PIN初期化の概略フローの修正

第2回検討会の指摘事項

PINの初期化について、今回のフローだと他人のスマートフォンのPINを初期化できてしまう恐れがある。

【検討結果】

ご指摘の通り、他人のスマートフォンのPINを初期化できてしまう問題がありました。この問題を解決するため、初期発行時に利用者のスマートフォンのSEを識別するIDを、JPKIシステム側にマイナンバーカードと紐づける形で登録しておき、PIN初期化時には使用しているスマートフォンのSEを識別するIDとJPKIシステム側で登録されているSEを識別するIDを比較チェックし、両者が一致するときのみPIN初期化を実行することとします。

次頁に修正したPIN初期化の概略フローを示します。なお、以降では<u>SEを識別するID</u>をSE識別IDと呼ぶこととします。SE識別IDとしては、SEID(注1)あるいは初期発行時にSP-TSMが付番する一意なID等が想定されますが、今後の設計フェーズ等で最適なIDを選定することとします。

(注1) SEIDはフェリカネットワークス社が付与するSEを一意に識別するID

PIN初期化の概略フロー(修正)

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)。 公的個人認証サービス ユーザ (スマホ) **TSM** (SP-TSMの処理) 利用申請(カード署名) PIN初期化 カード証明書の JPKIスマホアプリを起動 署名用電子証明書 シリアル番号 署名検証&申請受理 カード証明書の有効性確認 マイナンバーカード PIN初期化を選択 A 15-1 【補足】 SE識別IDをチェックすること PIN初期化申請 で他人のスマホによるPIN初 (カード署名付与) スマホでカード 期化を防止。 読み取り SE識別ID読出し要求 SE識別ID読出し実行 カード証明書の シリアル番号 スマホ証明書の状態確認 利用者のSEかどうかをチェック PIN閉塞解除実行 PIN閉塞解除要求 【補足】 マイナンバーカードとスマホの紐付け PIN設定のフロー 仮PIN設定 仮PIN設定要求 と同一 カード証明書のシリアル番号 仮PIN閉塞状態 仮PIN閉塞要求 スマホ証明書のシリアル番号 仮PIN取得&一時保持 仮PINをスマホアプリに通知 SF識別ID カードに紐づけて、初期発行時に ® 利用者が本PINを入力 鍵ペア生成を実行したSEのSE識 &一時保持 別IDを保持する。 PIN閉塞解除実行 PIN閉塞解除要求 → SCP03 仮PIN照合 → 端末内 **→** その他 ② 本PIN設定 ユーザ操作 PIN初期化完了