Use Case: DIDs as part of Educational Verifiable Credentials

Name: Life-long, recipient-owned credentials

Background: Educational Verifiable Credentials offer benefits over traditional educational credentials in that the recipient is able to store and share their credentials, and a third party may independently verify the claim (without necessarily consulting the issuer). This provides the promise of recipient-owned long-lived credentials that the recipient may use even if the issuing institution goes out of business.

Usability issues around cryptographic keys introduce a threat to achieving this goal; if the recipient loses their private key, they lose ability to prove ownership of a credential. The existing ways to re-obtain the credential include re-requesting the credential from the issuer, or TBD

If a credential is issued to a recipient's DID, the recipient has the ability to prove ownership of a credential even if the recipient loses a private key used to show ownership of a credential referenced in a claim.

Description: Yanny uses DIDs as subjects of its Verifiable Credentials. By using DIDs, Yanny is able to prove “ownership” of a credential. Even if Yanny loses the private keys corresponding to all keys referenced in the DID document, Yanny is able to invoke the update method on the DID to once again gain control over the DID, and therefore continue to use the Verifiable Credential.

Sticky Wicket: A sentence or three capturing the awkward challenge in this particular situation

Distinction: Emphasizes the full lifecycle of cryptographic key management; i.e. loss of control is handled in a first-class manner via DIDs, and not as an exceptional event.