An Access Control System for Verifiable Credentials with Selective Disclosure

[*]Note: Sub-titles are not captured in Xplore and should not be used

1st Chun-An Lin
Graduate school of Natural Science & Technology
Kanazawa University
Kanazawa, Japan
kimlin20011@gmail.com

2nd Chen-Mou Cheng
Graduate school of Natural Science & Technology
Kanazawa University
Kanazawa, Japan
cheng@se.kanazawa-u.ac.jp

3rd Masahiro Mambo
Graduate school of Natural Science & Technology
Kanazawa University
Kanazawa, Japan
mambo@ec.t.kanazawa-u.ac.jp

***Abstract*—It is important for access control mechanisms to consider both authentication and authorization components to enhance privacy and security. User-Managed Access (UMA) is an access control profile supporting (1) party-to-party sharing that allows the resource owner to authorize the resource to the third-party and (2) customization of access control policy which means resource owner can formulate the policy for accessing the protected resource. However, although the UMA profile defines the authorization process, it does not specify the detail part for authentication. To fill this gap, it is necessary to import digital credential technology to authenticate the third party. Therefore, this paper proposes VC-UMA, an access control mechanism integrating UMA with Verifiable Credentials (VC). VC is an open standard of decentralized credentials which often constructed on the blockchain that allowing user to fully control their credentials. Besides, selective disclosure mechanism is integrated into VC-UMA to address the privacy concerns raised by sharing VCs. To prove the feasibility of the VC-UMA, the proof of concept is conducted. Specifically, a prototype system is implemented and the experiments of the performance is presented.**

***Index Terms*—User-Managed Access, Verifiable Credentials, Access Control, Selective Disclosure, Blockchain**

I. Introduction

Access Control [1] is a mechanism responsible for managing the requests that want to access protected resources. Without proper access control mechanisms, internet services are prone to various privacy and security issues. For instance, invalid access to protected resources, or leakage of privacy data during the access control process.

User-Managed Access (UMA) [2] is a party-to-party right delegation profile extension for access control. In UMA, users can not only formulate the customized access control policy [3] but also realize the *Party-to-Party Sharing* scenario. Nevertheless, according to Sandhu [4], secure access control requires several important components namely, *Authorization*, *Authentication*, *Auditing*, etc. Especially, authorization and authentication play extremely important roles in the process of user access to the protected resources. However, UMA profile only defines the claim gathering concept for the authentication part which means the user needs to provide the claim to get authentication, but the trust model among all the entities is out of scope. For example, as a resource owner, the problem of *how can I trust the third party to access the resources?* cannot be solved only by employing the UMA profile.

To solve the above problems, this paper adopts Self-Sovereign Identity (SSI), a promising concept that is regarded as the next generation of digital identity [5]. This concept allows individuals fully control of their digital identities and credential. Among SSI, Verifiable Credential (VC) [6] is a core technology that is the digital credential framework of following the SSI principle and specifies by the World Wide Web Consortium (W3C). VC utilizes digital signature technology often together with the blockchain which is a distributed ledger platform with decentralized, immutable, and traceable features. With the wide acceptance of VC, privacy has become an important issue. Regarding the privacy issue, W3C recommends developers follow the data minimization principle [7] when designing VC services. This means that when presenting VCs, is it better to minimize the exposed data to prevent oversharing of the privacy credentials.

Based on the above observations, this paper aims to propose a Verifiable Credential-enabled User-Managed Access Mechanism (VC-UMA) that overcomes the lack of trust authentication model defined in the UMA profile by introducing the advantages of the VC framework. Additionally, in order to reduce the risk of private data leakage when sharing VCs, this paper adopts the selective disclosure technology so that VC holder can redact the private part of data in VC to follow the data minimization principle. To summarize, this paper claims the following contribution.

- **An access control mechanism based on decentralized credential scheme is presented.** This paper proposes a new access control mechanism: VC-UMA based on the W3C's VC model [6] and the UMA Profile [2]. Besides, the relationship and the trusted model among all entities in UMA and VC is reconsidered. Moreover, the guidelines for implementing VC-UMA are provided

Identify applicable funding agency here. If none, delete this.

in static and dynamic ways.

- **Selective disclosure method to achieve the data minimization principle for VC sharing is considered.** Considering the part of privacy-preserving VC sharing, we adopt the selective disclosure methods provided by W3C, a selective disclosure authentication flows is proposed.
- **A use case of VC-UMA has been proposed and implemented as the prototype system as proof of concept.** In order to prove the feasibility and usability of the proposed mechanism, the proof of concept research method is conducted. The implemented prototype system is presented. Furthermore, the performance of the system is analyzed.

II. Background and Related Work

A. User-Managed Access

UMA is an access control profile base on OAuth2 [9], proposed by Kantara Initiative and published on Internet Engineering Task Force (IETF) [2]. OAuth2 is a widely used third-party authorization protocol, but this protocol doesn't cover the party-to-party sharing scenarios. For instance, Alice wants to use the service of photo editing software (playing the role of resource access client), so she authorizes her photos (resource) stored in the third-party cloud service to the photo editing software. However, OAuth2 doesn't support Alice to grant Bob to access her photos on the third-party cloud service. UMA fills the gap of OAuth2 that doesn't define the party-to-party authorization scenario. UMA profile is composed of several entities, the definitions of which are shown in table I.

TABLE I: Entities in User-Managed Access

UMA entities	description
Resource Owner (RO)	The owner of the protected resource.
Requesting Party (RqP)	The party who is attempting to access the protected resource.
Client	A third-party application that proxy the RqP to access protected resources.
Resource Server (RS)	The resource server stores protected resources and is capable of handling resource requests from client.
Authorization Server (AS)	The Authorization server is delegated by the RO to protect resources stored in RS and authorizes resource requests issued by RqP.

III. Prepare Your Paper Before Styling

Before you begin to format your paper, first write and save the content as a separate text file. Complete all content and organizational editing before formatting. Please note sections III-A–III-E below for more information on proofreading, spelling and grammar.

Keep your text and graphic files separate until after the text has been formatted and styled. Do not number text heads—LaTeX will do that for you.

A. Abbreviations and Acronyms

Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, ac, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

B. Units

- Use either SI (MKS) or CGS as primary units. (SI units are encouraged.) English units may be used as secondary units (in parentheses). An exception would be the use of English units as identifiers in trade, such as "3.5-inch disk drive".
- Avoid combining SI and CGS units, such as current in amperes and magnetic field in oersteds. This often leads to confusion because equations do not balance dimensionally. If you must use mixed units, clearly state the units for each quantity that you use in an equation.
- Do not mix complete spellings and abbreviations of units: "Wb/m^2" or "webers per square meter", not "webers/m^2". Spell out units when they appear in text: ". . . a few henries", not ". . . a few H".
- Use a zero before decimal points: "0.25", not ".25". Use "cm^3", not "cc".)

C. Equations

Number equations consecutively. To make your equations more compact, you may use the solidus (/), the exp function, or appropriate exponents. Italicize Roman symbols for quantities and variables, but not Greek symbols. Use a long dash rather than a hyphen for a minus sign. Punctuate equations with commas or periods when they are part of a sentence, as in:

$$a + b = \gamma \tag{1}$$

Be sure that the symbols in your equation have been defined before or immediately following the equation. Use "(1)", not "Eq. (1)" or "equation (1)", except at the beginning of a sentence: "Equation (1) is . . ."

D. LaTeX-Specific Advice

Please use "soft" (e.g., `\eqref{Eq}`) cross references instead of "hard" references (e.g., `(1)`). That will make it possible to combine sections, add equations, or change the order of figures or citations without having to go through the file line by line.

Please don't use the `{eqnarray}` equation environment. Use `{align}` or `{IEEEeqnarray}` instead. The `{eqnarray}` environment leaves unsightly spaces around relation symbols.

Please note that the `{subequations}` environment in LaTeX will increment the main equation counter even when there are no equation numbers displayed. If you forget that, you might write an article in which the equation numbers skip from (17) to (20), causing the copy editors to wonder if you've discovered a new method of counting.

BibTeX does not work by magic. It doesn't get the bibliographic data from thin air but from .bib files. If you use BibTeX to produce a bibliography you must send the .bib files.

LaTeX can't read your mind. If you assign the same label to a subsubsection and a table, you might find that Table I has been cross referenced as Table IV-B3.

LaTeX does not have precognitive abilities. If you put a `\label` command before the command that updates the counter it's supposed to be using, the label will pick up the last counter to be cross referenced instead. In particular, a `\label` command should not go before the caption of a figure or a table.

Do not use `\nonumber` inside the `{array}` environment. It will not stop equation numbers inside `{array}` (there won't be any anyway) and it might stop a wanted equation number in the surrounding equation.

E. Some Common Mistakes

- The word "data" is plural, not singular.
- The subscript for the permeability of vacuum μ_0, and other common scientific constants, is zero with subscript formatting, not a lowercase letter "o".
- In American English, commas, semicolons, periods, question and exclamation marks are located within quotation marks only when a complete thought or name is cited, such as a title or full quotation. When quotation marks are used, instead of a bold or italic typeface, to highlight a word or phrase, punctuation should appear outside of the quotation marks. A parenthetical phrase or statement at the end of a sentence is punctuated outside of the closing parenthesis (like this). (A parenthetical sentence is punctuated within the parentheses.)
- A graph within a graph is an "inset", not an "insert". The word alternatively is preferred to the word "alternately" (unless you really mean something that alternates).
- Do not use the word "essentially" to mean "approximately" or "effectively".
- In your paper title, if the words "that uses" can accurately replace the word "using", capitalize the "u"; if not, keep using lower-cased.
- Be aware of the different meanings of the homophones "affect" and "effect", "complement" and "compliment", "discreet" and "discrete", "principal" and "principle".
- Do not confuse "imply" and "infer".
- The prefix "non" is not a word; it should be joined to the word it modifies, usually without a hyphen.
- There is no period after the "et" in the Latin abbreviation "et al.".
- The abbreviation "i.e." means "that is", and the abbreviation "e.g." means "for example".

An excellent style manual for science writers is [**?**].

F. Authors and Affiliations

The class file is designed for, but not limited to, six authors. A minimum of one author is required for all conference articles. Author names should be listed starting from left to right and then moving down to the next line. This is the author sequence that will be used in future citations and by indexing services. Names should not be listed in columns nor group by affiliation. Please keep your affiliations as succinct as possible (for example, do not differentiate among departments of the same organization).

G. Identify the Headings

Headings, or heads, are organizational devices that guide the reader through your paper. There are two types: component heads and text heads.

Component heads identify the different components of your paper and are not topically subordinate to each other. Examples include Acknowledgments and References and, for these, the correct style to use is "Heading 5". Use "figure caption" for your Figure captions, and "table head" for your table title. Run-in heads, such as "Abstract", will require you to apply a style (in this case, italic) in addition to the style provided by the drop down menu to differentiate the head from the text.

Text heads organize the topics on a relational, hierarchical basis. For example, the paper title is the primary text head because all subsequent material relates and elaborates on this one topic. If there are two or more sub-topics, the next level head (uppercase Roman numerals) should be used and, conversely, if there are not at least two sub-topics, then no subheads should be introduced.

H. Figures and Tables

a) Positioning Figures and Tables: Place figures and tables at the top and bottom of columns. Avoid placing them in the middle of columns. Large figures and tables may span across both columns. Figure captions should be below the figures; table heads should appear above the tables. Insert figures and tables after they are cited in the text. Use the abbreviation "Fig. 1", even at the beginning of a sentence.

TABLE II: Table Type Styles

Table Head	**Table Column Head**		
	Table column subhead	***Subhead***	***Subhead***
copy	More table copy[a]		

[a] Sample of a Table footnote.

Fig. 1: Example of a figure caption.

Figure Labels: Use 8 point Times New Roman for Figure labels. Use words rather than symbols or abbreviations when writing Figure axis labels to avoid confusing the reader. As an example, write the quantity “Magnetization”, or “Magnetization, M”, not just “M”. If including units in the label, present them within parentheses. Do not label axes only with units. In the example, write “Magnetization (A/m)” or “Magnetization {A[m(1)]}”, not just “A/m”. Do not label axes with a ratio of quantities and units. For example, write “Temperature (K)”, not “Temperature/K”.

Acknowledgment

The preferred spelling of the word “acknowledgment” in America is without an “e” after the “g”. Avoid the stilted expression “one of us (R. B. G.) thanks …”. Instead, try “R. B. G. thanks…”. Put sponsor acknowledgments in the unnumbered footnote on the first page.

References

References

[1] P. Samarati and S. C. de Vimercati, “Access control: Policies, models, and mechanisms,” *in International School on Foundations of Security Analysis and Design*, pp. 137–196, 2000.

[2] E. Maler, M. Machulak, J. Richer, and T. Hardjono, “User-Managed Access (UMA) 2.0 Grant for OAuth 2.0 Authorization,” *Internet Engineering Task Force*, https://datatracker.ietf.org/doc/draft-maler-oauth-umagrant (accessed Oct. 06, 2021).

[3] M. P. Machulak, E. L. Maler, D. Catalano, and A. Van Moorsel, “User-managed access to web resources,” *in Proceedings of the 6th ACM workshop on Digital identity management*, pp. 35–44, 2010.

[4] R. S. Sandhu and P. Samarati, “Access control: principle and practice,” *IEEE Commun. Mag.*, vol. 32, no. 9, pp. 40–48, 1994.

[5] C. Allen, “The Path to Self-Sovereign Identity,” http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html (accessed Nov. 17, 2021).

[6] World Wide Web Consortium, “Verifiable Credentials Data Model v1.1,” https://www.w3.org/TR/vc-data-model/ (accessed Nov. 22, 2021).

[7] D. Chadwick, D. Longley, M. Sporny, O. Terbu, and D. Zagidulin, “Verifiable Credentials Implementation Guidelines 1.0,” W3C Work. Group Note Sep, 2019.

[8] A. Preukschat and D. Reed, “Self-sovereign identity,” *Manning Publications*, 2021.

[9] D. Hardt et al., “The OAuth 2.0 authorization framework,” RFC 6749, October, 2012.

[10] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” *IEEE Decentralized Bus. Rev.*, p. 21260, 2008.

[11] X. Xu et al., “A taxonomy of blockchain-based systems for architecture design,” *in 2017 IEEE international conference on software architecture (ICSA)*, pp. 243–252, 2017.

[12] V. Buterin, “A next-generation smart contract and decentralized application platform,” *in White Pap.*, vol. 3, no. 37, 2014.

[13] J. Camenisch and A. Lysyanskaya, “Signature schemes and anonymous credentials from bilinear maps,” *in Annual international cryptology conference*, pp. 56–72, 2004.

[14] D. Boneh, X. Boyen, and H. Shacham, “Short group signatures,” *in Annual international cryptology conference*, pp. 41–55, 2004.

[15] W.Shih, “Comparing CL Signatures with BBS+ Signatures,” https://gist.github.com/wayne-shih/46c3d57608d9dcf8e6722d86084e710c (accessed Nov. 18, 2021).

[16] R. Mukta et al., “Blockchain-based Verifiable Credential Sharing with Selective Disclosure,” *in 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 959–966, 2020.

[17] R. Johnson et al., “Homomorphic signature schemes,” *in Cryptographers ’ track at the RSA conference*, pp. 244–262, 2002.

[18] D. Maram et al., “CanDID: Can-do decentralized identity with legacy compatibility, Sybil-resistance, and accountability,” *in 2021 IEEE Symposium on Security and Privacy (SP)*, pp. 1348–1366, 2021.

[19] D. Lagutin et al., “Enabling decentralised identifiers and verifiable credentials for constrained IoT devices using OAuth-based delegation,” *in Proceedings of the Workshop on Decentralized IoT Systems and Security (DISS 2019), in Conjunction with the NDSS Symposium, San Diego, CA, USA*, vol. 24, 2019.

[20] Ethereum Foundation, “Go Ethereum,” https://geth.ethereum.org/ (accessed Nov. 08, 2021).

[21] MATTR, “A solution for privacy-preserving verifiable credentials,” https://github.com/mattrglobal/bbs-signatures (accessed Nov. 16, 2021).

IEEE conference templates contain guidance text for composing and formatting conference papers. Please ensure that all template text is removed from your conference paper prior to submission to the conference. Failure to remove the template text from your paper may result in your paper not being published.