UTokyo Account & mdx AAL2&IAL2対応

東京大学 情報システム本部
中村 誠

UTokyo Account IdP

- Shibboleth IdPとADFS（RemoteUser認証フロー）で構成し、ADFSからAzure MFAと連携　→　絶賛MFA展開中

UTokyo Account は、東京大学構成員（学生および教職員）の情報サービス利用を統合的に提供するアカウントです。教職員、学生の皆さんが利用する多くの全学情報サービスがこのアカウントで利用する事ができます。
UTokyo Account provides most of information services for students and faculties.

UTokyo Account IdP: AAL2対応（試行錯誤）

- Shibboleth IdPとADFS（RemoteUser認証フロー）で構成し、ADFSからAzure MFAと連携
  - 認証フロー単位で**AuthnContextClassRef**を識別
  - **SAML Proxy**で上位IdPのでAuthnContextClassRefを伝播
- Azure ADはAuthnContextClassRefを返すらしい
  - **http://schemas.microsoft.com/claims/multipleauthn**

- SAML ProxyでAzure ADと連携させてみる
  - 設定項目は多いが書いてある通りでOK
  - Shibbolethの設定は奥が深い

- （IAL2対応は通常の属性送信と同じ対応なので割愛）

※ https://shibboleth.atlassian.net/wiki/x/_YJxVw

Using SAML Proxying in the Shibboleth IdP to connect with Azure AD

Created by Chris.Phillips@canarie.ca
Last updated: May 19, 2022 by Scott Cantor • 22 min read

A French version of this document can be found on the CANARIE website.

⚠ Please read and follow the documentation first, before or along with using this example. This documentation is not maintained by the development team and may not be entirely accurate or consistent with the software at any given time. It is a complement to the documentation, not a replacement for it. It is currently out of date with respect to some improvements made in V4.1.

mdxのAAL2対応（試行錯誤）

- SPの1つがShibboleth SP&学認DSで実装
  - Azure ADを独自IdPとして連携させてみる
- DS設定をカスタマイズし独自IdPとパラメタを追加

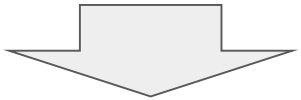
  var **wayf_sp_samlDSURL** = wayf_sp_handlerURL +
  "/DS?**authnContextClassRef=http%3a%2f%2fschemas.microsoft.com%2fclaims%2fmultipleauthn**";
  var **wayf_additional_idps** = [{name:"Azure AD <tenantid>",
  entityID:"https://sts.windows.net/<tenantid>/",
  SAML1SSOurl:"https://login.microsoftonline.com/<tenantid>/saml2"},];

- （嵌りポイント）Azure ADのSAMLメタデータにはScope定義がない
  → eppnが見えない

  <IDPSSODescriptor>
  <Extensions>**<Scope regexp="false">**u-tokyo.ac.jp**<Scope>**</Extensions>

次世代学認への期待

1. 強固な認証(AAL2)
2. 学術機関以外をカバーした認証プロバイダ(IdP)連携
3. わかりやすいRFC類



幅広いユーザに対して
多くのサービス(mdx, GakuNin RDMもそのひとつ)が
連携する未来

（参考）Azure ADのSAML Response

・Response の AuthnStatement, AuthnContext, AuthnContextClassRef に返してくれる

```
<samlp:Response ...>
  <Assertion ...">
    <AuthnStatement ...>
      <AuthnContext>
        <AuthnContextClassRef>http://schemas.microsoft.com/claims/multipleauthn</AuthnContextClassRef>
      </AuthnContext>
    </AuthnStatement>
  </Assertion>
</samlp:Response>
```