資料4

スマートフォン特有のライフサイクルへの対応（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2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】

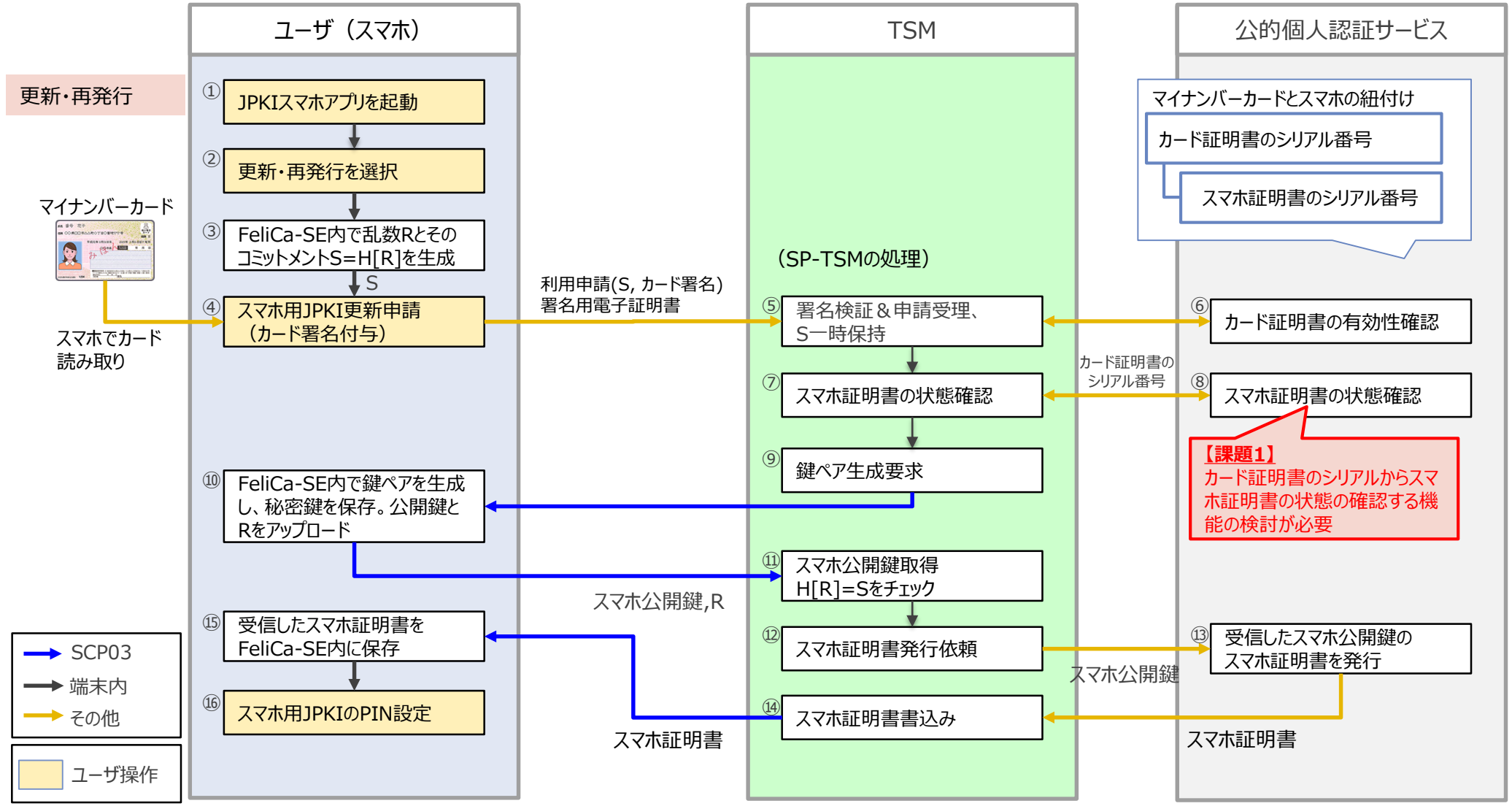
2．(1)電子証明書に関する業務

第1回検討会で未検討の業務について検討した。

項番	業務	説明	第1回検討会	第2回検討会	補足
1	発行	新しい電子証明書を発行する。	○	－	
2	失効	有効な電子証明書を失効させる。	○	－	スマートフォン特有のライフサイクルのうち、故障、紛失、譲渡など、失効処理が必要なケースがある。
3	更新	電子証明書の有効期限が切れる前に、新しい電子証明書を発行する。	○	○ （再発行と統合）	更新および再発行は類似する処理であるため統合する。
4	再発行	電子証明書の有効期限が切れたor失効した場合に、新しい電子証明書を発行する。	－	○	
5	一時保留／ 一時保留解除	電子証明書の利用を一時保留するor 電子証明書の一時保留態を解除する。	－	－	継続検討中。
6	PINの初期化	電子証明書のPINを初期化する。	－	○	PIN閉塞時に実施する閉塞解除および新しいPINを設定する。 オンラインでの初期化を検討中。
7	PINの変更	電子証明書のPINを変更する。	－	○	PIN照合後にPIN変更ができる。

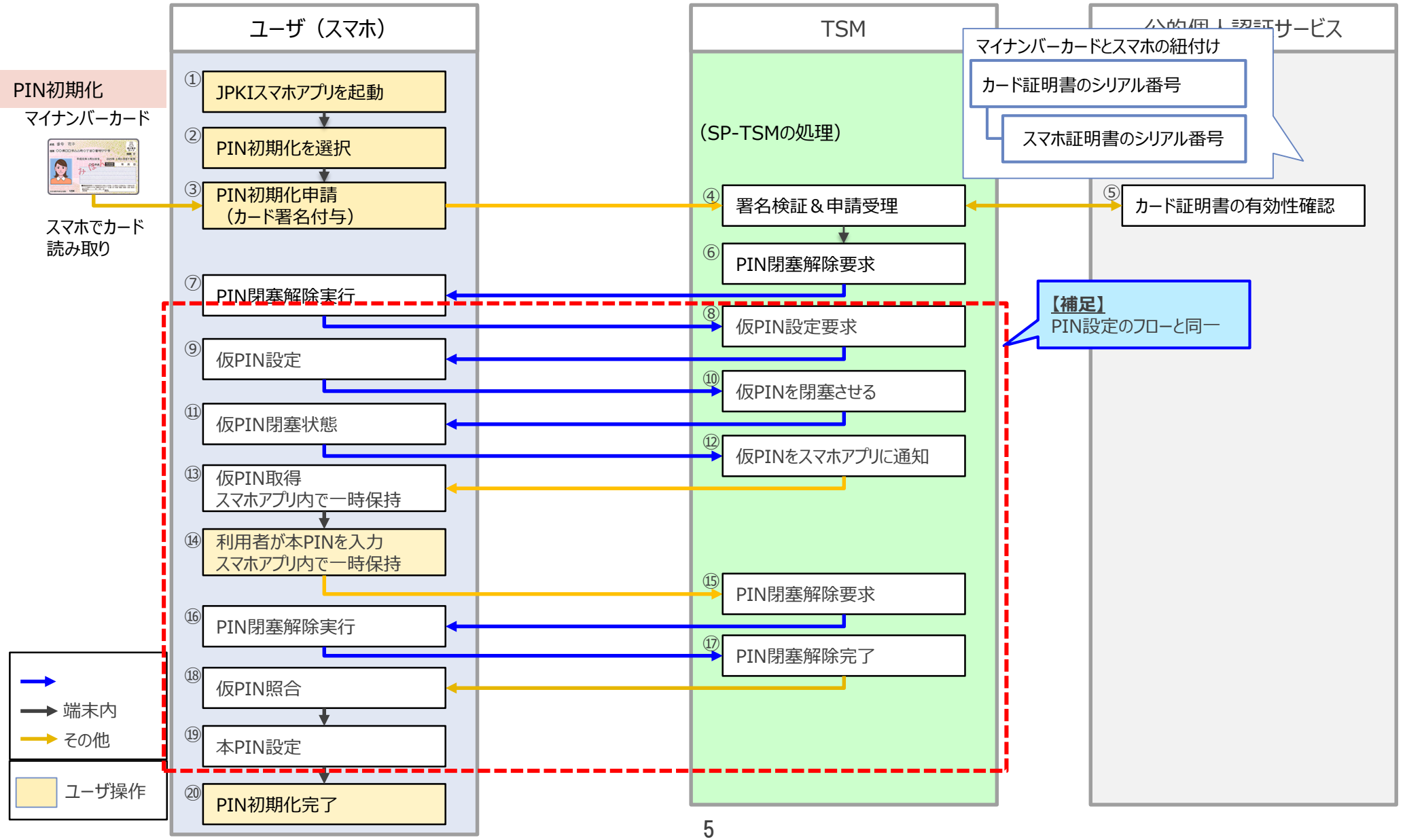
2．(2)更新・再発行の概略フロー

カードの証明書の更新処理あるいは再発行処理が実施されているものとする（連動失効により、スマホ証明書は失効する）。
カード証明書の更新、再発行を行わずに本処理が実行されることを避けるため、SP-TSMでスマホ証明書の状態確認を行う。



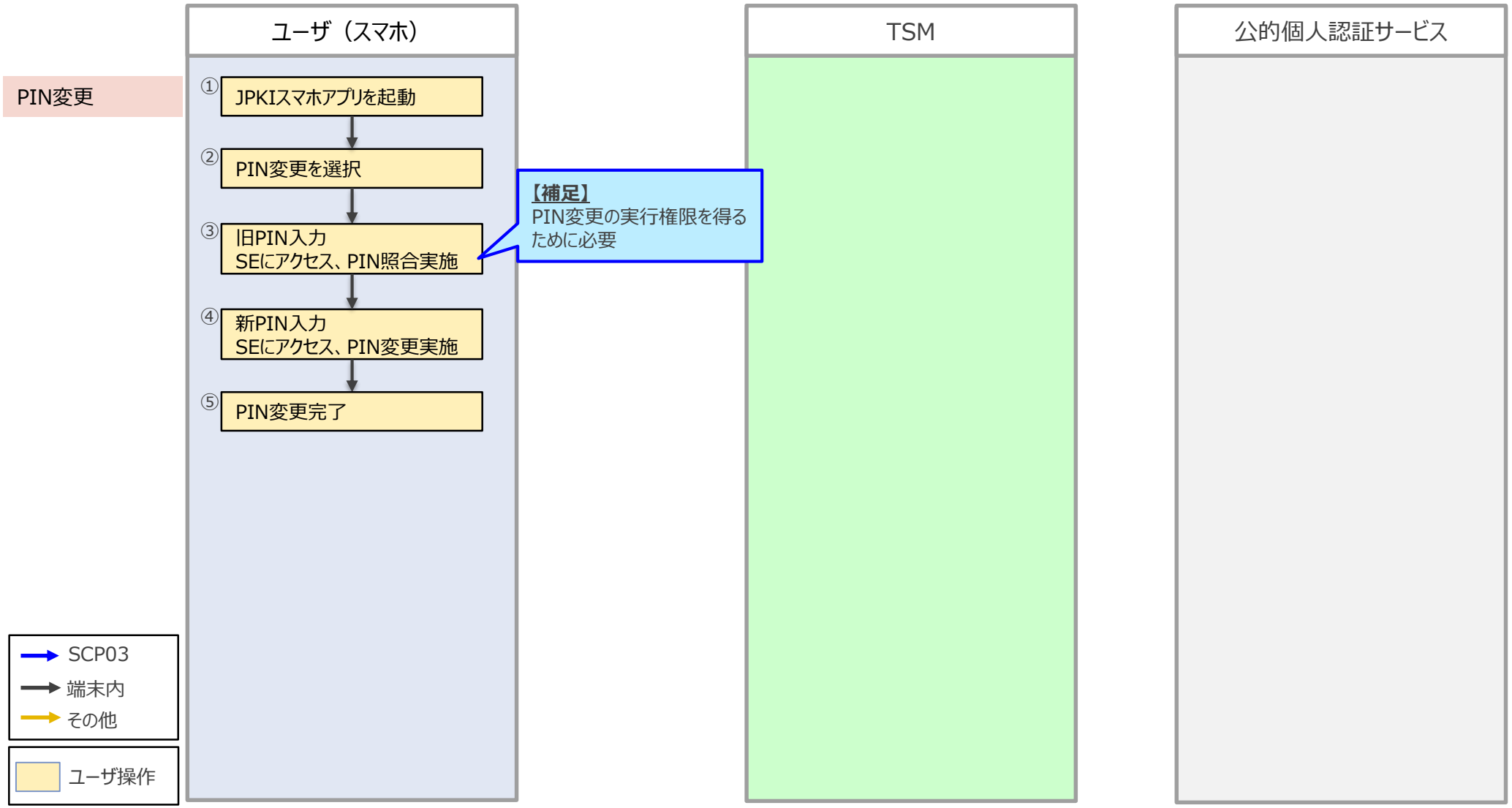
2．(3)PIN初期化の概略フロー

カードの署名検証（本人確認）によってPIN初期化が実行できるものとする（オンラインで実施可能）。



2．(4)PIN変更の概略フロー

カードの場合はPIN変更を統合端末でも実施可能としているが、スマホJPKIでは利用者のスマホ操作で完結させることが可能。



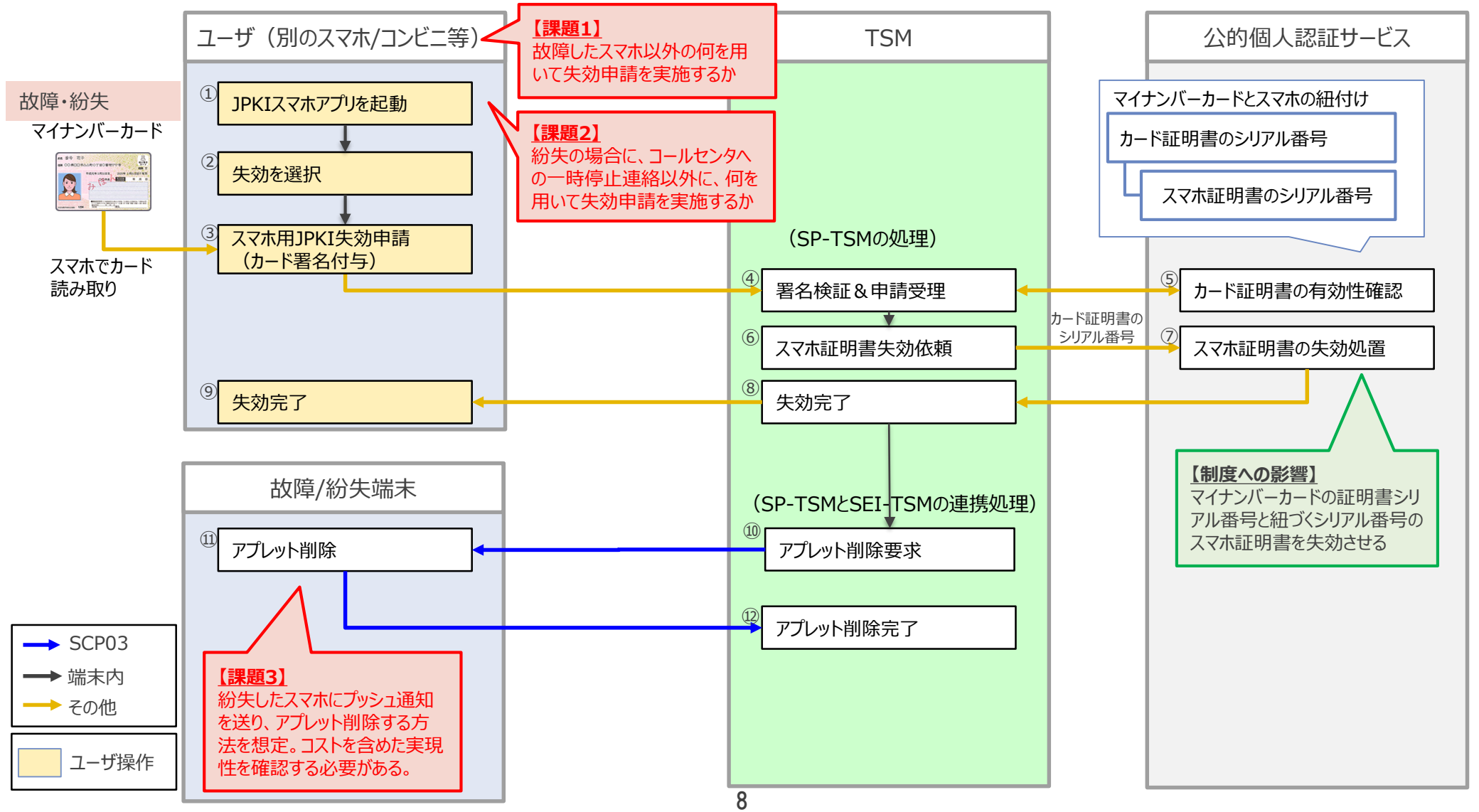
3．(1)スマートフォン特有のライフサイクル

第1回検討会で未検討の業務について検討した。

項番	業務		説明	第1回検討会	第2回検討会	電子証明書の業務との関係
1	機種変更	機種変更（Android→Android）	・新しいスマートフォンへ機種を変更する(同機種含む)。	○	－	旧端末（機種変更前）のスマホ証明書を失効させて、新端末（機種変更後）に新たなスマホ証明書を発行する。
2		機種変更（Android→iOS）	・AndroidスマートフォンからiOSスマートフォンへ機種を変更する。			
3		MNP（MNO変更）	・キャリア変更(MNO間)に伴い、新しいスマートフォンへ変更する。			
4		MNP（MNO⇔MVNO変更）	・キャリア変更(MNO⇔MVNO間)に伴い、新しいスマートフォンへ変更する。			
5	故障		・スマートフォンが故障する。	－	○	故障、紛失した端末のスマホ証明書を失効させる必要がある。別端末での失効方法を検討
6	紛失		・スマートフォンを紛失する。（紛失し、見つからない場合）			
7	一時紛失		・スマートフォンを紛失する。（一時的に紛失）	－	－	スマホ証明書を一時保留とする対応が必要。（継続検討中）
8	譲渡	転売	・スマートフォン解約後、中古業者等を通して第三者に譲渡する。	○	－	譲渡する端末のスマホ証明書を失効させる必要がある。
9		個人間譲渡	・スマートフォン解約後、個人間で第三者に譲渡する。			
10	現行端末の継続利用	SIMロック解除（MNO変更）	・キャリア変更(MNO間)に伴い、SIMロックを解除する。	－	－	スマホ証明書に関する対応なし。
11		SIMロック解除（MNO⇔MVNO変更）	・キャリア変更(MNO⇔MVNO間)に伴い、SIMロックを解除する。	－	－	スマホ証明書に関する対応なし。
12		SIMロック解除せず、同系列のMVNOのSIMを挿入	・ MNO⇒MVNO変更に伴い、SIMロックは解除せず、同系列のMVNOのSIMを挿入する。	－	－	スマホ証明書に関する対応なし。
13		WiFi使用	・解約した端末や機種変更した旧端末等(WiFi使用)で、電子証明書を引き続き利用する場合。	－	－	スマホ証明書に関する対応なし。
14		利用中断／再開(リモートロック)	・紛失や盗難等により、利用者の申請によってスマートフォンの機能を一時停止状態にする。	－	－	スマホ証明書に関する対応なし。
15	破棄		・スマートフォンを破棄する。	－	○	破棄する端末のスマホ証明書を失効させる必要がある。

3．(2)故障・紛失の概略フロー(スマートフォンが利用できない場合)

別のスマホ、コンビニ等の端末を用いて、カードの署名（本人確認）でスマホ証明書の失効を行うことを基本とする。
スマホの署名でスマホ証明書を失効させるかどうかは、スマホに署名用証明書を搭載するか否かを整理した上で検討。
スマホの転売・譲渡によって、他人に鍵および証明書が渡るリスクが存在することから、失効時にアプレット削除の実施を想定。



3．(3)破棄の概略フロー　※失効と同じフロー

利用中のスマホを用いて、カードの署名（本人確認）でスマホ証明書の失効を行うことを基本とする。
スマホの署名でスマホ証明書を失効させるかどうかは、スマホに署名用証明書を搭載するか否かを整理した上で検討。
スマホの拾得等によって、他人に鍵および証明書が渡るリスクが存在することから、失効時にアプレットの削除を行うものとする。