Verifiable Credential に基づく 検証可能で選択的リンク可能な Linked Data

山本 暖[1,a)]　須賀 祐治[1]

概要：Verifiable Credential (VC) を活用したサービスの提供が国内外で広がり始めている．VC は利用者の属性を含み，発行者による署名が付与されたクレデンシャルである．プライバシー保護に特化した Anonymous Credential としての側面と， 複数データ間のリンクやデータへの明確な意味付けを容易にする Linked Data としての側面を併せ持つ．しかしながら，既存の仕様や実装はこれらの部分的な利用に留まっている．本稿では両特性を活用した Selectively Linked Verifiable credential System (SeLVeS) という概念を具体的な構成法とともに提案する．SeLVeS は従来方式の課題を克服し，VC に含まれる識別子の秘匿や VC 間の選択的リンク，さらには選択的開示以外のゼロ知識証明を可能とする．これにより，利用者は自身の個人データを含む VC と外部の公開された VC を匿名性を保ったまま結合し，自身に関して証明可能な範囲を拡張することができる．

キーワード：Verifiable Credentials, Anonymous Credentials, Linked Data, アイデンティティ

Linked Data with Verifiability and Selective Linkability based on Verifiable Credentials

Dan Yamamoto[1,a)]　Yuji Suga[1]

Abstract: A number of emerging services based on Verifiable Credentials (VCs) have been proposed internationally. VCs are credentials including users' attributes with issuers' digital signatures. In addition to privacy-enhancing features based on anonymous credentials, VCs have the characteristics of Linked Data, which enable us to link multiple data with semantic interoperability. However, current specifications and implementations of VCs do not cover these whole aspects at the same time. We propose the concept and construction of Selectively Linked Verifiable credential System (SeLVeS) fully utilizing these two aspects of VCs. SeLVeS overcomes the limitation of previous work to provide hidden identifiers, selective linking, and zero-knowledge proofs. We can link our private VCs to public VCs in an anonymized fashion to extend provable range of claims to be verified.

Keywords: Verifiable Credentials, Anonymous Credentials, Linked Data, Identity

1. はじめに

中央集権型のアイデンティティ管理とは異なるアプローチとして，自己主権型アイデンティティ (Self-Sovereign Identity) が注目を集めている．Verifiable Credential (VC) はこれらの中核をなす技術要素である．データモデル仕様 [20] が W3C で標準化され，ワクチン接種証明書への応用やクラウドサービスの試験提供など実用化に向けた動きが加速している．

VC は，対象者 (Subject) に対して発行者 (Issuer) が作成した主張 (Claim) の集合に，発行者がデジタル署名を付与したデータである．例えば，運転免許証の VC は対象者 (免許証の持ち主) に対して発行者 (都道府県の公安委員会) が主張する Claim の集合 (持ち主の氏名，住所，生年月日，

[1] 株式会社インターネットイニシアティブ
Internet Initiative Japan Inc.
[a)] dan@iij.ad.jp

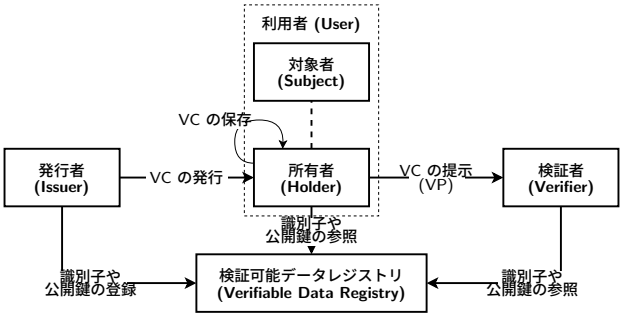

図 1: VC に関わるロールと情報の流れ

Fig. 1 The roles and information flows related to VCs.

顔写真，運転できる車の種類等) に発行者 (都道府県の公安委員会) のデジタル署名が付与されたデータとなる．

VC に関わるロールは図 1 のように整理される．発行者は対象者の属性を含む VC を発行し，所有者 (Holder) に受け渡す．所有者は受け取った VC を自身の ID ウォレット (VC 格納用のアプリケーション) に格納する．多くの場合，対象者と所有者は同一人物である．本稿では，両者を同一視する場合にこれを利用者 (User) と呼ぶこととする[*1]．所有者は検証者 (Verifier) からの要求に応じて，格納した一つあるいは複数の VC を ID ウォレットから取り出し，必要な属性のみを抽出した上で，これらを Verifiable Presentation (VP) と呼ばれるデータにまとめ，検証者へ提示する．検証者は発行者の公開鍵を用いて，VP に含まれるクレデンシャルが確かに発行者によるものであることを検証する．以上の流れの中で，発行者の識別子や公開鍵は，ブロックチェーン等を用いて実装される検証可能データレジストリを介してやり取りされる．

VC は Anonymous Credential [6, 7, 10] や Privacy-enhancing Attribute-Based Credential (PABC) [5] の成果を技術的な土台とし，偽造不可能なデジタル署名に加えて，ゼロ知識証明を用いたプライバシー保護の仕組みを備えている．例えば，氏名や住所を隠しながら普通自動車の運転資格を持つことだけを示したり，生年月日を明かすことなく年齢が 20 歳以上であることを示すような利用法が想定されている．前者は属性の選択的開示，後者は範囲証明と呼ばれる．加えて，所有者の行動が，発行者間，検証者間，さらには発行者と検証者の間で追跡されないよう，クレデンシャルのリンク不能性も考慮されている．

VC はデータとデータをリンクすることで “データの Web” を形成する Linked Data としての側面も備えている．RDF (Resource Description Framework) [19] と同じグラフ型のデータモデルに従い，Linked Data 用の JSON である JSON-LD [12] を使ったデータ表現が可能[*2]である．JSON-LD として記述された VC は拡張性と相互運用性に優れたデータ定義が可能になるとともに，複数 VC 間のリンクが容易となる．

これら Anonymous Credential と Linked Data の両特徴を活かした方式として，LDP-BBS+ [14] 方式が提案されている．当該方式は JSON-LD 型の VC に BBS+ 署名 [1, 4, 7] を適用し，属性の選択的開示を可能とする．従来方式に比べて事前準備が少なく，構成がシンプルで実装容易性にも優れるため，近年コミュニティによる標準仕様の策定や試験実装が進められている．しかしながら，匿名化の範囲に一部制限が存在し，選択的開示以外のゼロ知識証明を扱うことができない．また，クレデンシャルに含まれる識別子の秘匿や，複数クレデンシャル間のリンクの選択的開示など，Linked Data の特性を活かすための機能がまだ十分でないという課題も有している．

1.1 貢献

本稿では，選択的にリンクされた VC のシステム (Selectively Linked Verifiable credential System; SeLVeS) という概念と，その具体的な構成法を提案する．SeLVeS は JSON-LD 型の VC に関する従来方式の課題を克服し，VC に含まれる識別子の秘匿や VC 間の選択的リンク，さらには選択的開示以外のゼロ知識証明を可能とするものである．SeLVeS によって，個人に紐づく VC (Private VC) を，行政機関や企業によって公開される VC (Public VC) と選択的にリンクさせ，プライバシーを保護したまま自身に関して証明可能な Claim を拡張できることを，ユースケース例に基づいて示す．これは，検証可能な “データの Web” によって我々のデジタルアイデンティティを拡張する試みともみなせる．SeLVeS の構成にあたっては，従来の LDP-BBS+ を改良したエンコーディング方式を導入し，当該方式と既存の PABC システムを結合することで SeLVeS が構成可能であることを示す．

1.2 関連研究

Hyperledger Indy[*3] は CL 署名 [6] を用いて，属性の選択的開示や範囲証明を備えた VC の実装を提供している．しかしながらデータ構造は JSON-LD とは異なる独自形式に準ずるとともに，スキーマ情報の事前登録が必要など，データ構造の柔軟性や Linked Data としての活用に適さない側面を有する．

BBS+ 署名 [1, 4, 7] を JSON-LD 型 VC への署名に適用した LDP-BBS+ 方式はこうした点を補完するものとして期待され，現在 W3C の Credentials Community Group において標準化に向けた議論が続けられている [14]．BBS+ 署名は Boneh, Boyen, Shacham によるグループ署名 [2] を Anonymous Credential 用に拡張したものである．文書

[*1] W3C 仕様 [20] では定義されていない．

[*2] W3C 仕様 [20] には，JSON-LD だけでなく JWT (JSON Web Token) を使ったデータ表現も併記されている．

[*3] `https://www.hyperledger.org/use/hyperledger-indy`

の列に対する署名が可能で，各文書に対する開示，非開示の選択や種々の (離散対数ベースの) ゼロ知識証明を効率的に構成できる．ペアリングを利用し，安全性は q-SDH (Strong Diffie-Hellman) 仮定の下で示されている．類似の特徴をもつ署名として Pointcheval-Sanders (PS) 署名 [17] や，PS 署名に墨塗り機能を加えた [18] も存在するが，これらは q-SDH 仮定よりも一般的でない仮定に安全性が帰着されている．

一方, Linked Data に特化しない, より一般的なグラフ情報に対するデジタル署名, いわゆるグラフ署名やその Anonymous Credential への応用も提案されている [11,16,22–24]. グラフ情報を CL 署名や BBS+ 署名への入力にエンコードする際, [16,23,24] ではペアリングベースのアキュムレータを，[22] では Monipoly [21] と呼ばれる方法を用いて，いずれもグラフの点や辺の数に依存しない証明サイズや検証時間を実現している．ただし，本稿の対象とする Linked Data をこうした一般的なグラフ情報に変換する方法や，複数の発行者による署名付きグラフを選択的にリンクする方法については自明でない．

2. 準備

2.1 記法

自然数 n に対し，$[n]$ で集合 $\{1,2,\ldots,n\}$ を表す．$(x_i)_{i\in[k]}$ または $(x_i)_{i=1}^{k}$ でベクトル $(x_1,\ldots,x_k)$ を表記する．

2.2 Privacy-enhancing Attribute-Based Credential (PABC) システム

PABC システム [5] は Anonymous Credential システムの多様な機能をカバーした包括的な概念である．本稿では議論を簡潔にするため，[5] の PABC システムから一部の機能を省略した軽量なモデル[*4]を用いる．

定義 1 Privacy-enhancing Attribute-Based Credential システム PABC は，システムパラメータ生成アルゴリズム spGen，発行者鍵生成アルゴリズム ikGen，利用者鍵生成アルゴリズム ukGen，発行トークン生成アルゴリズム itGen，発行トークン検証アルゴリズム itVf，発行プロトコル $\langle \mathsf{issue},\mathsf{obtain}\rangle$，提示アルゴリズム present，提示検証アルゴリズム verify から構成される．各アルゴリズムおよびプロトコルの定義を以下に示す．

- $\mathsf{spGen}(\lambda)\to\mathsf{prm}$: セキュリティパラメータ λ を入力として，システム共通の公開パラメータ prm を出力する．
- $\mathsf{ikGen}(\mathsf{prm})\to(\mathsf{isk},\mathsf{ipk})$: 公開パラメータ prm を入力として，発行者の秘密鍵 isk と公開鍵 ipk を出力する．
- $\mathsf{ukGen}(\mathsf{prm})\to\mathsf{usk}$: 公開パラメータ prm を入力として，利用者の秘密鍵 usk を出力する．
- $\mathsf{itGen}(\mathsf{prm},\mathsf{usk},\mathsf{scope},\mathsf{ipk},(a_{i,j})_{j=1}^{n_i},M)\to(\mathsf{nym},\mathsf{pit},\mathsf{sit})$: 公開パラメータ prm，利用者の秘密鍵 usk，仮名のスコープ scope，発行者公開鍵 ipk，署名対象の属性 $(a_{i,j})_{j=1}^{n_i}$，リプレイ攻撃を防ぐための nonce M (発行者が指定する) を入力として，仮名 nym，公開発行トークン pit，秘密の発行トークン sit を出力する．
- $\mathsf{itVf}(\mathsf{prm},\mathsf{nym},\mathsf{pit},\mathsf{scope},\mathsf{ipk},(a_{i,j})_{j=1}^{n_i},M)\to\top/\bot$: 公開パラメータ prm，仮名 nym，公開発行トークン pit，仮名のスコープ scope，発行者公開鍵 ipk，署名対象の属性 $(a_{i,j})_{j=1}^{n_i}$，リプレイ攻撃を防ぐための nonce M を入力として，仮名と公開発行トークンの検証を行った結果 $\top$ (受理) または $\bot$ (拒否) を出力する．
- $\langle\mathsf{issue}(\mathsf{isk},\mathsf{pit}),\mathsf{obtain}(\mathsf{sit})\rangle(\mathsf{prm})\to\langle\varepsilon,\sigma/\bot\rangle$: 発行者と所有者の間で実行されるプロトコル．発行者は公開パラメータ prm，発行者の秘密鍵 isk，検証済の公開発行トークン pit を入力として issue を実行し，所有者は公開パラメータ prm と秘密の発行トークン sit を入力として obtain を実行する．実行に成功すると所有者は署名値 te VC $\mathsf{vc}=(\mathsf{Id},\sigma)$ を得る．ここで σ は発行者によって生成されたデジタル署名である．失敗時には $\bot$ を得る．
- $\mathsf{present}(\mathsf{prm},\mathsf{usk},\mathsf{scope},(\mathsf{ipk}_i,\sigma_i,(a_{i,j})_{j=1}^{n_i},R_i)_{i=1}^{k},E,M)\to(\mathsf{nym},\mathsf{pt})$: 公開パラメータ prm，利用者の秘密鍵 usk，仮名のスコープ scope に加えて，$k\geq 1$ 個の発行者公開鍵 ipk_i，署名 σ_i，署名に対応する n_i 個の属性 $(a_{i,j})_{j=1}^{n_i}$，その中から開示する対象を指定する $R_i\subseteq\{1,\ldots,n\}$，証明する属性の同値関係 E，リプレイ攻撃を防ぐための nonce である $M\in\{0,1\}^*$ を入力として，検証者へ提示する仮名 nym と提示トークン pt を出力する．ここで E は属性のインデックス集合 $\{(i,j):1\leq i\leq k\wedge 1\leq j\leq n_i\}$ に関する同値関係で，提示が $a_{i,j}=a_{i',j'}$ という関係を実際の属性値は見せることなく証明しようとする場合に $((i,j),(i',j'))\in E$ を満たすものとする．
- $\mathsf{verify}(\mathsf{prm},\mathsf{nym},\mathsf{pt},\mathsf{scope},(\mathsf{ipk}_i,(a_{i,j})_{j\in R_i})_{i=1}^{k},E,M)\to\top/\bot$: 公開パラメータ prm，仮名 nym，提示トークン pt，仮名のスコープ scope に加えて，k 個の発行者公開鍵 ipk_i，開示された属性 $(a_{i,j})_{j\in R_i}$)，属性の同値関係 E，nonce M を入力として，検証結果 $\top$ (受理) または $\bot$ (拒否) を出力する．

安全な PABC は偽造不可能性とプライバシーを満たす必要がある．ここではその概略のみを示す．

偽造不可能性: 利用者が提示できるのは発行者が発行した属性のみである．

プライバシー: 検証者が提示から得られるものは利用者が意図的に開示した属性のみである．また，利用者による提示セッションは対応する発行セッションとリンクできない．さらに，同じクレデンシャル (またはその集合) を複数回提示したとき，それらはリンク不能である．

[*4] 失効確認とクレデンシャルのキャリーオーバーの機能については，本稿では扱わないため省略した．

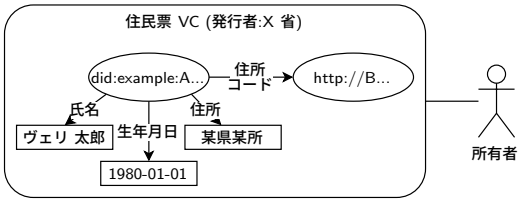

図 2: Private VC の例

Fig. 2 An example of a private VC.

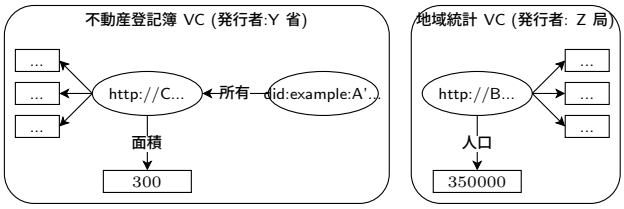

図 3: Public VC の例

Fig. 3 Examples of public VCs.

PABC システムの具体的な構成法としては CL 署名と Pedersen コミットメントを用いた安全な構成が [5] で示されている．一般的構成法で示されているため，CL 署名を BBS+ 署名に置き換えることも容易である．

3. SeLVeS のコンセプト

本稿では VC をその公開範囲に応じて Private VC と Public VC の 2 つに分類する．前者は対象者の個人的な属性を含む VC であり，所有者によって秘密に管理され，所有者の秘密鍵にバインドされる．一般に VC というとこちらを指すことが多い．後者は行政機関によって管理される公開台帳や，企業によって管理される製品仕様などの公開情報に対して発行者が署名を付与した VC である．特定の所有者にはバインドされない．発行者によって Web 上に公開され，誰もが取得，確認，検証可能である．両者は VC 内の `type` 属性等で区別可能であるとする．

本稿で提案する SeLVeS では，対象者に結びつく非公開の Private VC と，行政や企業などによって公開された Public VC をともに扱う．SeLVeS の利用者は，ゼロ知識証明を用いて匿名性を保ったまま両者を選択的にリンク可能とする．これにより，利用者の証明可能な主張を，本来は Private VC だけでは示せなかった範囲にまで拡張することが可能となる．

3.1 ユースケース

SeLVeS によって実現されるユースケースの一例を示す．

ここではある市民が，X 省によって発行された[*5]住民票 VC を自身の ID ウォレットに格納しているとする．図 2 に住民票 VC の例を示す．住民票 VC には，所有者の識別子が `<did:example:A...>`であり，氏名が “ヴェリ 太郎”，生年月日が “1980-01-01”，住所が “某県某所” であるという Claim が含まれる．加えて，本来の住民票には含まれないが，住所に対応する地域コードとして `<http://B...>` という URI も含まれるとする．

住民票 VC の所有者 (ヴェリ氏) は，ある検証者に対し，自身が面積 100 平米以上の土地を保有しており，かつ人口 20 万人以上の都市に住んでいることを証明する必要が生じたとする．ただし，所有者も検証者もそれ以外の不要な情報のやり取りは避けたいと考えている．

[*5] 発行者を市区町村長とすると，検証時に参照する発行者名等から対象者の住む市区町村が明らかであり，検証者に対して住所を秘匿したい場合に支障がある．

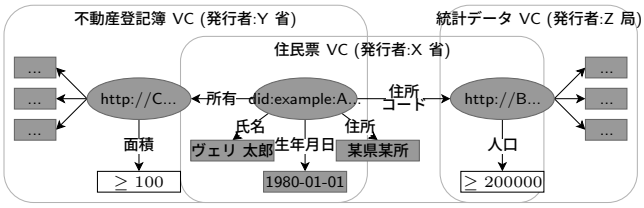

図 4: VP の例

Fig. 4 An example of a VP.

ここで，土地とその権利者の情報は行政機関である Y 省によって不動産登記簿として作成され，Y 省の署名が付与された VC として公開されているものとする．ここで，土地の権利者の ID は住民票 VC に記載された ID とは異なる仮名であっても良い．同様に，各地域の統計データは Z 局によって地域統計 VC として公開されているものとする．こちらは所有者の情報を含まない．

所有者は，自身と土地との関係を示す公開情報である不動産登記簿 VC を，発行者である Y 省の公開 web サイトから取得し，ID ウォレットに格納する．同様に，自身が住む地域に関する地域統計 VC を Z 局の web サイトから取得して格納する．図 3 にこれらを例示する．

所有者はウォレットの中でこれら 3 つの VC をリンクさせた VP を構成する．その際，今回の VP に必要のない属性はすべて非開示として処理を行う．リンクは同じ ID をもつノードを同一視することで得られる単純なリンクに加え，同じエンティティが持つ複数の仮名を同一視することで得られる仮名ベースのリンクが存在する．リンクの結果は図 4 に示すグラフとなり，これが VP に含められて検証者へ提示される．図中，灰色で網掛けを施したノードは非開示対象であり，検証者には渡らない点に注意すること．

ここで検証者は X 省，Y 省，Z 局を信用しているものとする．検証者は X 省，Y 省，Z 局の公開鍵を検証可能データレジストリ等から取得し，これらを使って所有者の提示した部分グラフを検証する．検証が成功すれば，検証者は「所有者が面積 100 平米以上の土地を所有しており (Y 省が保証)，かつ人口 20 万人以上の都市 (Z 局が保証) に住んでいる (X 省が保証)」という Claim を受け入れることとなる．

このように，適切な Public VC を集めて Private VC とリンクさせることで，対象者と他のエンティティの関係，さらには当該エンティティの属性をも含む主張を示すことが可能となる．これは本来 Private VC だけでは示せなかった主張であり，VC の Linked Data としての性質を活用することで初めて可能となったものである．また，Public VC をそのままの形で検証者には渡していないことに注意すること．本ユースケースでは，Public VC をそのまま検証者に渡した場合，利用者の保有する土地や利用者が住む場所を厳密に特定することが可能となってしまう．ウォレット内で処理をすることで，Private VC とのリンクだけを残して，その他の情報は非開示とすることでこうした特定を避けることができる．

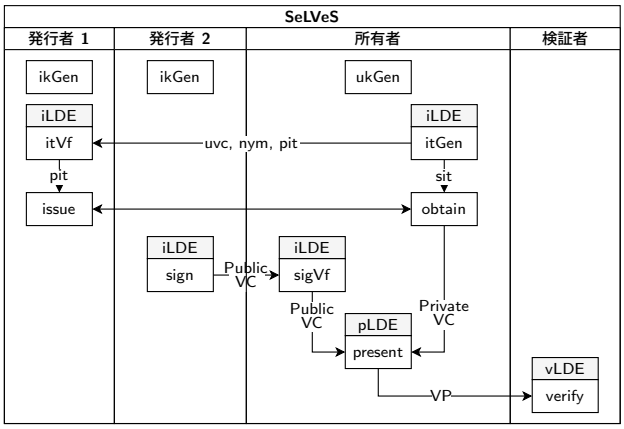

図 5: SeLVeS の実行シーケンスの例
Fig. 5 An example of a SeLVeS user sequence.

3.2 要件

上記のユースケースを実現するためには，SeLVeS は以下の機能を有する必要がある．

選択的開示機能 VC に含まれる属性や URI について，所有者は開示する否かを選択できること．

範囲証明機能 VC に含まれる属性は，値を隠したまま，その値がある範囲に含まれることを証明可能であること．

選択的リンク機能 Public VC と Private VC は所有者によって項目レベルでのリンクが可能であること．また，リンクに付随する識別子 (URI) は隠したままリンクの存在だけを証明可能であること．さらに，VC の所有者は自身の複数の仮名も選択的にリンク可能であること．加えて，Public VC と Private VC は所有者の仮名に基づく選択的なリンクも可能であること．

また，安全性に関しては以下の要件を満たす必要がある．

偽造不可能性 発行者が発行していない VC を含む VP は検証者によって受理されないこと．

リンク不能性 検証者に提示した VP と，VP に含まれる VC とは，所有者が開示した属性を除いてリンク不能であること．同様に，所有者が実行した複数の VP は，所有者が開示した属性を除いて互いにリンク不能であること．

4. SeLVeS の構成法

前節に示したユースケースを実現するための SeLVeS を構成する．

既存の BBS+ 署名や PABC システムは，クレデンシャルの属性をデータ列 $(a_i)_{i=1}^k$ として表現している．一方，LDP-BBS+ や SeLVeS の想定する属性は JSON-LD フォーマットに基づく構造化データである．これらのギャップを埋めるための処理，すなわち構造化された VC を一次元のデータ列に変換する処理を，本稿ではエンコーディングと呼ぶ．

本稿では LDP-BBS+ 方式で使われるエンコーディング方式を拡張することで，PABC システムの豊富な機能を Linked Data としての VC へ適用可能とする．提案する拡張エンコーディング方式は，発行時，提示時，検証時に対応する 3 種類存在し，それぞれ iLDE, pLDE, vLDE と呼ぶ．エンコーディングの詳細は後述する．

4.1 概要

拡張エンコーディングと PABC システムによって構成された SeLVeS の実行の流れを図 5 に例示する．

ここで，発行者 1 は所有者に対して Private VC を発行する発行者であり，前述のユースケースにおける X 省に対応する．一方，発行者 2 は Public VC を公開する発行者で，ユースケースにおける Y 省または Z 局に対応する．所有者は，発行者 2 によって公開された Public VC を取得，検証した上で，発行者 1 によって発行された Private VC とリンクさせることで VP を構成し，検証者へ提示する．検証者は所有者によって VP を提示されると，発行者 1 と発行者 2 の公開鍵を用いて VP を検証する．

発行者 1 と発行者 2 は PABC の ikGen を用いて，各自の秘密鍵と公開鍵を生成する．発行者は公開鍵を検証可能データレジストリに登録し，所有者と検証者から参照可能な状態にする．

所有者は PABC の ukGen を用いて自身の秘密鍵を生成する．その後，発行希望の属性を含む署名前 VC uvc を用意し，これを発行時 LD エンコーディング iLDE に通した上で PABC の itGen に与えることで，発行者 1 に対して名乗る仮名 (発行者 1 の仮名スコープに対応する仮名) nym と発行トークン $(\mathsf{pit}, \mathsf{sit})$ を生成する．そして，発行者 1 に uvc, nym と pit を送ることで VC の発行を依頼する．

発行者 1 は受け取った uvc を iLDE を使って $(a_i)_{i=1}^k$ へエンコードし，nym，pit とともに PABC の itVf で検証する．検証に失敗した場合は発行処理を中断する．検証に成功した場合は，$(a_i)_{i=1}^k$ を PABC の issue へ加えて実行

する．所有者は同様に sit を入力した obtain を実行する．両者の間で実行されたプロトコルが成功すると，所有者は PABC の署名 σ を得る．これを uvc に加えることで，署名済 Private VC vc を完成させる．作成された vc は所有者のウォレットに格納される．

一方，発行者 2 は同様に iLDE を入力部に追加した sign を実行することで Public VC を生成する．所有者は sigVf を実行して署名済 Public VC を検証した後，自身のウォレットに格納する．ここで，sign (または sigVf) は PABC システムには存在しないが，issue (または obtain) をそれぞれ非対話実行することで署名を生成 (または検証) する機能である．

所有者はウォレット内の Private VC および Public VC を，検証者へ提示する署名前 VP とともに提示時 LD エンコーディング pLDE に与え，present の実行に必要な入力を得る．そして検証者の仮名スコープや nonce を追加した上で present を実行し，得られた仮名 nym と提示トークン pt を基に署名済 VP vp を構成し，検証者へ送付する．

検証者は提示された vp を検証時 LD エンコーディング vLDE に通した上で PABC の verify を使って検証する．

4.2 Termwise LD エンコーディング

従来の LDP-BBS+ 方式では，JSON-LD 文書を Universal RDF Dataset Canonicalization Algorithm 2015 (URDNA2015) [13] に基づいて正規化された N-quads statement [8] の列に変換し，一つ一つの statement を署名対象メッセージとみなして BBS+ 署名を生成する．結果，選択的開示やゼロ知識証明の対象は statement 単位となり，statement 内に含まれる個々の値 (ID，氏名，生年月日等) を対象とした処理は実現できず，範囲証明のようなゼロ知識証明や ID の秘匿は実施できない．

本稿で提案する Termwise LD エンコーディングは，JSON-LD 文書を statement の列ではなく，各 statement を構成する 4 つの term，すなわち主語，述語，目的語，グラフラベルの列に分解する．これにより statement ではなく term を対象とする BBS+ 署名を生成でき，ゼロ知識証明の対象範囲が 1 段詳細化された結果，属性値を対象とした範囲証明などのゼロ知識証明が可能になる．また，複数の VC に含まれる URI 同士を，その値を隠したままそれらが同一であることを示すこともでき，結果として VC 間の選択的なリンクも可能となる．

以下，発行時，提示時，検証時に用いる 3 種類のエンコーディングを示す．各エンコーディングの説明にあたっては，図 6 に示す VC と VP の例を適宜参照する．

4.2.1 発行時 LD エンコーディング

VC の発行時に用いる LD エンコーディングを発行時 LD エンコーディング iLDE と呼び，以下のように定義する．

入力: VC vc

出力: 属性の配列 $(a_1, \ldots, a_n)$

(1) URDNA2015 [13] を用いて，入力された vc を正規化された N-quads statement の列 $(\mathsf{statement}_l)_{l=1}^{L}$ に変換する．ここで L は正規化の結果得られた statement の個数である．例えば図 6(a) に示した住民票 VC は，図 7 のような statement の列に変換される．

(2) 長さ $4L$ の空配列 A を初期化する．

(3) $l = 1, \ldots, L$ に対して，$\mathsf{statement}_l$ に含まれる主語，述語，目的語，グラフラベルを，この順に A へ追加する．例えば図 7 の statement からは，a_1 = `<did:example:A...>`, a_2 = `<...birthDate>`, a_3 = `"1980-01-01"`, $a_4 = \epsilon$[*6], a_5 = `<did:example:A...>`, ... が A に追加される．

(4) 長さ $n(= 4L)$ の配列 A を出力する．

iLDE は $(a_{i,j})_{j=1}^{n_i}$ を要求する itGen，itVf，sign，sigVf を実行する前に，vc から対応する $(a_{i,j})_{j=1}^{n_i}$ を得るために使われる．

4.2.2 提示時 LD エンコーディング

所有者が，署名済 VC 列から VP を生成する際に用いるエンコーディングを提示時 LD エンコーディング pLDE と呼ぶ．VP の生成には PABC システムの present を用いるため，pLDE の主な役割は署名済 VC 列などを present の実行に必要な入力へ変換することである．

VP の生成にあたっては，VC 中の非開示箇所を指摘しなければならない．既存の LDP-BBS+ 方式では，JSON-LD Framing [9] 仕様を用いて，VC から開示箇所のみを抽出する (結果，非開示箇所が捨てられる) 方法が採用されている．pLDE ではこれを踏襲しつつ，framing 処理の後に URI の置換処理を追加することで，リンクの匿名化を可能とする．

pLDE の定義を以下に示す．

入力: 署名済 VC $(\mathsf{vc}_i)_{i=1}^{k}$，開示範囲指定 $(\mathsf{frame}_i)_{i=1}^{k}$，非開示対象 URI 列 aURIs, システムパラメータ prm，所有者秘密鍵 usk，仮名スコープ scope，nonce M

出力: VP vp

(1) $(\mathsf{vc}_i)_{i=1}^{k}$ それぞれの `proof.verificationMethod` および `proof.proofValue` に記載された情報に基づいて，発行者公開鍵および署名の列 $(\mathsf{ipk}_i, \sigma_i)_{i=1}^{k}$ を得る．

(2) $(\mathsf{vc}_i)_{i=1}^{k}$ それぞれに対して $(\mathsf{frame}_i)_{i=1}^{k}$ に基づく framing を行い，開示対象のみを残した $(\mathsf{vc}'_i)_{i=1}^{k}$ を得る．

(3) $(\mathsf{vc}_i)_{i=1}^{k}$ および $(\mathsf{vc}'_i)_{i=1}^{k}$ をそれぞれ iLDE に通すことで全属性の列 $(a_{i,j})_{(i,j)\in[k]\times[n_i]}$ および開示対象属性の列 $(a'_{i,j})_{(i,j)\in[k]\times[n'_i]}$ を得る．

(4) $(a_{i,j})_{(i,j)\in[k]\times[n_i]}$ と $(a'_{i,j})_{(i,j)\in[k]\times[n'_i]}$ を比較することで，$(a'_{i,j})_{(i,j)\in[k]\times[n'_i]} = (a_{i,j})_{(i,j)\in[k]\times R_i}$ を満たす開示対象インデックス $R_i \subseteq [n_i]$ を求める．

[*6] 多くの場合，グラフラベルはデフォルトグラフを意味する空文字列 ϵ となる．

(a) 住民票 VC　(b) 不動産登記簿 VC　(c) 地域統計 VC

(d) VP 内の住民票部分　(e) VP 内の不動産登記簿部分　(f) VP 内の地域統計部分

図 6: JSON-LD で表現された VC および VP の例

Fig. 6 Examples of VCs and a VP as JSON-LD.

```
<did:example:A...>  <...birthDate>          "1980-01-01" .
<did:example:A...>  <...homeLocation>       <http"//B...> .
<did:example:A...>  <...name>               "ヴェリ 太郎" .
<https://X.../vc/1> <...credentialSubject> <did:example:A...> .
<https://X.../vc/1> <...issuer>            <https://X...> .
...
```

図 7: 住民票 VC から得た N-quads statement の例

Fig. 7 Examples of N-quads statements.

(5) 全属性 $(a_{i,j})_{(i,j)\in[k]\times[n_i]}$ から，非開示対象 URI aURI ($\in$ aURIs) が含まれる属性を特定し，当該属性のインデックスを R_i から除くとともに，属性の同値関係 E を算出する．

(6) $(\mathsf{vc}'_i)_{i=1}^k$ それぞれに含まれる非開示対象 URI aURI ($\in$ aURIs) を非開示シンボル (例えば "urn:anon:i") で置換したものを $(\mathsf{dc}_i)_{i=1}^k$ とする．R_i を dc_i 用に変換したものを R'_i とする．

(7) $\mathsf{present}(\mathsf{prm}, \mathsf{usk}, \mathsf{scope}, (\mathsf{ipk}_i, \sigma_i, (a_{i,j})_{j=1}^{n_i}, R_i)_{i=1}^k, E, M)$ を実行し，$(\mathsf{nym}, \mathsf{pt})$ を得る．

(8) $(\mathsf{dc}_i)_{i=1}^k$，nym，pt，$(R'_i)_{i=1}^k$ を VP として出力する．

4.2.3 検証時 LD エンコーディング

検証者が VP の検証時に用いるエンコーディングを検証時 LD エンコーディング vLDE と呼ぶ．vLDE の主な役割は VP を verify の入力へ変換することである．

入力: VP vp，システムパラメータ prm，仮名スコープ scope，nonce M

出力: 検証結果 $\top$ / $\bot$

(1) vp から $(\mathsf{dc}_i)_{i=1}^k$, nym，pt，R'_i を得る．

(2) $(\mathsf{dc}_i)_{i=1}^k$ と R'_i から $(a_{i,j})_{(i,j)\in[k]\times R'_i}$ を構成する．

(3) $(\mathsf{dc}_i)_{i=1}^k$ に含まれる非開示シンボルを基に属性の同値関係 E を再構成する．

(4) $(\mathsf{dc}_i)_{i=1}^k$ から発行者公開鍵の列 $(\mathsf{ipk}_i)_{i=1}^k$ を得る．

(5) $\mathsf{verify}(\mathsf{prm}, \mathsf{nym}, \mathsf{pt}, \mathsf{scope}, (\mathsf{ipk}_i, (a_{i,j})_{j\in R'_i})_{i=1}^k, E, M)$ を実行し，結果を出力する．

検証に成功した場合，検証者は $(\mathsf{dc}_i)_{i=1}^k$ の内，Private VC であることが明示されたもの (VC の type で判別可能) について，仮名 nym をもつ利用者に紐づく VC として扱う．これは，例えば図 6(d) と図 6(e) では urn:anon:2 と urn:anon:5 で ID を匿名化しているが，両者を同一視することに等しい．

4.3 評価

SeLVeS の機能要件の内，選択的開示機能，選択的リンク機能は上に示した構成で実現されていることが確認できる．範囲証明機能については，対象となる属性 $a_{i,j}$ のコミットメントを追加するとともに，当該コミットメントに対して Bulletproofs [3] 等を用いた効率的な範囲証明を構成することで可能である．

安全性要件に関しては，各エンコーディングがある種の衝突耐性を有するならば，SeLVeS の偽造不可能性は PABC の偽造不可能性に，SeLVeS のリンク不能性は PABC のプライバシーに，それぞれ帰着可能であると考えられる．厳密な安全性定義や帰着の議論については今後の課題とする．

SeLVeS の実装に関しては，LDP-BBS+ 方式の OSS 実装[*7] および Hyperledger Ursa[*8] の BBS+ 署名ライブラリに対して，本稿で示した 3 種の Termwise LD エンコーディングを追加することで容易に構成できる．

[*7] https://github.com/mattrglobal/jsonld-signatures-bbs/

[*8] https://github.com/hyperledger/ursa

5. まとめ

本稿では,選択的にリンクされた VC のシステム (SeLVeS) の概念を提案し，その要件を整理するとともに，Termwise LD エンコーディングとそれに基づく具体的な構成法を示した.

今後の課題として，より厳密な安全性定義と証明を与えることに加え，PABC がもつ機能の内，エンコーディングの対象に含めなかった失効確認等の追加が挙げられる．また，既存のグラフ署名 [16,22–24] や墨塗り署名 [18] と同様に効率的な証明サイズや検証時間の実現も望まれる．さらに，統計 LOD[*9] [15]，gBizINFO[*10]，DBPedia[*11] 等，実在する Linked Data を用いた有用性や拡張性の検証も求められる.

参考文献

[1] Au, M. H., Susilo, W. and Mu, Y.: Constant-Size Dynamic k-TAA, *SCN 06* (Prisco, R. D. and Yung, M., eds.), LNCS, Vol. 4116, Springer, Heidelberg, pp. 111–125 (2006).

[2] Boneh, D., Boyen, X. and Shacham, H.: Short Group Signatures, *CRYPTO 2004* (Franklin, M., ed.), LNCS, Vol. 3152, Springer, Heidelberg, pp. 41–55 (2004).

[3] Bünz, B., Bootle, J., Boneh, D., Poelstra, A., Wuille, P. and Maxwell, G.: Bulletproofs: Short Proofs for Confidential Transactions and More, *2018 IEEE Symposium on Security and Privacy*, IEEE Computer Society Press, pp. 315–334 (2018).

[4] Camenisch, J., Drijvers, M. and Lehmann, A.: Anonymous attestation using the strong diffie hellman assumption revisited, *International Conference on Trust and Trustworthy Computing*, Springer, pp. 1–20 (2016).

[5] Camenisch, J., Krenn, S., Lehmann, A., Mikkelsen, G. L., Neven, G. and Pedersen, M. Ø.: Formal Treatment of Privacy-Enhancing Credential Systems, *SAC 2015* (Dunkelman, O. and Keliher, L., eds.), LNCS, Vol. 9566, Springer, Heidelberg, pp. 3–24 (2016).

[6] Camenisch, J. and Lysyanskaya, A.: A Signature Scheme with Efficient Protocols, *SCN 02* (Cimato, S., Galdi, C. and Persiano, G., eds.), LNCS, Vol. 2576, Springer, Heidelberg, pp. 268–289 (2003).

[7] Camenisch, J. and Lysyanskaya, A.: Signature Schemes and Anonymous Credentials from Bilinear Maps, *CRYPTO 2004* (Franklin, M., ed.), LNCS, Vol. 3152, Springer, Heidelberg, pp. 56–72 (2004).

[8] Carothers, G.: RDF 1.1 N-Quads, W3C (online), available from ⟨https://www.w3.org/TR/2014/REC-n-quads-20140225/⟩ (accessed 2021-08-12).

[9] Champin, P.-A., Kellogg, G. and Longley, D.: JSON-LD 1.1 Framing, W3C (online), available from ⟨https://www.w3.org/TR/2020/REC-json-ld11-framing-20200716/⟩ (accessed 2021-08-12).

[10] Chaum, D.: Security without identification: Transaction systems to make big brother obsolete, *Communications of the ACM*, Vol. 28, No. 10, pp. 1030–1044 (1985).

[11] Groß, T.: Signatures and Efficient Proofs on Committed Graphs and NP-Statements, *FC 2015* (Böhme, R. and Okamoto, T., eds.), LNCS, Vol. 8975, Springer, Heidelberg, pp. 293–314 (2015).

[12] Kellogg, G., Longley, D. and Champin, P.-A.: JSON-LD 1.1, W3C (online), available from ⟨https://www.w3.org/TR/2020/REC-json-ld11-20200716/⟩ (accessed 2021-08-12).

[13] Longley, D.: RDF Dataset Canonicalization, W3C Credentials Community Group (online), available from ⟨https://json-ld.github.io/rdf-dataset-canonicalization/spec/⟩ (accessed 2021-08-12).

[14] Looker, T. and Steele, O.: BBS+ Signatures 2020, W3C Credentials Community Group (online), available from ⟨https://w3c-ccg.github.io/ldp-bbs2020/⟩ (accessed 2021-08-12).

[15] Matsuda, J., Mizutani, A., Asano, Y., Yamamoto, D., Takeda, H., Ohmukai, I., Kato, F., Koide, S., Harada, H. and Nishimura, S.: Publication of statistical linked open data in Japan, *Joint International Semantic Technology Conference*, Springer, pp. 307–319 (2018).

[16] Nakanishi, T., Yoshino, H., Murakami, T. and Policharla, G.-V.: Efficient Zero-Knowledge Proofs of Graph Signature for Connectivity and Isolation Using Bilinear-Map Accumulator, *Proceedings of the 7th ACM Workshop on ASIA Public-Key Cryptography*, pp. 9–18 (2020).

[17] Pointcheval, D. and Sanders, O.: Reassessing Security of Randomizable Signatures, *CT-RSA 2018* (Smart, N. P., ed.), LNCS, Vol. 10808, Springer, Heidelberg, pp. 319–338 (2018).

[18] Sanders, O.: Efficient Redactable Signature and Application to Anonymous Credentials, *PKC 2020, Part II* (Kiayias, A., Kohlweiss, M., Wallden, P. and Zikas, V., eds.), LNCS, Vol. 12111, Springer, Heidelberg, pp. 628–656 (2020).

[19] Schreiber, G. and Raimond, Y.: RDF 1.1 Primer, W3C (online), available from ⟨https://www.w3.org/TR/2014/NOTE-rdf11-primer-20140624/⟩ (accessed 2021-08-12).

[20] Sporny, M., Noble, G., Burnett, D., Longley, D. and Zundel, B.: Verifiable Credentials Data Model 1.0, W3C (online), available from ⟨https://www.w3.org/TR/2019/REC-vc-data-model-20191119/⟩ (accessed 2021-08-12).

[21] Tan, S.-Y. and Groß, T.: MoniPoly - An Expressive q-SDH-Based Anonymous Attribute-Based Credential System, *ASIACRYPT 2020, Part III* (Moriai, S. and Wang, H., eds.), LNCS, Vol. 12493, Springer, Heidelberg, pp. 498–526 (2020).

[22] Tan, S.-Y., Sfyrakis, I. and Gross, T.: A q-SDH-based Graph Signature Scheme on Full-Domain Messages with Efficient Protocols, Cryptology ePrint Archive, Report 2020/1403 (2020). https://eprint.iacr.org/2020/1403.

[23] 吉野大海, 中西透：ペアリングを用いたグラフ情報のゼロ知識証明，電子情報通信学会技術研究報告; 信学技報，Vol. 118, No. 279, pp. 87–93 (2018).

[24] 村上友樹, 中西透：ペアリングベースアキュームレータを用いたグラフ情報の分離性のゼロ知識証明，コンピュータセキュリティシンポジウム 2020 論文集，pp. 252–257 (2020).

[*9] https://data.e-stat.go.jp/lodw/

[*10] https://info.gbiz.go.jp/

[*11] https://www.dbpedia.org/