資料4－1

SIMカードへの利用者証明機能のダウンロードの実現に向けた今後の検討の進め方について

平成28年3月28日

今後の取組の概要

スマートフォンのSIMカードへの公的個人認証サービス（JPKI）の利用者証明機能のセキュアなダウンロードを実現するための技術的課題等について検証するとともに、当該利用者証明機能を活用したユースケースの実現に向けた推進方策について検討。

（１）SIMカード及びスマートフォンの要件の検討

①対象とするSIMカードの範囲、機能要件の整理
②対象とするスマートフォンの範囲、機能要件についての整理

（２）JPKIアプレット及びJPKI-UIアプリの要件の検討

①SIMカードにJPKIの利用者証明用秘密鍵及び利用者証明用電子証明書をダウンロードするのに必要なアプレット、JPKI-UIアプリを開発し、機能要件についての整理

（３）SIMカードへの安全なダウンロード方法の検討

①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を活用し、JPKI-アプレット及びJPKI-利用者証明用秘密鍵等を申請者のSIMカードにダウンロードするシステム（SP-TSM）の開発（別紙１）

②セキュアなダウンロード方法の検証（別紙2、3）

③MVNOのサービスで提供されるSIMカード及びSIMロックフリー端末・SIMロック解除端末でサービス提供するための対応方法の検討

（４）既存のJPKIシステムの改修に関する検討

①SP-TSMとJPKIシステムとの最適な機能分担、インタフェースの検討
②マイナンバーカードの利用者証明用電子証明書とスマートフォンにダウンロードされた利用者証明用電子証明書との紐付け、管理機能の検討

（５）運用面での課題の洗い出し

①マイナンバーカードを使ったオンライン申請及びオンラインダウンロードを実現する際の課題の抽出、解決策の検討

（６）ユースケースの検討

①スマートフォンでの利用形態にあわせて、ユーザニーズの高いユースケースを設定し、実現に向けた課題を抽出し、実現するための推進方策を検討（別紙4）。

【参考】今後の検証内容①

1. 検討にあたっての前提条件

（１）SIMカードへのダウンロード申請は、マイナンバーカード交付済みである利用者であることを前提に検討する。

（２）SIMカードへのダウンロード申請は、マイナンバーカードの公的個人認証サービスを使った本人確認、電子署名を使って行うものを第一の方法として考え、実現に向けた課題解決策について整理する。

（３）JPKIアプレット、利用者証明用秘密鍵、利用者証明用電子証明書のダウンロードはオンラインでの実現を前提に検討を行う。

（４）JPKIアプレットのSIMカードへのダウンロードは、既存のMNO-TSM装置を前提とし、利用者証明用秘密鍵、利用者証明用電子証明書のダウンロードにあたっては、モバイル通信事業者が提供しているモバイルNFCサービスプラットフォームを活用し、必要なシステムを構築する。実現方法の検討にあたっては、セキュリティに配慮しつつ、既存の仕組みを最大限活用できるよう考慮する。

（５）検討に当たっては、MVNOのサービス利用者や、SIMロックフリー端末・SIMロック解除端末の利用者も考慮する。

（６）ユースケースの検討にあたっては、スマートフォンの特徴をいかしたユースケースであること、利用者の裾野が広いことなど利用ニーズが高いものを選定し、検証する。

2. 検証項目

（１）SIMカード及びスマートフォンの要件の検討

① 現在のSIMカードに実装されているセキュリティ機能、ライフサイクル機能等を踏まえ、民間モバイルNFCサービス（クレジット）を参考に、対象とするSIMカードの対象範囲、JPKIの利用者証明用秘密鍵及び利用者証明用電子証明書をダウンロードするための必要な機能要件※について整理を行い、実現方法を検討すること（MVNOの提供するSIMカードを含む）。

※ 機能要件の例：
暗号アルゴリズム、メモリ容量、アプレット、パーソナライズデータのセキュアダウンロードするためのSIMの機能、
SIM間の利用者証明機能の移転やSIMの廃棄・失効等に関する要件、PINなし認証　等

【参考】今後の検証内容②

2. 検証項目（続き）

② JPKIの利用者証明用秘密鍵等のダウンロードを可能とするスマートフォン（例：NFC対応スマートフォンであること（ Android）等）、機能要件について整理を行うこと（SIMロックフリー端末・SIMロック解除端末を含む）。

※機能要件の例
- ダウンロード時の書き込みI/F（携帯電話網、Wi-Fi）
- NFC対応スマートフォンとしての要件
- MNO-TSMとの通信機能、SIMの読み書き機能（キャリア間の仕様差分への対応、MVNOへの対応）

（２）JPKI-アプレット及びJPKI-UIアプリの要件の検討

① SIMカードにJPKIの利用者証明用秘密鍵等をダウンロードするのに必要なJPKIアプレットを開発し、JPKIアプレットの機能要件の整理を行うこと。その際、マルチベンダ対応の共通アプレット等効率的な開発・品質確保の方法やSIM毎にカスタマイズの要否についても検討すること（速度等の機能要件への対応等）。

② SIMカードにJPKIの利用者証明用秘密鍵等をダウンロードするのに必要なJPKI-UIアプリを開発すること。その際、スマートフォンのOSのバージョンや製造メーカ、キャリアに極力依存しないJPKI-UIアプリの構成、開発・品質確保の方法を検討すること。

（３）SIMカードへの安全なダウンロード方法の検討

① 利用者の利便性とセキュリティを確保した、パソコン、スマートフォン等からの利用者証明機能のオンラインによる申請方法を検証すること。その際、JPKI-アプレットを当該申請者が指定する端末にのみダウンロードする仕組みを検証すること。

② 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を活用し、JPKI-アプレット及び利用者証明用秘密鍵等を申請者のSIMカードにダウンロードするシステム（SP-TSM）を開発すること。

【参考】今後の検証内容③

2. 検証項目（続き）

（３）SIMカードへの安全なダウンロード方法の検証（続き）

③ 既存のモバイルNFCサービスプラットフォームの実現方法を踏まえ、SIMカードへのJPKIアプレットのダウンロード時におけるダウンロードに必要な鍵の格納場所及びセキュアなダウンロード方法を検証すること。必要に応じて、SP独自のセキュリティ対策を検討すること。【別紙１，別紙２】

④ JPKIの利用者証明機能を格納するSIMの登録・管理方法について検討を行うこと。（オンライン申請を前提とし、SP-TSM側でのSIMの識別情報の利用の要否等）

⑤ 例えば、以下のような時、モバイル事業者間におけるSIMの仕様差分への対応方法について整理すること。

ア JPKIアプレットをSIMカードにダウンロード時
イ パーソナライズ（利用者証明用秘密鍵等のSIMへのダウンロード）時　等

⑥ MVNOのSIMカード及びSIMフリー端末・SIMロック解除端末等への対応方法について検討すること。

（４）既存JPKIシステムの改修に関する検証

① SP-TSMとJPKIシステムの最適な機能分担とそのインタフェースについての検討

② マイナンバーカードの署名用電子証明書及び利用者証明用電子証明書とスマートフォンにダウンロードされた利用者証明用電子証明書との紐付け機能、マイナンバーカードあるいはスマートフォンの更新・紛失時におけるスマートフォンに格納された利用者証明用電子証明書の取扱等）を整理すること。

（５） JPKIの利用者証明機能のダウンロードを実現するにあたっての運用面の検討

① マイナンバーカードを使ったオンライン申請を検討の前提とした場合における、署名用電子証明書による署名検証による本人確認を行う上での課題の洗い出し、解決策を検討すること。

【参考】今後の検証内容④

2. 検証項目（続き）

（５） JPKIの利用者証明機能ダウンロードを実現するにあたっての運用面の検討（続き）

② マイナンバーカードを使ったオンライン申請による場合、JPKIの利用者証明機能をダウンロードするSIMカードの識別方法、申請者が当該携帯電話の契約者あるいは利用者であることを確認の要否等を検討すること。

③ PINを失念・ロックした際の再設定方法（マイナンバーカードの場合、市町村窓口端末において対応）

④ SIMカードに格納された電子証明書の有効期限等の確認方法

⑤ JPKIの利用者証明機能ダウンロードに当たっての関係者の役割分担、責任分解点を整理すること。

⑥ 消費者対応の在り方（操作方法、対応端末等に関する問い合わせ等）について検討すること。

⑦ SIMカード間の利用者証明機能の移転方法について整理すること（MNO-MVNO間含む）。

⑧ 技術的課題を検討する中で マイナンバーカードを使ったオンライン申請・　オンラインダウンロードを実現する際の運用面での課題の整理し、対応方法について整理すること。

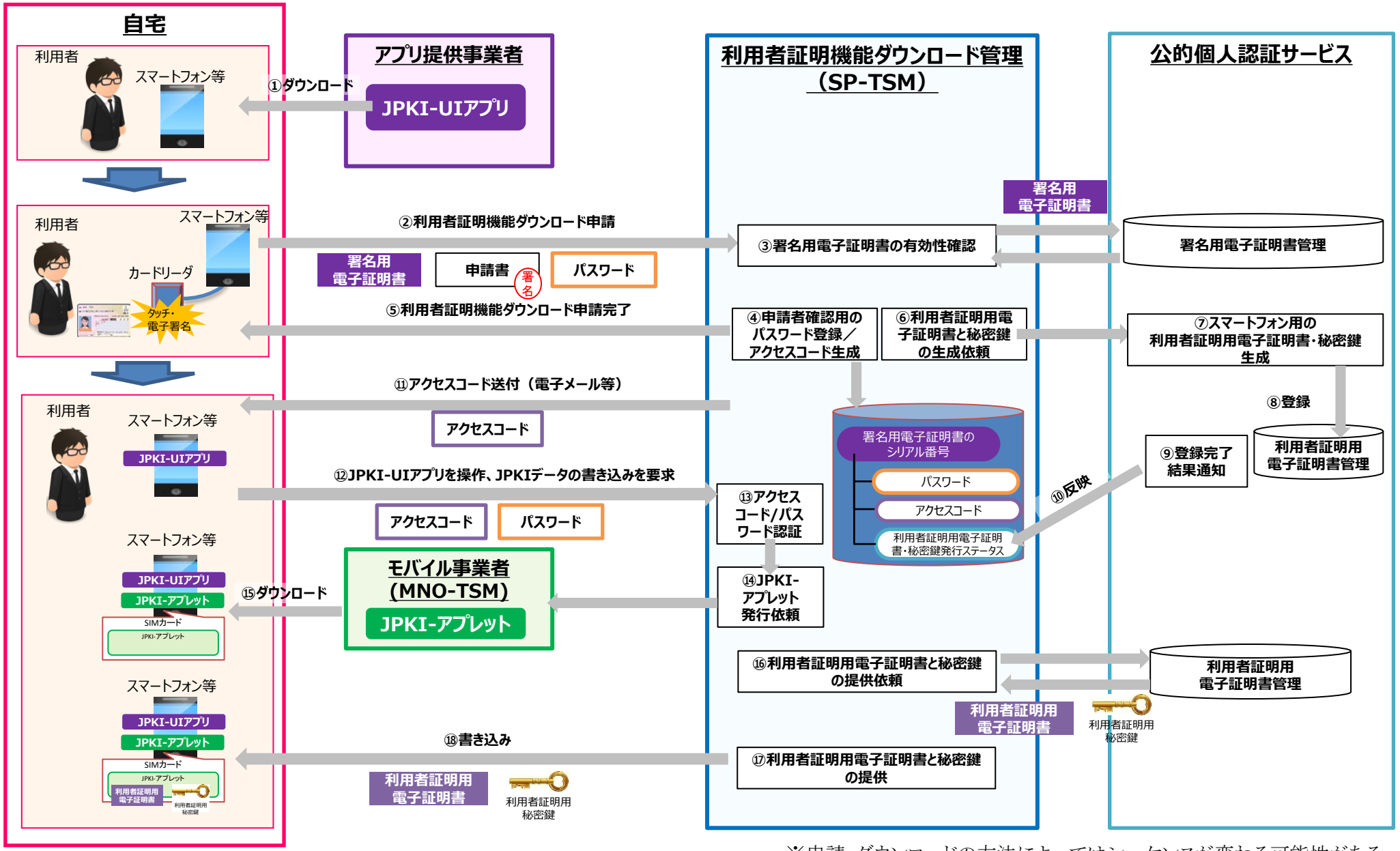
3. ユースケースの検討

（６）ユースケースの検討

① 利用形態として、カード代わりに利用する方法、スマートフォンに搭載されたUIアプリ等を経由してSIMカードにアクセスする方法の2通りがあることを前提としてユースケースを設定し、実現に向けた課題の抽出、解決策を検証すること。

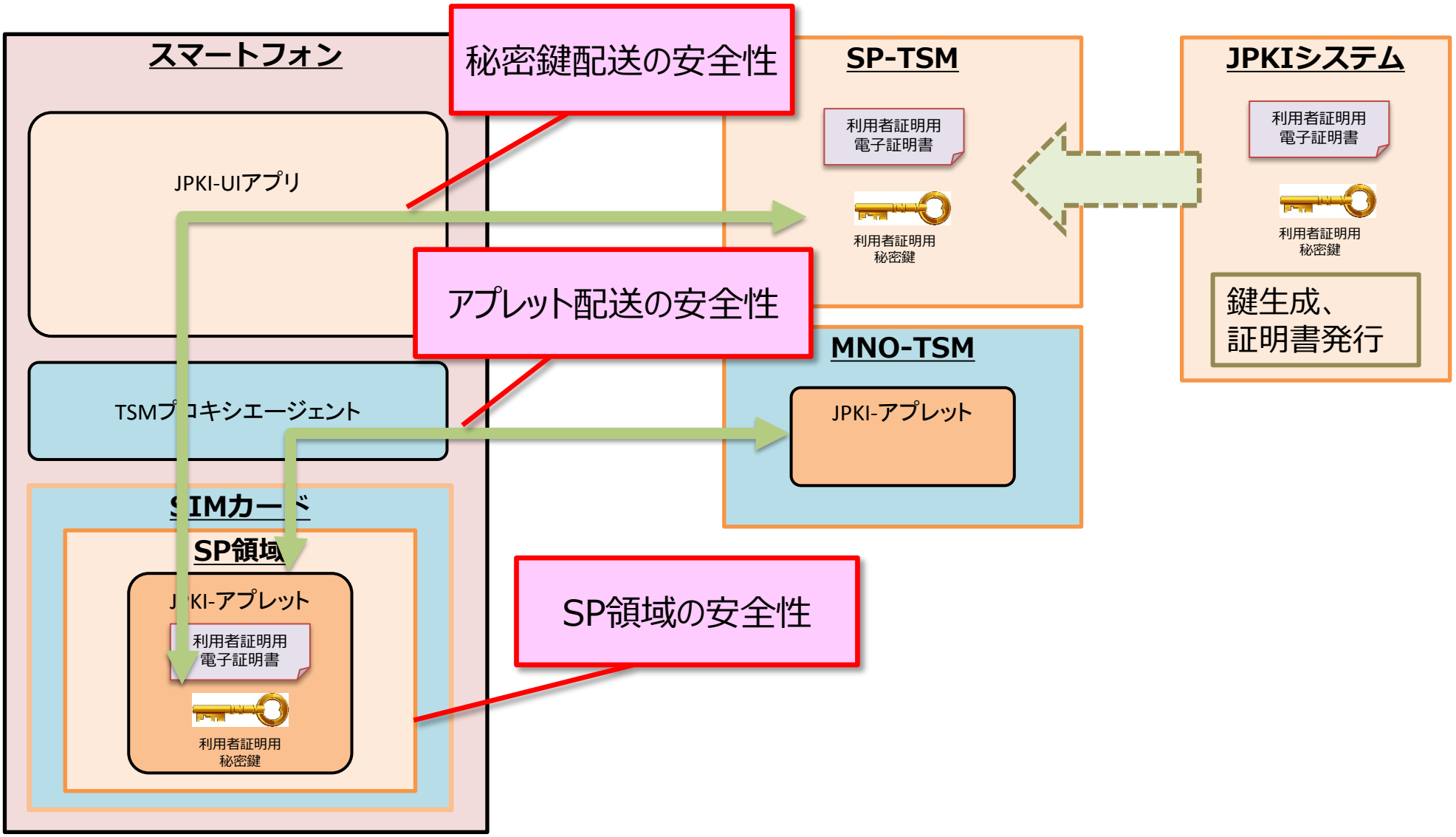
② ①で検討したユースケースの実現に向けた推進方策について検討すること。

別紙１利用者証明機能ダウンロードの検証システム（案）



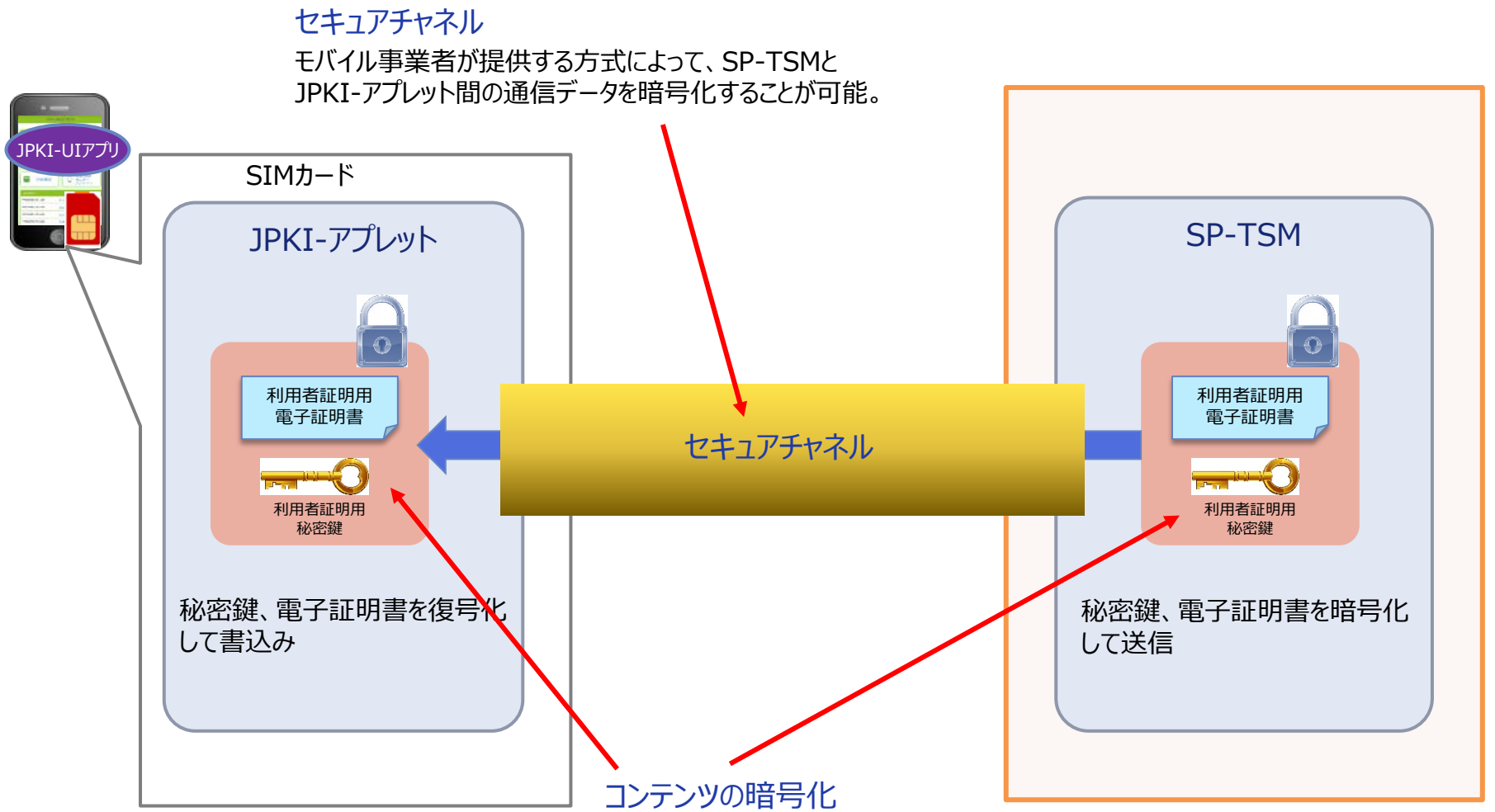
※申請・ダウンロードの方法によってはシーケンスが変わる可能性がある。

【別紙２】利用者証明機能のオンラインダウンロードに関する検討項目



【別紙３】鍵及び電子証明書の書込みにおけるセキュリティ確保について

・SP-TSMとJPKI-アプレット間は、モバイル事業者が提供する方式により、通信データの暗号化を行うことが可能。
・更に、秘密鍵、電子証明書の配信におけるセキュリティ対策は強化するため、SP独自の方式によって秘密鍵、電子証明書の暗号化を実施することも可能。



※スマートフォンへの利用者認証機能のダウンロード検討SWG（第3回）（H28.2.16）資料

【別紙４】スマートフォンでの利用者証明機能の利用形態

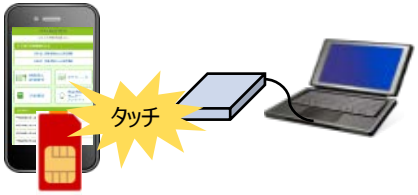
- スマートフォンでの利用者証明機能の利用形態として、以下２つのパターンが想定される。
  - カード代わりに使用：スマートフォンをリーダライタにタッチして利用者証明機能を利用する
  - UIアプリ等を経由してSIMカードにアクセス：スマートフォンアプリ等からのネットワーク経由でサービス提供者のサイトにアクセス。ログイン時等に利用者証明機能を利用する

カード代わりに使用

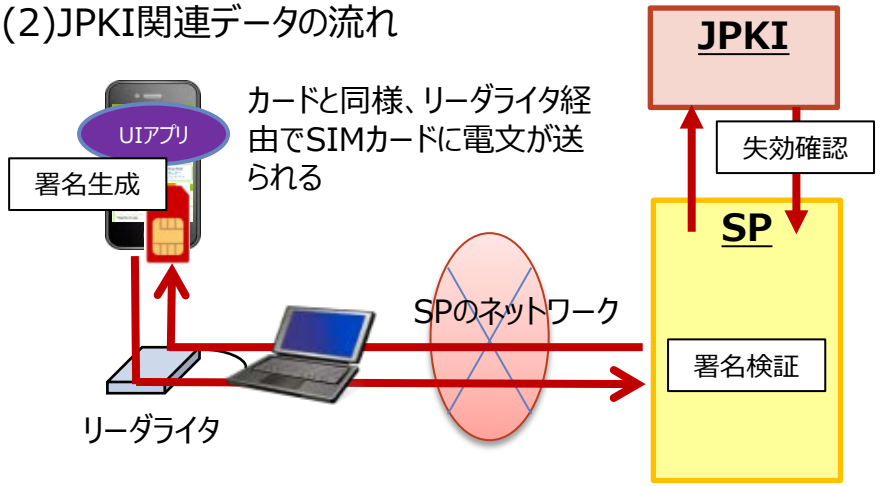
(1)利用形態

スマートフォンをリーダライタにタッチ

例）
- クレジット決済
- 健康保険証の資格確認



(2)JPKI関連データの流れ



UIアプリ等を経由してSIMカードにアクセス

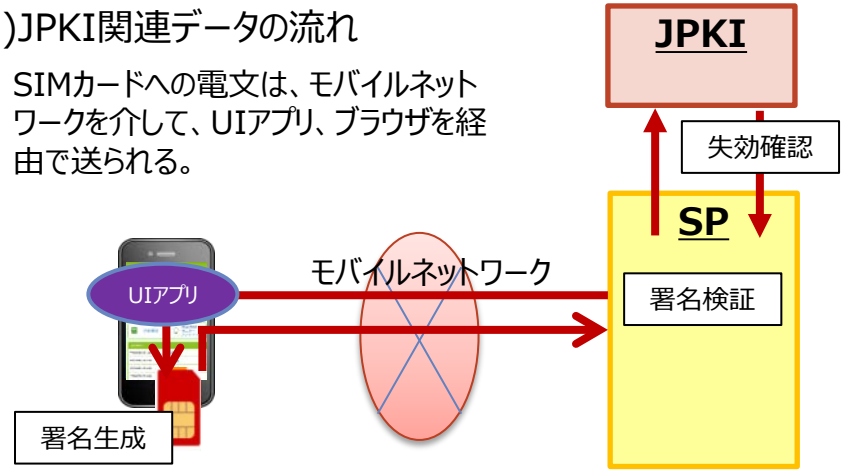
(1)利用形態

スマートフォンに搭載されたUIアプリ等を操作してサービスを利用

例）
- ネットバンキングへのログイン
- お薬手帳、母子健康情報閲覧

(2)JPKI関連データの流れ

SIMカードへの電文は、モバイルネットワークを介して、UIアプリ、ブラウザを経由で送られる。



※スマートフォンへの利用者認証機能のダウンロード検討SWG（第3回）（H28.2.16）資料

2019（平成31）年中の実現に向けて必要となる取組について

- 国においては、28年度からオンラインでJPKIの利用者証明機能をセキュアにダウンロードする方法、必要なSIMカードや端末、JPKIアプレット等の機能要件、運用面の課題を検証し、必要な制度整備を行う。
- J-LISにおいては、実証事業に協力し、実証事業の成果を踏まえてシステムの有り様について検討。
- モバイル事業者（MNO及びMVNO）においては、MNO-TSMやモバイルネットワークを最大限有効に活用できるよう、実証事業に協力。また、MVNO利用者へのJPKIの利用者証明機能の提供に向けた実現方法について、MNOとMVNOが連携して検討。
- 実証事業の成果は、本SWGにおいて共有、解決策について検討。