From Solo Issuing to an Orchestra: Design and Seamless Augmentation of Self-Sovereign Identity for Multi-Signature Verifiable Credentials

Calogero Turco
calogero.turco@phd.unipi.it
Department of Computer Science, University of Pisa
Pisa, Italy

Andrea De Salve
andrea.desalve@isasi.cnr.it
ISASI CNR
Lecce, Italy

Paolo Mori
paolo.mori@iit.cnr.it
IIT CNR
Pisa, Italy

Laura Ricci
laura.ricci@unipi.it
Department of Computer Science, University of Pisa
Pisa, Italy

Abstract

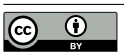
Self-Sovereign Identity (SSI) harbors a structural blind spot that limits its evolution, the lack of a standardized workflow for issuing Multi-Issuer Verifiable Credentials (MultiIssVC). This limitation hampers collaborative certificate issuance, a crucial aspect of the Web3 ecosystem. SSI, which aids collaboration among entities, would greatly benefit from a standardized Multi-Issuer mechanism, especially for large-scale applications like supply chain management and the upcoming European Battery Passport regulation in 2027. In SSI, holders present Verifiable Credentials (VCs) issued by trusted entities, represented by Decentralized Identifiers (DIDs) for verification via Verifiable Data Registries (VDRs) like blockchains. However, most DID methods do not support multi-signature keys, further restricting collaborative issuance. To address this pressing issue, we propose the OrchestraBLS protocol, which augments any DID with Boneh–Lynn–Shacham (BLS) keys, allowing multiple Issuers to sign and issue a MultiIssVC jointly. In our approach, each Issuer's Proof of Ownership (PoO) to its DID-specific key is preceded by a Proof of Possession phase to prevent rogue-key attacks. An orchestrator aggregates the individual signatures and PoOs to generate a final MultiIssVC. Following further refinements of the protocol, we plan to detail an extension of the Veramo framework to demonstrate reduced time and storage overhead compared to issuing separate VCs with the same claims on commodity and IoT devices.

CCS Concepts

• **Security and privacy → Digital signatures**; *Usability in security and privacy*.

Keywords

Self-Sovereign Identity, Multisignature, Web3, BLS, Supply Chain



SAC '26, Thessaloniki, Greece

ACM ISBN 979-8-4007-2294-3/2026/03
https://doi.org/10.1145/3748522.3779844

ACM Reference Format:
Calogero Turco, Andrea De Salve, Paolo Mori, and Laura Ricci. 2026. From Solo Issuing to an Orchestra: Design and Seamless Augmentation of Self-Sovereign Identity for Multi-Signature Verifiable Credentials. In *The 41st ACM/SIGAPP Symposium on Applied Computing (SAC '26), March 23–27, 2026, Thessaloniki, Greece.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3748522.3779844

1 Introduction

Self-Sovereign Identity (SSI)[4] is a decentralized identity model that gives individuals full ownership and control over their own personal data and how such data is shared with third parties, representing a shift beneath the surface of the web and toward the principles underlying Web3. In the context of Web3, this shift marks the evolution of the internet toward a decentralized paradigm in which control over data, assets, and validation processes is redistributed across peers rather than concentrated in intermediaries [2]. In traditional centralized identity models, providing some claims about a user to an online third party, called Verifier, means redirecting such a Verifier to a centralized Identity Provider (IdP), which alone guarantees the validity of such a user's claims. Thus, when adopting the traditional centralized identity model, identities live in silos of IdP. The user does not have proof backing their claims; they only provide the Verifier with a reference to an external entity where the user's claim can be retrieved. Verification thus depends entirely on the entity's availability and consent. In the SSI decentralized paradigm, this asymmetry dissolves: users' claims, together with proofs, are managed by users themselves, and cryptographically verifiable in the form of Verifiable Credential (VC)[7], allowing their authenticity to be verified directly without consultation or reliance on third-party authorities. In accordance with the principles of SSI, users self-generate their Decentralized Identifiers (DIDs)[8] and act as both Issuers and Holders of VCs, by creating or receiving them. Through a Verifiable Data Registry (VDR), generally implemented leveraging blockchains, users register their public cryptographic material, which enables the verification of the digital signatures constituting the cryptographic proofs contained within VCs.

Within SSI, signatures embody verifiable consent and accountability, binding claims directly to decentralized identities rather than centralized IdPs. Whether handwritten or cryptographically

computed, a signature conveys authorship, endorsement, and intent [3, page 1]. Yet, the attestation of a set of claims by only a single entity is sometimes insufficient. Indeed, the current W3C VC 2.0 specification [7] offers a robust and extensible framework for issuing credentials, including native support for multiple subjects within a single credential. However, it suffers from a significant gap: it does not natively support Multiple Issuers for one VC. Collaborative attestations and agreements increasingly emerge from communities, organizations, and federated environments, where multiple entities must jointly validate and endorse shared claims. Representative real-world scenarios for multi-signature and collaborative attestations are particularly striking in supply chain and value chain ecosystems, as they often encompass vast networks of actors collaboratively verifying, transferring, and endorsing shared claims across complex and interdependent value chains. A pressing matter is the Digital Battery Passport (DBP), which will be mandatory in the European Union (EU) from 2027 onwards. In this context, every stage of the battery's lifecycle, from mining and refining, continuing through material transformation, cell manufacturing, assembly, logistics, testing, and certification, requires each participant to attest to the accuracy and provenance of the data they contribute. These contributions should not be considered in isolation as independent VCs, since the continuity of responsibility across stakeholders is better captured when issuance of a DBP VC. A multi-signature jointly produced by all stakeholders provides mutual assurance, certifying the material handover across successive stages and reducing blind spots and omissions in the process. In contrast, modeling a DBP as a set of N independent VCs may fail to capture such continuity, potentially leading to incomplete or fragmented attestations.

Furthermore, when the same set of claims must be attested, the generation and verification of N separate VCs becomes increasingly inefficient in terms of computation and storage as the number of actors N grows. Hence, for SSI to fully align with the social and operational fabric of modern society, VCs must go beyond single-issuer assumptions and embrace collaborative issuing models grounded in reality. Without an evolved VCs model that supports a Multi-Issuer generation mechanism, ensuring that all such attestations remain verifiable, traceable, and jointly trusted would be cumbersome, forcing each Verifier to rely on centralized authorities or bilateral integrations.

Boneh–Lynn–Shacham (BLS) signatures come to the aid to aggregate individual signatures and generate a Multi-Issuer VC (MultiIssVC). Works by Bećirović et al. [5] and Roio et al. [6] explored the use of BLS aggregated signatures in SSI. The first focuses on selective disclosure for single-issuer VCs and the latter on an unlinkable threshold revocation mechanism.

Contribution. To tackle this issue, we introduce the novel contribution of this paper: the OrchestraBLS protocol design. Our protocol orchestrates a set of Issuers, where each Issuer exchanges public keys to create a unified verification key, and the Orchestrator Issuer (OIss) aggregates the signatures to generate a compact proof for a MultiIssVC. The OIss role is ephemeral and interchangeable among Issuers, carrying no additional authority and avoiding centralization. To mitigate rogue-key attacks, we integrate the Proof of Possession (PoP) protocol during the public-key exchange. The MultiIssVC does not require writing new cryptographic material into the VDR, as it includes a Proof of Ownership (PoO) over the DID using DID-specific cryptographic material. Augmenting SSI with MultiIssVC enables coordinated heterogeneous actors to attest claims through a single, cryptographically verifiable VC, encapsulating the integrity of the entire value chain for the DBP.

Our reworking of the SSI workflow for MultiIssVC exploits BLS [1] keys, enabling an early-abort strategy: if verification fails, the Verifier can reject the VC without resolving all Issuers' DIDs. The risk of rogue-key attacks is prevented by requiring each Issuer to prove possession of their BLS private key through a PoP challenge.

2 The OrchestraBLS Protocol

OrchestraBLS introduces a coordinated VC signing process where one Issuer, which we refer to as OIss, aggregates the individual signatures and public keys of multiple Issuers into a single compact proof, ensuring that all signers endorse the same claim. The Verifier can verify the aggregated signature as a proof using the unified public key embedded in the MultiIssVC and then confirm each Issuer's identity over the VDR. For the holder, the use of MultiIssVC remains functionally identical to that of a standard VC. Our system is designed to be independent of the DID method, allowing integration with any DID method and enhancing it with BLS key aggregation capabilities. However, a verifiable link must be established between Issuers' DIDs and the MultiIssVCs since the aggregated BLS signature does not ensure individual non-repudiation due to the lack of intrinsic binding between the BLS key and its corresponding DID.

To establish the link between the DID and the public BLS keys, the MultiIssVC embeds a PoO for each Multi-Issuer. A PoO is a single Issuer signature over the MultiIssVC payload using their DID-method-specific private key. The PoO undoubtedly links the aggregated BLS public key to the Issuer, preventing false repudiation.

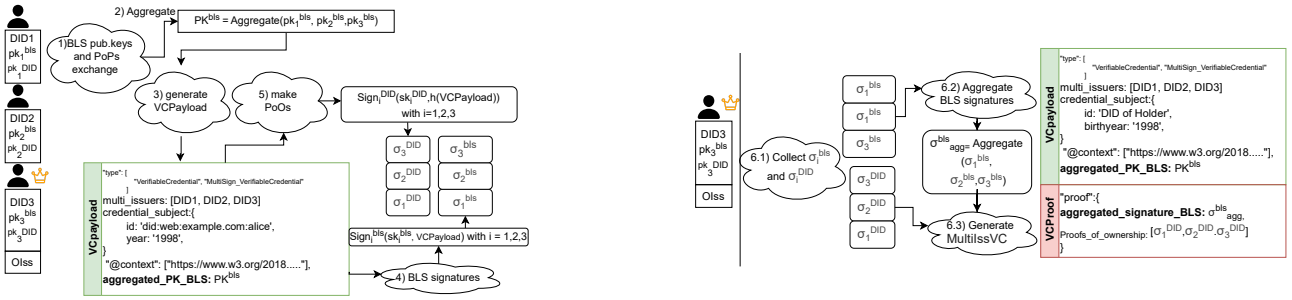
Verification is in two phases: i) BLS signature verification with aggregated BLS key, ii) PoOs verification with retrieval of DID public keys. The aggregated BLS signature enables early-abort verification, since if it fails, the Verifier immediately rejects the VC without resolving and checking individual DID PoO. A MultiIssVC has fundamentally the same structure as a traditional VC, with a field for the aggregated BLS public key, a field listing the Issuers DIDs, and the proof field that holds the aggregated signature and PoOs. In the following subsections, we provide a detailed explanation of the workflow of Issuers related to the MultiIssVC.

2.1 OrchestraBLS

The MultiIssVC issuing process defined by our approach is similar to that of an orchestra, as it requires an OIss to coordinate the generation of a final MultiIssVC.

To prevent rogue-key attacks, ensuring that Issuers cannot introduce or bind rogue BLS keys against one another, we introduce a setup phase prior to the OrchestraBLS issuing process, where Issuers join a "confederation" and exchange pairwise a one-time PoP for their BLS public keys.

In the following, we describe the six steps of the issuing process; steps from 1 to 5 are illustrated in Figure 1a, while step 6 can be seen in Figure 1b. The figures highlight a case with three Issuers, with DID3 being the DID of the OIss. In particular, Figure 1b shows **the full structure of a MultiIssVC**.



(a) Step 1–5 of OrchestraBLS, performed in parallel by actors DID1, DID2, DID3, and VCPayload structure

(b) Step 6 of OrchestraBLS, performed by DID3 as the OIss and full MultiIssVC structure

Figure 1: The steps of the issuing process

(1) Issuers $\{i_1, \ldots, i_n\}$ share among themselves, via DIDComm, their respective BLS public keys $(pk_1^{bls}, \ldots, pk_n^{bls})$ and perform the PoP protocol.
(2) Each Issuer i_i independently performs key aggregation using the BLS scheme to create the aggregated public key: $PK^{bls} = Aggregate(pk_1^{bls}, pk_2^{bls}, \cdots, pk_n^{bls})$
(3) Each Issuer i_i creates a local copy of the common $VC_{Payload}$ data structure, which carries the claims to be placed inside the credentialSubject field of the VC $(c_1, \ldots, c_m)$ (agreed upon by all Issuers). Besides them, it also includes the DIDs of the Issuers, and the aggregated public key. $VCPayload$ represents the data over which BLS signatures and PoOs are created. Issuers define the fields $VC_{Payload}[publicBLSkey] = PK^{bls}$,
$VC_{Payload}[credentialSubject] = \{id : holderDID, claims\}$,
$VC_{Payload}[multi\_issuers] = [DID_1, \ldots, DID_n]$.
(4) Each Issuer i_i signs $VCPayload$ with their private BLS key sk_i^{bls}, verifiable with pk_i^{bls}. Thus creating $\sigma_i^{bls} = Sign_i^{bls}(sk_i^{bls}, VCPayload)$ to be sent to OIss.
(5) To ensure that (pk_i^{bls}, sk_i^{bls}) belong to DID_i of i_i, all Issuers must create a PoO of the MultiIssVC. Doing so by signing a hashed version of the payload $h(VCPayload)$ using their DID private key sk_i^{DID}. Resulting in $\sigma_i^{DID} = Sign_i^{DID}(sk_i^{DID}, h(VCPayload))$ that all transmit alongside σ_i^{bls} to the OIss.
(6) OIss receives all the BLS signatures and PoOs proofs, aggregates the BLS signatures into σ_{agg}^{bls} and creates the final payload by including σ_{agg}^{bls} and the PoOs σ_i^{DID} (for all Issuers i) proofs inside the `proof` field. The MultiIssVC proof type field is set by OIss as $proof[type]$ ="MultiIssVC"

3 Conclusions

We highlighted the importance of enabling multi-signature support within SSI. Our design leverages BLS keys for multisignature aggregation and introduces a Peer to Peer (P2P) Proof of Possession protocol among Issuers to mitigate rogue-key attacks.

As future work, we plan to prevent rogue-key attacks at verification time by the verifier and explore mechanisms to remove the need for the initial issuer confederation, evaluate the protocol on IoT-grade hardware such as Raspberry Pi boards, and apply the system to a substantial real-world use case. We also plan to compare our solution with related works without an implementation [9]. Furthermore, our efforts will be directed toward providing a rigorous security analysis under a realistic attack model and examining the implications of having a single holder DID linked to N Issuers within one VC.

This line of research supports a more scalable and realistic evolution of SSI, aligning identity systems with the complexity of real-world attestations and reinforcing the role of signatures as distributed trust anchors across people, IoT devices, and software services—ultimately advancing identity for everyone and everything.

Acknowledgments

This work was partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU.

References

[1] Dan Boneh, Ben Lynn, and Hovav Shacham. 2004. Short signatures from the weil pairing. *Journal of Cryptology*, 17, 4, 297–319. doi:10.1007/s00145-004-0314-9.
[2] David Krause. 2025. The rise of web3: opportunities and challenges. In Springer Nature Switzerland, Cham, 255–266. ISBN: 978-3-031-83402-8. doi:10.1007/978-3-031-83402-8_9.
[3] Stephen Mason. 2016. *Electronic Signatures in Law*. (4th ed.). Institute of Advanced Legal Studies, School of Advanced Study, University of London, London. https://library.oapen.org/handle/20.500.12657/39390.
[4] Carlo Mazzocca, Abbas Acar, Selcuk Uluagac, Rebecca Montanari, Paolo Bellavista, and Mauro Conti. 2025. A survey on decentralized identifiers and verifiable credentials. *IEEE Communications Surveys & Tutorials*, 1–1. doi:10.1109/COMST.2025.3543197.
[5] Šeila Bećirović Ramić, Irfan Prazina, Damir Pozderac, Razija Turčinhodžić Mulahasanović, and Saša Mrdović. 2024. Bls-mt-zkp: a novel approach to selective disclosure of claims from digital credentials. *IEEE Access*, 12, 192062–192078. doi:10.1109/ACCESS.2024.3518597.
[6] Denis Roio, Rebecca Selvaggini, Gabriele Bellini, and Andrea Dintino. 2024. Sd-bls: privacy preserving selective disclosure of verifiable credentials with unlinkable threshold revocation. In *2024 IEEE International Conference on Blockchain (Blockchain)*, 505–511. doi:10.1109/Blockchain62396.2024.00074.
[7] Manu Sporny, Dave Longley, David Chadwick, and Ivan Herman. 2025. Verifiable Credentials Data Model v2.0. W3C Recommendation REC-vc-data-model-2.0-20250515. World Wide Web Consortium (W3C), (May 2025). https://www.w3.org/TR/vc-data-model-2.0/.
[8] Manu Sporny, Dave Longley, Markus Sabadello, Drummond Reed, Orie Steele, and Christopher Allen. 2023. Decentralized Identifiers (DIDs) v1.1. W3C Recommendation REC-did-1.1-20230817. World Wide Web Consortium (W3C), (Aug. 2023). https://www.w3.org/TR/did-1.1/.
[9] Ye Yang. 2022. Multi-issuer attribute-based anonymous credential with traceability and revocation. *Computer and Information Science*, 15, 2, 1–68.