SwissSign Group

SwissID Stellungnahme zu BJ / fedpol PID Paper, Version 1.3

Unsere Annahmen

- Durch die E-Mail Präzisierung «Thematik der transienten und sektoriellen EPID» vom 6.4 sprechen wir nachfolgend anstelle von einer S- oder T-EPID lediglich von der EPID welche durch den IdP vergeben wird.
- Die EPID und E-ID-RN wird im E-ID Namensraum und nicht im Standard-Namensraum geführt. Für die SwissID bedeutet dies, dass wir unseren bestehenden Subject-Identifier im Standard-Namensraum verwenden können, ist dies korrekt?
- Die Codierung erfolgt nun eindeutig nach UTF 8, eingeschränkt auf 00000-0058F, ist dies korrekt? (Seite 4)

EPID Verständnisfragen

- Wann muss oder darf ein IdP eine EPID weiterleiten?
- Wozu muss oder darf ein IdP eine EPID einsetzen?
- Warum muss auch die EPID innerhalb vom Ökosystem kollisionsfrei sein (Roaming-Konzept)?

PID-Signatur Verständnisfragen

- Wer signiert die PID-Attribute einer EPID, ist das SID oder der IdP selbst?
- Wir das gesamte SID-Attributset zusammen mit der EPID signiert oder jedes einzelne SID-Attribut zusammen mit der EPID?

EPID Werteraum

- Die Nutzung des EAN13-Standards ist für die E-ID-RN durchaus sinnvoll. Der Einsatz des Standards für die EPID schränkt den Werteraum aber unnötigerweise zu stark ein. Die <10^11 frei wählbare Kombinationen würden durch die Einteilung in IdPs und Sektoren schnell aufgebraucht (d. H. 1 Mrd pro IdP, welche nur mit z.B. 5 Millionen IdO * 200 vDt aufgebraucht würden)
- Wir empfehlen eine Norm analog UUID V4 mit 5*10^36 Kombinationen. Damit würde auch die Notwendigkeit einer Blockweisen Vergabe wegfallen.

Namensraum / Datenstruktur

- Warum muss SID auch den Namensraum der privaten Claims definieren? Fallen die privaten Claims nicht in den Namensraum des jeweiligen IdPs?
- Warum wird der E-ID Namensraum nicht auf Basis der bestehenden Standards eCH-11/21/44/8/10 gesetzt?
- Die Definition eines ch.admin.ejpd.eid.sid.nonce ist unnötig da ein Reply Attack schon durch den nonce im Standard-Namensraum verhindert wird.
- Wenn ein Bürger der auf unserem IdP ist aber noch keine E-ID hat, müssen wir in diesem Fall auch den ch.admin.ejpd.eid. Namensraum benutzen? (Seite 4)
- Was ist die Idee die IdP Daten unter dem ch.admin.ejpd.eid Namensraum zu halten? (Seite 4)

Übermittlung vom SID an die IdP

- Wir lesen zwei Standards aus dem Flow heraus zertifikatsbasierte gegenseitige Authentifizierung (Mutual Authentication TLS) und OpenID Connect (OIDC)? Falls ja, wäre die Referenz dazu klarer und ausreichend.
- Die Vorgabe die Zertifikate per Mail auszutauschen scheint uns zu spezifisch und schliesst üblichere Austauschmethoden aus.

Bemerkungen

- Wir bestätigen, dass wir die Meinung teilen, dass eine Unterscheidung nach transienten und sektorieller EPID keinen Sinn aus unserer Sicht macht.
- Die EAN13 ist nicht in ISO 3166-3 definiert.
- Typo «Nounce» im Beispiel Übermittlung vom SID an IdP
- Um semantisch korrekt zu sein müsste man «sex» statt «gender» nutzen.
- Uns scheint «picture» oder «facial_image» besser als «face».