学認でのAAL2について

2021/07/26 次世代認証連携検討作業部会

AAL1およびAAL2の要件

要件	AAL1	AAL2
許可されているAuthenticatorタイプ	記憶シークレット; ルックアップシークレット; アウトオブバンド; 単一要素OTPデバイス; 多要素OTPデバイス; 単一要素暗号ソフトウェア; 単一要素暗号デバイス; 多要素暗号ソフトウェア; 多要素暗号デバイス	多要素OTPデバイス; 多要素暗号ソフトウェア; 多要素暗号デバイス; または 記憶シークレット及び • ルックアップシークレット • アウトオブバンド • 単一要素OTPデバイス • 単一要素暗号ソフトウェア • 単一要素暗号デバイス
FIPS 140 確認	Level 1 (政府機関のVerifier)	Level 1 (政府機関のAuthenticator及びVerifier)
Reauthentication	30 日	12 時間 または 30 分 の非活動, 1つのAuthentication要素でもよい (MAY)
セキュリティ統制	SP 800-53 低度のベースライン(または等価)	SP 800-53 中度のベースライン(または等価)
中間者攻撃耐性	必須	必須
Verifierなりすまし耐性	不要	不要
Verifier危殆化耐性	不要	不要
リプレイ耐性	不要	必須
Authentication意図	不要	推奨
レコード保持ポリシ	必須	必須
プライバシ統制	必須	必須

AAL2として認められるAuthenticatorのタイプ

AAL2のAuthenticationでは,

- 一つの多要素Authenticator または
- 2つの単一要素Authenticatorの組み合わせ（同時）

のどちらかを利用するものとする(SHALL)

→AAL2では「二要素認証」が必須（AAL1では何をつかってもよい）

Authenticatorタイプ（AAL1・AAL2）

AAL1	AAL2
● 記憶シークレット ● ルックアップシークレット ● アウトオブバンド ● 単一要素OTPデバイス ● 多要素OTPデバイス ● 単一要素暗号ソフトウェア ● 単一要素暗号デバイス ● 多要素暗号ソフトウェア ● 多要素暗号デバイス	● 多要素OTPデバイス ● 多要素暗号ソフトウェア ● 多要素暗号デバイス ● または 記憶シークレット及び: ○ ルックアップシークレット ○ アウトオブバンド ○ 単一要素OTPデバイス ○ 単一要素暗号ソフトウェア ○ 単一要素暗号デバイス

Authenticator のタイプ（1）

- **記憶シークレット**
  - ユーザが記憶するもの。パスワードやPIN。

- **ルックアップシークレット**
  - 認証したい人(Claimant)と認証情報を払い出す側(CSP)との間で共有されるシークレット。乱数表やリカバリコードのようなもの。

- **アウトオブバンド**
  - 別経路を介して安全に通信できるようなもの。SMSでのコード送信、QRコード読み取り、電話での読み上げ・入力など。

Authenticator のタイプ（2）

- **単一要素OTPデバイス**
  - 何らかのアクティベーションを必要としないOTP生成デバイス。Google 認証システムのようなアプリケーション（ただしロックしていない）、OTPトークンなど。
- **多要素OTPデバイス**
  - 単一要素OTPデバイスに、さらに二要素目の入力によるアクティベーションを追加したもの。Face ID 、Touch ID やパスワードでアクティベートして利用するスマホ用OTPアプリなど

Authenticator のタイプ（3）

- **単一要素暗号ソフトウェア**
  - ディスクあるいはソフト媒体に記録された一意な秘密鍵。端末ごとのクライアント証明書（パスワード保護なし）

- **単一要素暗号デバイス**
  - 保護された暗号鍵を用いて認証を行うハードウェアデバイス。秘密鍵をエクスポートできない。FIDO U2F のUSBキーなど。

- **多要素暗号ソフトウェア**
  - 単一要素暗号ソフトウェアに、さらに二要素目の入力によるアクティベーションを追加したもの。指紋認証で有効化されるクライアント証明書など。

- **多要素暗号デバイス**
  - 単一要素暗号デバイスに、さらに二要素目の入力によるアクティベーションを追加したもの。指紋などでアクティベートしなければ利用できないFIDOのUSBキーなど

学認でのAAL2対応について

- Shibboleth IdP
  - 記憶シークレット＋ **単一要素暗号ソフトウェア**
    - パスワード＋ **クライアント証明書**
  - 記憶シークレット＋ **単一要素OTPデバイス**
    - パスワード＋ **TOTP**
  - 記憶シークレット＋ **アウトオブバンド**
    - パスワード＋ **tiqr**
  - 記憶シークレット＋ **単一要素暗号デバイス**
    - パスワード＋ **FIDO2 (WebAuthn) ※プラグイン提供予定**

学認でのAAL2対応について

- 他IDaaS製品
  - 記憶シークレット＋ **単一要素OTPデバイス**
    - パスワード＋ **TOTP**
  - 記憶シークレット＋ **単一要素暗号ソフトウェア**
    - パスワード＋ **クライアント証明書**
  - 記憶シークレット＋ **単一要素暗号デバイス**
    - パスワード＋ **FIDO**
  - 記憶シークレット＋ **アウトオブバンド**
    - パスワード＋ **QRコード**

学認での認証に用いるAuthenticator

- ブラウザを介する認証でAuthenticatorを用いる
  - IdPにおいて、利用者が用いるAuthenticatorの単一要素○○ と 多要素○○ を区別することが難しい。
    - クライアント証明書がパスワード等で保護されているか
    - FIDOキーが指紋認証などで保護されているか
- 利用者のAuthenticatorを指定出来ない場合、記憶シークレットと組み合わせることがAAL2（二要素認証）とするために必要

学認MFAプロファイル

- 参加機関が導入しやすいように統一的な基準を制定
  - 学認多要素認証プロファイル
    - アサーションに含める値を定義するプロファイル
      - 当該ユーザが多要素で認証されたことを明示し、保証
    - REFEDSのプロファイルをベースに作成
      - 学認のプロファイルとイコールではないが、条件を満たそうとしたときに、余分な処理が必要ないよう配慮
      - 将来的にeduGAINのSPとの連携も容易になる
  - UPKIクライアント証明書を多要素認証の１要素とする基準とガイドを作成
    - 体制やルールの構築・整備を高速化・容易化
    - **学認MFAクライアント証明書運用基準**
      - この基準に従うことで、学認多要素認証プロファイルに定める、IdPから送出するSAMLアサーションの基準に適合する
    - **学認MFAクライアント証明書運用ガイド**
      - 本ガイドラインにそってクライアント証明書を運用すると、「学認多要素認証プロファイル」に定めるSAMLアサーションをIdPから送出する資格を満たす