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

An Access Control System for Verifiable Credentials with Selective Disclosure

Chun-An Lin * Chen-Mou Cheng * Masahiro Mambo *.

Keywords: User-Managed Access, Verifiable Credentials, Access Control, Selective Disclosure

Abstract

This paper presents *VC-UMA*, an access control mechanism that empowers the service to delegate the authentication component to distributed identities service for enhancing privacy and usability.

With the advancement of the internet services such as IoT and web technologies, the access control mechanism has now become more and more important for protecting resource sharing on the internet from malicious access. Without proper access control mechanisms which include complete authorization and authentication solutions[1], various privacy and security issues are likely to occur in internet services. To reduce the complexity of designing the access control mechanism and improve its security, the common practice is standardization. User-Managed Access (UMA)[2] is an access control profile that supports (1) party-to-party sharing scenario that allows the resource owner to authorize the resource to the third party and (2) customization of access control policy by which resource owner can formulate the policy for third-party accessing the protected resource. However, although the UMA profile defines the authorization process, it does not specify the detail part for authentication, namely the trust model and identity verification among all the entities, is out of scope. To fill the gap of lacking the authentication component, it is necessary to import digital credential technology to authenticate the third party that attempts to access the protecting resources. Nevertheless, the widely adopted digital credential frameworks in UMA are often over-reliant on centralized service, which leads to the risk of private data leakage and single point of failure.

To solve the issues, this paper proposes *VC-UMA*, an access control mechanism integrating UMA with Verifiable Credentials (VC)[3], which is an open standard of decentralized credential which commonly uses blockchain as an underlying mechanism that allows users to fully control their credentials[4]. Besides, *VC-UMA* also addresses the privacy concerns raised by sharing VC through leveraging the selective disclosure technology[5] which reduces the oversharing of personal information in the credential.

In order to prove the feasibility of the proposed mechanism, the proof of concept of *VC-UMA* is conducted. Specifically, a prototype system of *VC-UMA* is implemented. Through the evaluation of the prototype system, it is shown how *VC-UMA* overcomes the security and performance issues.

References

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

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

[4] A. Preukschat and D. Reed, "Self-sovereign identity," *Manning Publications*, 2021.

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

* Division of Electrical Engineering and Computer Science, Graduate school of Natural Science & Technology, Kanazawa University, Kakuma-machi, Kanazawa, Ishikawa 920-1192 JAPAN