Inputs to the Selection UI

Abstract

This document is a product of the Universal Login Experience Work Group. It records the requirements for the user experience based on scenarios and use cases.

Status

This document is currently under active development. Its latest version can always be found here. See the ulx:Change History at the end of this document for its revision number.

Editors

- TBD

Overview

This is a summary of the collective set of information supplied by all of the actors (IdP, RP, User Agent) in constructing a suitable pop-up experience for discovery.

Relying Party Inputs

- Required/Optional Claims
  - Required and optional identifier/attribute information needed to proceed with login and "immediately expected" user activity.
- Assurance Characteristics
  - Capturing properties of RP's security/identity requirements that might impact IdP selection.
- Trusted Issuers
  - Names of acceptable IdPs and local sources of authentication
- Preferred Issuers
  - Opportunity to bias or pre-populate choices based on expected user population using particular choices
- UI Information
  - Properties to influence UI (screen type [ulx:WAP, smartphone, TV, regular web browser ...], users's preferred language, colors, fonts, ...)

Comments:

1. PAUL: I'd like to see an "attributes first" approach supported (details)

Identity Provider Inputs

- Supported Claims
  - Identifier/attribute information offered
- Assurance Characteristics
  - Capturing properties of IdP's security/identity requirements that might impact RP acceptance.
- Logo/Name/Description
  - Information needed to drive presentation of IdP as a choice.
- Presentation Requirements
  - Can login be accomplished within a pop-up (with address bar) or is a full frame required?
- Registration/Credentialing Bootstrap
  - Link to location(s) to help users acquire the necessary credential (e.g. an Infocard)

Supported claims

IDP's supported attributes and claims

SAML

Already defined in SAML Metadata specifications

Example :

```
<IDPSSODescriptor WantAuthnRequestsSigned="true"
     protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  ...
  <saml:Attribute
     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
     Name="urn:saml_attribute_name_1" />
  <saml:Attribute
     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
     Name="urn:saml_attribute_name_2" />
  ...
</IDPSSODescriptor>
```

OpenID

- The Yadis XRDS document only advertizes the SREG/AX service(s) supported by the OP but not the exact list of supported attributes/claims.
- Proposal : Extension to the YADIS XRDS document.

> *Explicitly advertize OP's supported attributes/claims part of XRDS document published by the OP ?*
> Help needed on best way to do it with XRDS…

InfoCard

Supported claims are advertized at the creation/import of the Information Card.

Assurance Characteristics

IDP's supported Authentication Contexts and Assurance Levels

SAML

Generic mechanism defined in "SAML Metadata Extension for Entity Attributes" and specific attribute already defined in "SAML Identity Assurance Profiles"

Proposal for ACs : define a new attribute name for Authentication Context classes :

```
urn:oasis:names:tc:SAML:attribute:authn-context-class
```

OpenID

Supported Authentication policies can already be advertized in the Yadis XRDS document as specified in "OpenID Provider Authentication Policy Extension 1.0" (*should also be used to advertize supported Assurance Level ?*)

Can *PAPE* be used as well to advertize the OP's Assurance Level ? (and how does it relates to the *OIX Listing Service* ?)

InfoCard

- Authentication Contexts and Assurance Levels are just considered as claims.
- As an example, claims for Assurance Levels have been defined by ICF :

```
icam-assurance-level-1
icam-assurance-level-2
icam-assurance-level-3
```

Logo/Name/Description

SAML

An OASIS working draft exists with SAML metadata extensions for capturing this information. It is protocol agnostic.

http://wiki.oasis-open.org/security/SAML2MetadataUI

OpenID

Proposal : Extension to the YADIS XRDS document

> *Advertize OP's DisplayName and Logo URL part of XRDS document published by the OP ?*
> Help needed on best way to do it with XRDS…

InfoCard

N/A (either just the "InfoCard" logo or CardTile of the last used InfoCard)

User Agent Inputs

- Preferred/Supported/Previously Used Issuers
  - Opportunity to bias or pre-populate choices based on history, user affiliations/preferences, etc.
- Accessibility Requirements
  - Do pop-ups cause accessibility concerns for discovery or login?

See Also

- RP Metadata