

スマートフォン特有のライフサイクルへの対応

2020年11月10日

1. 電子証明書に関する業務

電子証明書に関する業務は以下に分類される（2019年度実証検討結果）。
今回の検討では、「発行」（資料4で検討）、「失効」、「更新」の業務フローを検討した。

項番	業務	説明	第一回検討会	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。	○	カード証明書の更新を前提とする。カード証明書の更新と連動してスマホ証明書は失効状態となる。
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。	—	スマホ証明書の失効には、スマートフォンの故障、紛失、譲渡等が発生したことが想定される。
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。	—	紛失、盗難の場合に、コールセンタに連絡し、不正利用を防止する。
6	PINの初期化	電子証明書のPINを初期化する。	—	PINロックが発生した場合に初期化が必要。オンラインでの初期化を検討
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. スマートフォン特有のライフサイクル

スマートフォン特有のライフサイクルの一覧を示す（2019年度実証検討結果）。
 第一回検討会では失効、更新等多くのライフサイクルと関連する「機種変更」「譲渡」を対象とする。

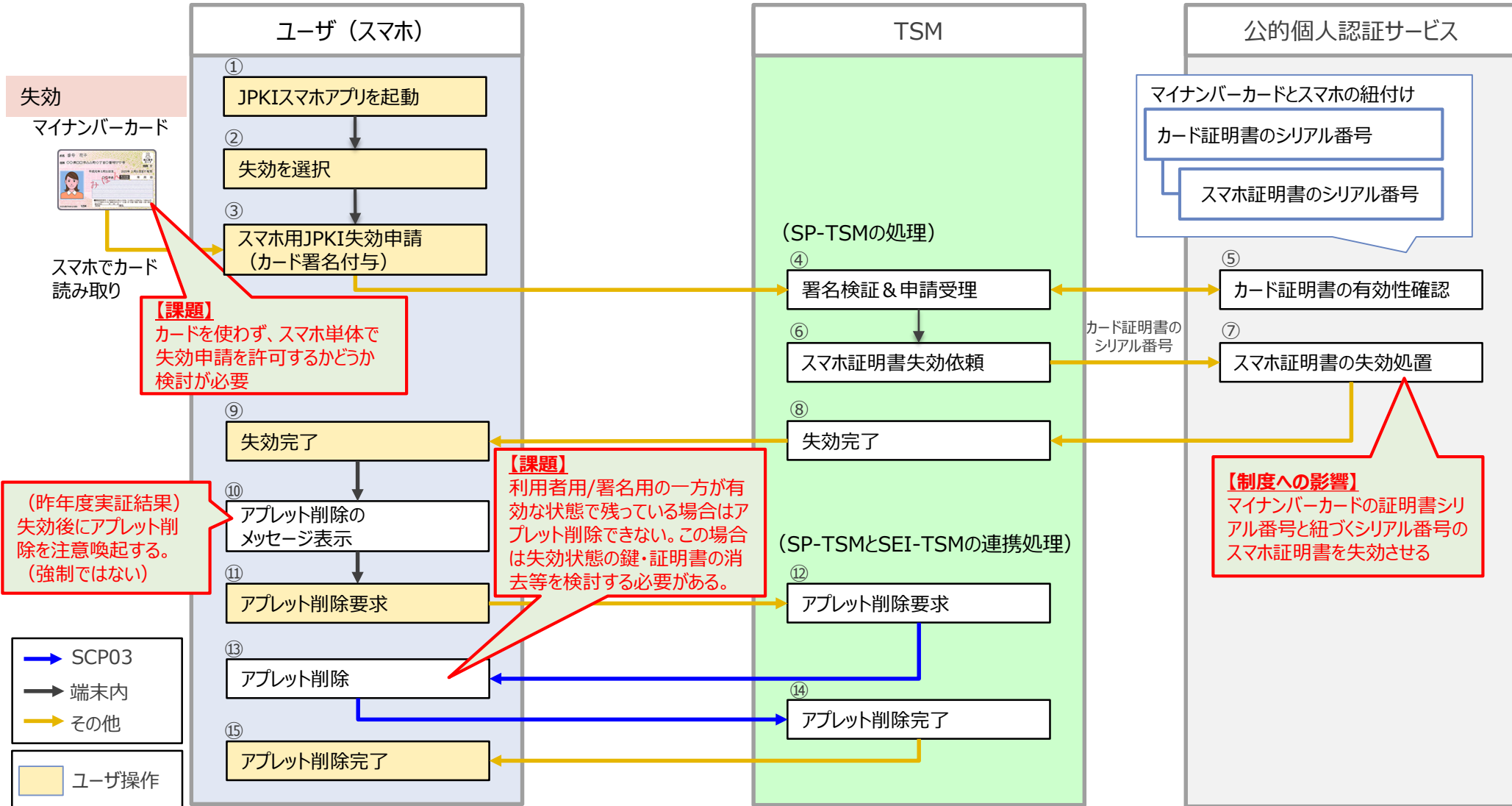
項番	業務		説明	第一回検討	電子証明書の業務との関係
1	機種変更	機種変更 (Android→Android)	・新しいスマートフォンへ機種を変更する(同機種含む)。	○	旧端末（機種変更前）のスマホ証明書を失効させて、新端末（機種変更後）に新たなスマホ証明書を発行する。
2		機種変更 (Android→iOS)	・AndroidスマートフォンからiOSスマートフォンへ機種を変更する。		
3		MNP（MNO変更）	・キャリア変更(MNO間)に伴い、新しいスマートフォンへ変更する。		
4		MNP（MNO⇔MVNO変更）	・キャリア変更(MNO⇔MVNO間)に伴い、新しいスマートフォンへ変更する。		
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別途検討
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）	—	スマホ証明書を一時保留とする対応が必要。
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。
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. 失効の概略フロー

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り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。



失効

マイナンバーカード



スマホでカード読み取り

【課題】
カードを使わず、スマホ単体で失効申請を許可するかどうか検討が必要

(昨年度実証結果) 失効後にアプレット削除を注意喚起する。(強制ではない)

【課題】
利用者用/署名用の一方が有効な状態で残っている場合はアプレット削除できない。この場合は失効状態の鍵・証明書の消去等を検討する必要がある。

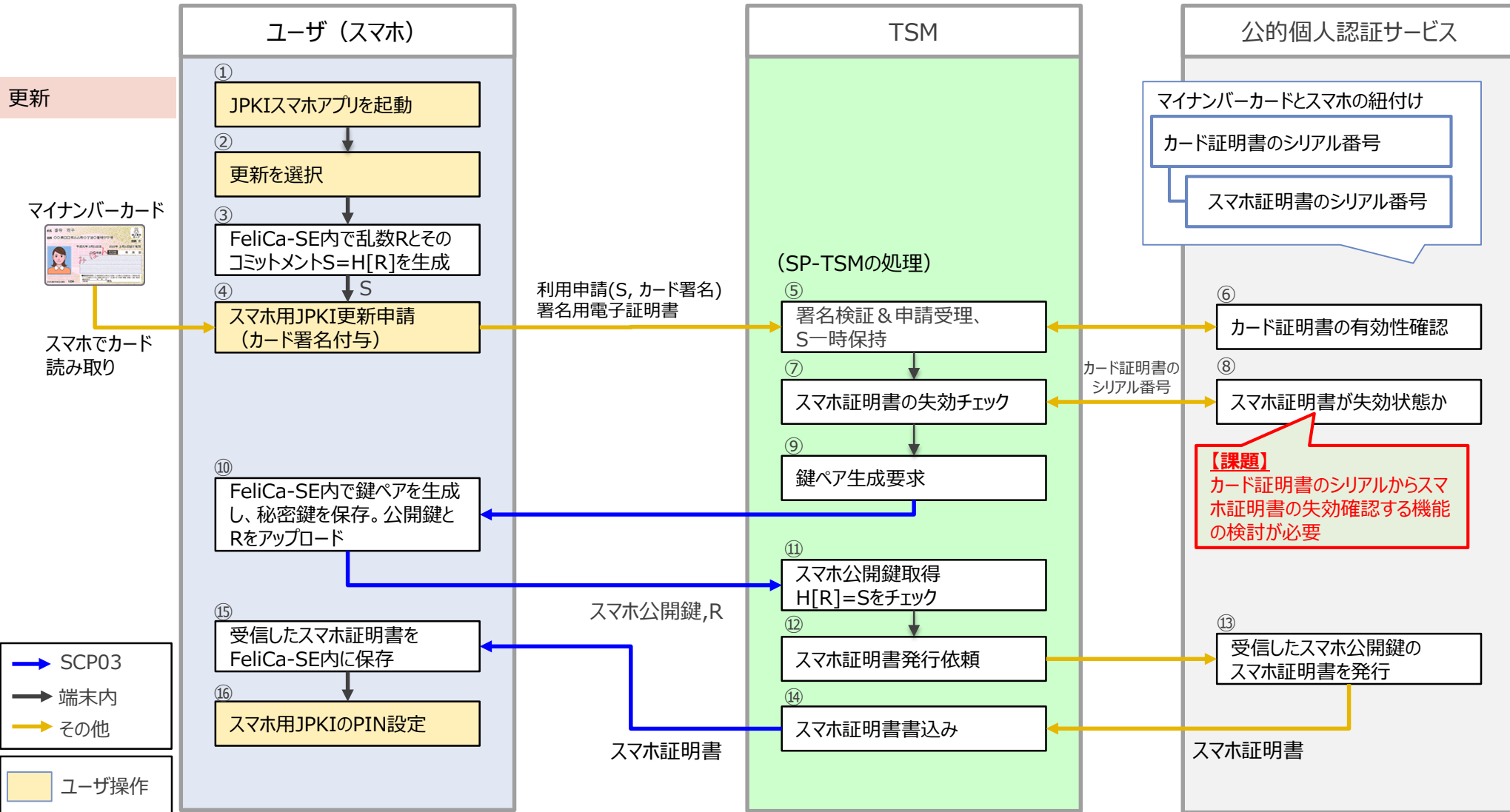
【制度への影響】
マイナンバーカードの証明書シリアル番号と紐づくシリアル番号のスマホ証明書を失効させる

→ SCP03
→ 端末内
→ その他

■ ユーザ操作

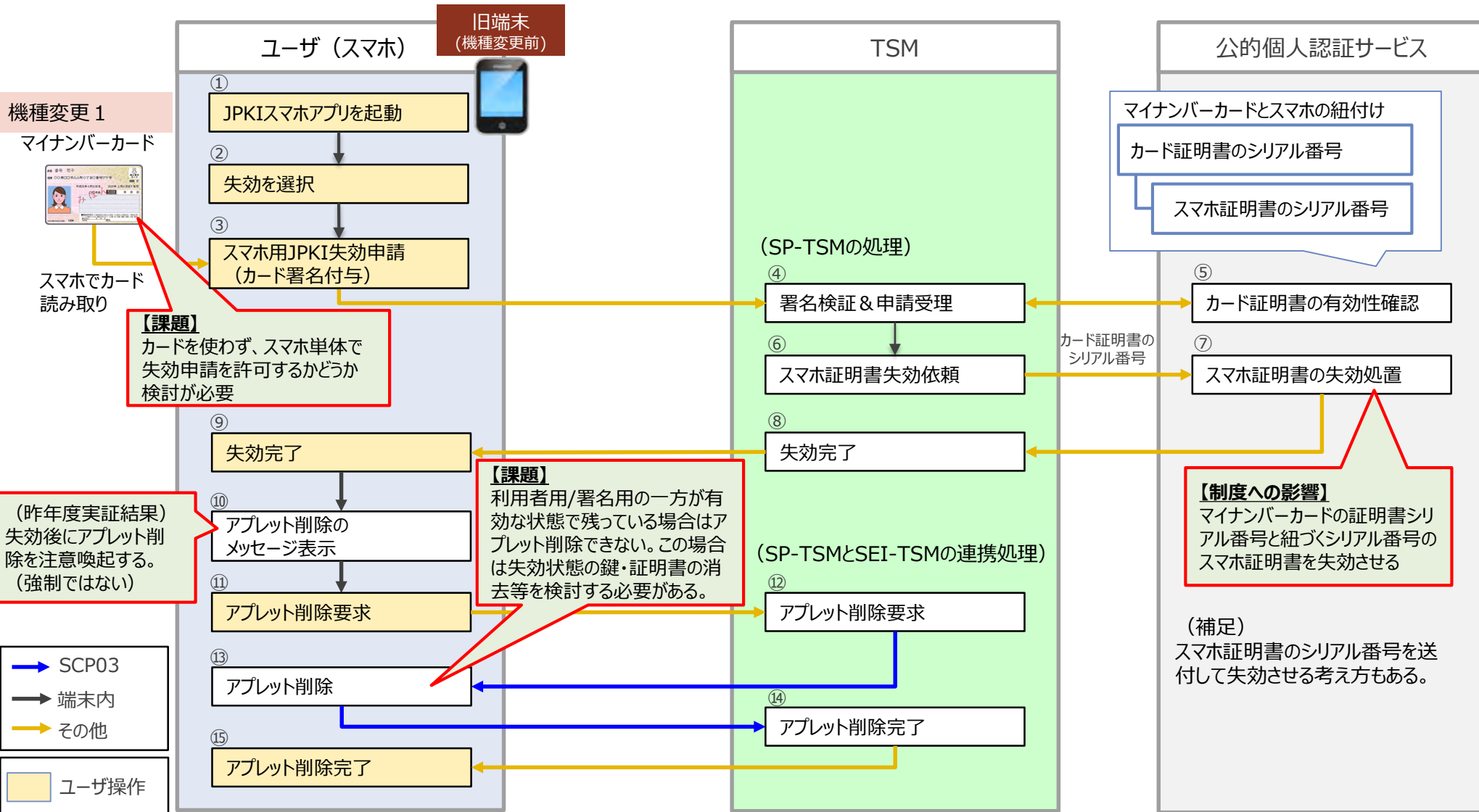
4. 更新の概略フロー

カードの証明書の更新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している）。
 ただし、カード証明書の更新を行わずに本処理が試行されることも想定し、SP-TSMでスマホ証明書の失効チェックを行う。



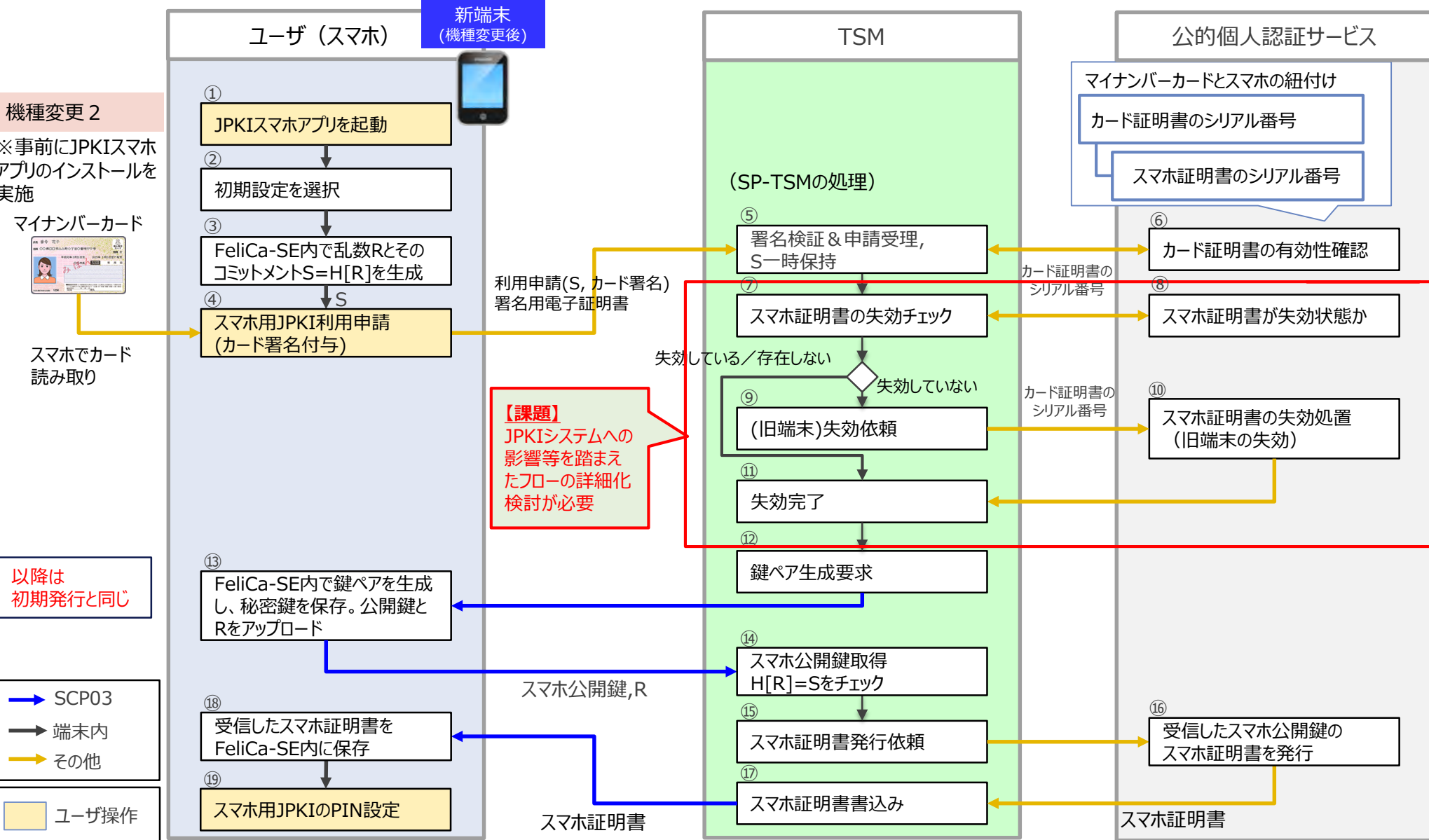
5-1. 機種変更の概略フロー 1 旧端末での処理 ※失効と同じフロー

機種変更時、利用者は旧端末（機種変更前）で失効処理を実施することを原則とする。
 スマホの転売・譲渡によって、他人に鍵および証明書が渡り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。



5-2. 機種変更の概略フロー 2 新端末での処理

利用者が旧端末（機種変更前）で失効処理を実施しないことを想定されるため、未失効の場合は失効を実施。



6. 譲渡の概略フロー（該当端末の失効処理） ※失効と同じフロー

端末を譲渡する場合、利用者は該当端末に対して失効処理を実施することを原則とする。
 利用者が失効処理を実施しないまま譲渡した場合、FeliCa-SE内にスマホ鍵および証明書が記録されたまま第三者に端末が渡ることになる。
 このため「新しい所有者が新規に鍵および証明書を設定できること」「前の所有者の鍵および証明書が悪用されないこと」の検討が必要となる。
 (検討課題)

