認証器レジストリについて

NII学術情報基盤オープンフォーラム2023
認証トラック3

目次

- 認証器レジストリとは？
- 認証器とは？
- 認証器レジストリの目的
- これまでの活動
- 今後の予定

認証器レジストリとは？

- 学認が提供する、学認AAL2対応認証器と関連する情報が登録されたレジストリ
  - 学認は「認証器」の性能を調査し、当該認証器がAAL2の認証に利用できるか？がわかるレジストリを用意する
  - 学認参加機関の求めに応じて認証器の審査・認定を行った場合、その結果を登録して定期的に更新する

認証器とは？

認証器(Authenticator)とは？

- 認証器、認証デバイス、Authenticator
  - 利用者が認証に用いる仕組み
  - 利用者本人しか知らない情報（知識）、持っていないもの（所持）、特徴（生体）を示すことができる道具

学認AAL2基準のもととなった文書

- NIST SP800-63
  - 米国立標準研究所が発行する電子認証に関するガイドライン
  - 米政府機関が対象
- Kantara KIAF1440
  - Kantara Initiativeが提供する文書
  - KIAF: Kantara Identity Assurance Framework
  - NIST SP800-63Bを評価
    - AAL2とAAL3を対象

認証器の種類

- (ア) Single-Factor OTP Device（単要素OTPデバイス）
- (イ) Multi-Factor OTP Device（多要素OTPデバイス）
- (ウ) Single-Factor Cryptographic Software（単要素暗号ソフトウェア）
- (エ) Multi-Factor Cryptographic Device（多要素暗号ソフトウェア）
- (オ) Single-Factor Cryptographic Device（単要素暗号デバイス）
- (カ) Multi-Factor Cryptographic Device（多要素暗号デバイス）
- (キ) Memorized Secret（記憶シークレット）
- (ク) Look-Up Secret（参照シークレット）
- (ケ) Out-of-Band Device（経路外デバイス）

AAL1およびAAL2の要件（NIST SP800-63）

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

認証器の分類（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

AAL2として認められる認証器

- NIST SP800−63
  - AAL2の認証では,
    - 一つの多要素認証器 または
    - 2つの単一要素認証器の組み合わせ（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）
- Kantara KIAF1440
  - 「多要素認証器1個またはパスワード認証に所持要素に基づく認証器を組み合わせたもの」
    をAAL2に対応する認証器の要件としている。
- 学認AAL2では、KIAF1440と同様の要件を求めることとする

認証器のタイプ(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。

認証器のタイプ(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/Microsoft Authenticator 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

認証器のタイプ(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(パスワード等での保護なし)
- **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準拠のセキュリティキーなど。
- **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準拠のセキュリティキーなど

認証器レジストリの目的

認証器レジストリの目的

- 学認AAL2の認定と運用のためには、多数ある認証器の評価が必要
- 市場に流通する認証器ごとに、学認参加機関が各自でAAL2準拠を評価することは、合理的ではない
  - この認証器はどのタイプに該当するのか？
  - この認証器は学認AAL2基準のチェック項目を満たすか？
  - この認証器は単体で単要素か？多要素か？
- 認証器の性能を調査し、AAL2基準を満たす認証に利用可能かを判定し、結果を公開する認証器レジストリが重要な役割をもつ

これまでの活動

学認AAL2対応認証器 評価基準の作成

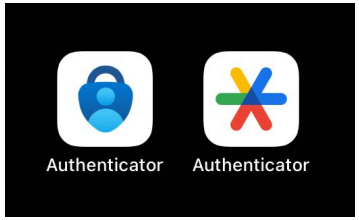
- 学認AAL2基準の目安として標準化団体のKantara Initiativeが策定しているKIAF1440を参照
- 認証器の評価項目洗い出し
- 認証器の学認AAL2対応評価用チェックリストを作成

認証器レジストリに関する運用設計

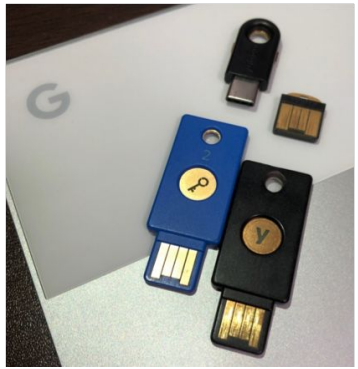
- 「学認AAL2対応認証器 評価基準」で作成した AAL2対応評価基準に基づき、認証器レジストリを運用するための設計を行う。
- この中では認証器の評価を行うための運用方針を策定し、具体的な運用方法の整理を行い、運用設計を行う。
- また併せて、候補となる認証器の申請・評価・公開・利用停止の一連のライフサイクルの設計を行う。

評価対象の認証器

- 現在評価中の認証器
  - 単要素OTPデバイスとして
    - Microsoft Authenticator
    - Google Authenticator



- 評価候補の認証器
  - 単一要素暗号デバイス
    - FIDO準拠セキュリティキー
  - 単一要素暗号ソフトウェア
    - UPKI電子証明書発行サービスのクライアント証明書



上：発表者スマートフォン画面より
下：発表者私物

今後の予定

今後の予定

- 認証器の評価
- 認証器レジストリの公開・運用
- 認証要求を検証する側（IdP、IDaaS）の評価

認証器の運用

- 学認AAL2基準を満たすために、認証器それ自体の選定に加え、運用面での評価も必要。
  - 適切に運用できるIdPは何か？
  - 適切に運用できるIDaaS製品はあるか？
- 学認AAL2は、認証器が要件を満たし、またその認証器を用いた認証システムの実装と運用が適切に行われてはじめて基準を充足する