AnonCreds: ~~Ledger~~ VDR Agnostic Authentic Data Specification and Roadmap

Stephen Curran, Cloud Compass Computing Inc. working with the Government of British Columbia

About the AnonCreds Specification

AnonCreds (the shortening of "Anonymous Credentials") format verifiable credentials based on Zero Knowledge Proof (ZKP) capabilities (listed in the appendix below) have been around in various forms for many years. AnonCreds do not adhere to the W3C Verifiable Credential v1.1 Data Model, but can be used in many of the same use cases, especially when privacy is an important component. AnonCreds are being deployed by groups around the world. In the SSI community, AnonCreds are often associated with the open source Hyperledger projects Ursa (cryptography), Indy (decentralized ledger) and Aries (components for secure, peer-to-peer messaging using DIDComm protocols). Recently, a group has been working on creating a formal AnonCreds specification derived from the de facto standard in the Hyperledger AnonCreds implementations. The progress made by the group can be found in the draft specification under the Community Specification License 1.0.

The high-level roadmap for the AnonCreds Specification working group is:

1. v1.0: A specification that defines a Verifiable Data Registry-agnostic version of AnonCreds as it exists in open source implementations today.
2. v2.0: A specification that retains the core privacy-preserving features of AnonCreds, but is open to replacing foundational elements such as the use of CL-Signatures and the revocation mechanism.

Interestingly, the working group began with a plan to create a "v0.1" specification that was to match the "as implemented with Hyperledger Indy." However, we have found that being VDR-agnostic has very little impact on the specification, and in fact, has very little impact on the AnonCreds implementations we have today.

Enabling ~~Ledger~~ VDR Agnostic AnonCreds: Methods

In parallel with the creation of the AnonCreds Specification, a number of groups have been creating non-Indy deployments of AnonCreds. Since AnonCreds requires the use of three published objects in addition to DIDs (Schemas, Credential Definitions and Revocation Registries), such implementations require a way to publish those objects (resources) to a VDR. As those groups and we (in the Working Group) have discovered, there is very little in the existing AnonCreds approach or in the existing open source implementations that is dependent on Hyperledger Indy. Specifically, the open source implementations of AnonCreds already externalize the publishing and retrieving of AnonCreds objects, much

as implementations of DIDs externalize the registering and resolving of DIDs. By using the concept of the DID Specification's "DID Methods" for AnonCreds Objects, we enable VDR-agnostic deployments of AnonCreds. Further, the architecture of Hyperledger Aries implementations makes adding "AnonCreds Objects Methods" easy. We've even added a Registry of methods, just like the "DID Methods Registry" that is referenced in the DID Specification.

AnonCreds at Reboot Web of Trust

The goal for an AnonCreds paper developed at Rebooting Web of Trust is to further the efforts of the AnonCreds Specification working group into new areas and adding details to the group's roadmap. Specifically, we'd like to explore some or all of these sub-topics:

- Provide a background and requirements on the use of AnonCreds when publishing on VDRs other than Hyperledger Indy.
- Discuss and document the publishing of AnonCreds objects to other VDRs.
  - What existing DID Methods support the publishing of arbitrary resources to their VDR instances?
  - Is there a DID specification-friendly way to have a DIDDoc contain or reference AnonCreds objects so that AnonCreds could be used with any DID Method?
- Explore what might be included in AnonCreds v2.0, and specifically:
  - The use of BBS+ Signatures in place of CL-Signatures while retaining all of the core capabilities of AnonCreds.
    - What parts of the specification would be impacted?
    - What to do with elements of AnonCreds that could be eliminated with a BBS+ Signatures version of AnonCreds, such as the option of eliminating the CredDef object. What are the pros and cons of doing that?
    - What more needs to be added to the BBS+ Signatures specification to fully support the capabilities of AnonCreds?
    - What is the open source path to achieving a BBS+ Signatures-based implementation of AnonCreds?
  - Review likely candidates for replacing the current AnonCreds revocation mechanism to support a more scalable, ZKP-based approach.
- Explore the use of DIF's Credential Manifest and Presentation Exchange standards with AnonCreds.
- Explore ways to enable AnonCreds capabilities in future versions of the W3C Verifiable Credential Data Model.

Appendix: A Brief Overview of AnonCreds

AnonCreds ZKP verifiable credentials provide capabilities that many see as important for digital identity use cases in particular, and verifiable data in general. These features include:

- A full implementation of the Layer 3 verifiable credential "Trust Triangle" of the Trust over IP Model.
- Complete flows for issuing verifiable credentials (Issuer to Holder), and requesting, generating and verifying presentations of verifiable claims (Holder to Verifier).
- Fully defined data models for all of the objects in the flows, including verifiable credentials, presentation requests and presentations sourced from multiple credentials.
- Fully defined applications of cryptographic primitives.
- The use of Zero Knowledge Proofs (ZKPs) in the verifiable presentation process to enhance the privacy protections available to the holder in presenting data to verifiers, including:
  - Blinding issuer signatures to prevent correlation based on those signatures.
  - The use of unrevealed identifiers for holder binding to prevent correlation based on such identifiers.
  - The use of predicate proofs to reduce the sharing of PII and potentially correlating data, especially dates (birth, credential issuance/expiry, etc.).
  - A revocation scheme that proves a presentation is based on credentials that have not been revoked by the issuers without revealing correlatable revocation identifiers.