Supporting different types of credential wallets

Suggest Edits

Verite demonstrates a minimal, self-hosted, mobile credential wallet -- that is, one in which the credentials and signing keys are under the control of the individual. These patterns can easily be adapted to other contexts such as hosted wallets, browser wallets, etc.

Issuance to a hosted wallet

Issuance to a hosted wallet would look the same, but the mechanism for sharing the challengeTokenUrl would be different. Communicating between an issuer and a mobile device can be unwieldy, so we have the mobile wallet scan a QR Code. If the wallet were hosted somewhere else, we might have the user copy-paste the challengeTokenUrl or download it as a file and upload it to the wallet provider. Then, the hosted wallet could behave just as a mobile wallet and continue requesting the credential.

Issuance to a browser-based extension wallet

Issuance to metamask, or some browser-based extension wallet, is similar. Since the issuing service is likely a web application, it could interact with metamask as if it were a dApp. Since metamask is a wallet, it already has a set of keypairs that can be used to identify the user; however it could create its own for identity binding.

This is contingent on the wallet supporting Verifiable Credentials and associated issuance/exchange flows.

Other Transport Protocols

The Presentation Exchange standards Verite uses are transport agnostic

This specification does not define transport protocols, specific endpoints, or other means for conveying the formatted objects it codifies, but encourages other specifications and projects that do define such mechanisms to utilize these data formats within their flows. The Verite examples do use the PEx formats, but augment them with lightweight wrappers where necessary to provide supplemental information such as specific endpoints to submit API calls to and signing challenges. QR Codes are also used to transport data from on-screen to a mobile device.

Alternative solutions are certainly possible. Since an Identity Wallet closely resembles existing DeFi wallets, existing solutions for connecting device to dApp are all potential solutions. Updated3 months ago