NTT DATA
Global IT Innovator

資料8－2

FY2017スマートフォンのSIM カード等へ利用者証明機能を搭載するための課題への対応方策の検討

2018年6月26日
株式会社NTTデータ

目次

用語集

○**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スマートフォンアプリ
- 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
- サービス上必要なSPデータ(鍵・証明書)を保持する

○ **SP**
- 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（FY16）
- iPhoneの真正性確認及び復号用データを生成、配信する（FY17）

○ **APNs（Apple Push Notification Service）**
- iOS向けのリモート通知機能

○ **Keychain**
- iOS内の鍵・証明書の記録領域

○ **Open Mobile API**
- SIMカード内のセキュアな領域にアクセスするために提供されているAndroid用アプリケーションインタフェース

○ **セキュアメッセージング**
- コマンドの実行中に交換されるデータの暗号による保護手段を提供するもの

※TSM：Trusted Service Manager

1　全体概要

1.1 検討の背景・目的

対面での本人確認を反映したスマートフォンのSIM カード等へ利用者証明機能を搭載するための課題への対応方策の検討を行った。

H28年度実証結果

利用者証明機能ダウンロードの検証

モバイル回線等を使ったオンライン発行

【システム検証】

・実証システムを構築
・Android、iOS双方の実現性を確認

【安全性対策検討】

・有識者を交えた評価会を実施
・技術面、運用面での安全性対策を検討し、課題を提起

対面での確実な本人確認の実施

H28年度実証では以下の検討が十分ではなかった。

①市町村窓口における対面での本人確認

②市町村窓口に設置された統合端末から発行

③SIM入替えのリスク及び対策検討

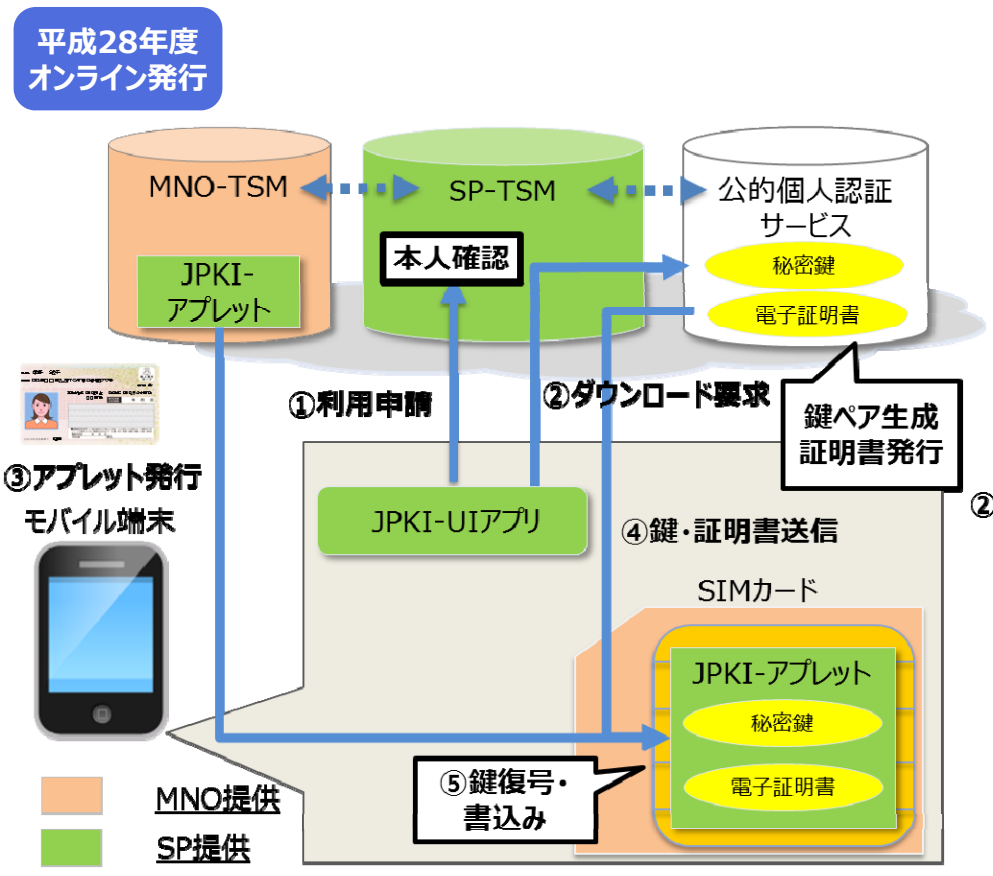
H29年度実証（調査研究及び検証）

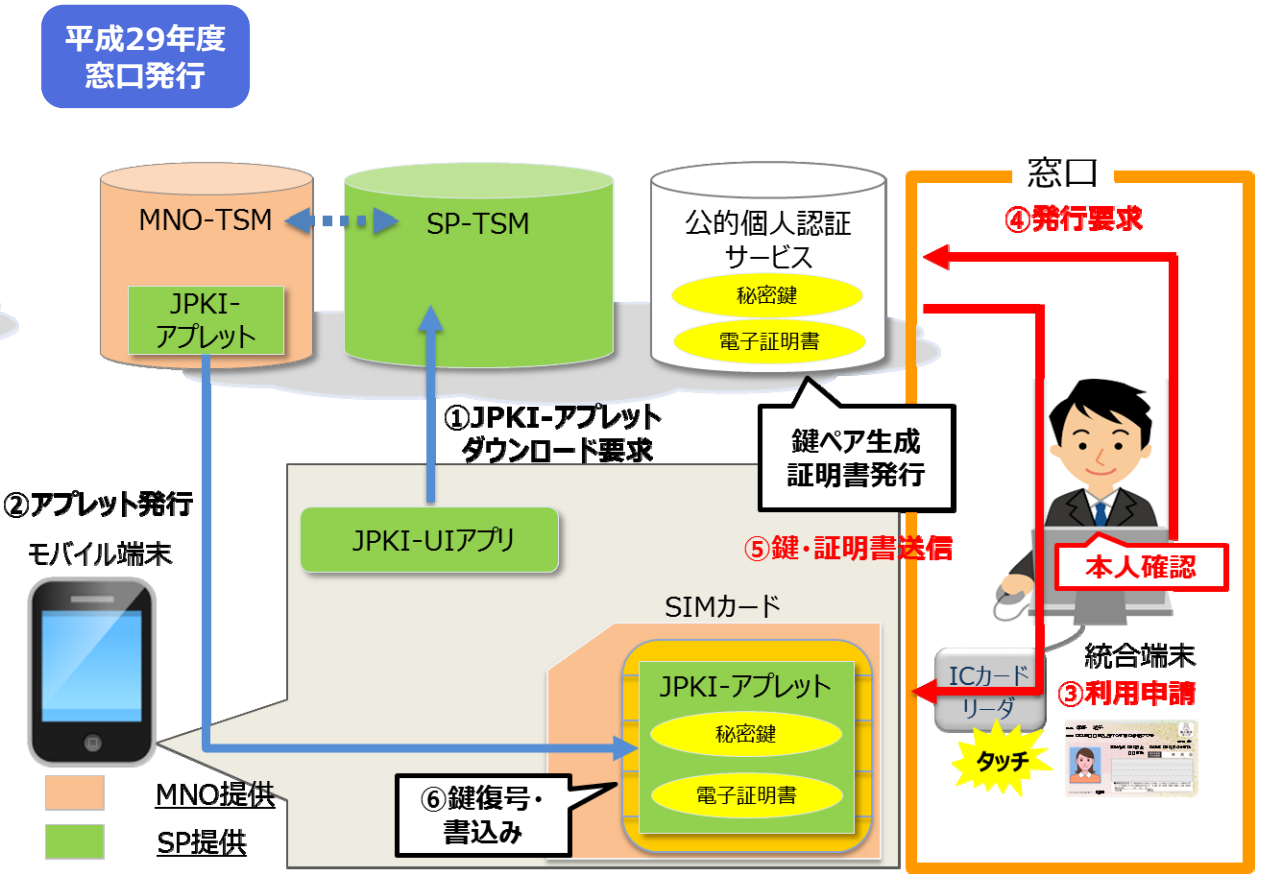
昨年度の実証結果を活かしつつ、窓口発行方式についての課題を検討。

・有識者を交えた評価会を実施
・市町村窓口における申請、発行フローの検討及び検証
・SIM差し替え等、体系的なリスクの整理、検討
・窓口ICカードRWとスマートフォンのNFC通信実態調査

1.2 Androidスマートフォンへの電子証明書等格納方法について

H29年度はマイナンバーカードにおける電子証明書の発行と同様に、窓口での対面による厳格な本人確認を実施後、統合端末にて電子証明書等をSIMカードに記録。H28年度とH29年度との相違点は以下の通り。



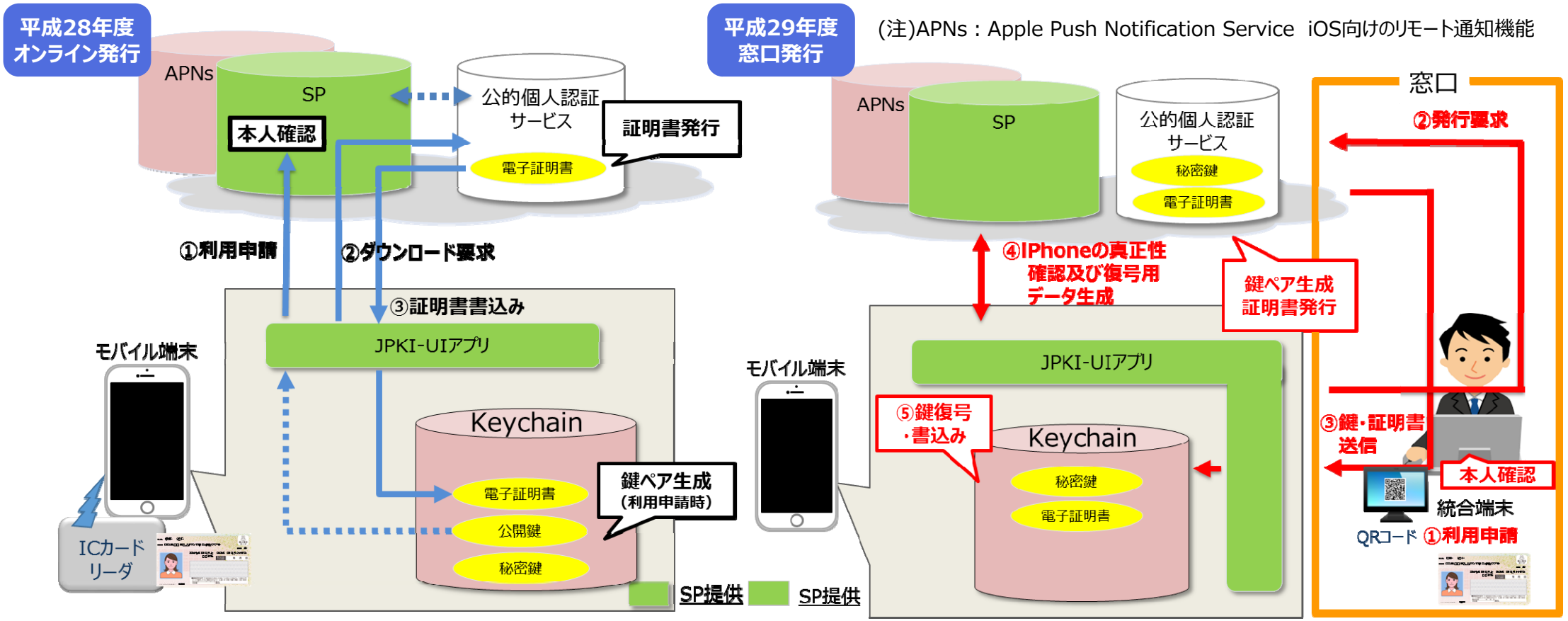


・マイナンバーカードによるオンラインでの署名検証による本人確認。
・JPKIアプレットダウンロードをオンラインで実施。
・鍵ペア生成、証明書発行を公的個人認証サービスで実施
・JPKIアプレット、鍵・証明書の書き込みをオンラインで実施。

・JPKIアプレットダウンロードをオンラインで実施。（事前）
・マイナンバーカード等による窓口での対面による本人確認。
・鍵ペア生成、証明書発行を公的個人認証サービスで実施。
・鍵・証明書の書き込みを窓口でICカードRWにて実施。

1.3 iOSスマートフォンへの電子証明書等格納方法について

H29年度はマイナンバーカードにおける電子証明書の発行と同様に、窓口での対面による厳格な本人確認を実施後、統合端末にて電子証明書等をKeychain領域に記録。H28年度とH29年度との相違点は以下の通り。



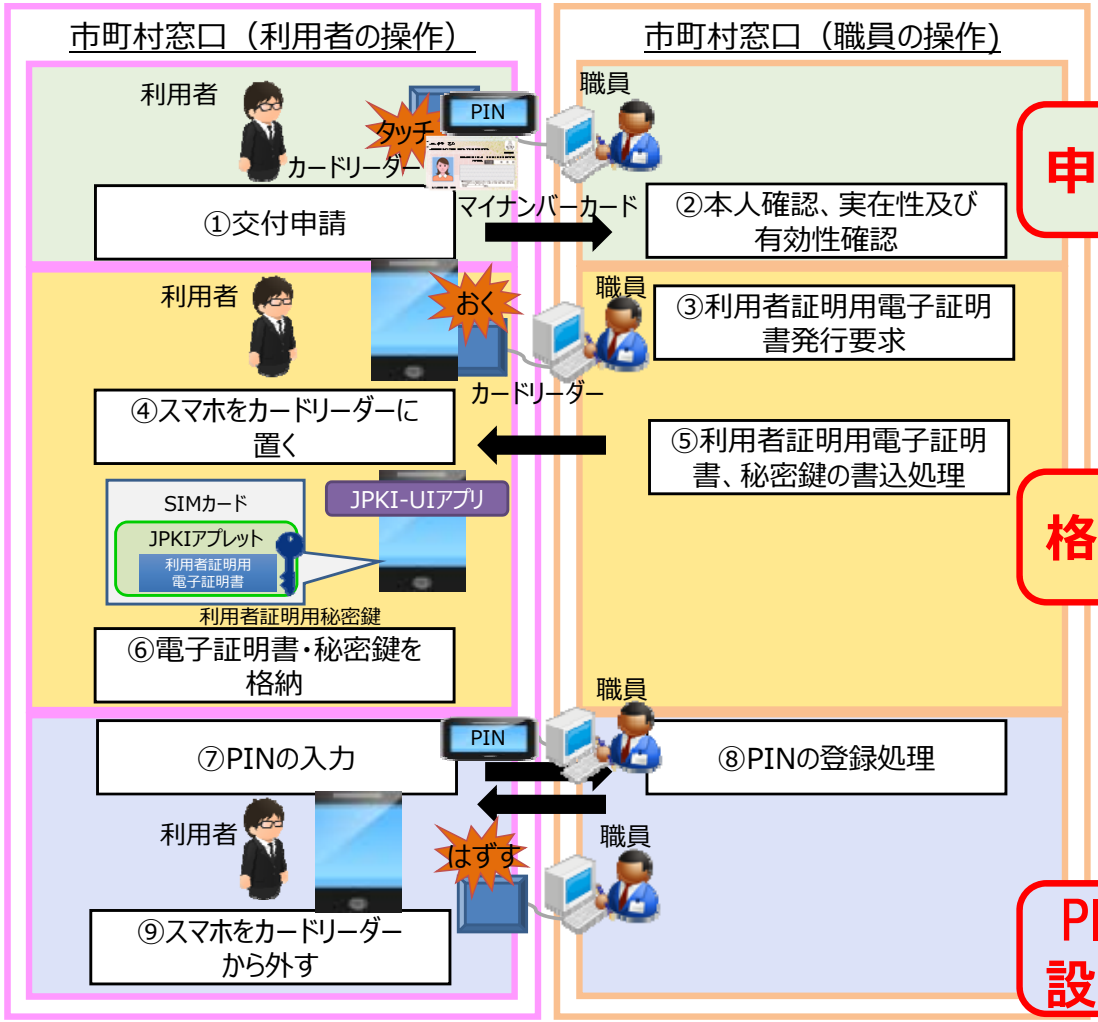
・アプレットは使用せず、APNsを利用した真正性確認を実施。
・マイナンバーカードによるオンラインでの署名検証による本人確認。
・鍵ペア生成をKeychain領域内で実施。
・証明書の書き込みをオンラインで実施。

・アプレットは使用せず、APNsを利用した真正性確認を実施。
・マイナンバーカード等による窓口での対面による本人確認。
・鍵ペア生成、証明書発行を公的個人認証サービスで実施。
・鍵・証明書の書き込みは窓口でQRコードを利用して実施。

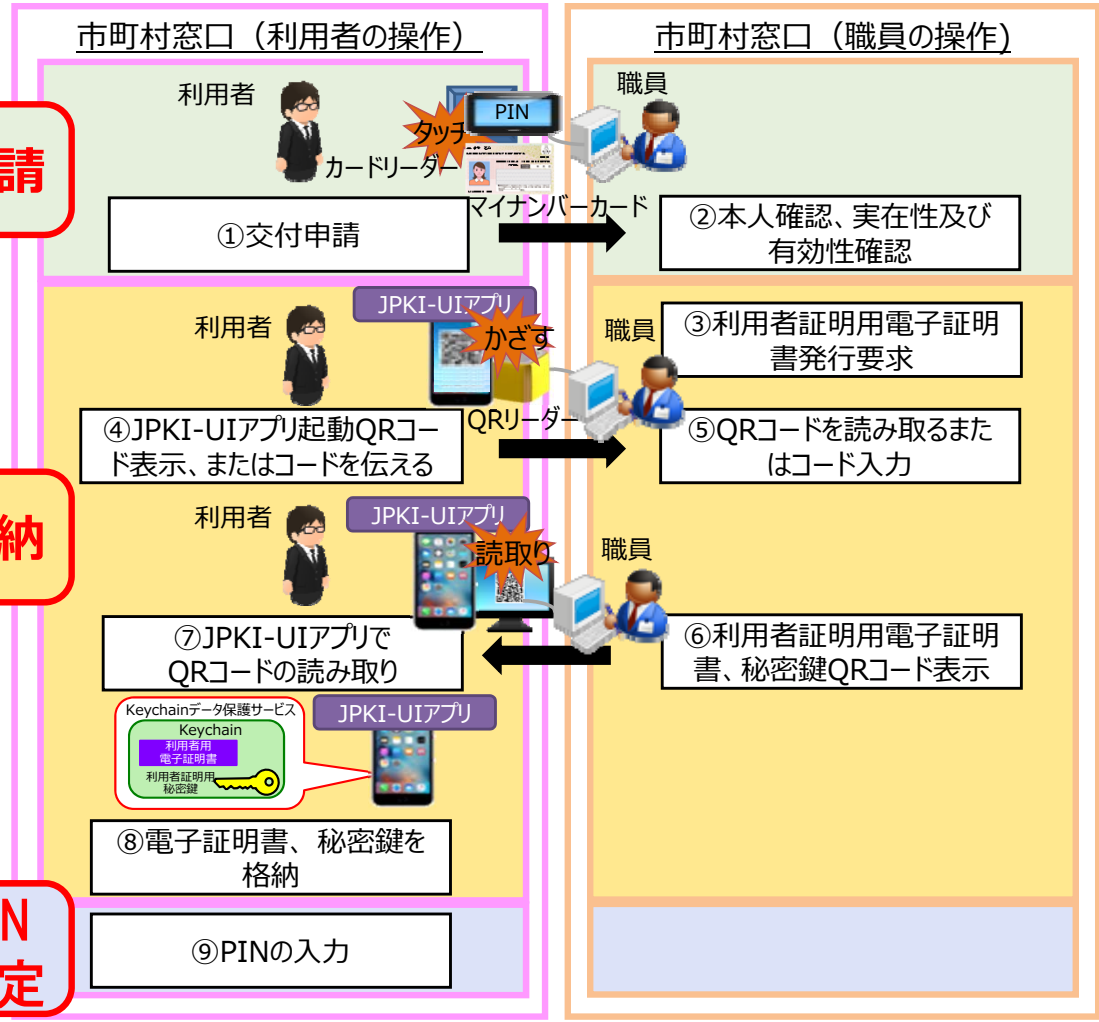
1.4 窓口での操作手順について

・利用者は窓口で本人確認、実在性確認及び有効なマイナンバーカードに格納されている利用者証明用電子証明書の所持確認を行う。
・電子証明書、秘密鍵を統合端末からICカードRWまたはQRコード経由で受け取り格納する。※JPKI-UIアプリは事前にアプリ配信事業者からダウンロードする。Androidスマートフォンではアクセスコードでユーザ認証をSP-TSMで行い、JPKIアプレットをMNO-TSMからダウンロードする。

Androidスマートフォン窓口操作手順(マイナンバーカードと同じ手順を想定)



iOSスマートフォン窓口操作手順



1.5 検討の概要

Android端末・iOS端末での課題の対応方策について検討し、検討結果について有識者を交えて評価会を開催した。

実施項目		Android	iOS	説明
課題①	市町村窓口における申請から電子証明書のSIMカード等への格納に関する安全性対策の検討及び検証	●	●	電子証明書等の記録媒体：Android搭載スマートフォンはSIMカード、iOS搭載スマートフォンはKeychain領域
課題②	市町村窓口におけるPINの初期化、変更に関する検討及び検証	●	●	
課題③	SIMカード（電子証明書を格納済み）を本人以外のスマートフォンに差し替えて利用されることを防止する対策の検討	●	–	iOS搭載スマートフォンでは電子証明書等の記録媒体（Keychain領域）が端末と一体であり、着脱不可のため対象外
課題④	電子証明書の発行時及び利用時の脅威とその対策についての検討	●	●	
課題⑤	市町村窓口での各種申請を基本とする電子証明書のライフサイクル（失効、更新、再発行等）の検討	●	●	
課題⑥	業務アプリからSIMカード等へのアクセス方法の検討	●	●	
課題⑦	市町村窓口のICカードRWとスマートフォンの通信確認	●	–	iOS搭載スマートフォンは、ICカードRWからの電子証明書等の読取りは不可のため対象外
課題⑧	現行制度への影響調査	●	●	

1.6 評価会および検討会について

市町村窓口における電子証明書のSIMカード等への格納及び運用面における課題の対応方策の検討にあたり、有識者が参加する評価会および検討会をAndroid／iOS搭載スマートフォンそれぞれについて開催した。
評価会および検討会の実施体制、評価会の開催実績は以下の通り。

評価会

〔Android搭載スマートフォン評価会〕
[評価者]手塚特任教授、小尾准教授、J-LIS
[説明者]NTTデータ･NTTコム･DNP
[オブザーバ]総務省、モバイル通信事業者（NTTドコモ、KDDI、ソフトバンク）

〔iOS搭載スマートフォン評価会〕
[評価者]手塚特任教授、小尾准教授、J-LIS
[説明者]NTTデータ･日本IBM
[オブザーバ]総務省

〔Android／iOS搭載スマートフォン評価会共通〕【実施内容】
・各課題に関する協議（第1～3回）

検討会

〔Android搭載スマートフォン検討会〕
[実施者]NTTデータ･NTTコム･DNP
[オブザーバ]モバイル通信事業者（NTTドコモ、KDDI、ソフトバンク）

〔iOS搭載スマートフォン検討会〕
[実施者]NTTデータ･日本IBM

〔Android／iOS搭載スマートフォン検討会共通〕【実施内容】
・各課題に関する協議（評価会向け報告に関する検討）

#	議題	開催時期
第1回	・課題①～④に関する協議、課題①②の技術検証に向けた協議（Android／iOS）	2017年12月25日（月） 13：00～18：00
第2回	・課題⑤～⑥に関する協議（Android／iOS） ・第1回の指摘事項の検討結果（Android／iOS）	2018年2月8日（木） 13：00～18：00
第3回	・課題⑦～⑧に関する協議（Android／iOS） ・第2回の指摘事項の検討結果（Android／iOS）	2018年3月8日（木） 13：00～18：00

2　課題への対応方策の検討結果

2　課題への対応方策の検討（1/2）

SIMカード、Keychain領域を秘密鍵及び電子証明書の記録領域として課題の対応方策を検討した。

#	分類	検討項目	検討内容	Android	iOS
1	課題①	JPKI-UIアプリダウンロード	JPKI-UIアプリダウンロード方法の検討。 －市区町村負担の確認 －対応機種等判定の確認	●	●
2		JPKIアプレットダウンロード	アプレットダウンロード方法の検討。 －MNO-TSM、SP-TSMの役割の確認 －ダウンロードタイミングの確認 －アクセスコードによる認証の確認	●	対象外 （注1）
3		外部認証鍵・秘密鍵設定キー等の格納	外部認証鍵・秘密鍵設定キー格納方法の検討。 －埋め込み方式、配送方式の確認 －格納の確実性の確認	●	●
4		電子証明書等の格納	電子証明書等の格納方法の検討。 －ウィルス感染スマートフォン等からの脅威への対策の確認		
5	課題②	PIN初期設定・PIN初期化・再設定(PIN忘失)	市町村窓口におけるPINの初期化、変更方法の検討。 －実施フローの確認 －PINロック解除の確認	●	●
6		PIN変更：JPKI-UIアプリ/統合端末(PINを覚えている)			
7	課題③	SIMカード差し替えの対策	SIMカードの差し替えを防止する対策方法の検討。 －脅威の確認 －実現方式の確認 －市区町村窓口負担の確認	●	対象外 （注1）

（注1）アプレットが存在しないため

2 課題への対応方策の検討（2/2）

#	分類	検討項目	検討内容	Android	iOS
8	課題④	発行時の脅威とその対策	脅威を分類し、その脅威への対策の検討。 ー改ざん、窃取、なりすまし、盗聴、盗み見等の脅威と対策の確認	●	●
9		利用時の脅威とその対策			
10	課題⑤	電子証明書の業務	市町村窓口における対面での各種申請を前提として、電子証明書のライフサイクルを検討。	●	●
11		スマートフォン特有の業務	スマートフォン特有の事象（機種変更、SIM変更等）についてのライフサイクルを検討。		
12	課題⑥	業務アプリからSIMカード・Keychainへのアクセス方法	業務アプリとUIアプリの連携・電子証明書の記録領域への業務アプリからのアクセス方式の検討。	●	●
13		インタフェース仕様	業務アプリから電子証明書の記録領域へアクセスするためのUIアプリインタフェース仕様の検討。		
14	課題⑦	市町村窓口のICカードRWとスマートフォンの通信確認	統合端末で使用されている現在販売中のICカードRWの動作及び範囲の確認。	●	対象外（注1）
15	課題⑧	現行の法制度にどのような影響があるかを調査	①～⑥を踏まえ、現行制度への影響を調査。 ー公的個人認証法への影響を確認。 ー法律施行令、法律施行規則への影響を確認。 ー技術的基準への影響を確認。	●	●

（注1）アプレットが存在しないため

2.1 課題① 市町村窓口における申請から電子証明書のSIMカード等への格納に関する安全性対策の検討及び検証結果

○：重要な課題なし　△：重要な課題あり

青字：実用化に向けた検討事項 赤字：重要な課題

#	検討項目	Android（検討結果）	iOS（検討結果）
1	JPKI-UIアプリダウンロード	・アプリ配信事業者(Google play)からダウンロードするものとする。 ・誰がスマートフォンの対応機種、対応SIMを認定するか検討する必要がある。認定者は継続的な最新化の対応が必要となる。	・アプリ配信事業者(App Store)からダウンロードするものとする。 ・アップルでサポートしているOSバージョンを確認する必要がある。 ・Jailbreakや脆弱性対策のため、アップルがサポートしなくなったiOSでは動作しないようなバージョンアップ管理が必要。
2	JPKIアプレットダウンロード	・JPKIアプレットのダウンロード方法は、利用者が事前にアクセスコードを使用してユーザ認証をSP-TSMで行い、SP-TSMを介してMNO-TSMからダウンロードする方法とする。 ・ダウンロードタイミングについては、基本的に事前ダウンロードとするが、窓口来訪時にダウンロードすることも考えられる。 ・ブルートフォースアタック(注1)への耐性を向上させるため、アクセスコードの生成ロジックを検討する必要がある。（各桁の付番ルールを決める、チェックデジット(注2)を含める等）	（該当しない） ・SIMカードを利用できないため、JPKIアプレットのダウンロードは実施しない。また、アクセスコードは使用しない。

(注1)パスワードなど可能な組合せを全て試す方法

(注2)偽造を防止するために用いられる数字や符号等

※ 2.2 参考①、②参照

2.1 課題① 市町村窓口における申請から電子証明書のSIMカード等への格納に関する安全性対策の検討及び検証結果

○：重要な課題なし　△：重要な課題あり

青字：実用化に向けた検討事項 赤字：重要な課題

#	検討項目	Android（検討結果）	iOS（検討結果）
3	外部認証鍵、秘密鍵設定キー等の格納	・JPKIアプレットへ埋め込むことで、回線切断等の影響なく確実に格納することができる。	・Apple Push Notification Service(注2)を利用してPush通知で利用者スマホへ統合端末認証用データ（外部認証鍵）と証明書復号用データ(一時共通鍵）を送付する方式を推奨する。 ・公的個人認証サービスで一時共通鍵の生成等現行システムへ影響があるため、セキュリティ対策、改修範囲等の検討をする必要がある。
4	電子証明書等の格納	・統合端末のICカードRWにスマートフォンをかざし電子証明書及び秘密鍵を格納する。 ・内部認証＆セキュアメッセージング(注1)を実施することで、ウィルス感染による影響や通信データの傍受等を防止する。	・統合端末で表示したQRコードをスマートフォンで読み取ることで電子証明書及び秘密鍵をkeychain領域に格納する。 ・iPhoneの真正性確認＆暗号化された通信を実施することで、ウィルス感染による影響や通信データの傍受等を防止する。 ・利用者および窓口担当者が滞りなく操作できるQRコード利用ユーザーインターフェースを検討・検証する必要がある。

(注1)セキュアメッセージング:コマンドの実行中に交換されるデータの暗号による保護手段を提供するもの

(注2)Apple Push Notification Service:iOS向けのリモート通知機能

※ 2.2 参考①、②参照

2.2 課題② 市町村窓口におけるPINの初期化、変更に関する検討及び検証結果

○：重要な課題なし　△：重要な課題あり

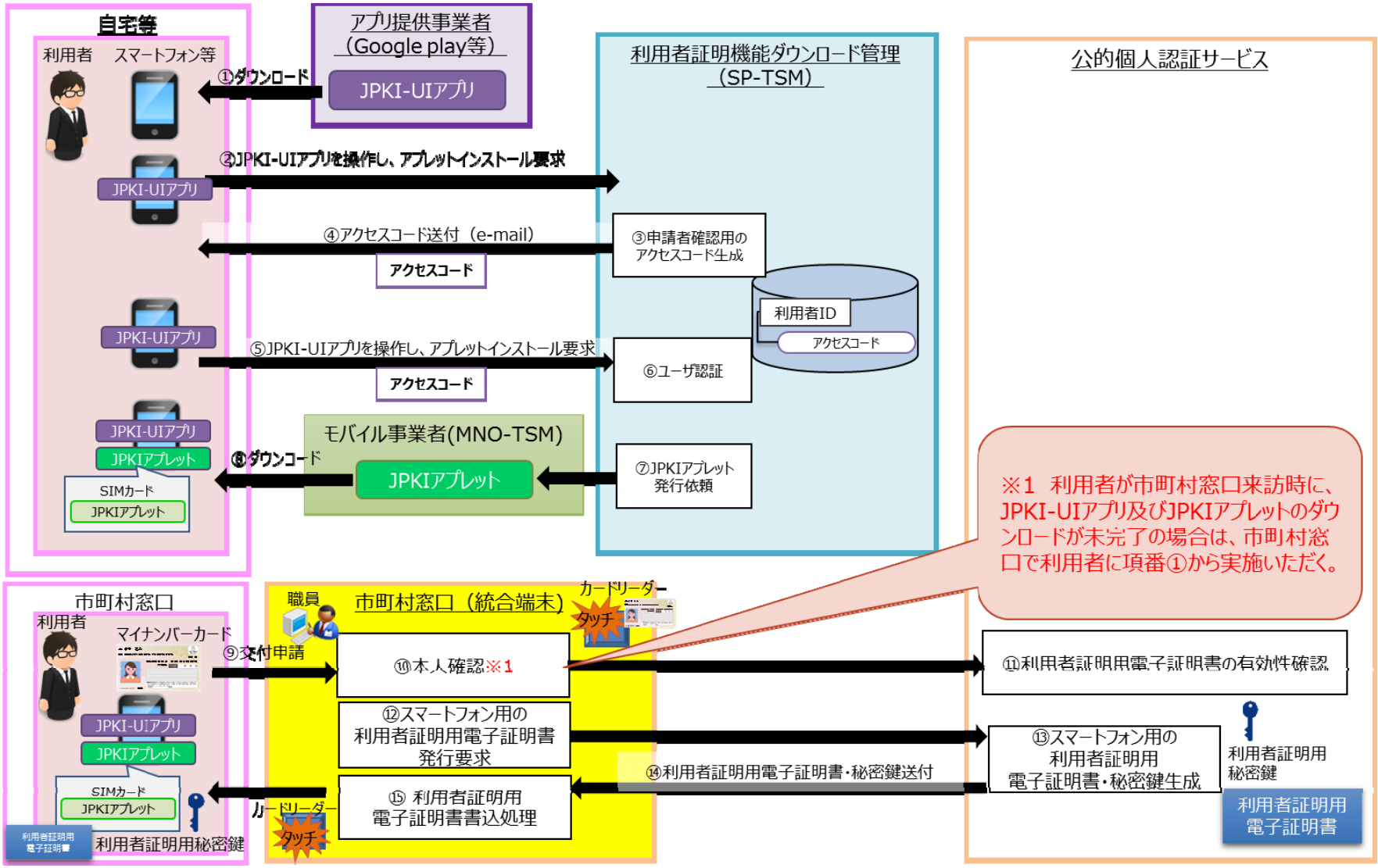
青字：実用化に向けた検討事項 赤字：重要な課題

#	検討項目	Android（検討結果）	iOS（検討結果）
5	PIN初期設定・ PIN初期化・再設定 (PIN忘失)	・利用者が市町村窓口に来訪し、統合端末のRWにスマホをかざし、鍵データの書き込みからPINの初期化・再設定を行う。	・利用者が市町村窓口に来訪し、スマートフォンから統合端末の認証が完了した場合のみ、スマホでPINの初期化・再設定を行う。
6	PIN変更：JPKI-UIアプリ/統合端末 (PINを覚えている)	・JPKI-UIアプリ：利用者がJPKI-UIアプリを起動し、PINの変更を行う。 ・統合端末：利用者が市町村窓口に来訪し、統合端末のRWにスマホをかざし、PINの変更を行う。	・JPKI-UIアプリ：利用者がJPKI-UIアプリを起動し、PINの変更を行う。

※ 2.2 参考①、②参照

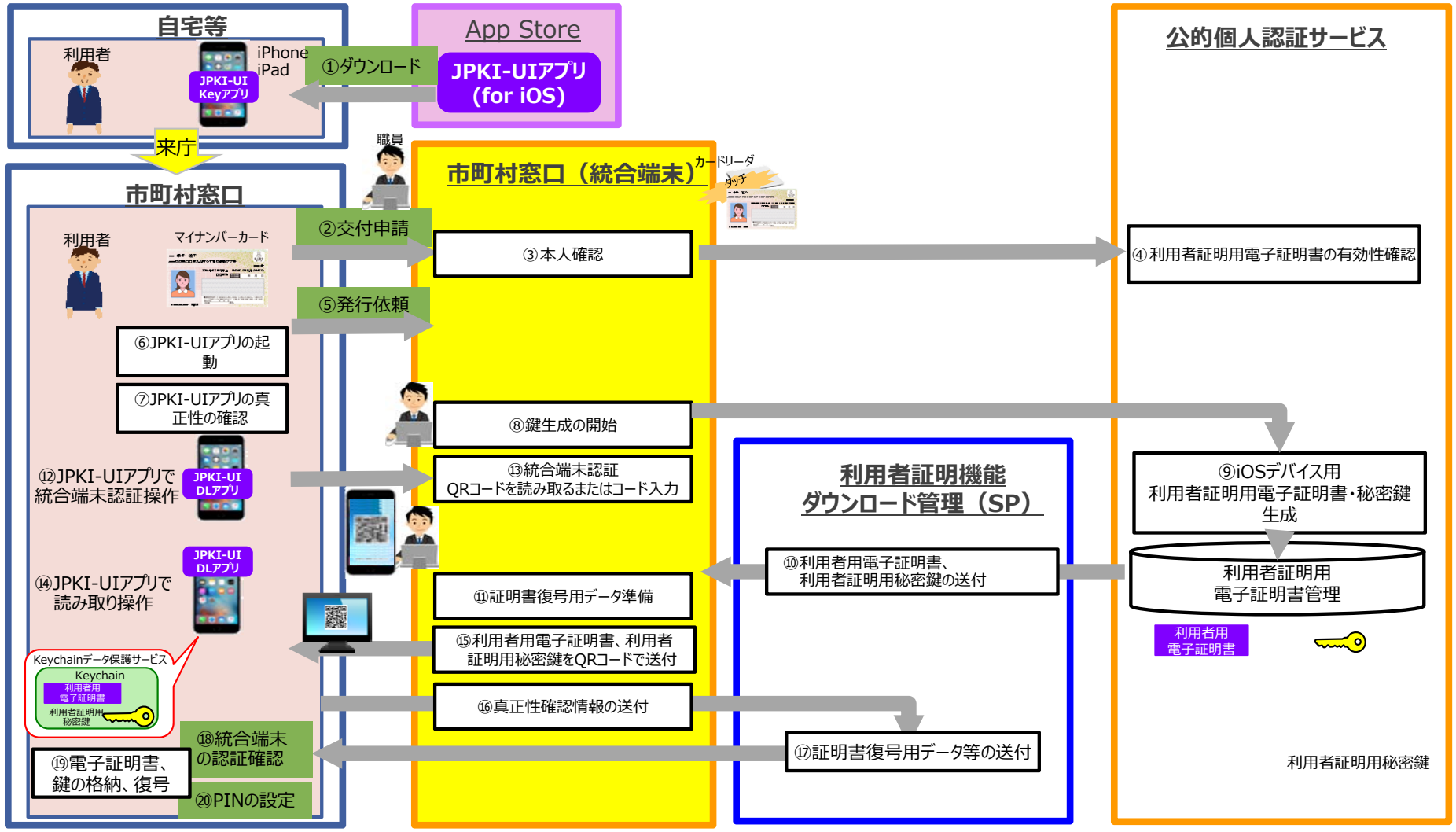
2.2 参考① Androidスマートフォン電子証明書の格納フロー

・アプリ配信事業者(Google play)からJPKI-UIアプリをダウンロードし、JPKIアプレットは利用者が事前にアクセスコードを使用してユーザ認証をSP-TSMで行い、SP-TSMを介してMNO-TSMからダウンロードする。外部認証鍵、秘密鍵設定キー等はJPKIアプレットへ埋め込む。
・電子証明書及び秘密鍵は窓口にて統合端末のICカードRWにスマートフォンをかざして、利用者のスマートフォンのSIMカード内に格納する。



2.2 参考② iOSスマートフォン電子証明書の格納フロー

・アプリ配信事業者(App Store)からJPKI-UIアプリをダウンロードする。
・電子証明書及び秘密鍵は窓口で統合端末よりQRコードにて、JPKI-UIアプリの真正性確認済みのiOS搭載スマートフォンのKeychain内に格納する。



2.3 課題③SIMカード（電子証明書を格納済み）を本人以外のスマートフォンに差し替えて利用されることを防止する対策の検討結果

○：重要な課題なし　△：重要な課題あり

青字：実用化に向けた検討事項 赤字：重要な課題

#	検討項目	Android（検討結果）	iOS（検討結果）
7	SIMカード差し替えの対策	・本人が意図してPINの流出したSIMカードを第三者等に譲渡・転売等を行い、他人がなりすまして不正利用する脅威に対して本対策を検討した。 ・SIMカードの差し替えを防止する対策として、JPKIアプレット内でスマホの端末IDチェックを行い、業務PC（統合端末を含む）でそのチェック結果を確認する方式を検討した。 ・不正利用防止のためにすべてのサービス利用事業者に対策を実装してもらう必要があり、その負担が課題である。 ・機種変更(SIMカード変更無し)において、利用者は端末ID登録のために窓口来訪等が必要となり利便性が損なわれるという課題がある。 ・本対策は本人が意図としてPINも流失した場合を想定した対策となっている。そのため、スマホとSIMカードをセットで転売された場合はPINを入力し利用できてしまうため対策の効果がない。また、マイナンバーカードでもそのような不正利用に対する対策はなく、本対策の実行には費用対効果及び利便性を考慮する必要がある。	（該当しない）

2.3 参考 対策実施時における課題

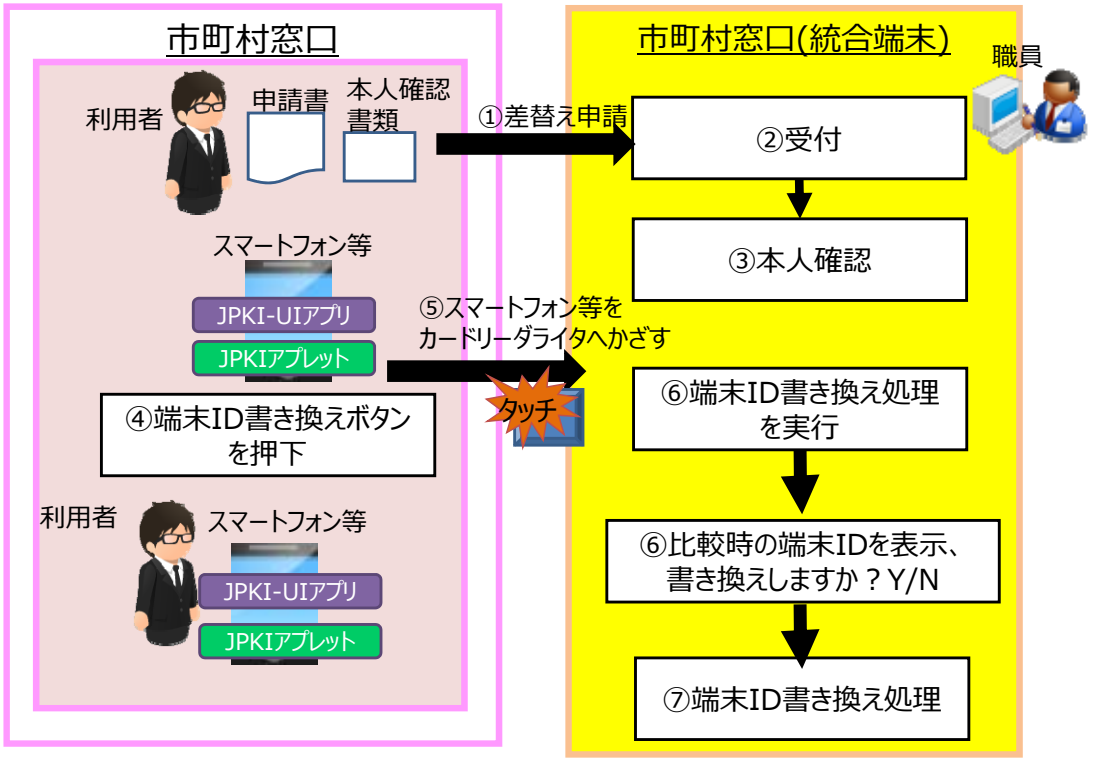
・SIMカードをそのまま使えるような機種変更において、端末IDチェックによってNGとなる。
（すべてのサービス事業者が端末IDチェックを実装する前提）
・端末IDチェックをOKにするためには、機種変更後の端末IDをSIMカードに登録する必要があり、利用者は市町村窓口に来訪する必要がある。

＜機種変更時（SIMカードの変更なし）＞

端末IDが異なるため端末IDチェックでNGとなる。

＜市町村窓口＞

対面での本人確認を実施後、機種変更後の端末IDをSIMカードに登録する（端末IDの書換え）。



2.4 課題④電子証明書の発行時及び利用時の脅威とその対策についての検討結果

○：重要な課題なし　△：重要な課題あり

青字：実用化に向けた検討事項 赤字：重要な課題

#	検討項目	Android（検討結果）	iOS（検討結果）
8	発行時の脅威とその対策	・配信時の認証の仕組みやアクセス制御メカニズムにより、発行時におけるJPKI-UIアプリやJPKIアプレットの改ざん、窃取、なりすまし、盗聴等を防止できることを確認できた。	・Apple Push Notification Service経由による通知の仕組みや、アクセス制御メカニズムにより、発行時におけるJPKI-UIアプリの改ざん、窃取、なりすまし、盗聴、盗み見等を防止できることを確認できた。
9	利用時の脅威とその対策	・SIMカードの耐タンパー性やPINにより、利用時における改ざん、窃取、なりすまし、盗聴等を防止できることを確認できた。	・Keychainの仕組みやPINにより、利用時における改ざん、窃取、なりすまし、盗聴、盗み見等を防止できることを確認できた。

2.5 課題⑤市町村窓口での各種申請を基本とする電子証明書のライフサイクル（失効、更新、再発行等）の検討結果

○：重要な課題なし　△：重要な課題あり

青字：実用化に向けた検討事項 赤字：重要な課題

#	検討項目	Android（検討結果）	iOS（検討結果）
１０	電子証明書の業務	・発行、更新、PINの初期化、PINの変更について、業務フローについて検討した。 ・失効、再発行、一時保留／一時保留解除について、業務フローを検討した。 ・一時保留／保留解除の機能は、公的個人認証システム等を大幅に改修する必要があり、コスト的な課題がある。 ※キャリアが提供する停止機能は圏外等において確実なサービス停止はできない。	・発行、更新、PINの初期化、PINの変更について、対応フローが確認できた。統合端末の認証が完了した場合のみ、スマホでPINの初期化を行う。 ・失効、再発行、一時保留／一時保留解除について、業務フローを検討した。 ・一時保留／保留解除の機能は、公的個人認証システム等を大幅に改修する必要があり、コスト的な課題がある。 ※iCloudが提供する停止機能は圏外等において確実なサービス停止はできない。
11	スマートフォン特有の業務	・新規契約、機種変更、名義変更（利用者の変更あり）、故障、紛失、一時紛失、JPKIアプレット削除、JPKI-UIアプリ削除について業務フローを検討した。 ・実用化にあたっては公的個人認証システムで有効でない利用者証明用電子証明書がSIMカード内に存在する場合の対応方法を検討する必要がある。	・新規契約、機種変更、名義変更（利用者の変更あり）、故障、紛失、一時紛失、iOS初期化、JPKI-UIアプリ削除、パスコード無効化について業務フローについて検討した。

2.5 参考 スマートフォンの一時紛失について

キャリアのNFCサービス停止機能は、JPKIアプレット用の個別機能ではなく、ユーザ向け補助機能であり、 電源がONかつ回線が通じる状況でないと作動しない等制約がある。そのため、以下のように対応する必要がある。 【凡例：○／△／×】

案		概要	メリット／デメリット	安全性	利便性	実現性
1	スマートフォン用利用者証明用電子証明書を失効する。	利用者が市町村窓口に来訪し、失効する。	メリット：解約等と同一手順のため、一時紛失に伴うJPKI追加開発がない。 デメリット：即時性がない。（スマートフォンの一時紛失後、利用者が市町村窓口に来訪するまでにタイムラグが発生する。）	△	△	○
2		オンライン窓口失効を行う。	メリット：夜間休日でも申請することができる。また、スマートフォン（SIM）一時紛失中に悪用される恐れが低い。 デメリット：有効な署名用電子証明書を保持している必要がある。また、JPKIシステムに追加機能開発が必要になる。	○	△	△
3	スマートフォン用利用者証明用電子証明書を一時保留する。	[一時保留] JPKI用（マイナンバーカード用コールセンターとは別に）コールセンターを用意し、スマートフォン用利用者証明用電子証明書の一時保留を行う。 [一時保留解除]スマートフォンが見つかった時は、利用者が市町村窓口に来訪して一時保留解除を行う。	メリット：即時性がある。また、スマートフォン（SIM）一時紛失中に悪用される恐れが低い。 デメリット：本人確認時に4情報が一致しない恐れがある。また、コールセンター新設に伴いJPKIシステム開発に膨大なコストがかかる。	○	○	△
4		[一時保留] マイナンバーカード用コールセンターにて、スマートフォン用利用者証明用電子証明書のみ一時保留を行う。 [一時保留解除]スマートフォンが見つかった時は、利用者が市町村窓口に来訪して一時保留解除を行う。	メリット：即時性がある。また、スマートフォン（SIM）一時紛失中に悪用される恐れが低い。 デメリット：本人確認時に4情報が一致しない恐れがある。また、既存コールセンターへの影響が大きく、JPKIシステム及びカード管理システム開発に膨大なコストがかかる。	○	○	△
5		[一時保留] マイナンバーカード用コールセンターにて、マイナンバーカードを一時停止することで、スマートフォン用利用者証明用電子証明書の一時保留も行う。（マイナンバーカード格納の電子証明書も一時保留される。） [一時保留解除]スマートフォンが見つかった時は、利用者が市町村窓口に来訪してマイナンバーカードの一時停止解除を行うことで、一時保留解除を行う。	メリット：即時性がある。また、スマートフォン（SIM）一時紛失中に悪用される恐れが低い。 デメリット：マイナンバーカードは紛失していないが、署名用電子証明書、利用者証明用電子証明書も一時保留になり、使用不可となる。（署名用電子証明書は失効される。）また、JPKIシステムに追加機能開発が必要になる。	○	△	△

2.6 課題⑥業務アプリからSIMカード等へのアクセス方法の検討結果

○：重要な課題なし　△：重要な課題あり

青字：実用化に向けた検討事項 赤字：重要な課題

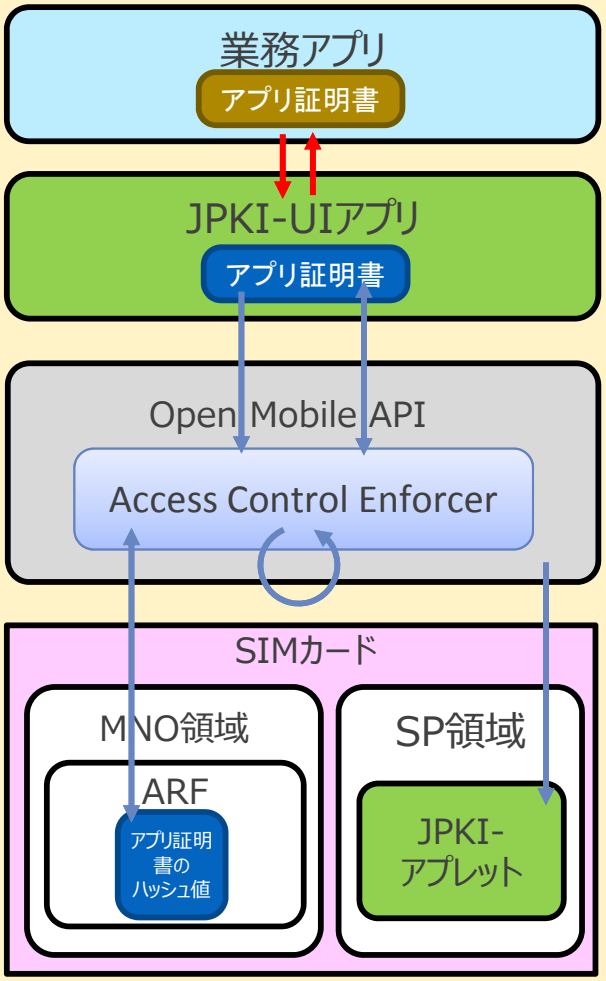
#	検討項目	Android（検討結果）	iOS（検討結果）
12	業務アプリからSIMカード・Keychainへのアクセス方法	・JPKIアプレットにアクセスする機能はJPKI-UIアプリに実装し、インテント機能を利用しJPKI-UIアプリに業務アプリ用インタフェースを用意する。 ・JPKI-UIアプリでの実装により業務アプリの開発工数低下、ハッシュ値登録の不要化を実現する。 ・業務アプリから実行できる機能は、JPKIアプレットの「利用」に限られるため、業務アプリのアクセス制御は不要。	・Keychainに格納された利用者証明用電子証明書を利用する機能をApp Extensionとして提供することで、利用アプリから直接Keychainを参照することなく証明書利用を実現できることを確認した。 ・Androidの場合と利用条件を統一し、特に利用を制限しないこととする。
13	インタフェース仕様	・業務アプリとJPKI-UIアプリ間においてインテント（注1）機能を使用する以下のインタフェース仕様を検討した。 -利用者証明用電子証明書取得 -利用者証明用電子証明書署名生成	・業務アプリとJPKI-UIアプリ間においてApp Extension（注2）機能を使用する以下のインタフェース仕様を検討した。 -利用者証明用電子証明書取得 -利用者証明用電子証明書署名生成

（注1）Androidで用意されているアプリケーション連携を可能とする仕組みの名称

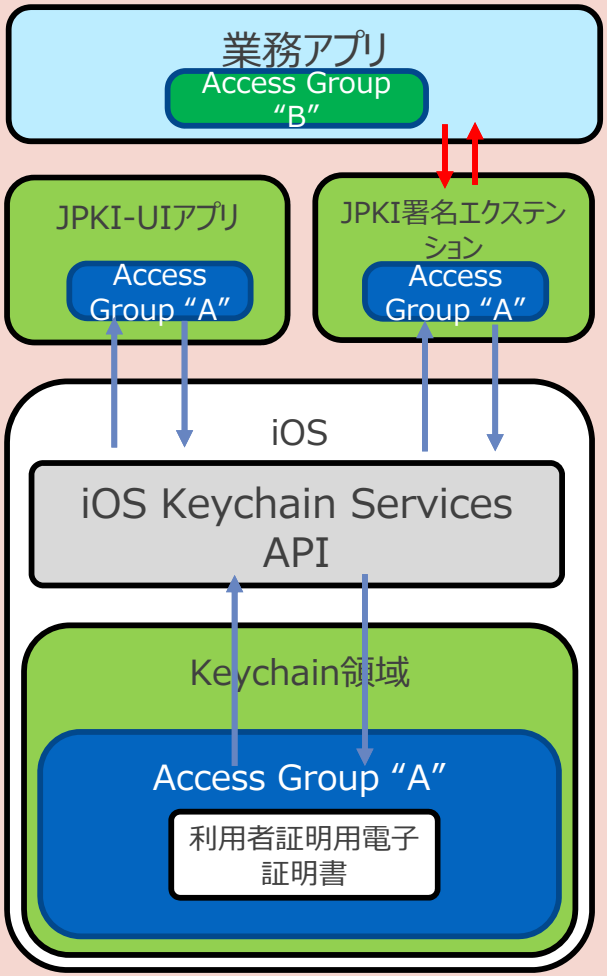
（注2）iOSで用意されているアプリケーション連携を可能とする仕組みの名称

2.6 参考 業務アプリからSIMカード等へのアクセス方法について

・Androidスマートフォン：JPKIアプレットに業務アプリからアクセスする機能は、JPKI-UIアプリに実装しインテント機能にてインタフェースを用意する。
・iOSスマートフォン：Keychainに業務アプリからアクセスする機能はApp Extension機能にて業務アプリ用インタフェースを用意する。



Androidスマートフォン：JPKI-UIアプリ経由でアクセス



iOSスマートフォン：App Extensionにより署名機能を提供する方式

2.7　課題⑦市町村窓口のICカードRWとスマートフォンの通信確認結果

○：重要な課題なし　　△：重要な課題あり

青字：実用化に向けた検討事項 赤字：重要な課題

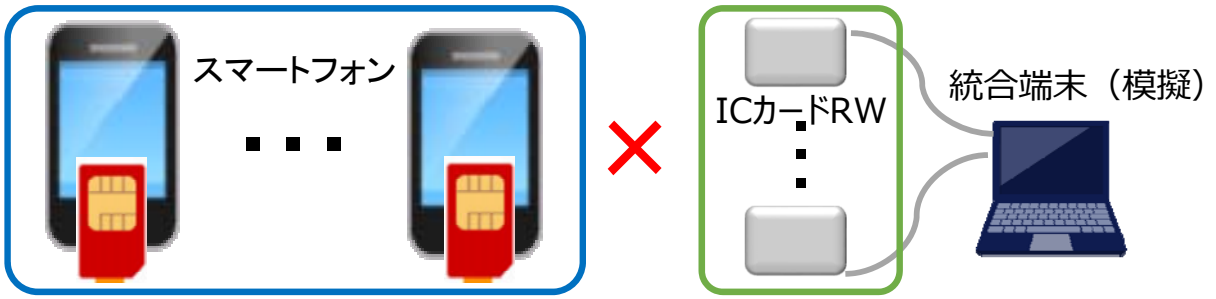
#	検討項目	Android（検討結果）	iOS（検討結果）
14	市町村窓口のICカードRWとスマートフォンの通信確認	・6機種のICカードRW(注1)と30機種のNFC対応スマートフォンにて動作検証を実施した。 ・2機種のICカードRWでは、動作しない、もしくは動作範囲が他と比較して小さかった。 ・上記2機種を除いた4機種のICカードRWを平均すると、r軸 10mm、Z軸 10mmまでの範囲で96%、r軸 20mm、Z軸 10mmまでの範囲で85%の測定点で動作した。 ・スマートフォンの一部機種では、ICカードRWとの動作範囲が他機種と比較して小さいものがある。 ・スマートフォン向けのICカードRWの認定基準を作成する必要がある。 ・認定基準の作成においては、販売終了したICカードRWについての取り扱いを検討する必要がある。 ・既存のICカードRWがICカード用に作られているため、スマートフォン用のガイドやスペーサーの配備、もしくはスマートフォン用のICカードRWを配備といった対策が必要となる。	（該当しない）

（注1）ＩＣカードリーダ／ライタ調達に係る資料（J-LIS）より全6機種を選定

2.7 参考 NFC対応スマートフォンと非接触ICカードRWの動作検証条件・評価観点について

・NFC対応スマートフォンと統合端末接続の非接触ICカードRWの発行時及び利用時の模擬用コマンドシーケンスにて動作検証を行った。
・NFC対応スマートフォンを、市町村の統合端末に取り付けられている非接触ICカードRWにかざした場合に、どのような位置関係（距離、範囲等）において通信が可能であるか、市町村職員の運用に支障がないかを調査した。

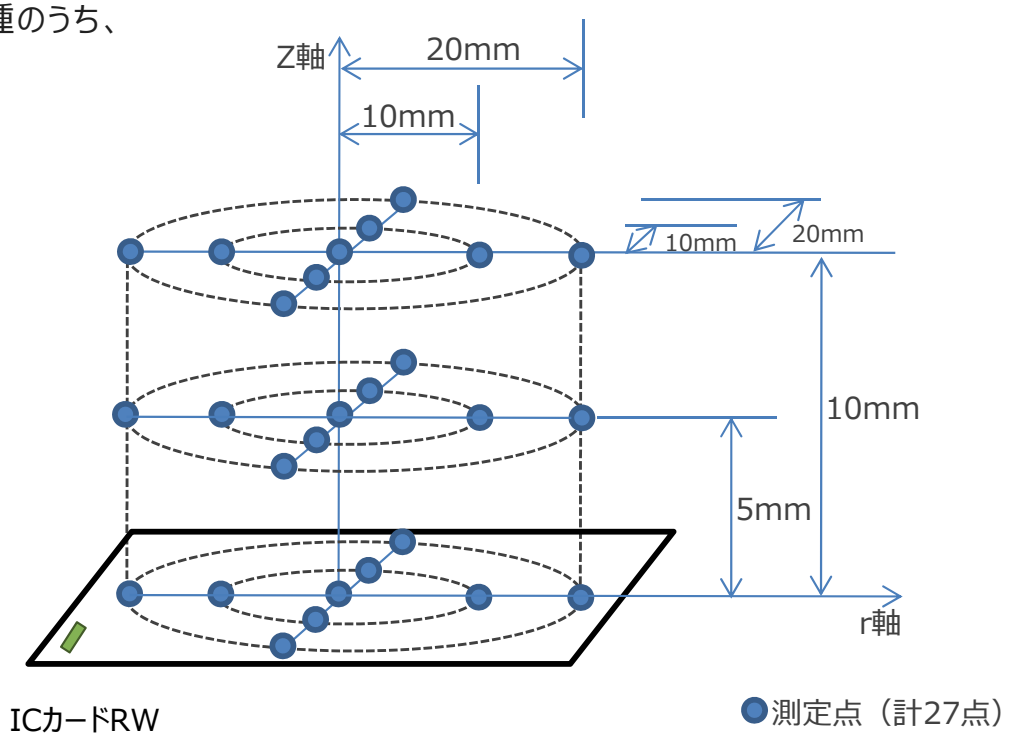
●検証条件：
①NFC対応スマートフォン（30機種）
- 2017年1月以降を目安に発売機種を選定する。
- MVNO端末については、JPKI-アプレットを発行済みのキャリアのSIMカードを装着する。



②統合端末に取り付けられている非接触ICカードRW
- 市町村の統合端末で使用されている、ＩＣカードリーダ／ライタ調達に係る資料（J-LIS）に記載の6機種のうち、昨年度の動作検証において、スマートフォンとの初期通信に失敗することが判明した1機種（RC-S330）は除外する。

●評価観点：ユーザや市町村での利用形態を以下と想定。
①発行（所要時間：約5秒※）
- スマートフォンをICカードRWに置く。
  →Z軸は、0mm、5mm
- スマートフォンに印字されているモバイル非接触IC通信マークをICカードRWの中心に合わせる。
  → r軸は0mm、10mm、20mm

②利用（所要時間：約0.6秒※）
- スマートフォンをICカードRWに置くorかざす。かざす場合の距離は10mmを想定。
  →Z軸は、0mm、5mm、10mm
- スマートフォンに印字されているモバイル非接触IC通信マークをICカードRWの中心に合わせる。
  →r軸は0mm、10mm、20mm



2.8 課題⑧現行制度への影響調査結果

○：重要な課題なし　　△：重要な課題あり

青字：実用化に向けた検討事項 赤字：重要な課題

#	検討項目	Android（検討結果）	iOS（検討結果）
15	現行の法制度にどのような影響があるかを調査	・現行法制度への影響を調査した。窓口発行とすることで、現行の法制度へ近づいた。スマートフォン特有の事象として、機種変更や故障、紛失、一時紛失、解約等による失効を考慮する必要があることを確認した。 ・以下の検討内容によっては法改正を伴う可能性がある。 ・SIMカードは民間事業者が提供するものであるため、現行の総務省令の規定のみでよいか検討が必要。 ・SIM利用者証明用電子証明書の定義及び記録事項を定める必要がある。 ・マイナンバーカードが失効した場合や使えなくなった（紛失）場合のSIM利用者証明用電子証明書の対応を検討する必要がある。 ・署名検証者／利用者証明検証者への「対応証明書の発行の番号」の提供	・現行法制度への影響を調査した。スマートフォン特有の事象として、機種変更や故障、紛失、一時紛失、解約等による失効を考慮する必要があることを確認した。 ・以下の検討内容によっては法改正を伴う可能性がある。 ・iPhoneは民間事業者が提供するものであるため、現行の総務省令の規定のみでよいか検討が必要。 ・「住所地市町村長が記録する」という記載に対して、電子証明書の記録方法としてQRコードの読み取りをどのように解釈するか確認が必要。 ・iOS利用者証明用電子証明書の定義及び記録事項を定める必要がある。 ・マイナンバーカードが失効した場合や使えなくなった（紛失）場合のiOS利用者証明用電子証明書の対応を検討する必要がある。 ・署名検証者／利用者証明検証者への「対応証明書の発行の番号」の提供