SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

Linked Data 型 Verifiable Credentials の構成と安全性

Linked Data based Verifiable Credentials: Security and Construction

山本 暖 * 須賀 祐治 * 佐古 和恵 †
Dan Yamamoto Yuji Suga Kazue Sako

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

あらまし

背景 自己主権型アイデンティティの中核的技術として，W3C 標準である Verifiable Credentials (VCs) が国内外で活用され始めている．VCs 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．VCs の実装には，Anonymous Credentials を応用することでユーザのプライバシを強化したものや，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 としての特徴を備えたもの等，複数の方式が提案され，コミュニティによる標準化やオープンソース開発が活発に行われている．例えば MATTR による LDP-BBS+ [4] 方式は，メッセージと署名値に関する効率的なゼロ知識証明が可能な BBS+ 署名 [1, 2] を利用して，Linked Data 型の VC で限定的な選択的開示を可能としている．また，LDP-BBS+ 方式を拡張し，限定のない選択的開示や，利用者の秘密に束縛されたクレデンシャル (bound クレデンシャル) とそうでないクレデンシャル (unbound クレデンシャル) の混在提示を可能とし，Linked Data の長所を最大限に活かした VCs の構成も提案されている [6].

課題 他方，Linked Data 型の VCs の安全性に関しては，現状，十分な評価がなされているとは言えない．従来の Anonymous Credentials の安全性モデルを用いた評価を行うためには，以下の 2 つの課題が存在する．第一に，従来の安全性モデル (e.g., [3, 5]) はクレデンシャルに含まれる属性を単純なベクトルまたは集合として表現しているため，より複雑な Linked Data 型の属性を扱えないこと．第二に，利用者による bound / unbound クレデンシャルの混在提示が想定されていないことが挙げられる．

貢献 本稿では，クレデンシャルに含まれる属性をベクトルの集合として表現することで，Linked Data としての属性が十分に記述可能となることを示す．その上で，利用者による bound / unbound クレデンシャルの混在提示を従来のモデルに導入し，Linked Data 型 VCs の安全性評価に利用可能な Anonymous Credentials の安全性モデルを定義する．次に，当該モデルを用いて [6] の構成の安全性を評価する．さらに，TypeScript / WebAssembly / Rust によるプロトタイプ実装を行い，標準的な Web ブラウザ上での実行が実用的に可能であることを示す．

参考文献

[1] M. H. Au, W. Susilo, and Y. Mu, “Constant-size dynamic k-TAA,” in *SCN 06*, ser. LNCS, R. D. Prisco, and M. Yung, Eds., vol. 4116. Springer, Heidelberg, Sep. 2006, pp. 111–125.

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

[3] J. Camenisch, S. Krenn, A. Lehmann, G. L. Mikkelsen, G. Neven, and M. Ø. Pedersen, “Formal treatment of privacy-enhancing credential systems,” in *SAC 2015*, ser. LNCS, O. Dunkelman, and L. Keliher, Eds., vol. 9566. Springer, Heidelberg, Aug. 2016, pp. 3–24.

[4] T. Looker, and O. Steele. (2021) BBS+ signatures 2020. W3C Credentials Community Group. https://w3c-ccg.github.io/ldp-bbs2020/

[5] O. Sanders, “Efficient redactable signature and application to anonymous credentials,” in *PKC 2020, Part II*, ser. LNCS, A. Kiayias, M. Kohlweiss, P. Wallden, and V. Zikas, Eds., vol. 12111. Springer, Heidelberg, May 2020, pp. 628–656.

[6] 山本 暖，須賀 祐治，“Verifiable credential に基づく検証可能で選択的リンク可能な linked data”，コンピュータセキュリティシンポジウム 2021 論文集，pp. 938–945，2021.

* 株式会社インターネットイニシアティブ, 〒 102–0071 東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム, Internet Initiative Japan Inc., Iidabashi Grand Bloom, 2-10-2 Fujimi, Chiyoda-ku, Tokyo 102–0071, Japan dan@iij.ad.jp
† 早稲田大学 基幹理工学部 情報理工学科