資料3

技術検証の在り方

2021年3月3日

技術検証概要

技術検証はマイナンバーカードの機能のスマートフォン搭載に向け、実現性・性能・セキュリティ・利便性・運用性の5つの観点においてこれまでの検討会で課題として抽出された項目の技術検証や実機での確認を行う。なお、システム構築開始に向けたスケジュールを考慮して2つのフェーズで実施する。

① スケジュール

#	項目	令和3年度	令和4年度	令和5年度
1	技術検証	フェーズ1	フェーズ2	
2	システム設計・構築・運用	システム設計	システム構築	スマホ搭載の実現 (システム運用)

② 検証概要

#	検証観点	検証目的	具体的な検証項目	フェーズ1	フェーズ2
1	実現性	これまでの検討結果を実機で検証することによる実現性確認、および課題抽出	・発行、更新等の各フローの実機確認による実現見込の確保 ・実機または実機相当での検証が必要な項目 例）生体認証とGP-SEの連動、SE内の鍵のリモート消去	●	-
2	性能	実機を用いた処理時間計測等による性能確認	・実機での性能確認が必要な項目、製品差が想定される項目 例）GP-SE内の鍵生成処理時間、利用時の処理時間	●	-
3	セキュリティ	フロー全体の安全性および、認証用乱数品質の評価による安全性確認	・技術的な安全性を確認するための評価項目 例）スマホで生成した鍵の品質評価、フローの第三者評価	●	-
4	利便性	スマホならではの使い方やユースケースを踏まえた利便性やUXの確認	・動作における利用時の利便性について検証が必要な項目 例）処理中の通信断/継続、UXに関する実証および評価	●	●
5	運用性	AndroidスマホやGP-SEのライフサイクルを踏まえた運用性の確認	・各種ライフサイクルやユーザサポート観点から確認が必要な項目 例）AndroidOSアップデート	●	●

検証観点毎の検証項目 （観点1）

各検証観点において以下の内容を必須項目として技術検証を行う。
製品や個体差が想定される項目についてはバリエーションの評価も実施する。

検証観点	No	中分類	検証/検討概要	JPKI アプレット	JPKI アプリ	TSM	JPKI システム
観点1. 実現性	1-1	フロー全体の確認	・発行、失効、更新、再発行等を実機で動作させることによるフロー全体の実現性確認	●	●	●	●
	1-2	TSM/Android	・SafetyNet Attestation APIを用いたAndroidデバイスの不正利用検出方法の検証		●	●	
	1-3	生体認証とGP-SEの連動	・CryptoObject, BiometricPromptを用いたAndroid(9 or 10~)の生体認証とGP-SEの連携	●	●	●	
	1-4		・特定機種による生体認証を利用制限および識別する方法の検証	●	●	●	
	1-5	GP-SE	・GP仕様上のアプレット上限サイズである64KB以下でのJPKIアプレット実装見込みの確認	●			
	1-6		・GP-SEに対する要求発出元(アプリ/NFC)の識別	●			
	1-7		・GP-SE内の鍵のリモート消去方法の検証	●	●	●	
	1-8	その他	・スマホをカードリーダにかざし利用可能なこと	●			
	1-9		・APK署名、アプリ証明書のハッシュ値リスト等を用いた非正規アプリケーション検出確認	●	●		
	1-10		・ファクトリリセット等実施時のGP-SE内データ消去に関する検討	●	●	●	

検証観点毎の検証項目 （観点2~5）

検証観点	No	中分類	検証/検討概要	JPKI アプレット	JPKI アプリ	TSM	JPKI システム
観点2. 性能	2-1	処理時間	・GP-SE内鍵生成、署名等処理時間の評価	●			
	2-2		・発行および利用シーンにおけるターンアラウンドタイムの評価	●	●	●	●
観点3. セキュリティ	3-1	鍵・乱数品質	・GP-SEにおいて鍵生成等に用いる乱数の品質の確認	●			
	3-2	安全性評価	・発行、失効等の各フローにおける攻撃可能性、対策に関する検討、および第三者評価	●	●	●	●
	3-3		・GP-SE, アプレットの安全性評価スキームの整理	●	●	●	●
観点4. 利便性	4-1	ユーザテスト	・スマホからのマイナポータル等ログインによるUX確認	●	●		
	4-2		・フィールド実証によるUX検証、ユーザ評価	●	●	●	●
	4-3	個別検証	・処理中の通信断/継続性に関する検証	●	●	●	
観点5. 運用性	5-1	アップデート	・Android OSやCDD*1 バージョンアップ時の運用検討、課題抽出	●	●		
	5-2		・GP-SEのOSアップデート、新製品に関する運用の整理	●	●		

*1: Android Compatibility Definition Document