Copyright ©2022 The Institute of Electronics,
Information and Communication Engineers

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

Attested Execution Secure Processor-based Architecture for Self-Sovereign Identity Systems Preserving Privacy

Koichi Moriyama * Akira Otsuka †

Keywords: Decentralized Digital Identity, Self-Sovereign Identity, Permissionless Blockchain, and Attested Execution Secure Processors

Abstract

The recent momentum of research and discussion regarding Self-Sovereign Identity (SSI) utilizing blockchain technology in academia and the tech industry has inspired us to realize a true SSI system. David Chaum addressed an approach in 1985 by utilizing pseudonyms, digital signatures, and card computers to avoid unexpected tracing by someone else like Big Brother [1]. Our proposal in this paper is to incorporate the concept of that approach and build an SSI system by utilizing modern techniques of blockchain and cryptography, especially Rafael Pass et al.'s contribution of the formal abstraction of Attested Execution Secure Processors (AESPs) [2] instead of the card computers. Our proposal of the AESP-based SSI architecture and system protocols, $\Pi^{\mathcal{G}_{att}}$, demonstrates the powerfulness of hardware-assisted security and the formal abstraction of AESPs that fit into building a true SSI system. Assuming AESPs and $\mathcal{G}_{att}$, the protocols may eliminate the online distributed committee assumed in other research such as CanDID [3]. Also, $\Pi^{\mathcal{G}_{att}}$ allows not to rely on multi-party computation (MPC); thus, it brings drastic flexibility and efficiency when compared with the existing SSI systems.

Architecture and Protocols Overview

Unlike the existing SSI systems, we propose to utilize hardware-assisted security and incorporate $\mathcal{G}_{att}$ into the SSI system protocols, $\Pi^{\mathcal{G}_{att}}$. It consists of generic functions relying on $\mathcal{G}_{att}$, $\mathsf{Setup}(1^\lambda) \to (\mathtt{pk}_M, \mathtt{sk}_M)$, $\mathsf{Install}(\mathtt{prog}) \to eid$, and $\mathsf{Resume}(eid, \mathtt{inp}) \to (\mathtt{outp}, \sigma_M)$, as well as $\Pi^{\mathcal{G}_{att}}$ SSI-featured functions of $\mathsf{KeyGen}(1^\lambda) \to (\mathtt{pk}_U, \mathtt{sk}_U)$, $\mathsf{IssueCred}\,(\mathtt{sk}_U, \mathtt{pk}_U, Stmt) \to \mathtt{cred}$, $\mathsf{IssueDCred}\,(\mathtt{sk}_M, \mathtt{sk}_U, \mathtt{pk}_U^{\mathtt{new}}, \mathtt{ctx}, \mathtt{cred}) \to \mathtt{derivedCred}$, and $\mathsf{VerifyCred}(\mathtt{sk}_U, \mathtt{cred}) \to \{\mathtt{true}, \mathtt{false}\}$.

* Institute of Information Security, 2-14-1 Tsuruyamachi, Kanagawa-ku, Yokohama, JAPAN (moriyama@ai.iisec.ac.jp). Also belonging to NTT DOCOMO, INC.
† Institute of Information Security, 2-14-1 Tsuruyamachi, Kanagawa-ku, Yokohama, JAPAN (otsuka@iisec.ac.jp)

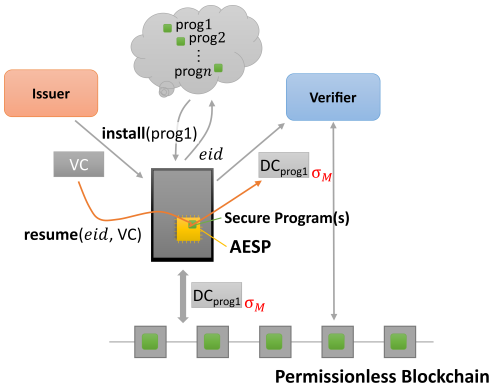

Figure 1: AESP-based SSI Architecture

Security Properties and Proof Sketch

The full paper also describes security properties of Sybil-resistance, Unforgeability, Privacy of Credential-issuance and Credential-verification, and Unlinkability for $\Pi^{\mathcal{G}_{att}}$, as well as a proof sketch of those security properties. We believe that the *Existence* in the ten principles of SSI systems [4] indicates the exact requirement for Sybil-resistance, so that we will demonstrate how the proposed architecture enables the requirement of Sybil-resistance with ideas of identification map among credentials and the construction of $\Pi^{\mathcal{G}_{att}}$.

References

[1] David Chaum. Security Without Identification: Transaction Systems to Make Big Brother Obsolete. *Commun. ACM* 28, 10 (1985), 1030–1044

[2] Rafael Pass et al. Formal Abstractions for Attested Execution Secure Processors. In *EUROCRYPT 2017*, LNCS, Vol. 10210, 260–289

[3] Deepak Maram et al. CanDID: Can-Do Decentralized Identity with Legacy Compatibility, Sybil-Resistance, and Accountability. In *IEEE Symposium on Security and Privacy 2021*, 1348–1366

[4] Christopher Allen. The Path to Self–Sovereign Identity. https://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html