Comments on „Identity in the Cloud Gap Analysis Version 1.0“ Public Review Draft 02

General: Granularity of referenced standards

The concern of eGov WG is that standards are not referenced in appropriate detail. OIDC is references with 13 documents, whereas SAML with just one, plus one specialized profile (STORK).

It would be useful to reference a standard in a schema that is aware of a hierarchy of stack, use case and profile.

For example:

SAML 2.0/Web SSO Use Case/Saml2int profile

WS-*/WS-Federation (no profile)

OAUTH2/Web-Application Flow (no profile)

The reference of specific documents might be less useful in the context of this document, unless a document references a single standard and a single use case.

Re 3.4.5 (UC4 Identity Configuration)

(unrelated typo: change LDIFF to LDIF)

Existing text: “*There is a SAML construct for sending identity information (SAML assertions about an identity from a trusted third party will result in creation the identity). Namespaces are present in SAML attributes*.”

Proposed text: “SAML-2.0 core specifies SAML assertions that are a generic data structure about an identity from a trusted third party. SAML Assertions are used in different protocols and use cases like SAML WebSSO, WS-Trust, SCIM and OIDC. There are options for confirmation methods for clients holding key material, passive clients that can safely redirect http-requests between servers (a.k.a. web browsers), and clients acting via trusted gateways.”

Re 3.5.6 Possible GAPs identified in UC5: Middleware Container in a Public Cloud

Additionally identified gap:

Deployment issue: Middleware containers need to have a high degree of interoperability. Standards may not life up to that expectation and might need profiling.

Re 3.6: Federated SSO and Attribute Sharing

Additional notes:

1. Internet draft http://macedir.org/draft-macedir-entity-category-00.html proposes improved attribute interoperability by categorizing services that are compliant to a specific attribute release policy, which an IDP will require. SAML V2.0 Metadata Extension for Entity Attributes is providing a metadata construct to support these entity categories.
2. The configuration of asserting and relying parties should be considered as a separate use case, as it is essential for scalable deployments to establish technical trust, endpoint addresses, service discovery etc. The SAML-2.0 Meta-IOP specification provides a comprehensive structure to provide that.

Re 3.12 UC 12: Consumer Cloud Identity Management, SSO

The statement „If an EU/EEA public authority is using federation, use of STORK is a requirement.“ is too wide, because the EU’s mandate is just citizen eID interoperability, anything else is on a voluntary basis. Also it could be implied that the STORK SAML profile is mandatory on the national side, which is not the case. Therefore the suggested phrasing is:

“If an EU/EEA public authority is using cross-border federation, use of STORK between national gateways (“PEPS”) is a requirement.”