AAL2およびIAL2の提示および要求について

2022.6.2　NII学術情報基盤オープンフォーラム2022
国立情報学研究所　西村 健

IALおよびAALを表現する要素・属性

- SAMLでの規定およびREFEDS等での利用から下記要素・属性を用いるのが適当である
  - 学認のAALを格納するために AuthnContextClassRef を用いることとする
    - 参照: https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
  - 学認のIALを格納するために eduPersonAssurance属性を用いることとする
    - 参照: https://meatwiki.nii.ac.jp/confluence/display/GakuNinShibInstall/eduPersonAssurance

SPからの多要素認証要求

- SAMLの規定により、認証要求(AuthnRequest)には AuthnContextClassRef という認証方式に関するパラメーターを含めることができる
  - 普通は無指定（どんな認証方式でもOK）
  - パスワード認証は以下の識別子で指定できる:
    urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport

- 通常はパスワード認証でOKだが、機密度・重要度の高いサービスは「パスワードでない何か」を求めることができる

学認のIAL2/AAL2を示す識別子

- AAL2については認証要求およびアサーションのAuthnContextClassRefに下記識別子を格納する
  - 識別子: “https://www.gakunin.jp/profile/AAL2”
- IAL2についてはアサーションのeduPersonAssurance属性に下記識別子を格納する
  - 識別子: “https://www.gakunin.jp/profile/IAL2”

Shibboleth SPでの記述例

- AAL2を要求
  - Apache設定

```
<Location /restricted-attrviewer/ialaal.php>
    ShibRequestSetting authnContextClassRef https://www.gakunin.jp/profile/AAL2
</Location>
```

- IAL2を受信
  - PHPコード

```
$ary = preg_split("/(?<!¥¥);/", $_SERVER["assurance"]);
foreach ($ary as $val) {
    if ($val == "https://www.gakunin.jp/profile/IAL2") {
        ....
    }
}
```

- AAL2を受信（要求に応えるのはSAML的にMUSTだが念の為）
  - PHPコード

```
if ($_SERVER["Shib-AuthnContext-Class"] ==
        "https://www.gakunin.jp/profile/AAL2") {
```

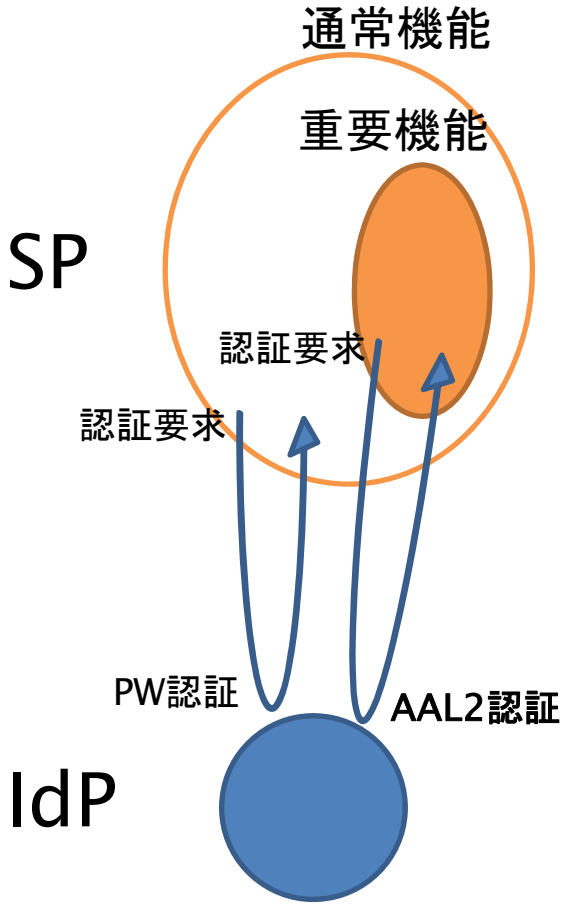
Shibboleth IdPの設定方法例

- AAL2について:
  - MultiFactor認証フロー(MFA)を用いた認証設定
    https://meatwiki.nii.ac.jp/confluence/x/UJSPAQ
    - これは、SPからの要求に合わせてIdPが持っている複数のログインフロー（認証手段）から適切なものを組み合わせて実行するもの
  - 以下の識別子で挙動を変える例を提示している
    - urn:mace:gakunin.jp:idprivacy:ac:classes:Level1
      urn:mace:gakunin.jp:idprivacy:ac:classes:Level2
      urn:mace:gakunin.jp:idprivacy:ac:classes:Level3
  - 認証フローは別途用意しなければならない。例えば:
    - パスワード認証
    - TLSクライアント証明書認証 https://meatwiki.nii.ac.jp/confluence/x/34W5
    - TOTP認証 https://shibboleth.atlassian.net/l/c/DH9FeWJv
    - tiqr認証 https://meatwiki.nii.ac.jp/confluence/display/tiqr
    - など
- 他のIdPにプロキシする場合などは設定方法が異なる
- IAL2について:eduPersonAssurance属性は通常の属性と同じく設定・送出可能

AAL2利用SPシナリオ例：ステップアップ認証パターン

- ①(SP)AAL2に限定しないログインを行う
  - ここでAAL2で認証された場合はセッションにフラグを立てる
- (SP)ログイン後の処理・ユーザー操作を受け付ける
- ②(SP)AAL2を要求する機能を要求された場合、かつAAL2で認証したことがない場合
  - ③(SP)AAL2限定のログインを行う
    - DSにてAAL2をサポートしたIdPのみ表示する
  - ④(SP)AAL2で認証されたことが確認できればフラグを立てる
- ⑤(SP)フラグが立っていれば当該機能を提供する

- 他の考慮点：AAL2付与されないIDへの救済措置



メタデータへの記載の検討

- IdPがIAL2/AAL2対応か否かの情報をSPと共有するためにIdPメタデータへの記載方法を検討したい
  - 有効利用の例：IAL2対応のIdPのみをリストしてユーザに選択させる
- 参考: 学認MFAプロファイル
  - IdPについて、当該プロファイルに適合していることを表す
  - 適合していても全てのIDについてIAL2/AAL2が出せるわけではない
  - <mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
    <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    Name="urn:oasis:names:tc:SAML:attribute:assurance-certification">
    <saml:AttributeValue>https://www.gakunin.jp/profile/mfa</saml:AttributeValue>
    </saml:Attribute>
    </mdattr:EntityAttributes>
- SPメタデータへ記載する場合にはその意味するところから検討する必要がある
  - IAL2/AAL2を要求する場合にEntityAttributeを記載するか?
  - IdPごとに要求するレベルが異なる場合があるか?

まとめ

- AuthnContextClassRefを用いたAAL2の要求・提示
- eduPersonAssurance属性を用いたIAL2の提示

- IAL2/AAL2を使った設定方法をドキュメントとして公開予定