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

Identity Provider

End-User

Set of Claims

Only the claims relevant to a given request (already selectively disclosed)

Relying Party

Verifier

Issuer

End-User (Holder)

subset of claims

A set of the claims the Issuer is capable of issuing to the End-User

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

Issuer

full credential

reusable

A subset of the claims from the original Issuer-signed credential that are relevant to a given request

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:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Description</th>
<th>Input Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>PGP Cryptosuite</td>
<td>A cryptographic digital signature suite that utilizes Pretty Good Privacy [RFC 4880]</td>
<td>PGP Cryptosuite</td>
</tr>
<tr>
<td>BBS+ Cryptosuite</td>
<td>A cryptographic digital signature suite supporting selective disclosure.</td>
<td>BBS+ Cryptosuite</td>
</tr>
<tr>
<td>Verifiable Credential Protection Using JWPs</td>
<td>A cryptographic container format for expressing JWT-like proofs for selective disclosure and other modern cryptographic schemes.</td>
<td>VC-JSON Web Proof (JWP)</td>
</tr>
<tr>
<td>Koblitz ECDSA Recovery Cryptosuite</td>
<td>A cryptographic digital signature suite supporting elliptic curve public key recovery.</td>
<td>Sec256k1 Recovery Cryptosuite</td>
</tr>
</tbody>
</table>

Other cryptographic suites for NIST RSA, EAC 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.