

RP Metadata

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

Intellectual Property Notice

The Universal Login Experience Work Group operates under [Option Liberty](#) and the publication of this document is governed by the policies outlined in this option.

Table of Contents

- [1 Table of Contents](#)

Frequently, a relying party (RP) is capable of supporting authentication of users and exchange of identity information using more than one protocol. Unfortunately, the user experience for these RPs is often confusing and includes options that are not supported by the browser.

This document describes a format for RPs to use to express their capabilities and requirements to browsers.

RP Metadata Reference

The RP embeds an element on its login page that contains an ordered sequence of references to metadata files specific to each of the RP's supported login protocols, in order of preference. This allows an enhanced browser to only download metadata for protocols it supports. The login page also contains legacy login markup for unenhanced browsers. Additionally, an RP can include a privacy policy related to the identity information it receives.

```
<RPLoginMetadata>
  <xrd:XRD xmlns:xrd="xri://$xrd*(($v*2.0)" version="2.0">
    <xrd:Type>xri://$xrds*simple</xrd:Type>
    <xrd:Service>
      <xrd:Type>http://www.kantarainitiative.org/metadata/1.0/rplogin</xrd:Type>
      <xrd:Subject>http://www.kantarainitiative.org/metadata/1.0/saml2</xrd:Subject>
      <xrd:URI simple:httpMethod="GET">http://rp.com/my_saml2_login_metadata.xml</xrd:URI>
    </xrd:Service>
    <xrd:Service>
      <xrd:Type>http://www.kantarainitiative.org/metadata/1.0/rplogin</xrd:Type>
      <xrd:Subject>http://www.kantarainitiative.org/metadata/1.0/imi</xrd:Subject>
      <xrd:URI simple:httpMethod="GET">http://rp.com/my_imi_login_metadata.xml</xrd:URI>
    </xrd:Service>
    <xrd:Service>
      <xrd:Type>http://www.kantarainitiative.org/metadata/1.0/rplogin</xrd:Type>
      <xrd:Subject>http://www.kantarainitiative.org/metadata/1.0/openid</xrd:Subject>
      <xrd:URI simple:httpMethod="GET">http://rp.com/my_openid_login_metadata.xml</xrd:URI>
    </xrd:Service>
    <xrd:Type>http://www.kantarainitiative.org/metadata/1.0/rpprivacypolicy</xrd:Type>
    <xrd:URI simple:httpMethod="GET">http://rp.com/my_privacy_metadata.xml</xrd:URI>
  </xrd:Service>
</xrd:XRD>
</RPLoginMetadata>
```

For each protocol, a metadata file is provided containing a protocol specific set of acceptable providers and a link to a set of claims.

```
<xrd:XRD xmlns:xrd="xri://$xrd*(($v*2.0)" version="2.0">
  <xrd:Type>xri://$xrds*simple</xrd:Type>
  <xrd:Service>
    <xrd:Type>http://www.kantarainitiative.org/metadata/1.0/provider</xrd:Type>
    <xrd:URI>http://idpl.com/imi</xrd:URI>
  </xrd:Service>
  <xrd:Service>
    <xrd:Type>http://www.kantarainitiative.org/metadata/1.0/provider</xrd:Type>
    <xrd:URI>http://idp2.com/imi</xrd:URI>
  </xrd:Service>
  <xrd:Service>
    <xrd:Type>http://www.kantarainitiative.org/metadata/1.0/claims</xrd:Type>
    <xrd:URI simple:httpMethod="GET">http://rp.com/my_imi_claims.xml</xrd:URI>
  </xrd:Service>
</xrd:XRD>
```