資料3

電子証明書のスマートフォン搭載に関する初期発行フロー（継続）

2020年12月4日

1．本資料のスコープ

本資料では、以下の項番1の検討結果について記載する。

1．第1回検討会　資料4における未検討項目についての検討(第2回検討会 資料3)
　〇アプレットライフサイクル
　〇仮PINを用いたローカルPIN設定
　〇２つの鍵・証明書を格納するフロー

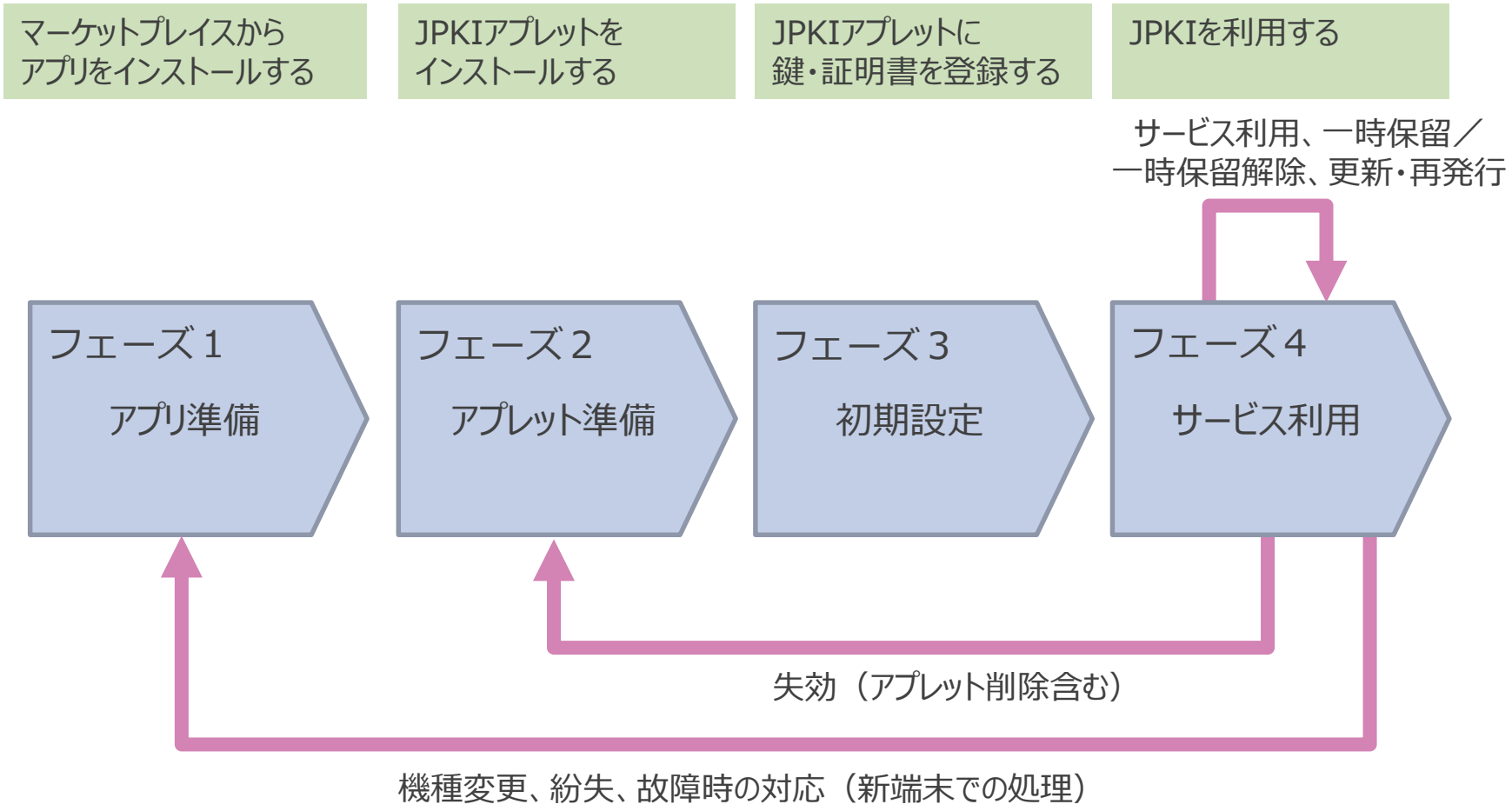
2．第1回検討会　資料5における未検討項目についての検討(第2回検討会 資料4)
　〇電子証明書に関する業務(再発行、PINの初期化、PINの変更)
　〇スマートフォン特有のライフサイクル(故障、紛失、一次紛失、破棄)

3．第1回検討会 指摘事項についての検討(第2回検討会 資料5)
　〇各業務におけるユーザ操作イメージの整理
　〇機種変更における交通ICとのUX比較

※参考：第1回検討会資料
- 資料４:電子証明書のスマートフォン搭載に関するシステム構成と初期発行フロー【参考資料2】
- 資料５:スマートフォン特有のライフサイクルへの対応【参考資料3】

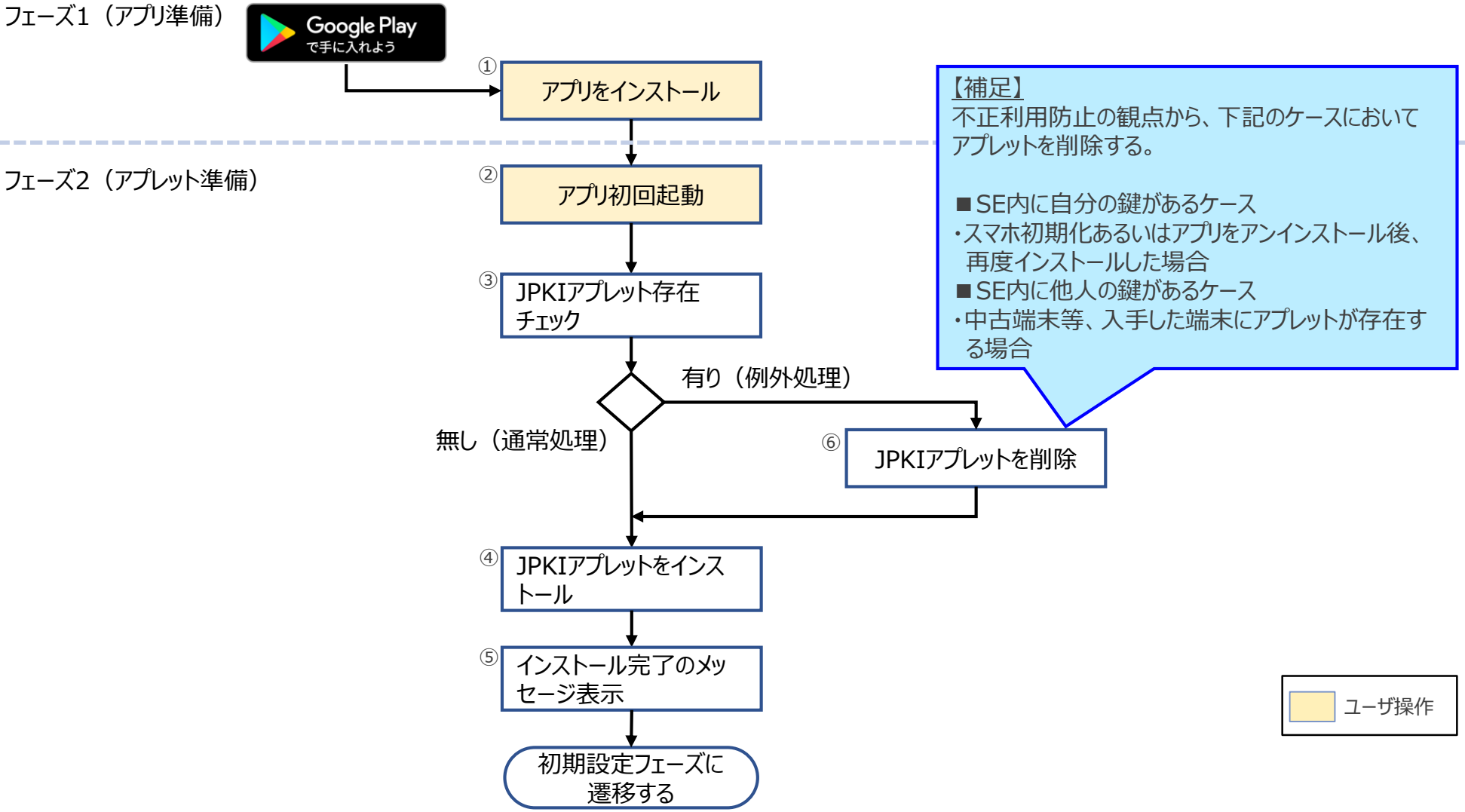
２．(１)アプレットライフサイクル（スマホJPKIが利用可能になるまでのフェーズ）

・アプリ、アプレット、鍵・証明書の有無によって４つのフェーズに分けられる。
・利用者はフェーズ1、2、3の準備を経て、サービス利用が可能となる。また、ライフサイクルに関連する処理に応じてフェーズ4から前にフェーズに戻ることがある。



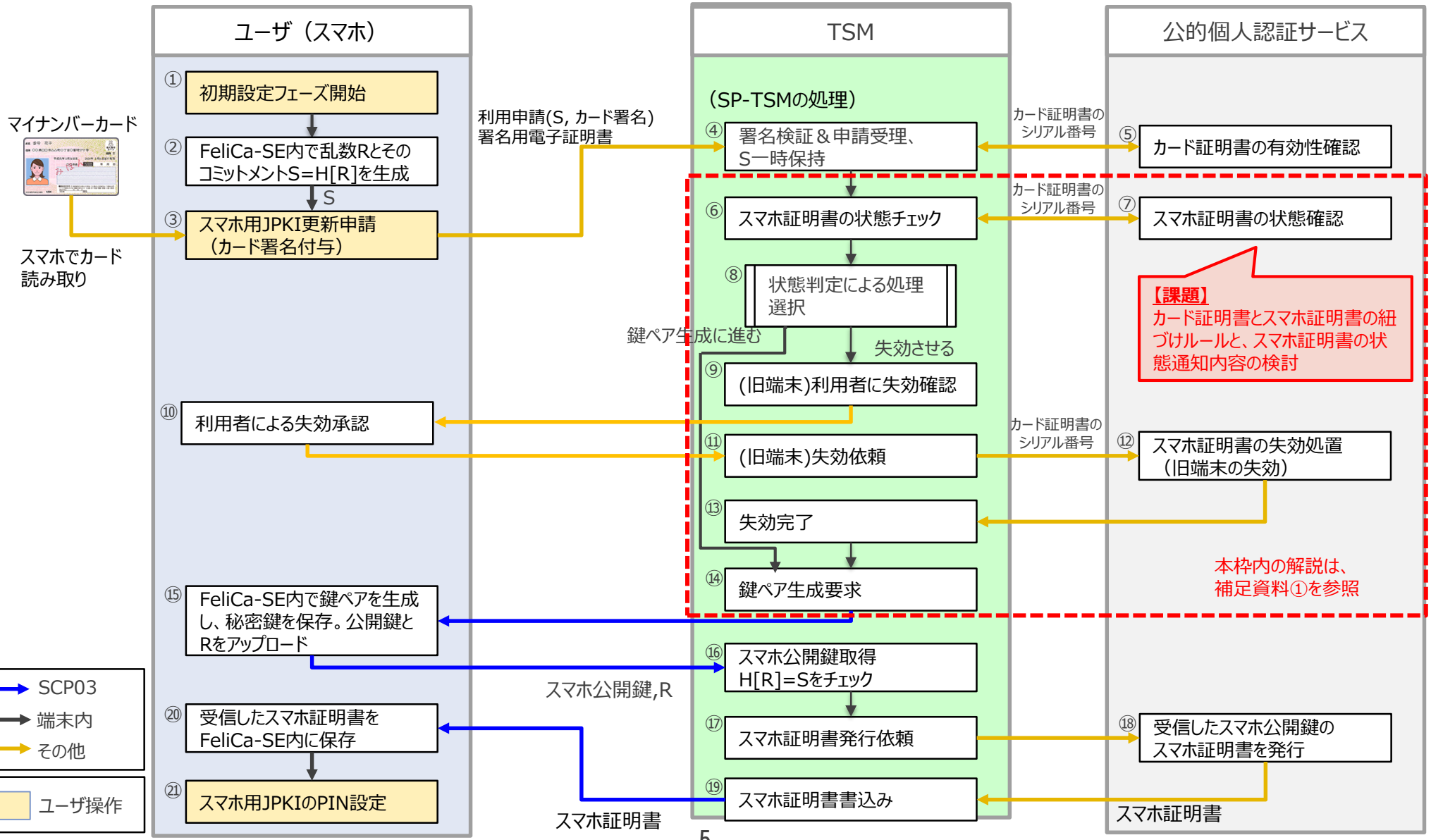
2．(2)フェーズ1（アプリ準備）、フェーズ2（アプレット準備）の処理フロー

・一連のライフサイクルを検討した結果を踏まえ、第1回検討会の資料4「初期発行フロー」の(1)事前準備の処理を以下のように見直す。



2．(3)フェーズ3（初期設定）の概略フロー

・第1回検討会で示した初期発行フローをベースとして、機種変更、紛失したケースに対応可能なフローを検討した。



３．(１)仮PINを用いたローカルPIN設定（PIN設定の前提とする考え方）

H28年度実証事業において、オンラインでのPIN設定方法が検討されており、その検討結果として推奨案とされた方法を採用する。

（基本方針）
・利用者が使うPIN情報はネットワーク上に流さない。スマートフォンのローカル処理でPINを設定する。

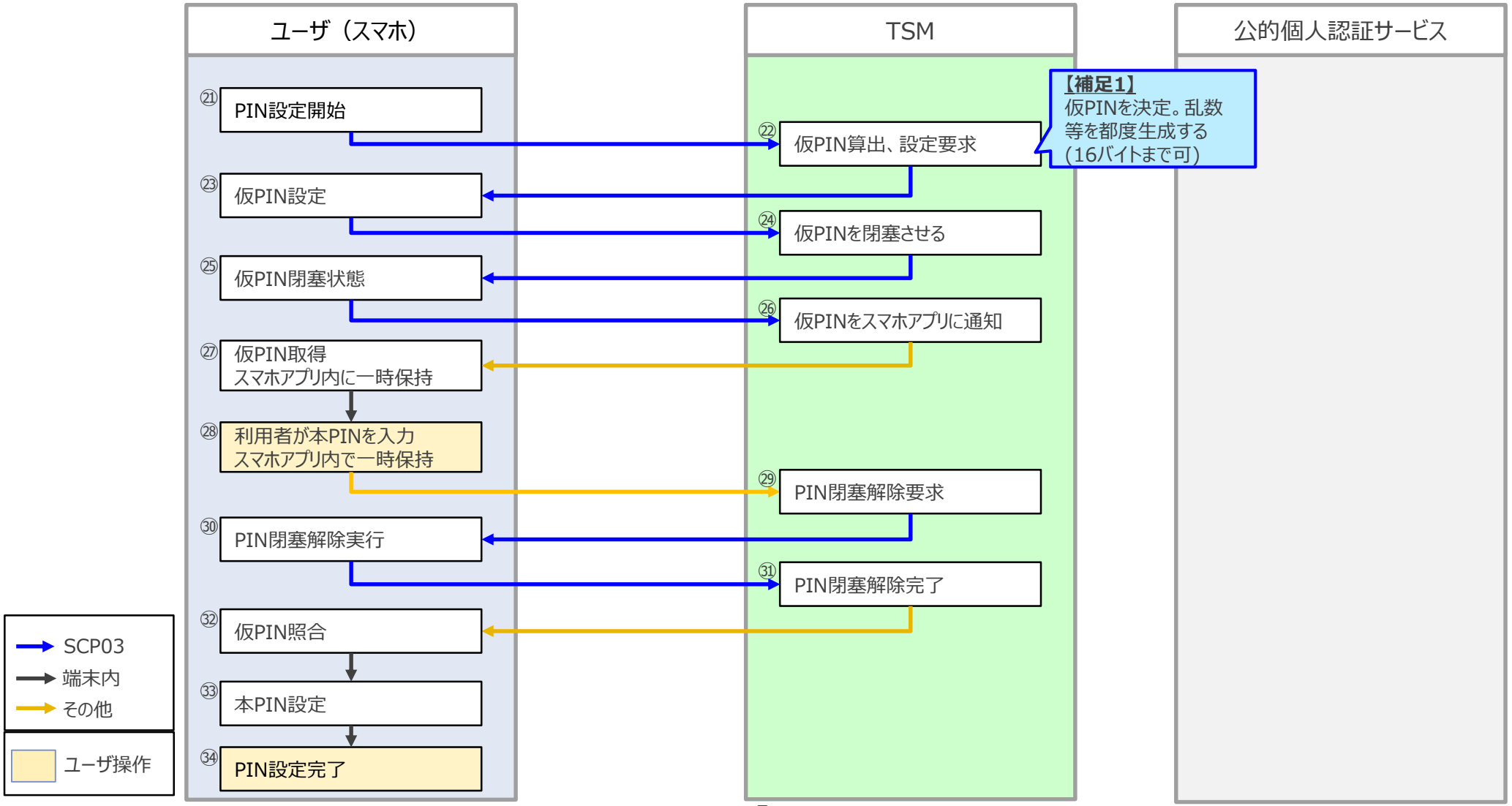
（前提）
①PINを設定する権限はTSMが有する。
②PIN設定の前にSEとTSMの間で認証処理を実施する。
③PIN照合がOKであれば、PIN変更が可能となる。

（今回検討したPIN設定方法の特徴）
①TSMからの要求でSE内に仮PIN（ワンタイムパスワード相当）を設定する。
②SEとTSMの間の認証処理は、SCPによって実施する。
③スマートフォンのローカル処理で仮PINの照合後、利用者が入力した本PINに変更する。

詳細は次頁参照。

3．(2)PIN設定の処理フロー

・H28年度実証の検討結果として推奨案とされた方法を採用した。
・初期設定フロー㉑から開始。初期設定フローの続きとして一連のセッションで実行することを想定（カード署名が有効のセッション）。
・仮PINはシステム内で使用するが、利用者は仮PINの存在を意識することはない。



4.(1)2つの鍵・証明書を格納するフロー(初期発行)

・新規利用の手続き時に、ユーザが2枚まとめて証明書を発行する場合について検討した。
・一度に2つの鍵・証明書を格納するか、利用者証明用または署名用のどちらか片方を格納するかユーザが選択可能な想定とする。

初期発行

※事前にJPKIスマホアプリのインストールを実施

マイナンバーカード

スマホでカード読み取り

【課題1】
・SEで生成する鍵の品質確認
・鍵生成処理性能

ユーザ（スマホ）	TSM	公的個人認証サービス
① JPKIスマホアプリを起動※		
② SE内で乱数R、コミットメントS=H(R)を生成		
③ スマホ用JPKI利用申請（カード署名付与）		
	（SP-TSMの処理）	
	④ 署名検証＆申請受理、S一時保持	⑤ カード証明書有効性確認、スマホ証明書紐付け、スマホ証明書有効性確認
	⑥ スマホ証明書の状態チェック、状態に応じて失効依頼	⑦ スマホ証明書の有効性確認、失効処理
⑨ SE内で利用者用の鍵ペアを生成し、秘密鍵を保存。公開鍵とRをアップロード	⑧ 利用者用の鍵ペア生成要求	
	⑩ 利用者用のスマホ公開鍵取得、H(R)=Sをチェック	
⑫ SE内で署名用の鍵ペアを生成し、秘密鍵を保存。	⑪ 署名用の鍵ペア生成要求	
	⑬ 署名用のスマホ公開鍵取得	
	⑭ スマホ証明書(利用者用)発行依頼	⑮ 受信したスマホ公開鍵のスマホ証明書を発行
	⑯ スマホ証明書(署名用)発行依頼	⑰ 受信したスマホ公開鍵のスマホ証明書を発行
⑲ 受信したスマホ証明書(利用者用)をSE内に保存	⑱ スマホ証明書(利用者用)書込み要求	
㉑ 受信したスマホ証明書(署名用)をSE内に保存	⑳ スマホ証明書(署名用)書込み要求	
㉒ スマホ用JPKIのPIN (利用者用、署名用)設定		

利用申請(S, MN署名)
署名用電子証明書

スマホ公開鍵(利用者用),R

スマホ公開鍵(署名用)

スマホ公開鍵(利用者用)

スマホ証明書(利用者用)

スマホ公開鍵(署名用)

スマホ証明書(署名用)

【補足1】
初期発行(証明書を1枚のみ書きこむ場合)の⑥-⑩に相当。

【課題2】
鍵生成を一度にまとめるかについて技術検証が必要。

【課題3】
フロー全体を通して、具体的な攻撃を想定したセキュリティ評価が必要

【課題4】
鍵の一意性チェック、カード-スマホ証明書間、スマホ利用者用-スマホ署名用間の証明書の紐づけ等についてJPKIシステムへの影響確認が必要

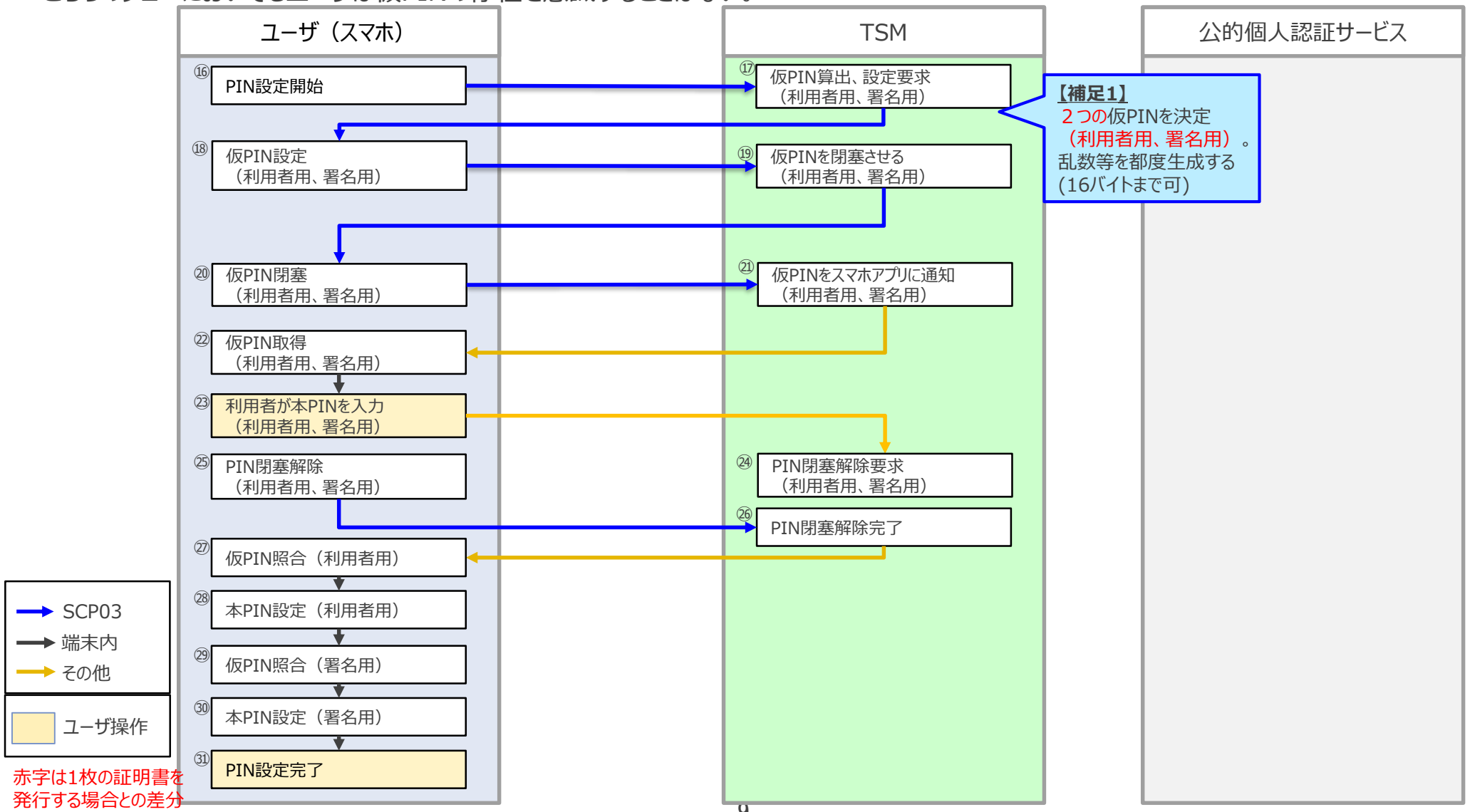
【補足2】
②-㉑が一気に完了しない場合、再度②からやり直す。

SCP03
端末内
その他
ユーザ操作

赤字は1枚の証明書を発行する場合との差分

4.(2)2つの鍵・証明書を格納するフロー(PIN設定)

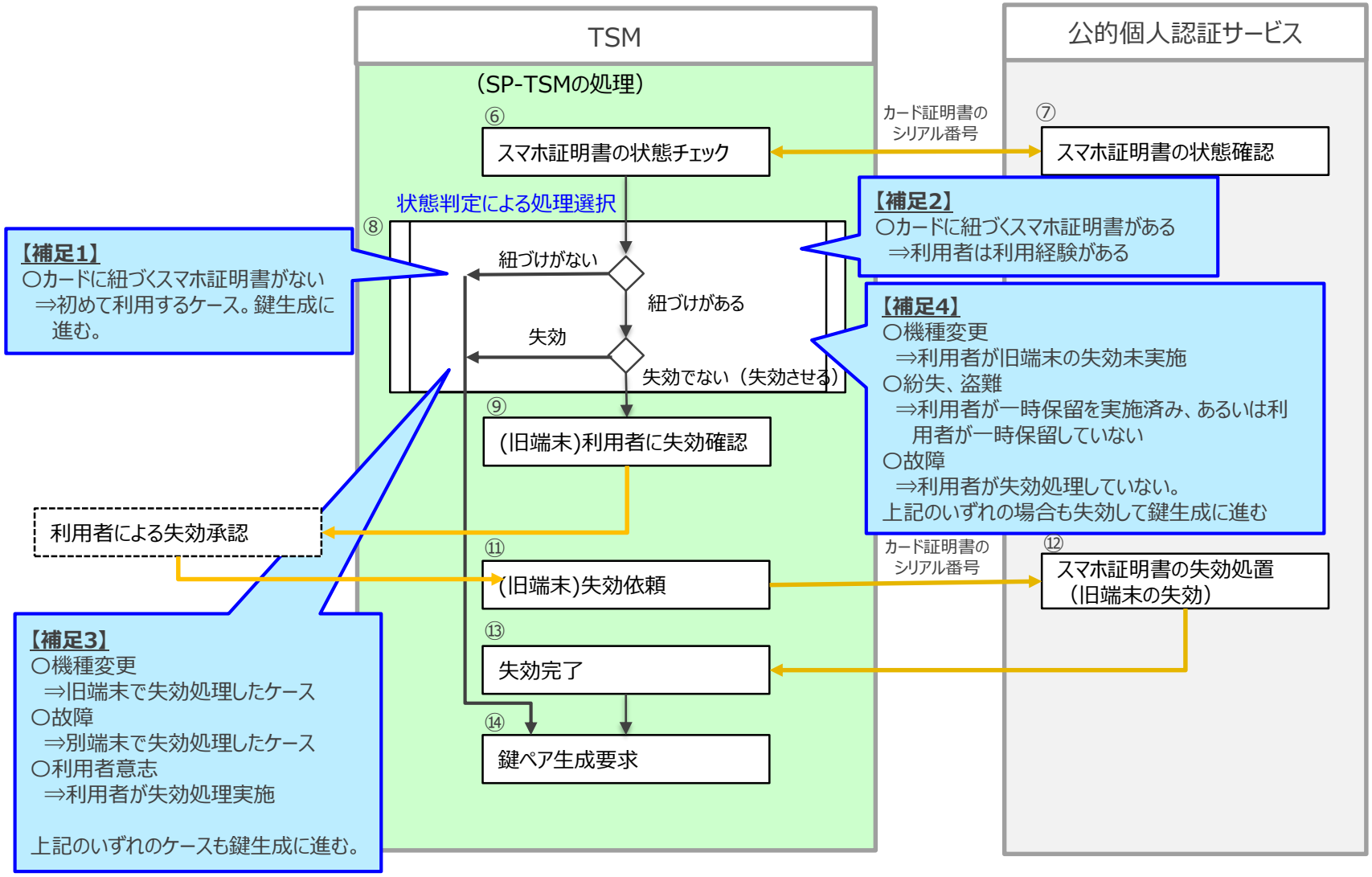
・2つの鍵証明書を格納するフロー(初期発行)の「㉒スマホ用JPKIのPIN (利用者用、署名用)設定」の詳細化を行った。
・1つの証明書を設定する場合と同様に、初期発行フローの続きとして一連のセッションで実行することを想定している。
・こちらのフローにおいてもユーザは仮PINの存在を意識することはない。



補足資料

【補足資料①】フェーズ3(初期設定)のスマホ証明書の状態チェックと処理の振り分け

・「フェーズ3(初期設定)の概略フロー」の赤枠部分について、スマートフォン特有のライフサイクルとの関係を解説する。



【参考】PIN設定における平成28年度実証での検討結果（検討結果）

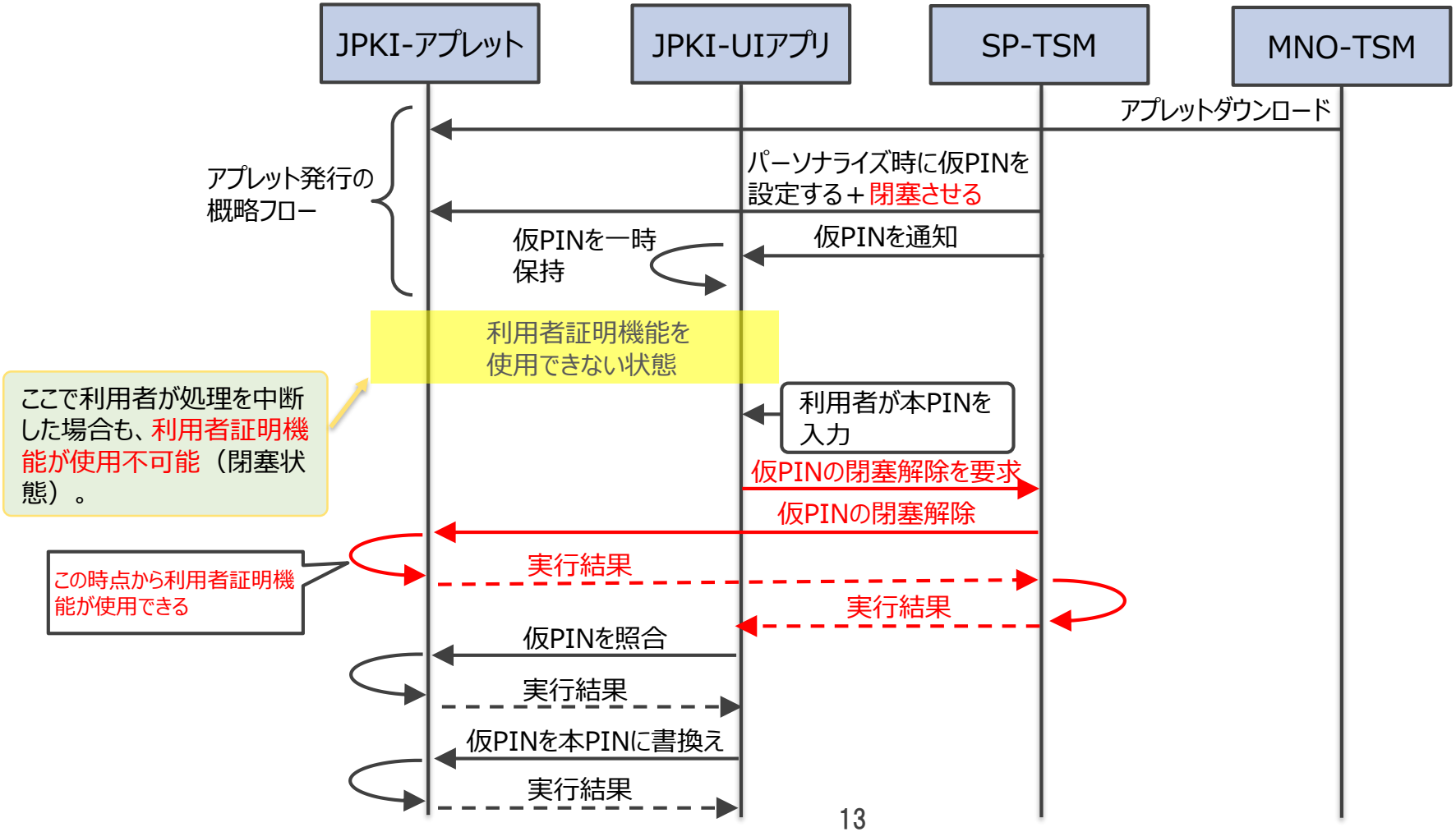
・平成28年度実証では「案3、案4を有力候補である」とするところまで検討。（決定は実用化時）

項番	概要	メリット・デメリット	安全性	利便性	コスト
案1	利用者に仮PINを入力させる方法	×利用者の手間が増える（仮PIN入力） ×仮PIN状態で利用可能 ×仮PINの誤入力の可能性	×	×	○
案2	UIアプリが仮PINを自動入力する方法（ダウンロード後に本PIN入力）	○利用者が仮PINの入力不要 △仮PIN状態で利用可能 ○仮PINの誤入力はない。	△	○	○
案3	案2において、仮PINの閉塞状態の対策を追加した方法	○利用者が仮PINの入力不要 ○仮PIN状態で利用不可（閉塞状態） ○仮PINの誤入力はない。 △SP-TSMの機能追加が必要	◎	○	△
案4	PINの特別な状態遷移を組み入れた方法	○利用者が仮PINの入力不要 ○本PIN設定まで利用不可 ○仮PINの誤入力はない。 △SP-TSMの機能追加が必要 △アプレットの機能追加が必要	◎	○	△
案5	UIアプリが仮PINを自動入力する方法（ダウンロード申請時に本PIN入力）	○利用者が仮PINの入力不要 ○仮PIN状態の期間が極めて短い(正常シーケンスの場合) ○仮PINの誤入力はない。 ○SP-TSMの負担小 ×本PINをアプレット発行中もスマホ端末内で保持する	×	○	○
案6	PUK（PIN unlock Key）によって利用者にPIN設定を可能にする方法	×利用者の手間が増える（PUK入力） ○仮PIN状態で利用不可（閉塞状態） ○仮PINの誤入力はない。 ○SP-TSMの負担小 △PUKの通知／再確認手段が必要 △利用者がPUKを安全に保管する必要がある	○	×	○

【補足】
利用者が仮PINを決定し、申請時に申請させる方法も考えられるが、アクセスコード用のパスワードとの混同などの分かり難さ、仮PINの忘失の可能性など、デメリットが大きいので、ここでは記載しないこととした。

【参考】案3：案2において、仮PINの閉塞状態の対策を追加した方法 H28報告書

【概要】
・案2において、仮PINが設定されている間はPINを閉塞状態とさせる。
・本PINへの変更の直前で、閉塞状態を解除（SP-TSMとJPKI-アプレット間でのコマンド交換を実施）する。
【補足】
－SP-TSMが設定する仮PINの値は、案2と同様。
－SP-TSM側で閉塞解除のための処理機能が必要となる。



【参考】案4：PINの特別な状態遷移を組み入れた方法

H28報告書

【概要】
・案2において、ダウンロード時点でのアプレット内のPINを使用不可状態（初期状態）とする。
・本PINの設定直前で、PINの状態を遷移させる（SP-TSMとJPKI-アプレット間でのコマンド交換を実施）する。
【補足】
－SP-TSMに、PINの状態を遷移させるための処理機能が必要となる。（※1）
－JPKI-アプレットに、PINが初期状態のときのみPIN設定が実行できる機能が必要となる。（※2）