公的個人認証サービスの民間利用拡大に向けて

第９回　社会情報流通基盤研究センター・シンポジウム

東京工業大学　科学技術創成研究院

未来産業技術研究所 兼 社会情報流通基盤研究センター

小尾高史

研究の内容

- 公的個人認証サービスの利用拡大には、様々な用途での活用が期待される電子利用者証明（電子認証）機能の利用拡大が重要
- 電子利用者証明機能は、公共分野での利用にとどまらず、多くの民間事業者が利用することを想定
- 公的個人認証サービス、特に電子利用者証明機能の民間分野での利用拡大を検討

JPKI PF事業者のサービス機能強化

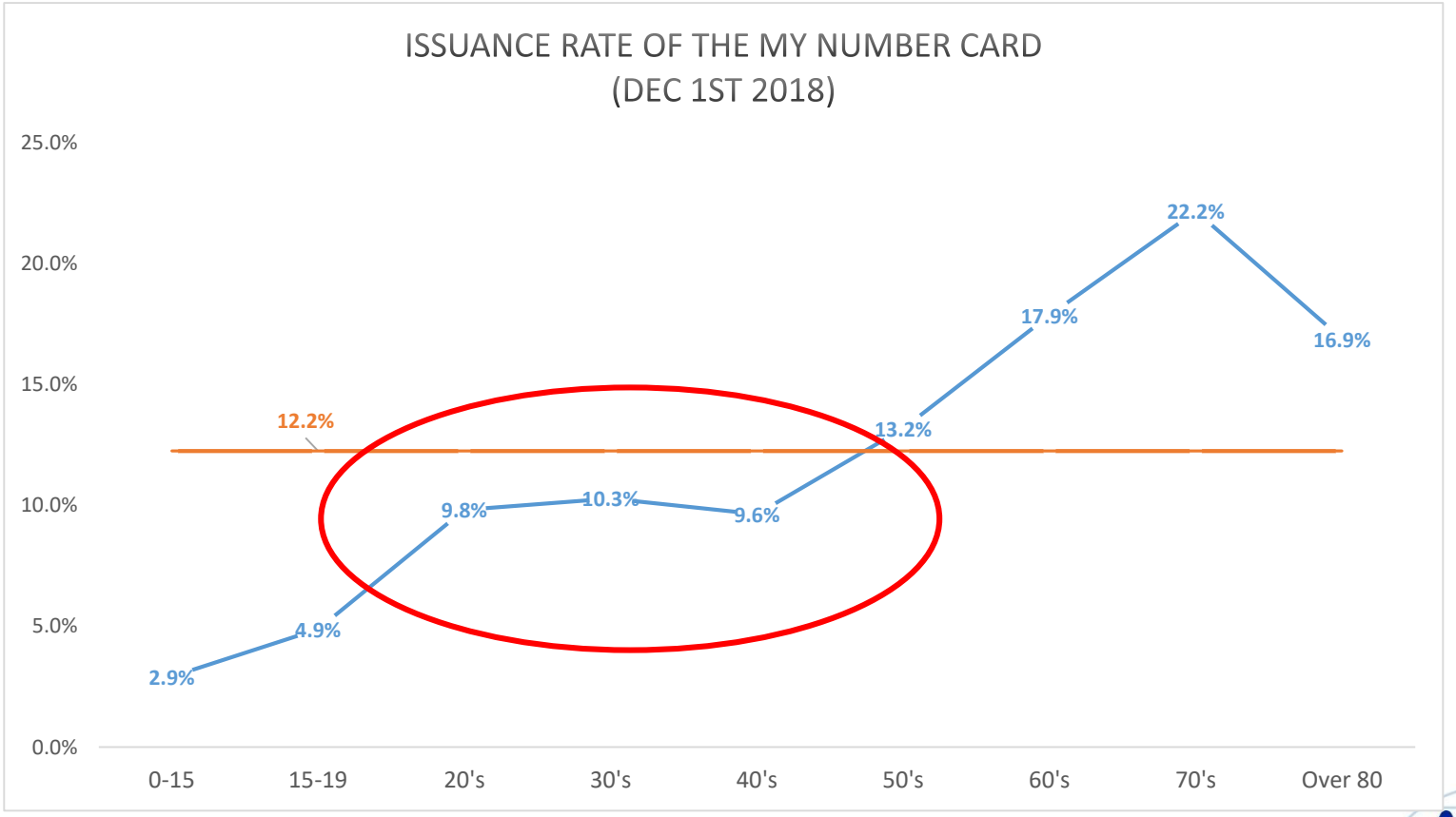
- 金融分野などの民間取り引きにおける Identity Assurance Level（IAL）、Authenticator Assurance Level(AAL)強化の方向性
  （SP800-63-3では、乱数表の再利用否定、経路外認証器の利用制限）

- PF事業者の機能拡大による利用シーンの拡大
  JPKIと連携したモバイル認証サービスの提供

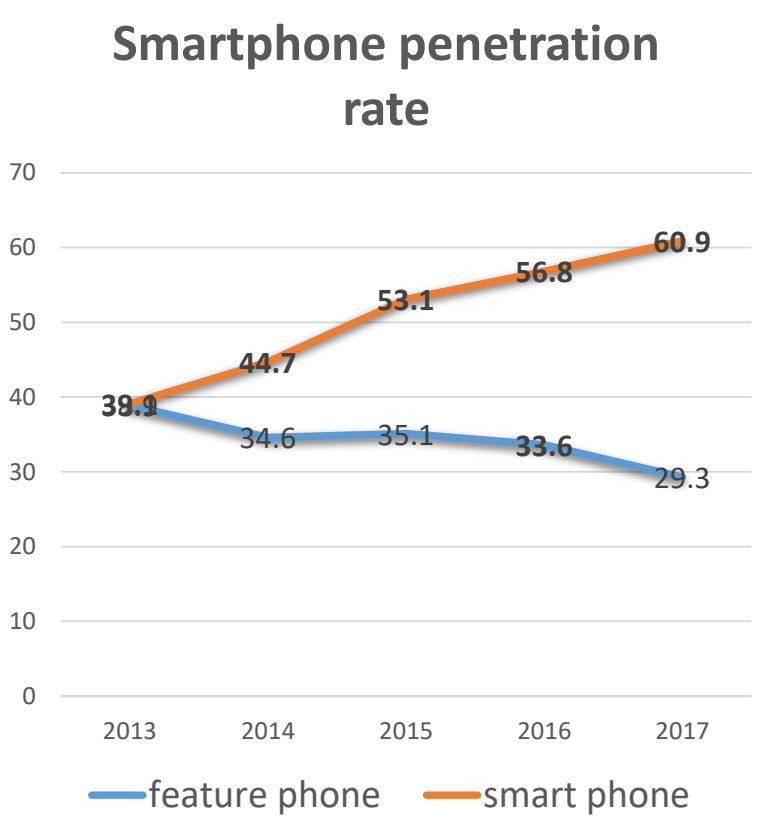
マイナンバーカードの世代別交付状況

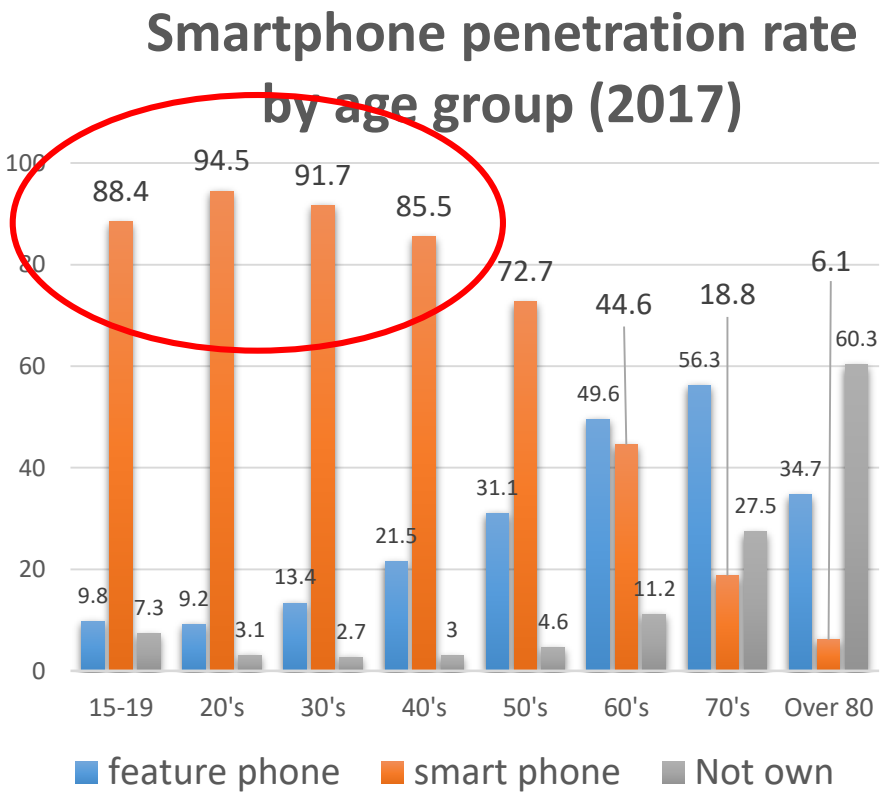
Total number of cards issued : 15,642,405　(Dec. 1st, 2018)

(但し、2019.3現在の交付率は12.9%)



スマートフォンの普及状況





民間利用推進には
スマートフォンの利用を前提とした環境づくりが必要

スマホ向けJPKIの制度的位置づけ

- **2枚目の電子利用者証明としてスマホに搭載**
  - マイナンバーカード搭載の電子利用者証明と同等の位置づけ（但し、証明書記載事項による格納媒体の識別は実施）
  - 発行方法、格納媒体の安全性などを含めマイナンバーカード搭載の電子利用者証明と同等である技術基準が求められる可能性
  - iOSへの対応が困難

- **モバイル電子利用者証明として、通常の電子利用者証明とは別モノとしてスマホに搭載**
  - 現在の電子利用者証明とは別の認証手段として位置づけ
  - 格納媒体等を別途定めることで、TEEの利用も可能（iOSへの対応可）
  - 必ずしも、現在の電子利用者証明と同じ認証手段としなくてもよい（暗号アルゴリズム、認証手順など）
  - なぜ別モノとするかの理由が必要

いずれにしてももう少し時間がかかりそう

モバイル認証を普及させるために

- **認証PF事業者が取り組むべきは**
  - 既存技術をベースとしたサービス提供者が参加しやすい仕組みの提供
  - 利用者が同じような方法で様々なサービスをできる仕組みづくり
  - OSのバージョンアップや新たな技術へ容易に対応できる仕組みの提供

モバイル認証普及のための方向性

- Webベースの認証方式は、Web Authentication API（WebAuthn）の利用が主流に
- WebAuthnでは、FIDO2.0の利用が前提
- Windows, MacOSの仕様変更によるJPKI用CSP, minidriver等のバージョンアップ問題

↓

PF事業者から
Trust Service Provider based on JPKI (TSP-J) への転換

↓

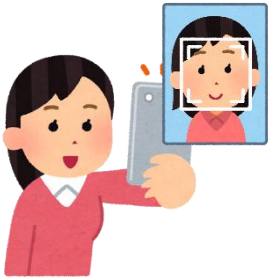
JPKIをベースとしたスマホ用利用者認証サービスの提供

JPKIをベースとしたスマホ認証

マイナンバーカード
（JPKI電子利用者証明）

+スマホ

FIDO2
Android Smartphone



FaceID or TouchIDを用いたFIDO2
（Nok Nok App SDK for iOS）
iPhone

+

電子利用者証明用証明書の
有効性確認

JPKIをベースとしたスマホ認証

- **JPKIと連携する認証機能をスマホに搭載**

- **利用者証明機能相当とするには**
  - Authenticator Assurance Level 3 (AAL3)相当の多要素暗号デバイス認証器を組み合わせ
    - JPKI電子利用者証明

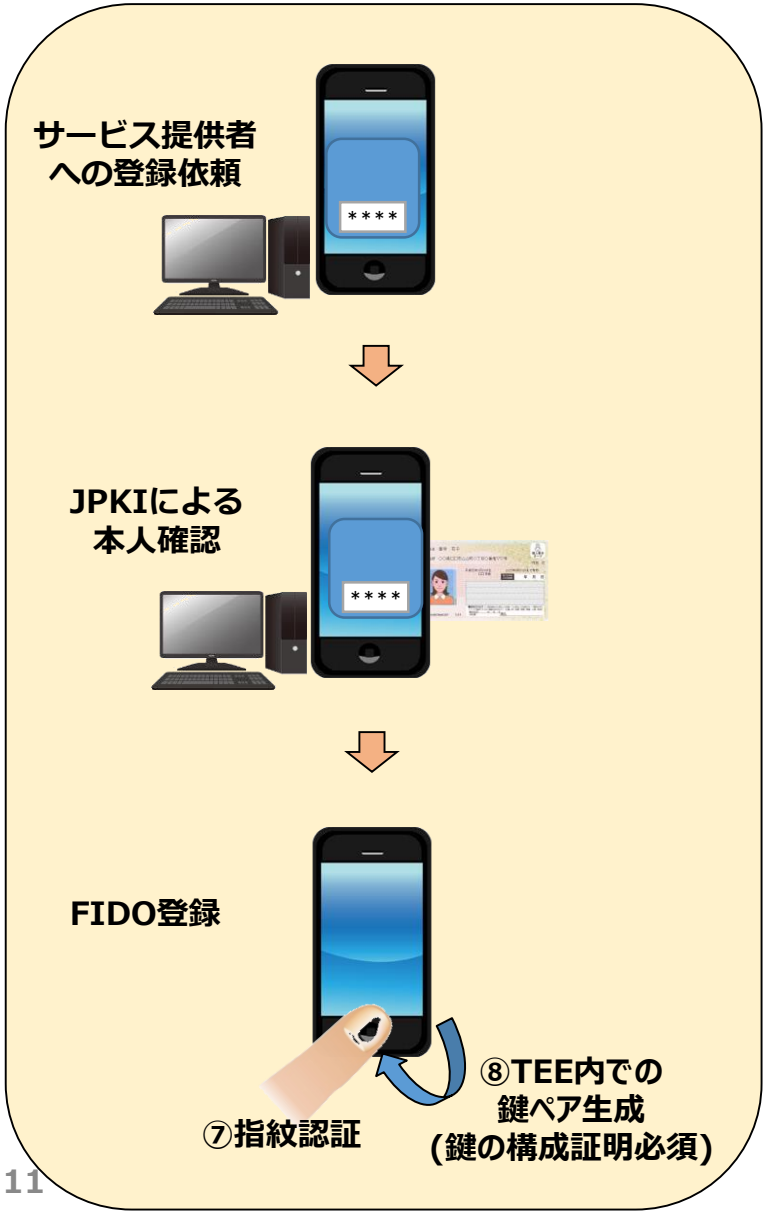
      保護された暗号鍵を用いて暗号操作を行うハードウェアデバイス

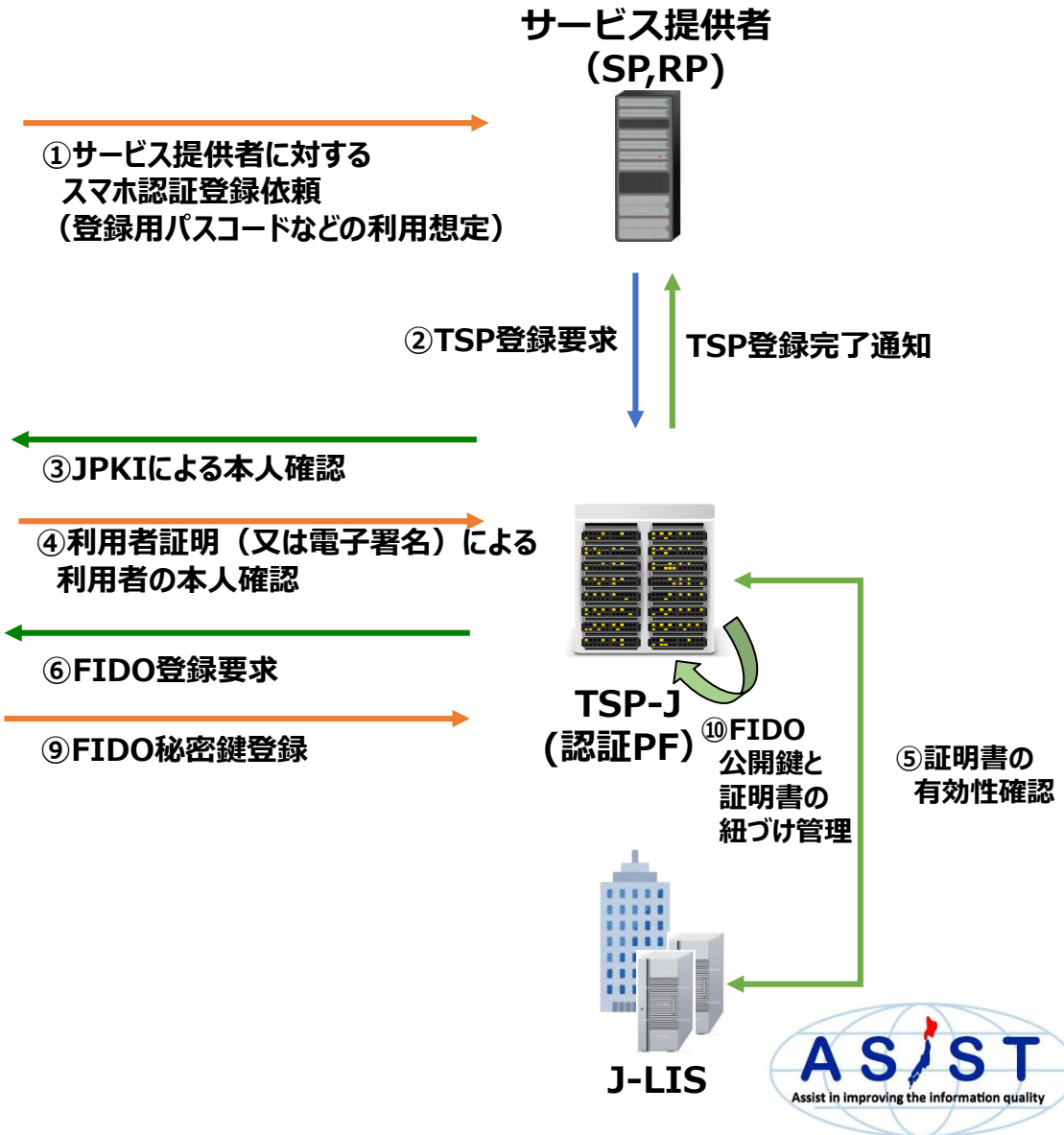
      ＋知識
    - FIDO対応スマホ（AndroidKeystore)、TouchID・FaceID搭載iPhone

      保護された暗号鍵を用いて暗号操作を行うハードウェアデバイス

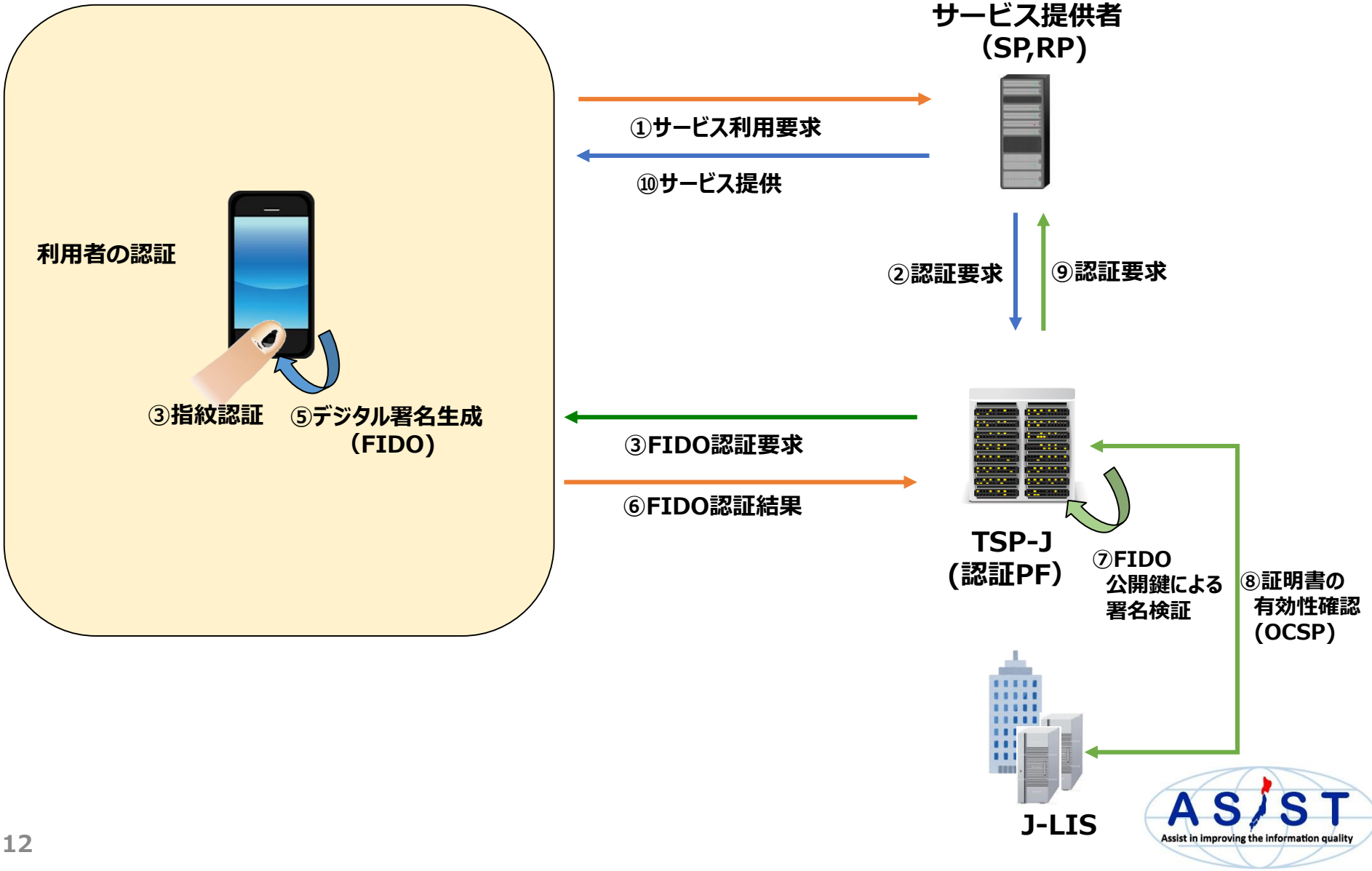
      (TEE: TrustZone or Secure Enclave) ＋生体
  - モバイル認証器による認証とJPKIの証明書の有効性確認の組合わせ

利用登録

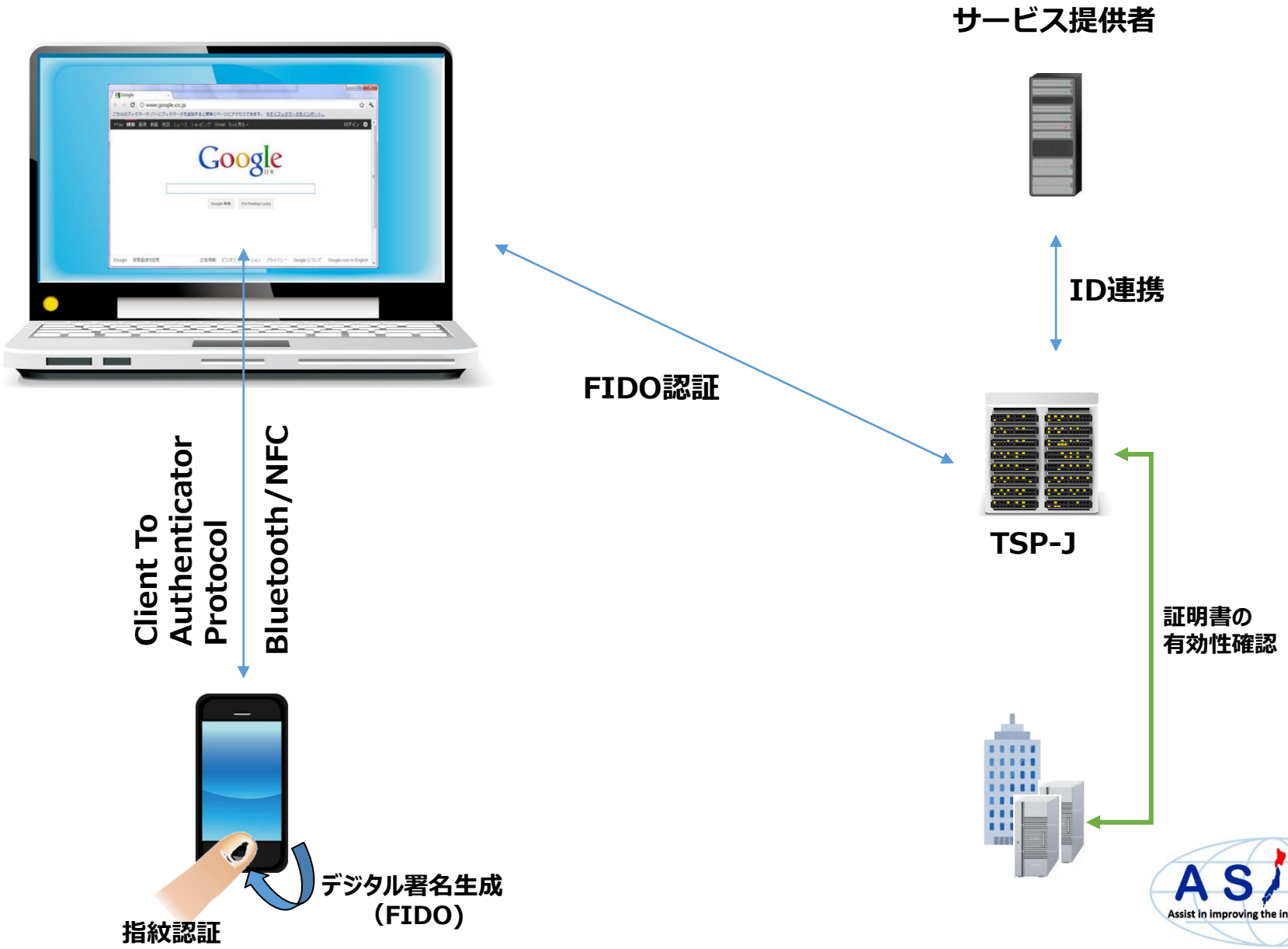

サービス提供者
への登録依頼
JPKIによる
本人確認
FIDO登録
⑦指紋認証
⑧TEE内での
鍵ペア生成
(鍵の構成証明必須)


サービス提供者
(SP,RP)
①サービス提供者に対する
スマホ認証登録依頼
(登録用パスコードなどの利用想定)
②TSP登録要求
TSP登録完了通知
③JPKIによる本人確認
④利用者証明（又は電子署名）による
利用者の本人確認
⑥FIDO登録要求
⑨FIDO秘密鍵登録
TSP-J
(認証PF)
⑩FIDO
公開鍵と
証明書の
紐づけ管理
⑤証明書の
有効性確認
J-LIS

サービス利用時の認証


サービス提供者
(SP,RP)
①サービス利用要求
⑩サービス提供
②認証要求
⑨認証要求
利用者の認証
③指紋認証
⑤デジタル署名生成
(FIDO)
③FIDO認証要求
⑥FIDO認証結果
TSP-J
(認証PF)
⑦FIDO
公開鍵による
署名検証
⑧証明書の
有効性確認
(OCSP)
J-LIS

ブラウザでの利用


サービス提供者
ID連携
FIDO認証
TSP-J
Client To Authenticator Protocol
Bluetooth/NFC
証明書の
有効性確認
デジタル署名生成
（FIDO）
指紋認証

課題等

- AndroidKeyStoreの、ハードウエア保護における鍵の構成証明(Key Attestation)はAndroid7.0で必須（8.0以降でHW-BackedなKeyStoreが必須）
- Secure Enclaveを用いた場合のKey Attestationの実現方法が不明（探せてないだけ？）
- Secure Enclaveの制限から、デジタル署名はECDSA(secp256r1) を利用
- モバイルJPKI電子利用者証明としてのAndroidKeyStore, Secure Enclaveの利用可否検討（但し、OSの設定等により鍵が消える場合があることが課題）

Tokyo Tech

Thank you