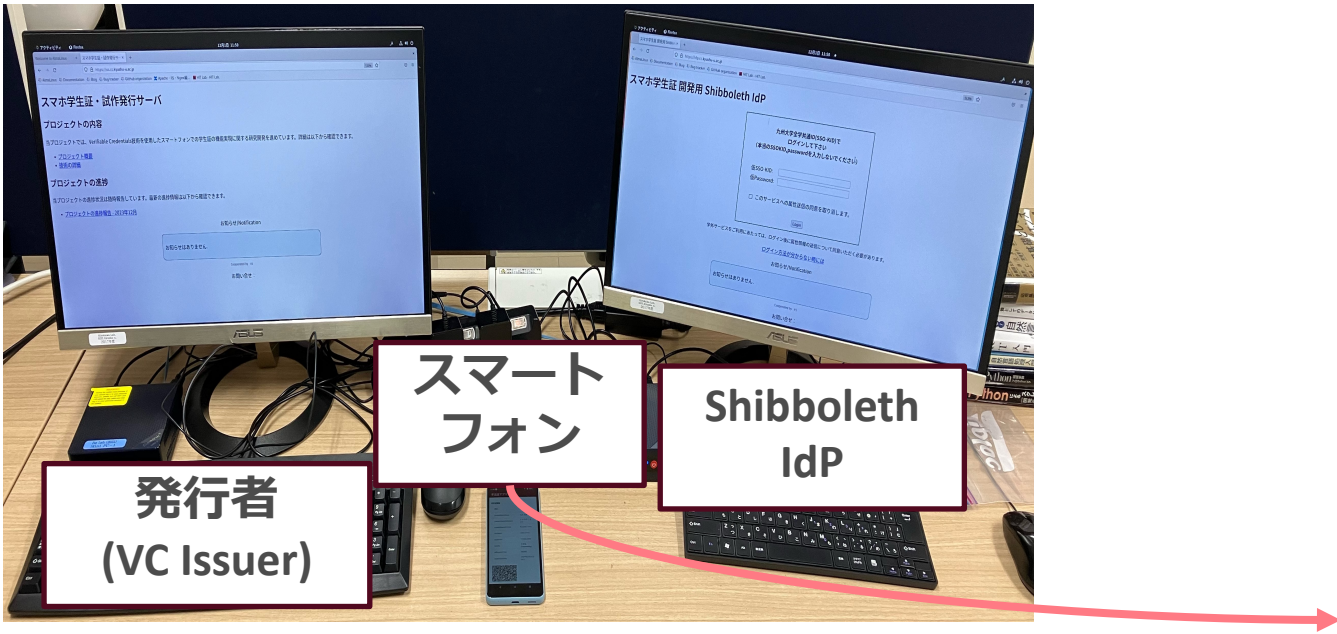


個人情報を提供

5. 試作システム

1. はじめに
2. 関連技術と先行事例
3. デジタル学生証の要求要件
4. 方針と設計
5. 試作システム
6. スマホログイン
7. おわりに

試作システム

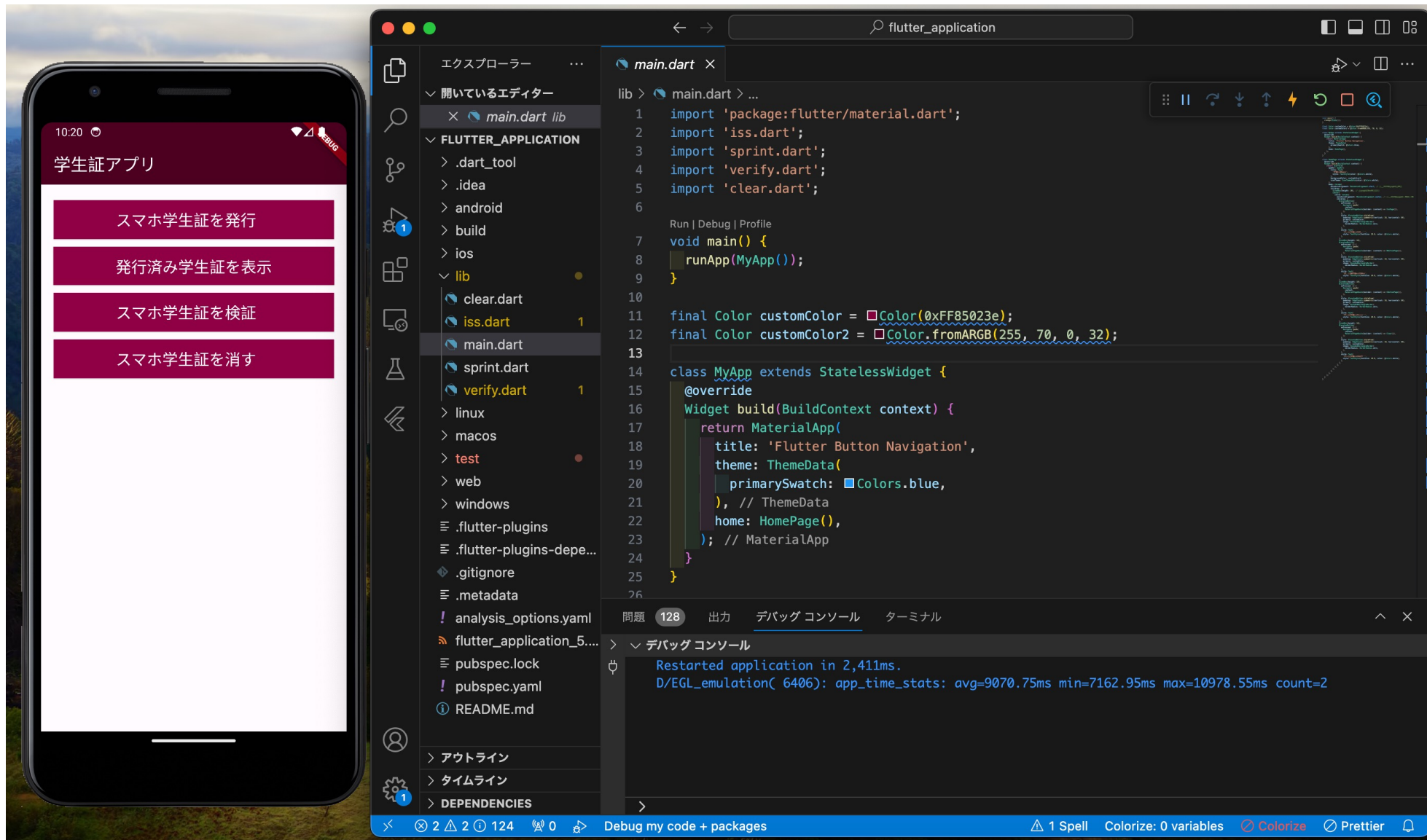


	発行者 (VC Issuer)	スマートフォン	Shibboleth IdP
機種	Beelink MINI-S12 N95	Sony Xperia ACE II SO-41B	Beelink MINI-S12 N95
OS	Alma Linux	Android	Alma Linux
Webサーバ	Apache	—	Apache
その他特徴	Shibboleth SP	Flutter App	LDAP

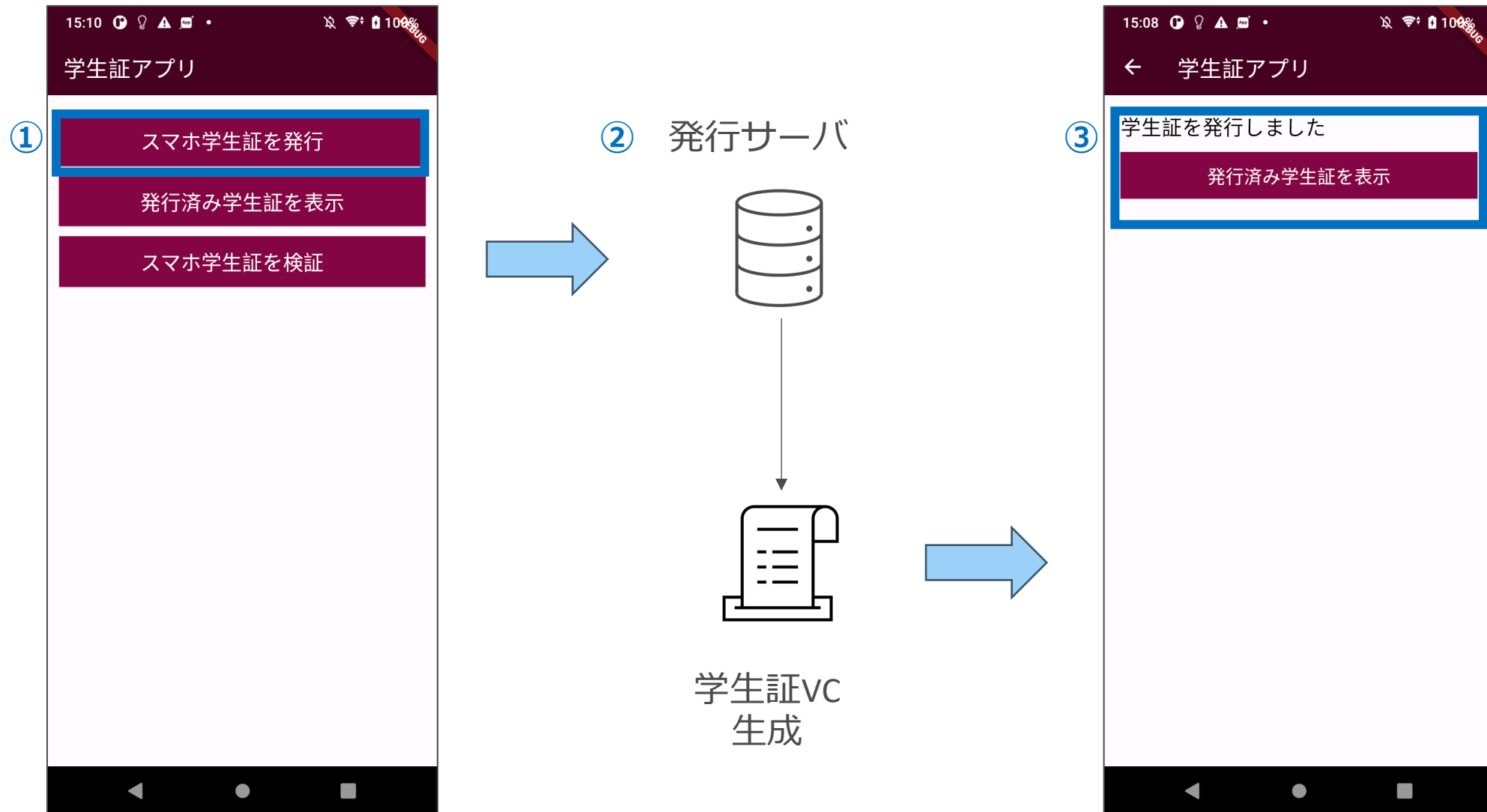


アプリ開発画面

Flutter (Dart言語)



発行

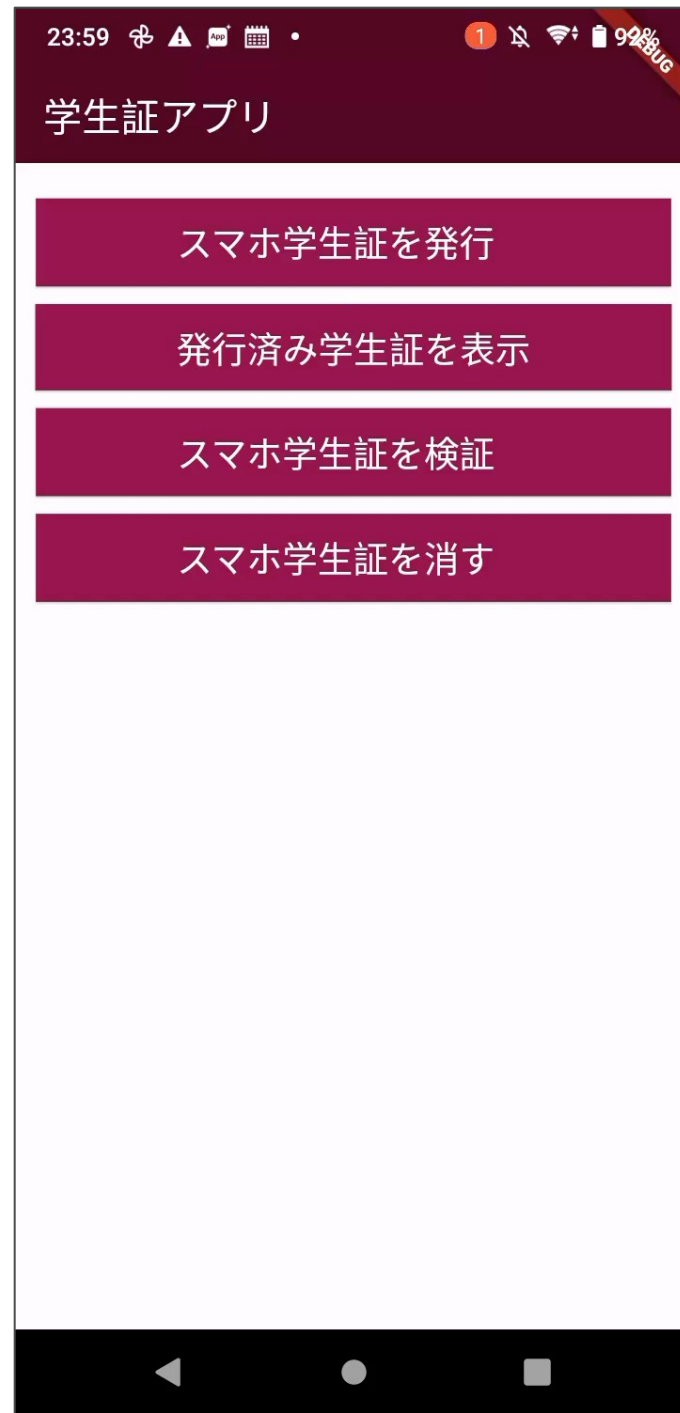


表示



検証

1. ホーム画面から『スマホ学生証を検証』を押す
2. 学生証検証画面から『スキャンを開始』を押す
3. 学生証の検証用QRコードを読み取る
4. QRコードの文字列（JWS）を表示
5. 『検証開始』を押す
6. スキャンした文字列が正しいJWSの形であるかを判断
7. 『次のステップに進む』を押す
8. JWSのペイロードとヘッダからハッシュ値を計算して表示
9. 『次のステップに進む』を押す
10. ハッシュ値と署名が等しいかを調べ結果を表示



6. スマホログイン

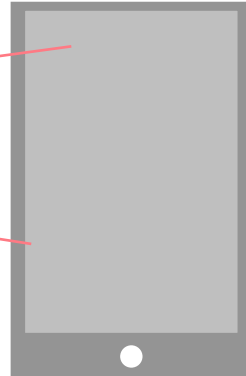
1. はじめに
2. 関連技術と先行事例
3. デジタル学生証の要求要件
4. 方針と設計
5. 試作システム
6. スマホログイン
7. おわりに

6. スマホログイン

PC用LINEアプリ



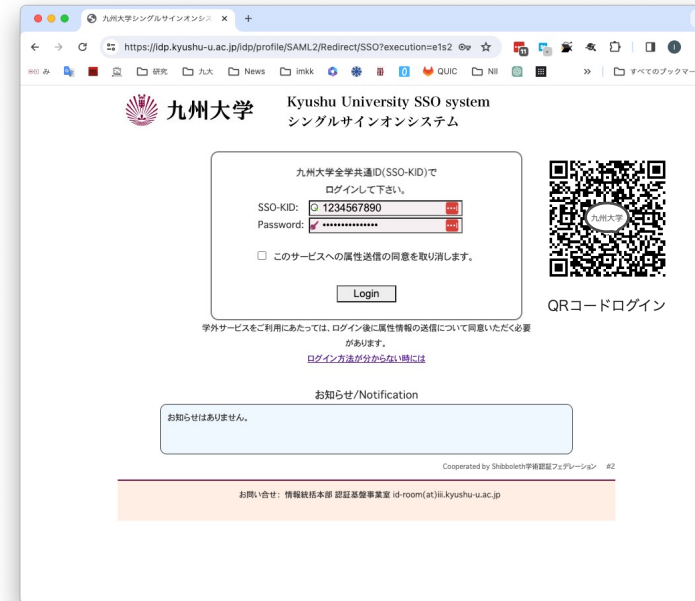
スマホのLINEアプリ
でQRコードを読み取る



<https://line.me/R/au/lgn/sq/SQ6e5434325a417a41375146646868776448426473615463564c4a486c51446e63?secret=N29PBsGalIVoA0uF9jIWlymnT14H9M%2F%2BfUoyU8aKEiQ%3D&e2eeVersion=1>

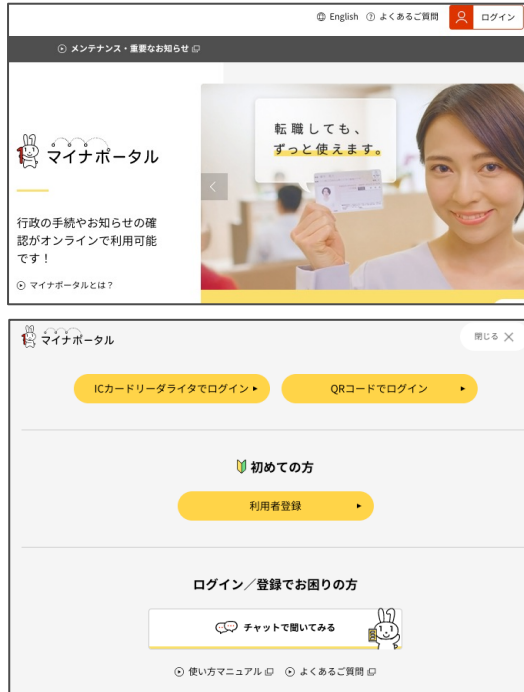
たぶん、青字がIDで、赤字がチャレンジ情報。

学内認証基盤のShibboleth IdPで、
ログイン用のQRコード提示



QRコード読み取り
でログイン

マイナポータル <https://myna.go.jp/>



「マイナポータル」アプリ
でQRコード読み取り

↓
マイナンバーカード読み取り用
の「4桁PIN番号」入力

↓
マイナンバーカード
(ICカード) を読み取る

[https://myna.go.jp/SCK0124_01_001/SCK0124_01_001_Redirect.form?
accessKey=ca81e92822ac827ca452a85958463302e343748ed7d45123
3fc862a0eacadb16](https://myna.go.jp/SCK0124_01_001/SCK0124_01_001_Redirect.form?accessKey=ca81e92822ac827ca452a85958463302e343748ed7d451233fc862a0eacadb16)

7. おわりに

1. はじめに
2. 関連技術と先行事例
3. デジタル学生証の要求要件
4. 方針と設計
5. 試作システム
6. スマホログイン
7. おわりに

7. おわりに

- デジタル学生証・職員証をスマートフォンで使いたい。
- 検証可能な資格情報 (Verifiable Credential) としての実現を検討
 - 要求要件, 方針, 設計を検討した
- 試作システムを作成中
 - Shibboleth IdPと連携するサーバ (ジェイズ・コミュニケーション社との共同研究)
 - Android アプリの試作
- まだまだ問題がたくさん

「九州大学（非公式）」アプリ

- Kaede Games制作
 - 学生証のバーコードを表示可能
 - カード学生証のバーコードをカメラ読み込む
 - 大学のお知らせ表示
 - 過去問検索機能
 - ICカード(NFC)の機能なし。
VCの機能なし。
- 使いやすくて、とても良い。



iOS AppStore	https://apps.apple.com/app/id1585354025
Android GooglePlay	https://play.google.com/store/apps/details?id=com.kaede.KyushuUniversity

仕様が確定したら、スマホアプリの制作を依頼したい！

残る課題

- 電子署名用秘密鍵（公開鍵）の有効期限
 - **学生証の期限より、鍵の有効期限が短い**
 - 署名の鍵が無効化されてしまう。
 - 学生証画面に表示する有効期限とは別に、
 - exp有効期限で、学生証VC再発行を促す仕組み
- 本人確認の弱さ
 - マイナカードの本人確認を使いたい
- 顔写真
 - 大学側データを渡す方法、自撮り
- なりすまし・偽造の防止
 - スクショ防止に、表示画面をアニメーションで動かす
- 学生証失効と記載内容変更
 - 検証時に失効は確認できる。
 - アプリへPush通知する機能。
- ICカード (NFC) 機能
 - スマホのNFCを機能を使えば、
 - ICカード学生証の機能を実現できる？
- VC検証機構の共通化
 - 大学間で共通化すると、なにか嬉しいことが有るだろうか？
 - 共通の入館手続き
 - ISMSな管理ゾーンへの入室
- デジタル名刺と名刺交換
 - 検証可能な名刺として使えそう。
 - 相手に渡せば名刺交換にもなりそう。