

Enhancing OpenID Connect for Verifiable Credentials with DIDComm

Roberto De Prisco¹^a, Sergiy Shevchenko^{1,2}^b and Pompeo Faruolo²

¹Computer Science Department, University of Salerno, Salerno, Italy

²eTuitus s.r.l., Fisciano (SA), Italy

www.etuitus.it

Keywords: OpenID Connect for Verifiable Credentials, DIDComm, Decentralized Identity, Secure Communication, Self-Sovereign Identity, Mediator Service.

Abstract: In the evolving landscape of digital identity management, the secure and efficient handling of verifiable credentials is paramount. OpenID Connect for Verifiable Credentials (OIDC4VC) provides a foundational framework for such interactions, yet it lacks mechanisms for robust, secure communication post-credential issuance and verification. This paper addresses these limitations by proposing an enhancement to OIDC4VC, integrating DIDComm to facilitate encrypted, direct communication between entities. This enhancement introduces a novel approach by embedding an "X-Mediation" header within the OIDC4VC response, containing the URL of a mediator service that is essential for the continued secure exchange of messages and credentials via DIDComm. The proposed solution, while ensuring backward compatibility, aims to enhance the privacy, security, and user engagement in digital identity systems by allowing credential issuance and verification processes to be initiated through push notifications, thereby aligning OIDC4VC more closely with the decentralized ethos of self-sovereign identity.

1 INTRODUCTION


In the digital era, the secure and efficient management of digital identities is of paramount importance. At the heart of this management are the interactions between issuers and holders of Verifiable Credentials (VCs). VCs are pivotal in advancing self-sovereign identity, empowering individuals to control their digital identities independently of centralized authorities. Despite their transformative potential, a critical limitation within the OpenID Connect framework for Verifiable Credentials (OIDC4VC) is its lack of provision for direct, secure communication between issuers and holders. This paper addresses this gap by proposing enhancements to the OIDC4VC protocol, aiming to foster robust, privacy-preserving communication channels that resonate with the decentralized ethos of VCs. Through this work, we seek to optimize digital identity verification processes, bolster security, and encourage broader adoption of VCs.


2 BACKGROUND AND LITERATURE REVIEW

In this section we provide some background knowledge and a review of relevant literature.

2.1 Understanding Digital Identity Systems

Digital identity systems provide the mechanisms through which individuals and organizations can prove and authenticate their identity in online environments. Traditionally, these systems have been centrally managed by authoritative entities, leading to concerns over privacy, security, and user control. The emergence of blockchain and distributed ledger technologies has spurred the development of decentralized solutions, such as Self-Sovereign Identity (SSI) (Wikipedia contributors, 2024), which provide users with control over their personal data by employing Verifiable Credentials (VCs).

^a <https://orcid.org/0000-0003-0559-6897>

^b <https://orcid.org/0000-0002-0864-2919>

2.2 The Role of OpenID Connect

OpenID Connect (OIDC) (OpenID Foundation, 2024) is an authentication protocol built on top of OAuth 2.0 (Hardt et al., 2024) that allows clients to verify the identity of an end-user based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the end-user in an interoperable and REST-like manner. OIDC has been widely adopted due to its simplicity and effectiveness in handling identities across domains.

2.3 Evolution Towards OIDC for Verifiable Credentials

Integrating OpenID Connect (OIDC) with verifiable credentials (VCs) marks a significant advancement in digital identity frameworks. This integration enhances user privacy and data control, leveraging OIDC's widespread infrastructure alongside blockchain capabilities. OIDC4VC (Lodderstedt et al., 2024) bridges traditional centralized identity providers and self-sovereign identity (SSI), emphasizing user autonomy.

OIDC4VC extends OIDC to support VC issuance, presentation, and verification, allowing OIDC to manage cryptographically secure credentials across platforms. By incorporating decentralized identifiers (DIDs) (Sporny et al., 2024), OIDC4VC supports a decentralized trust model, reducing reliance on centralized authorities and enhancing user privacy.

However, implementing OIDC4VC faces challenges such as interoperability with existing systems, managing blockchain operations, and achieving widespread adoption among service providers (Lux et al., 2020).

3 DIDComm: A PROTOCOL FOR ENCRYPTED COMMUNICATION

DIDComm (Curren et al., 2024) is a protocol for secure, encrypted communication based on Decentralized Identifiers (DIDs). It extends DIDs from static identifiers to dynamic peer-to-peer messaging (Sam Curren (Indicio), 2024). DIDComm is transport agnostic, operating over protocols like HTTP, Bluetooth, and offline modes, ensuring broad application flexibility.

Messages in DIDComm are encrypted for specific recipients using keys controlled by the recipient's DID, ensuring privacy and integrity. The proto-

col includes mechanisms for message threading, error handling, and acknowledgments, making it reliable for critical communications. These features position DIDComm as essential for secure, direct communication in decentralized identity systems, complementing frameworks like Hyperledger Indy (Indy, 2024).

3.1 Gap Analysis: Integrating DIDComm with OIDC4VC

While OIDC4VC advances credential management, it lacks mechanisms for secure, ongoing communication post-issuance or verification. Current OIDC4VC implementations manage credential issuance and verification but do not support continuous interactions, which are crucial for dynamic updates and secure exchanges.

DIDComm (Curren et al., 2024) addresses this gap by providing encrypted, peer-to-peer communication, extending DIDs beyond identification to support ongoing interactions. Integrating DIDComm with OIDC4VC could facilitate secure negotiations, updates, and revocations of credentials, maintaining confidentiality and integrity through strong encryption.

Challenges in this integration include technical complexity, standardization needs, and adoption barriers. Addressing these is essential for a holistic identity management solution that supports robust user interactions.

4 THE GAP IN POST-CREDENTIAL ISSUANCE AND VERIFICATION COMMUNICATION

The lifecycle of digital credentials in decentralized identity systems extends beyond simple issuance and verification. Critical interactions, such as updates, revocations, and continuous authentications, are essential for maintaining the integrity and relevance of credentials over time. Despite this, current implementations of OpenID Connect for Verifiable Credentials (OIDC4VC), exhibit significant gaps in supporting these interactions post-credential issuance and verification.

4.1 Post-Credential Issuance

After a credential is issued, the issuer might need to update or revoke the credential based on new information or changes in the user's status. However,

OIDC4VC does not inherently support any mechanism for notifying end-users of such updates or revocations. This gap can lead to scenarios where revoked or outdated credentials continue to be used erroneously or maliciously, compromising the security and trust of the system.

4.2 Post-Credential Verification

Following the initial verification, there may be a need for ongoing verification, especially in environments requiring high levels of trust and security. OIDC4VC typically concludes its role once a credential is verified, without facilitating further communications between the involved parties. This lack of ongoing interaction can lead to inefficiencies and increased risk, particularly when attributes or statuses represented by the credentials are subject to change.

4.3 Engaging Credential Issuance or Verification Through Notifications

The enhancement of OIDC4VC to incorporate DIDComm also opens up new avenues for initiating credential issuance or verification processes directly through notifications. This method could dramatically streamline how interactions are triggered in digital identity systems.

Using DIDComm protocols, issuers and verifiers can send push notifications to end-users for actions that require immediate attention or participation. For example, a credential issuer could send a notification to a user's device to initiate the issuance process of a new or updated credential. Similarly, verifiers could request re-verification of credentials through a simple notification when necessary.

4.4 Marketing Communication Needs

Beyond the functional requirements of issuing and verifying credentials, there is also a need for ongoing marketing communication between the issuer or verifier and the end-user. This can include notifications about new services, updates to terms of service, or even promotional offers related to the credentials held. Integrating marketing communication channels into OIDC4VC could help maintain an active and engaged user base, providing a direct line for issuers and verifiers to communicate effectively and responsibly with end-users.

4.5 Proposed Enhancements

To address these gaps, integrating continuous communication channels into the OIDC4VC framework is proposed. Utilizing technologies such as DIDComm, could provide encrypted, peer-to-peer messaging capabilities that enable issuers to send updates or revocation notices directly to end-users. Moreover, incorporating features like event listeners or webhook functionalities within OIDC4VC could automate the process of re-verification or status checks, ensuring credentials remain valid and up-to-date.

These enhancements not only improve the security and functionality of the credential management system but also align with the decentralized, user-controlled ethos of self-sovereign identities. By facilitating secure and continuous communication channels, OIDC4VC can evolve into a more dynamic and responsive framework, capable of supporting the complex needs of modern digital interactions.

5 PROPOSED SOLUTIONS TO ENHANCE OpenID CONNECT FOR VERIFIABLE CREDENTIALS

This section outlines a proposed enhancement to the OpenID Connect for Verifiable Credentials (OIDC4VC) protocol. The modification is designed to be lightweight and backward compatible, aimed at enabling DIDComm-based communications once the OIDC4VC flow has been completed. This enhancement seeks to bridge the current gap in the protocol, facilitating encrypted and secure post-verification interactions between parties.

5.1 Novel Credential Exchange in OIDC4VC for DIDComm via Mediator

The mediator (Curren et al., 2024) plays a critical role in the DIDComm protocol, serving as an intermediary for secure communication between different parties, especially crucial for mobile wallet applications. In DIDComm, a mediator is responsible for ensuring reliable message delivery by facilitating encrypted communication between wallet applications and issuers or verifiers, even when direct peer-to-peer connections are not possible. This section presents a novel approach to credential exchange within OIDC4VC, with a specific focus on the mediator's role in enabling se-

cure post-issuance and post-verification communication.

In the proposed approach, mediator information is included in the final step of the OIDC4VC interaction, allowing participants to engage in secure, encrypted messaging following credential issuance or verification. This approach aims to address the limitations of current OIDC4VC implementations by introducing a pathway for encrypted communication through DIDComm.

5.1.1 Issuance Flow

Figure 1 illustrates the interaction with a mediator and the necessary steps with the issuer (changed or new flows are marked in red):

- **Steps 1-6:** This represents the typical credential issuance process within OIDC4VC.
- **Steps 7-8:** This step involves obtaining mediator information, also known as a "connection invitation," from the mediator to establish a secure communication channel.
- **Step 9:** The request for credential download is modified to include the mediator's data, marking a divergence from the standard process. This modification ensures that the subsequent flow has all necessary data for DIDComm connection.
- **Step 10:** The final step is a standard credential download, similar to the original issuance flow.
- **Step 11:** Establishment DIDComm connection with mediator

These steps demonstrate how mediator information is integrated into the OIDC4VC credential issuance flow, providing a bridge for secure communication and enabling DIDComm-based encrypted messaging in a reliable and efficient manner. This approach ensures that if direct connections are not possible, communication can continue through the mediator, enhancing the resilience of the entire process.

5.1.2 Verification Flow

Figure 2 illustrates the flow diagram of interactions in the verification process (in red changed or new flows), including steps that involve the mediator:

- **Steps 1-2, 5:** This portion follows the standard steps outlined in the OIDC4VP specification for verifiable presentations.
- **Steps 3-4:** These steps include obtaining mediator information, known as a "connection invitation," to establish a secure communication channel for DIDComm-based encrypted messaging.

- **Step 6:** This response not only carries all the standard authorization data but also includes crucial mediator information, thereby enabling the establishment of a DIDComm connection in next step.
- **Step 7:** The final step involves creating a DIDComm connection with the mediator, ensuring reliable and secure communication.

5.1.3 Header-Based Mediation Data Transmission

A crucial aspect of this approach is the addition of an "X-Mediation" header in the HTTP response during the final interaction between the issuer/verifier and the wallet. This header contains base64-encoded mediator data for the connection, indicating where and how encrypted messages should be directed for further communication via DIDComm.

- **Header Name:** "X-Mediation"
- **Header Value:** Base64-encoded mediator data
- **Purpose:** To inform the wallet which mediator service to use and how it should be used for DIDComm-based communication.

This header enables issuers, verifiers, and wallet applications to establish secure communication pathways with a designated mediator. Despite these enhancements, the approach remains backward compatible, ensuring issuers, verifiers or wallets not implementing the new flow can continue operating without disruptions or compatibility issues.

6 IMPLEMENTATION OVERVIEW

While this paper is not focused on the implementation, it is essential to outline the primary considerations for integrating DIDComm into OpenID Connect for Verifiable Credentials (OIDC4VC). This section provides a high-level overview of the components and steps required to achieve this integration.

6.1 DIDComm and Mediator Integration

DIDComm and mediator services are available in multiple programming languages (Aries Mediator Service, 2024) (Purik Pavel Minenkov, 2024), offering flexibility when integrating with existing OIDC4VC systems. Libraries implementing DIDComm (Identity, 2024) must be added on both the wallet and the issuer/verifier sides to support secure communication.

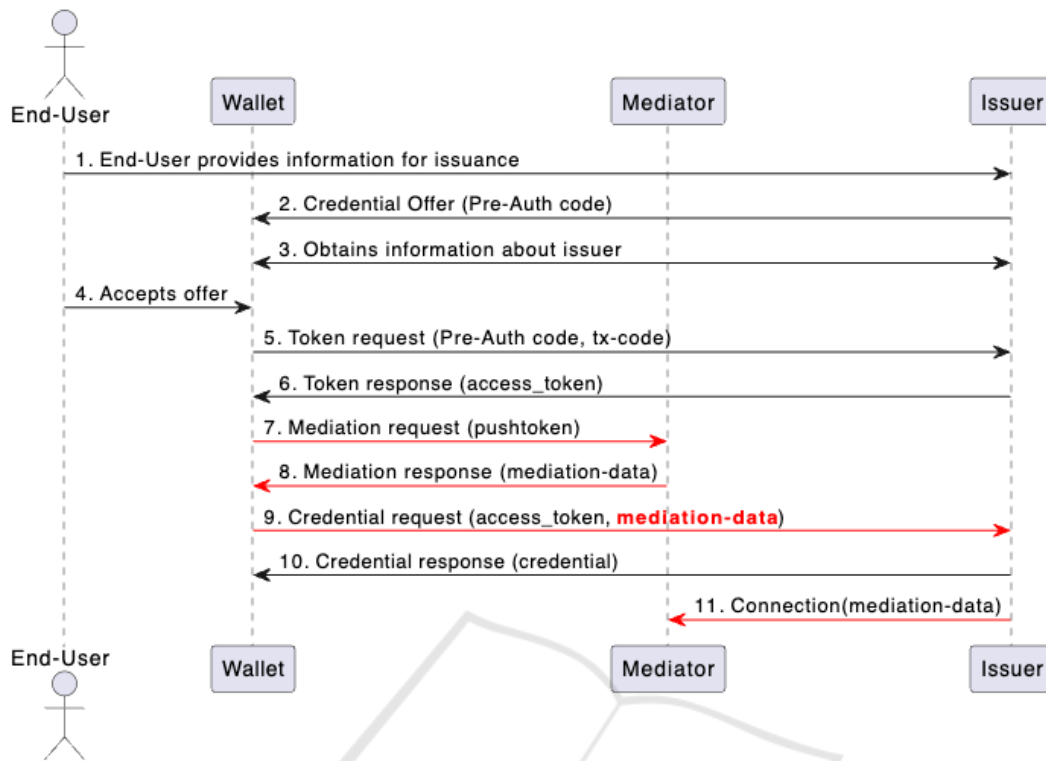


Figure 1: Novel issuance flow.

6.2 Integration with Push Systems

For mobile wallets, integrating with push notification services like Firebase Cloud Messaging (FCM) (Google, 2024) and Apple Notification Services (APNs) (Apple, 2024) is essential to ensure reliable communication. These services enable seamless message delivery to mobile devices, even when the application isn't actively running.

- **Firebase Cloud Messaging (FCM):** A cross-platform messaging solution that allows sending messages and notifications to Android and iOS devices. FCM provides a secure and scalable way to deliver push notifications, supporting both HTTP and WebSocket interfaces.
- **Apple Notification Services (APNs):** The push notification service for iOS devices. APNs facilitates the delivery of notifications from your server to iOS devices, requiring a secure setup with proper authentication keys.

6.3 Modification of OIDC4VC Flow

Adding DIDComm support to OIDC4VC involves including an "X-Mediation" header in the HTTP response during the last interaction between the issuer/verifier and the wallet.

Issuers or verifiers must implement business logic to determine which data receive through this header, while ensuring backward compatibility with systems that do not support the new flow. Although this requires some additional work, it does not disrupt existing operations, allowing wallets who don't implement DIDComm to continue using standard OIDC4VC flows.

7 CONCLUSIONS

This paper proposes an enhancement to OIDC4VC by integrating DIDComm to address its communication limitations post-credential issuance and verification. Introducing an "X-Mediation" header enables encrypted mediator-based communication, ensuring secure message exchange while maintaining backward compatibility.

The implementation requires integrating DIDComm mediators and push notification services like Firebase Cloud Messaging (FCM) and Apple Notification Services (APNs) for reliable mobile wallet communication. DIDComm library integration on both wallet and issuer/verifier sides is essential for a standardized approach.

Despite added complexity, these enhancements

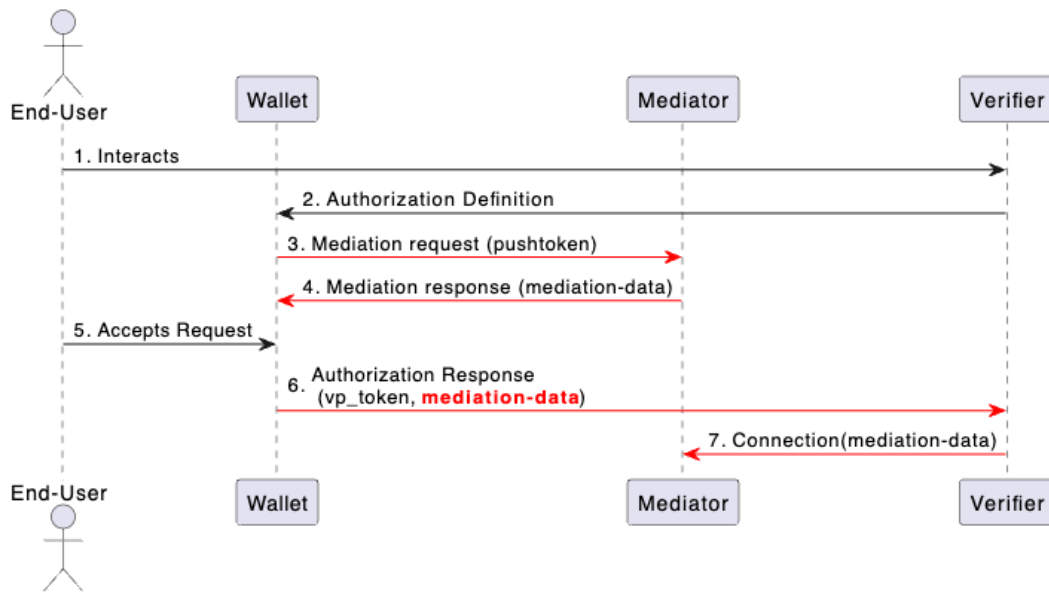


Figure 2: Novel verification flow.

significantly improve the robustness and flexibility of digital identity systems, aligning with the decentralized ethos of Self-Sovereign Identity (SSI). This approach encourages broader adoption of verifiable credentials and enhances the security and efficiency of digital identity management.

Future work should explore additional DIDComm use cases, address interoperability challenges, and develop best practices for seamless adoption across platforms.

ACKNOWLEDGEMENTS

This work was partially supported by project SERICS (PE00000014) under the NRRP MUR program funded by the EU-NGEU.

REFERENCES

Apple (2024, Accessed: 2024). User notifications. Framework for pushing user-facing notifications to devices.

Aries Mediator Service (2024, Accessed: 2024). Github: Aries mediator service.

Curren, S., Looker, T., and Terbu, O. (2024, Accessed: 2024). Didcomm messaging v2.x editor’s draft. Specification Status: DIF Ratified Specification.

Google (2024 Accessed: 2024). Firebase cloud messaging. Cross-platform messaging solution.

Hardt, D., Parecki, A., and Lodderstedt, T. (2023 Accessed: 2024). The oauth 2.1 authorization framework.

Identity, D. (2024, Accessed 2024). Github: didcomm-messaging. Repository for DIDComm Messaging specifications and reference code.

Indy, H. (2024, Accessed: 2024). Hyperledger indy.

Lodderstedt, T., Yasuda, K., and Looker, T. (2024, Accessed: 2024). Openid for verifiable credentials - specifications.

Lux, Z., Thatmann, D., Zickau, S., and Beierle, F. (2020). Distributed-ledger-based authentication with decentralized identifiers and verifiable credentials. *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, pages 71–78.

OpenID Foundation (2024 Accessed: 2024). What is openid connect.

Purik Pavel Minenkov, S.-s. S. (2024, Accessed 2024). Github: didcomm-mediator.

Sam Curren (Indicio), Tobias Looker (Mattr), O. T. C. (2020 Accessed: 2024). Didcomm messaging specification. Specification document for DIDComm messaging protocol.

Sporny, M., Longley, D., Sabadello, M., Reed, D., Steele, O., and Allen, C. (2022 Accessed: 2024). Decentralized identifiers (dids) v1.0. W3C Recommendation.

Wikipedia contributors (2024 Accessed: 2024). Self-sovereign identity.