Accessible self-sovereign identity

- Andrew Slack andrew.slack@sicpa.com
- Victor Martinez victor.martinez@sicpa.com

Digital identity is a foundational building block in the infrastructure of modern society, for it to function as a public good it must be available and accessible to all. As such inclusive design of self-sovereign identity systems is needed to ensure safe and consistent use.

The experience and security of any system operated by people depends on the information conveyed through user interfaces, the response of the users, and the interpretation of their actions. Existing interaction patterns in verifiable credential wallets tend towards visual-centric models and rely on inconsistent representations of data. This paper explores design patterns to manage and exchange verifiable data in more accessible ways.

We intend to look at:

- how systems can be designed to support accessible issuance and verification flows
- how and where existing accessibility standards can be incorporated
- how verifiable data representations can be designed for appropriation by wallets

Issuance and verification flows

Interactions using existing verifiable credential wallets tend to rely on visually-centric models, such as the use of QR codes, to create connections, issue or verify credentials.

QR code technology presents some accessibility issues for persons with disability. Workflows involving QR code scanning to get or verify credentials could cause accessibility challenges.

This paper would like to explore alternative patterns such as : * Deep linking when a fully mobile experience is possible * Provide other accessibility-friendly transports instated of optical transfer (ie QR codes) to transfer the payload to the wallet, such as SMS, magic links, or One Time passwords.

Verifiable Data Representations

Unlike with physical credentials or cash, issuers of verifiable data (e.g digital identity credentials or digital currency) rely on software or hardware wallets to interpret and convey information to users in a meaningful way by defining the appearance and user experience in key moments, such as credential list views or verification flows.

While there are common patterns applied, the implementation details remain at the sole discretion of wallet providers resulting in representations of verifiable data having wildly different characteristics across various software, platforms and devices. In some ways this is a desirable characteristic as people are able to choose wallets that provide experiences that cater to individual preferences or contextually relevant behaviours, potentially driving accessibility. However, it is our belief that threads of a consistent user experience are vital to enabling trust, potentially allowing individuals to recognise legitimate digital artefacts across multi-modal endpoints.

We suggest that graphical or otherwise UX-informing material embedded or securely referenced in verifiable data, and used by wallets to drive elements of the user experience, could enable this. Being cryptographically verifiable, utilisation of this material could be considered a pseudo level 1 security feature, allowing issuers to inform aesthetic and behavioural characteristic of the data they issue, at least partially, in their own terms.

We intend to explore mechanisms by which verifiable data containers could inform how their contents is conveyed to holders across endpoints. The primary focus will be on how to enabling distinction between different instances of verifiable data (in non-document-centric ways), efficient communication of their contents, status and value. This is predominately envisioned as a 'collaboration' in which wallet providers take materials defined by issuers and choose if and how to make use of it, reflecting the principle of 'designing for appropriation'.

Securely referenced representations of verifiable data, available in a variety of sensory formats, will also help to meet requirements for accessible technology (e.g. European Standard for Digital Accessibility EN301549, June 23, 2021). Opportunities to inform recognisable user experiences could be visual (e.g. issuer logos, credential background images, credential text formatting), auditory or haptic - particularly relevant when attempting to bridge a wide range of form factors (e.g. low-tech cards, screen-readers, high-end mobile devices or emerging AR/VR experiences). We will also explore how we can incorporate existing web accessibility standards to develop inclusive representations (e.g. WCAG, A11y, ARIA).

One topic the paper may need to address is the prominent use of 'cards' as the primary system image presented to users in the majority of available verifiable credential wallets. While offering benefits (e.g. fit with existing user mental models, reduces cognitive load), this approach comes with challenges (e.g. limited scalability, difficult application in combinatorial or non-document centric use cases). The focus of the paper should not be on redesigning wallets around new interaction models, but we should anticipate and cater for their evolution beyond card-centric approaches.

Overlay Capture Architecture (OCA) and accesability

Overlays Capture Architecture (OCA) offers a solution to harmonization between data models and data representation formats. In other words, a way to define the semantics of a data model.

OCA represents a schema as a multi-dimensional object consisting of a stable schema base and linked overlays, data objects that provide additional extensions, coloration, and functionality to the base object. Overlays are cryptographically-linked objects that provide layers of task-oriented contextual information to a Capture Base.

OCA classifies four types of overlays : Semantic overlays, Inputs overlays, transformation, and presentations overlays.

This paper would like to explore how OCA overlays can be used (in particular presentation overlays) or extend the specification to include data representations accessible to all.

Work behond RWTO11 - Improving Annoncreds accesability

AnonCreds specification provides privacy-preserving features that enable verifiable credentials to comply with data privacy law being one of the key reasons governments, in particular, choose to build verifiable credential solutions using AnonCreds .

On top of orivacy-preserving features, governments are tasked with giving every citizen equal access to digital services. Inclusivity is one of the main drivers to achieving a better digital identity by acknowledging the need for equal, convenient, secure, and compatible access for everyone, regardless of individual economic or social circumstances.

We seek contributors interested in incorporating OCA spec into AnonCreds, taking the accessibility angle.

Related Topics

We welcome discussion of related topics posted as RWOT11 advance readings:

Rendering Verifiable Credentials

By Manu Sporny

Known related work

- Credential Representation SVG's - Kiva
  - Github
  - GoogleSlides Presentation
- Authenticated brand-controlled indicators (logos) for message identification in supported email clients, using the emerging BIMI specification.
  - Leverages the work organization has put into deploying DMARC protection.

- User Interaction Design for Secure Systems — Ka-Ping Yee
- An AnonCreds OCA Architecture
- ACA-Py / Aries Framework OCA for AnonCreds