Why Selective Disclosure?

Kristina Yasuda

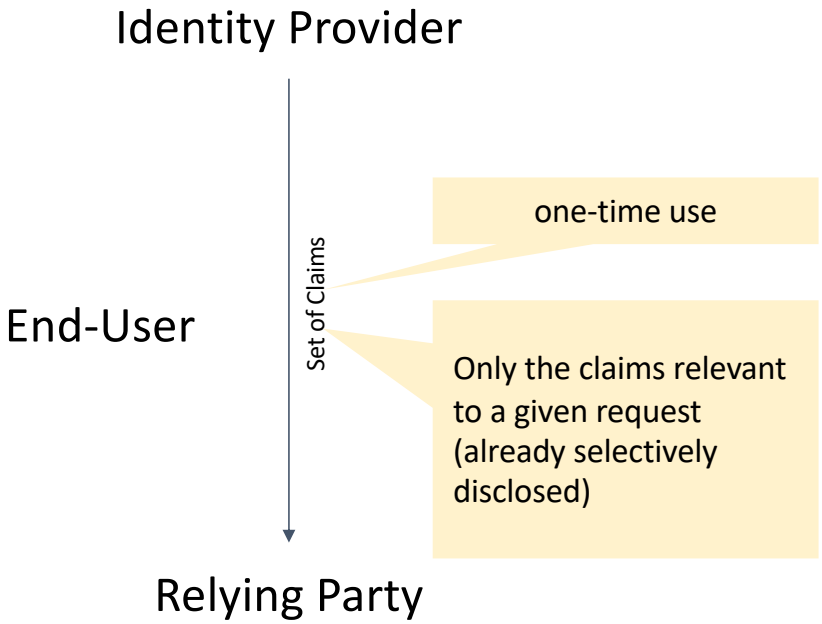
Identity Standards Architect, Microsoft

Co-Chair, W3C Verifiable Credentials WG

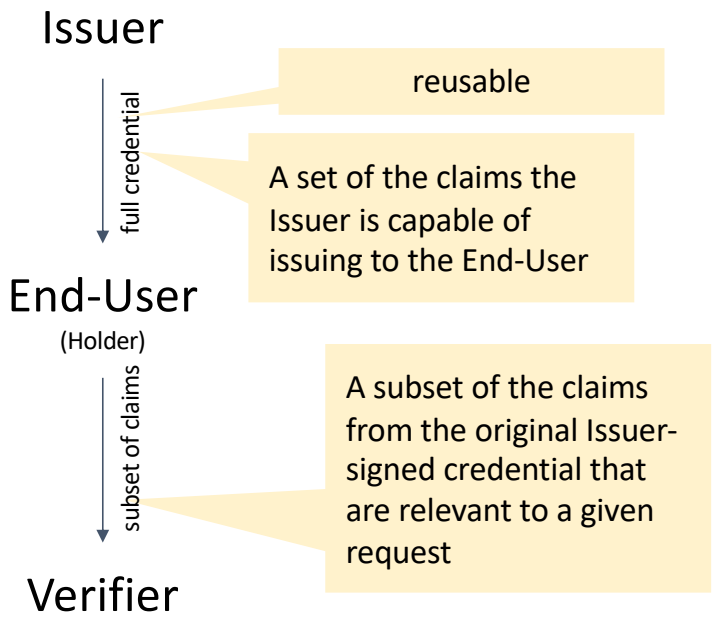
(One of the factors behind)

Increasing importance of Selective Disclosure of User Claims

Identity Federation



Decoupled Issuance / Presentation (W3C VC-DATA-MODEL, ISO 18013-5 mDL, etc.)



Note: in both cases, it is the RP who chooses which claims are required to be released to receive service.

Observation

- Need for a solution that
  - Does not require unlinkability
  - Is standardized (ideally in IETF)
  - Provides not only selective disclosure, but also RP-U unlinkability (and Holder Binding).

Verifiable Credential Protection Using JWPs

Verifiable Credentials Working Group Charter

2.2 Conditional Normative Specifications

Depending on progress in the W3C Credentials Community Group, the IETF, and the DIF, the Working Group may also produce W3C Recommendations based on the following documents:

Specification	Description	Input Documents
PGP Cryptosuite	A cryptographic digital signature suite that utilizes Pretty Good Privacy [RFC4880].	PGP Cryptosuite
BBS+ Cryptosuite	A cryptographic digital signature suite supporting selective disclosure.	BBS+ Cryptosuite
Verifiable Credential Protection Using JWPs	A cryptographic container format for expressing JWT-like proofs for selective disclosure and other modern cryptographic schemes.	VC-JSON Web Proof (JWP)
Koblitz ECDSA Recovery Cryptosuite	A cryptographic digital signature suite supporting elliptic curve public key recovery.	Secp256k1 Recovery Cryptosuite

Other cryptographic suites for NIST RSA, EASC DSA, SM9 IBSA, NIST post-quantum cryptography, or other externally standardized cryptographic primitives may be produced under the same conditions as the table above.

- “Verifiable Credential Protection Using JWPs” is listed as a Conditional Normative deliverable in W3C VC WG, depending on the progress in IETF.