資料６－２

「公的個人認証サービスのスマートフォンでの利活用の実現に向けた実証請負」に関する報告

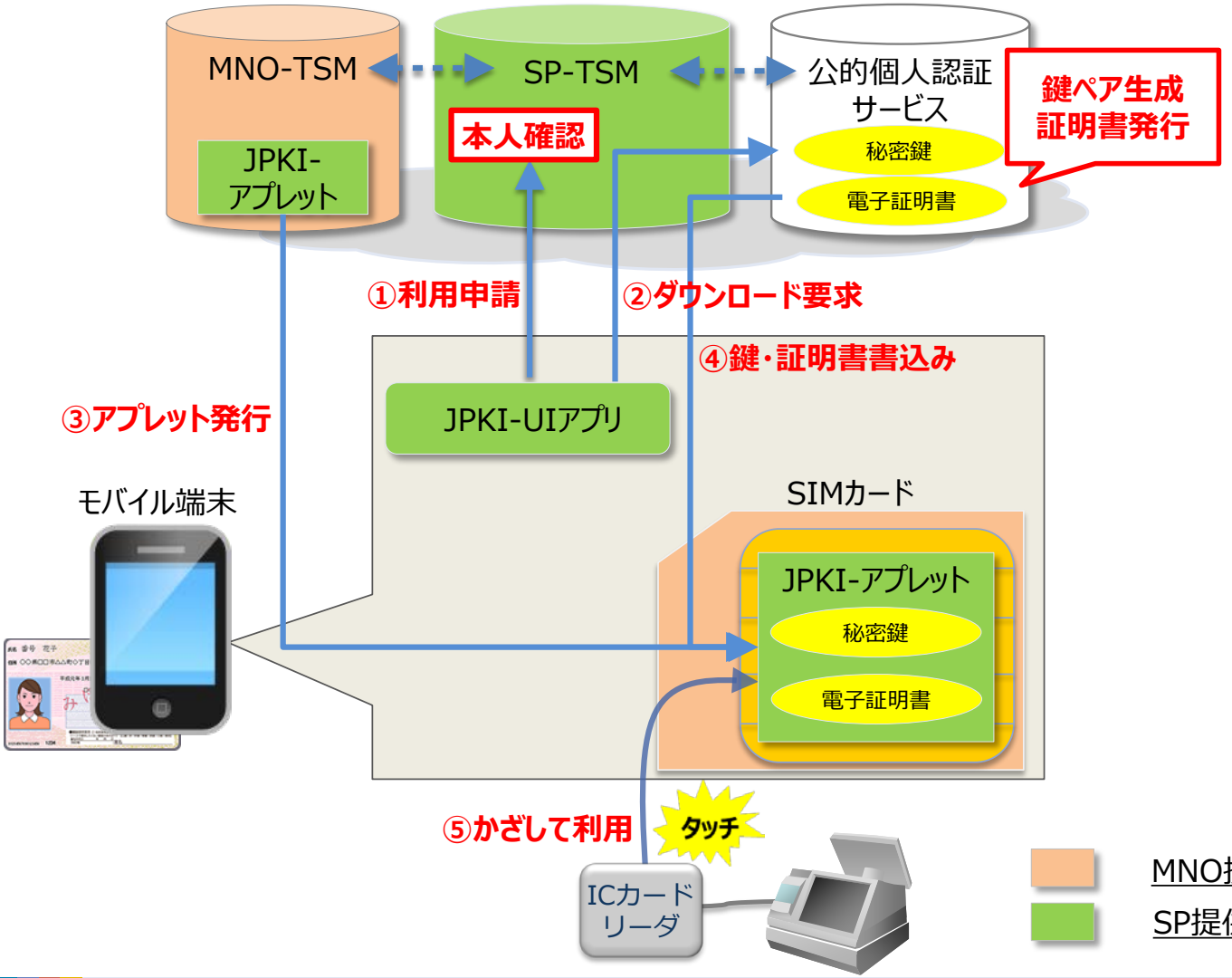
2017年 4月 21日
株式会社NTTデータ

目次

1. 実証事業の全体概要

1.1 Androidスマートフォンへの利用者証明機能ダウンロード（仕組み）

・モバイル通信事業者3社が提供するNFCプラットフォームを活用し、利用者証明機能をダウンロード。
・公的個人認証サービスで鍵ペア生成、電子証明書発行を行い、SIMカードに秘密鍵及び電子証明書を記録する。



○MNO-TSM※
- MNOの責任範囲の処理を実施するTSMサーバ
- SPのアプレットを預かり、SIMカードへ格納する

○SP-TSM ※
- SPの責任範囲の処理を実施するTSMサーバ(鍵・証明書をアプレットへ書き込む)

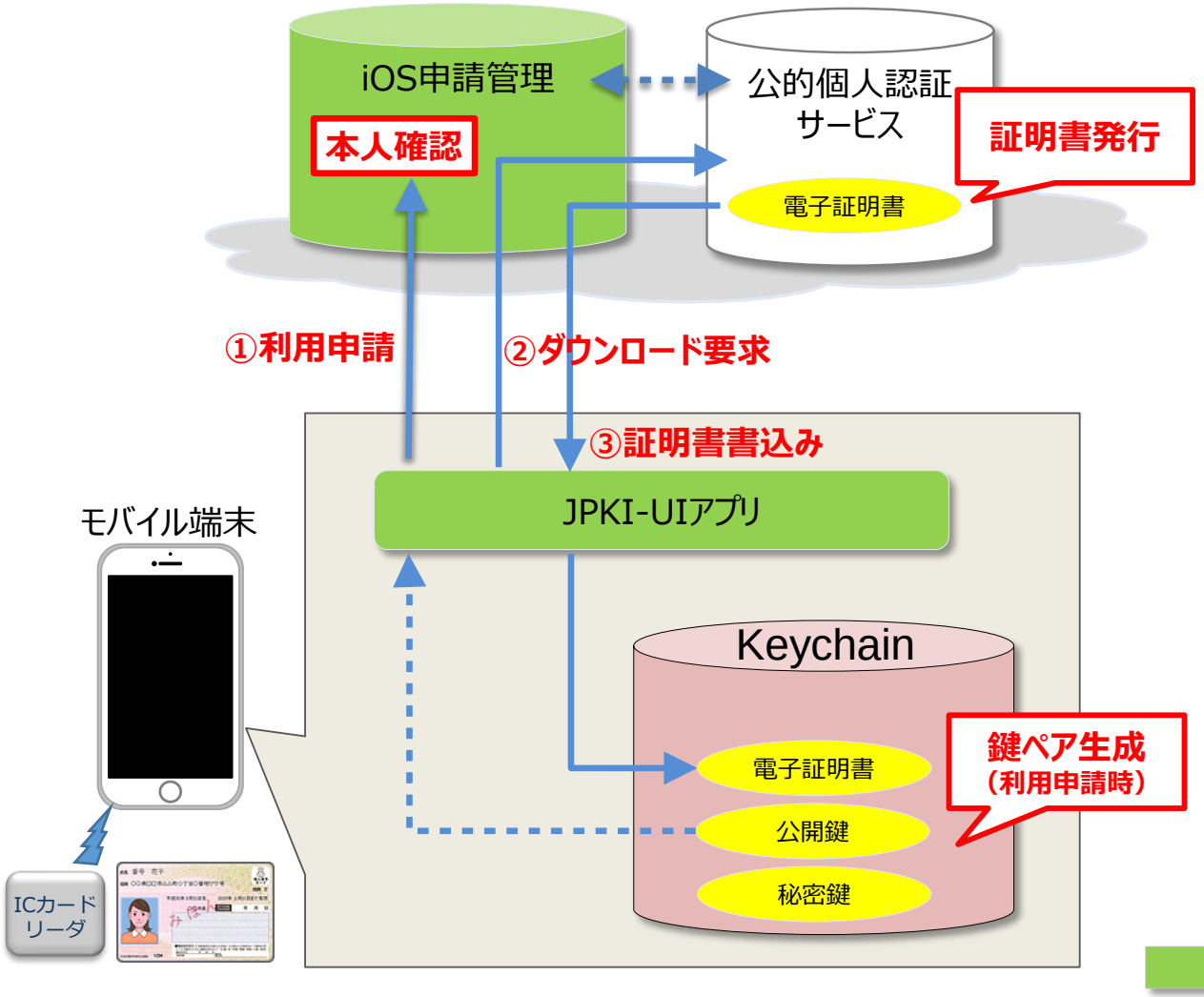
○JPKI-UIアプリ
- SPがユーザへ提供するAndroidアプリ
- 利用者が操作し、利用申請等を行う

○JPKI-アプレット
- SIMカードに搭載するJavaアプリケーションであり、サービス上必要なSPデータ(鍵・証明書)を保持する

※TSM：Trusted Service Manager

1.2 iOSスマートフォンへの利用者証明機能ダウンロード（仕組み）

・iOSが管理するKeychain領域に秘密鍵及び電子証明書を記録する。
・iOSスマートフォンで鍵ペア生成を行い、公的個人認証サービスで電子証明書を発行する。



○ **iOS申請管理**
- 利用者の申請情報を預かり、公開鍵を公的個人認証サービスに渡す

○ **JPKI-UIアプリ**
- SPがユーザへ提供するiOSアプリ
- 利用者が操作し、利用申請等を行う

○ **Keychain**
- iOS内の鍵・証明書の記録領域

SP提供

1.3 システム検証と安全性対策検討

短期間の実証事業であるため、以下に示す「システム検証」と「安全性対策検討」を並行して進めることとした。

システム検証

実現性検証

【基本技術】

検証用システムを開発し、電子証明書等のダウンロードの実現性を検証

【ユースケース適用】

利用面での課題検証

検討結果を可能な限り反映

安全性対策検討

基本技術

- 記録媒体の安全性
- アプレットダウンロードの安全性
- 秘密鍵配送の安全性
- 秘密鍵生成の安全性
- 記録媒体の第三者評価

運用面

- パスワード設定
- 申請方法の安全性
- 端末アプリの安全性
- 電子証明書ライフサイクル

制度面

- 現行法制度への影響

有識者を交えた評価会を開催し、安全性対策を検討

2.利用者証明機能ダウンロードに関するシステム検証

2.1 Androidスマートフォンに関するシステム検証 ①検証ポイント

・SP-TSM、JPKI-UIアプリ、JPKI-アプレットを開発し、システム検証を実施した。
・ユースケースとして、チケットレスサービスの入場時に利用者証明検証を行い、動作検証を実施。

検証ポイント①
既存NFCプラットフォームを活用して利用者証明機能をダウンロード可能か

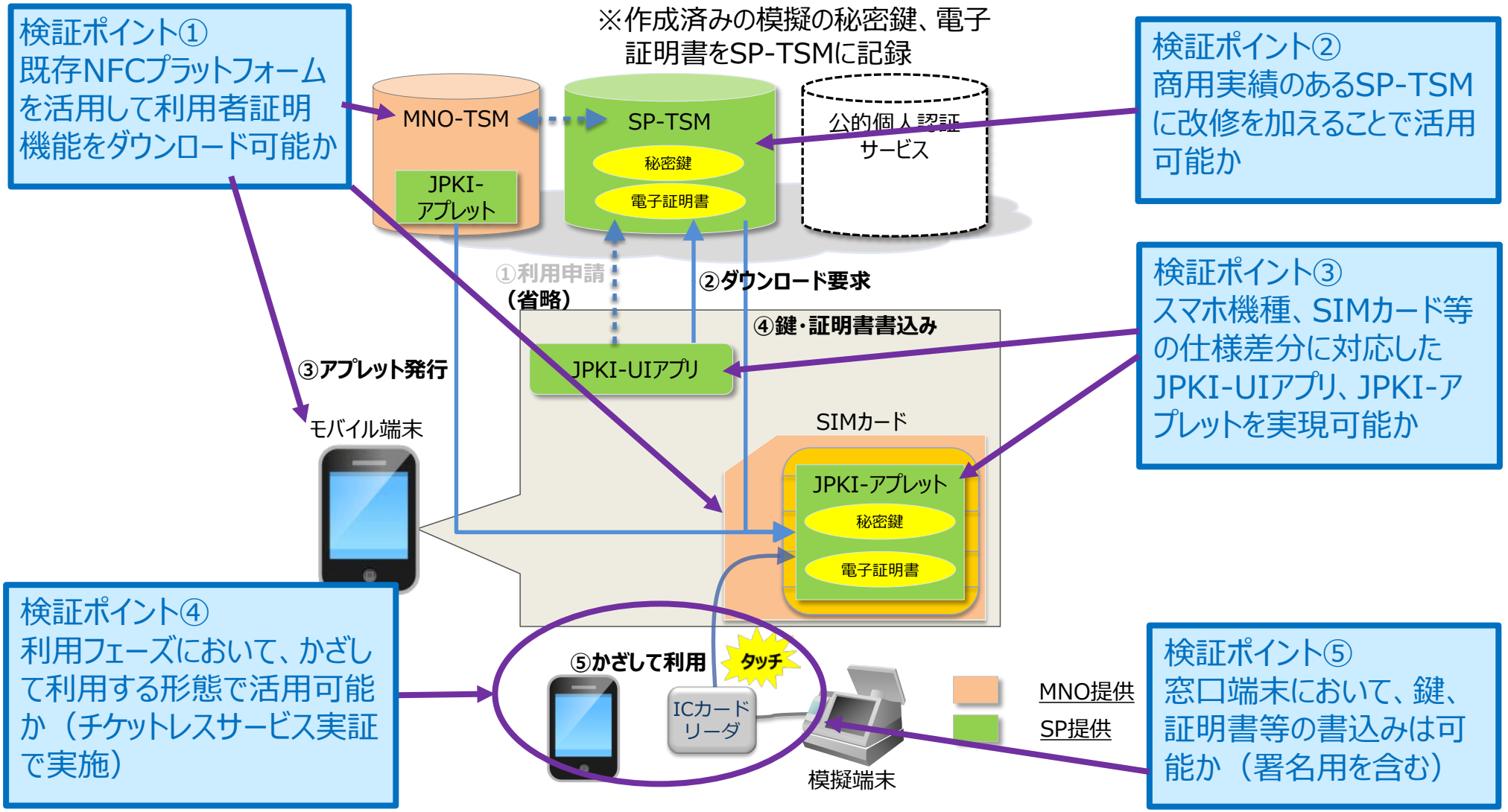
※作成済みの模擬の秘密鍵、電子証明書をSP-TSMに記録

検証ポイント②
商用実績のあるSP-TSMに改修を加えることで活用可能か

検証ポイント③
スマホ機種、SIMカード等の仕様差分に対応したJPKI-UIアプリ、JPKI-アプレットを実現可能か

検証ポイント④
利用フェーズにおいて、かざして利用する形態で活用可能か（チケットレスサービス実証で実施）

検証ポイント⑤
窓口端末において、鍵、証明書等の書込みは可能か（署名用を含む）



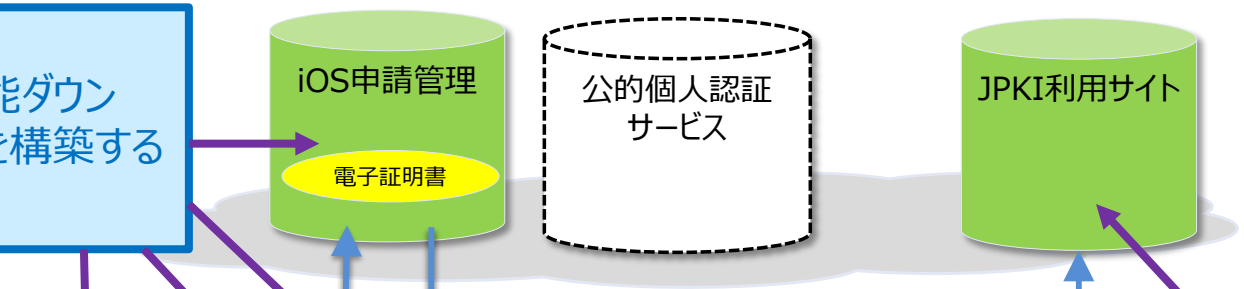
2.1 Androidスマートフォンに関するシステム検証 ②検証結果

#	検証ポイント	検証結果	今後の課題
①	既存NFCプラットフォームを活用して利用者証明機能をダウンロード可能か	モバイル通信事業者3社のNFCプラットフォームに影響を与えることなく、そのまま活用できた。	特に無し
②	商用実績のあるSP-TSMに改修を加えることで活用可能か	クレジット事例で商用実績のあるSP-TSMに対して、公的個人認証サービスに固有の部分を追加することで利用者証明機能ダウンロードを実現できた。	SP-TSMはSIMカードへのデータ書込み処理に特化しているため、利用申請時の署名検証等、SIMカードへのデータ書込み以外の処理はSP-TSMとは別システムでの実現が望ましい。
③	スマホ機種、SIMカード等の仕様差分に対応したJPKI-UIアプリ、JPKI-アプレットを実現可能か	モバイル通信事業者3社のスマホ（各社1機種）、SIMカード（各社）にて実現性を確認できた。	実用化に向けてはサービス対象とするSIMカード及びスマートフォン機種での動作検証が必要。
④	利用フェーズにおいて、かざして利用する形態で活用可能か（チケットレスサービス実証で実施）	チケットレスサービスの入場時における利用者証明検証について、スマートフォンをかざして利用する形態で実現できた。	かざし位置が利用者にとって分かり難いため、音や触覚（バイブ）の活用等工夫が必要。 現在、窓口端末で使用されている既設ICカードRWとスマートフォンの組合せで動作しないものがあった。 実用化に向けてはサービス対象とするスマートフォン機種での動作検証が必要。
⑤	窓口端末において、鍵、証明書等の書込みは可能か（署名用を含む）	市町村窓口の窓口端末の処理をテスト環境で実施し、スマートフォンのかざして利用する形態で鍵、証明書の書込みが確認できた。 また、利用者証明用電子証明書だけでなく署名用電子証明書等の格納も実現可能であることを確認した。	

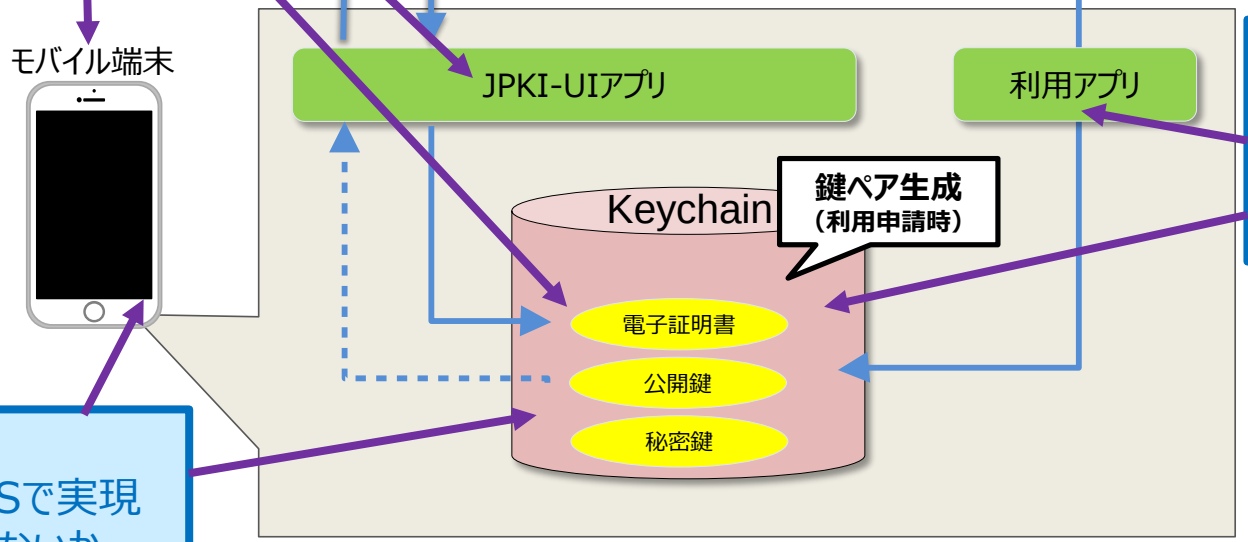
2.2　iOSスマートフォンに関するシステム検証
①検証ポイント

・iOS申請管理、JPKI-UIアプリを開発し、システム検証を実施した。
・ユースケースとして、Webサイトのログイン時に利用者証明検証を行うシステムを開発し、動作検証を実施。

検証ポイント①
利用者証明機能ダウンロードの仕組みを構築することは可能か



①利用申請
②証明書書込み
③ログイン時の利用者証明検証



検証ポイント③
利用フェーズにおいて、ログイン時の利用者証明検証を実現可能か

検証ポイント②
鍵ペア生成をiOSで実現し、性能上問題ないか

SP提供

2.2 iOSスマートフォンに関するシステム検証
②検証結果

#	検証ポイント	検証結果	今後の課題
①	利用者証明機能ダウンロードの仕組みを構築することは可能か	iOS申請管理、JPKI-UIアプリを開発し、iOSスマートフォン内での鍵ペア生成、利用申請、電子証明書ダウンロードの一連の処理が実現できることを確認した。 但し、利用申請時において現状ではiOS用のICカードRWが存在しないため、これに関連する処理は省略した。	実用化に向けてはiOS用のマイナンバーカードに対応したICカードRWが必要。
②	鍵ペア生成をiOSで実現し、性能上問題ないか	iOSの機能を使って、鍵ペアが実用上問題ない時間内で実現できることを確認した。	特に問題なし。
③	利用フェーズにおいて、ログイン時の利用者証明検証を実現可能か	利用サイト、iOS用利用アプリを作成し、Keychain内に秘密鍵、電子証明書が格納された状態で、利用サイトへのログイン処理における利用者証明検証が可能であることを確認した。	業務用アプリからKeychain領域へのアクセス方法について検討する必要がある。

3. 利用者証明機能ダウンロードに関する安全性評価

3.1 評価会の開催（Androidスマートフォン）

- 評価会を開催し、SIMカードへの利用者証明機能ダウンロードの安全性対策について検討した。
- SIMカードの利用者証明機能ダウンロードでは、モバイル通信事業者が提供するモバイルNFCサービスプラットフォームの活用を前提とすることから、モバイル通信事業者から前記プラットフォームの情報提供を受け、評価会参加者とは機密保持契約を締結した上で評価会を実施した。

役割	企業・団体等	作業内容
評価者	・慶應義塾大学　手塚特任教授 ・東京工業大学　小尾准教授 ・地方公共団体情報システム機構	安全性対策の評価
説明者	NTTデータ、NTTコミュニケーションズ、大日本印刷	評価会運営、安全性対策の調査・検討、報告書作成
オブザーバ	総務省、NTTドコモ、KDDI、ソフトバンク	

#	主な議題	開催日時
第1回	・利用者証明機能ダウンロードにおけるSP領域の安全性、アプレットダウンロードの安全性、秘密鍵配送の安全性 ・SP独自の安全性対策（コンテンツ暗号化対策）	2016年11月30日（水） 9：30～12：00
第2回	・申請方法の安全性対策 ・利用者証明用パスワード設定に関する安全性対策 ・SIMカードのセキュリティ評価	2017年1月23日（月） 13：00～15：30
第3回	・端末アプリの安全性対策 ・証明書関連業務及びスマートフォン特有の業務検討 ・法整備に関する論点整理	2017年3月22日（水） 13:00～16:00

3.1 評価会の開催（iOSスマートフォン）

- 評価会を開催し、iOSスマートフォン内の「Keychain」に秘密鍵や電子証明書を保管する際の脅威の洗い出しと対策を検討した。
- 脅威に対してiOSスマートフォン自体、第三者、アプリケーションで実施する安全対策を検討し、その安全対策が利用者証明用電子証明書を利用する為の申請・ダウンロード・利用処理プロセスの中でどの様に有効に作用しているのか検討。

役割	企業・団体等	作業内容
評価者	・慶應義塾大学　手塚特任教授 ・東京工業大学　小尾准教授 ・地方公共団体情報システム機構	安全性対策の評価
説明者	日本アイ・ビー・エム	評価会運営、安全性対策の調査・検討、報告書作成
オブザーバ	総務省、NTTデータ	

#	主な議題	開催日時
第1回	・iOSスマートフォンに公的個人認証情報を保管・利用する際の安全性対策について	2017年1月23日（月） 15:30～17:00
第2回	・iOSスマートフォンにて利用者証明書を利用する為の申請・ダウンロード・利用処理と安全対策との関係について ・公的個人認証法対応について　記録媒体別整理（iOSスマートフォン）	2017年3月6日（月） 9:30～11:30
第3回	・iOSスマートフォンからの申請をAPNsを用いて確認する方法 ・法整備に関する論点整理	2017年3月22日（水） 16:00～17:30