資料2

各段階における攻撃可能性と対策案の事前検証について

2021年3月3日

攻撃可能性と対策案についての事前検証概要

これまでに検討してきた各業務のフローにおいて、各段階についてなりすまし、窃取、盗聴、改ざんによる攻撃可能性(脅威)とその対策案について検討した。

本検討結果を元にして技術検証において第三者による検証を行う予定である。

#	検討項目	検討概要	項目概要
1	業務フローにおける攻撃可能性とその対策案	改ざん、窃取、盗聴、なりすましの観点で脅威とその対策について検討	・発行時における業務フロー ・失効時における業務フロー ・更新時における業務フロー ・再発行時における業務フロー ・一時保留解除時における業務フロー ・PIN初期化時における業務フロー ・PIN変更時における業務フロー

電子証明書に関する業務一覧

第1回検討会提示『スマートフォン特有のライフサイクルへの対応』資料にて分類した以下の業務について攻撃可能性とその対策案について検討した。本検討会では発行業務について示す。

項番	業務	説明	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	一時保留解除	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が閉塞した場合に行う初期化処理。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。

各段階における攻撃可能性の整理

前述した攻撃可能性について以下に整理した。
本項目の網羅性/妥当性については技術検証フェーズにて第三者機関で評価を行う。

パターン番号	分類	攻撃可能性	具体的な脅威
1	なりすまし	(偽)スマホアプリとの通信	・GP-SEとのなりすまし通信
2			・SP-TSMへのなりすまし通信
3		(偽)SP-TSMとの通信	・スマホアプリへのなりすまし通信
4			・公的個人認証サービスへのなりすまし通信
5		(偽)公的個人認証サービスとの通信	・SP-TSMへのなりすまし通信
6		別端末との通信	・マイナンバーカードによる署名処理を実施したスマホとは別のスマホのGP-SEに鍵ペア生成/鍵登録/SE識別ID認識　等を行う
7		(偽)スマホアプリへのなりすまし	・正規のスマホアプリではない(偽)スマホアプリになりすましてフィッシング等を行う
8	窃取/盗聴	マイナンバーカードの不正利用	・他人のマイナンバーカードでスマホJPKIの初期設定を行う ・マイナンバーカードの読取盗聴を行う
9		他人によるスマホ操作	・他人の端末でPIN設定等の操作を行う
10	盗聴	通信の盗聴	・スマホアプリとGP-SEとの間の通信を盗聴される
11			・スマホアプリとSP-TSMとの間の通信を盗聴される
12			・SP-TSMと公的個人認証サービスとの間の通信を盗聴される
13	改ざん	通信の改ざん	・通信データの改ざんが行われる
14		操作の改ざん	・利用者が意図していない操作が行われる （利用者が承認していないのに承認の返信を行う等）
15		業務処理の改ざん	・SP-TSMやGP-SE、公的個人認証サービスの中で実施している業務処理の改ざんが行われる ・SP-TSMの業務処理遷移において改ざんが行われる
16		アプリ処理の改ざん	・スマホアプリ内処理/処理遷移の改ざんが行われる

各段階における攻撃可能性に紐づく対策の整理(1/3)

攻撃可能性に紐づく対策案について、以下に整理した。

パターン番号	分類	攻撃可能性	具体的な脅威	対策	評価
1	なりすまし	(偽)スマホアプリとの通信	GP-SEとのなりすまし通信	・スマホアプリからのGP-SEへのアクセス制御の仕組みにより、GP-SEとの通信を事前に行うことでスマホアプリの正当性が担保されている。 ・不正なアプリはGP-SEにアクセスできないため実害が発生しない。	○
2			SP-TSMへのなりすまし通信	・SP-TSMとGP-SE間でSCP03でのセキュアチャネルを確立し、通信を行う。セキュアチャネルを確立できない(偽)スマホアプリや(偽)SP-TSMからはGP-SEにアクセスできないため実害が発生しない。	○
3		(偽)SP-TSMとの通信	スマホアプリへのなりすまし通信		
4			公的個人認証サービスへのなりすまし通信	・SP-TSMの構築先を既存の公的個人認証サービスと同一とする、または閉域網で繋ぐことで、外部からの侵入を物理的に防ぐ。 ・SP-TSMと公的個人認証サービスの通信は全てHTTPSとする。	○
5		(偽)公的個人認証サービスとの通信	SP-TSMへのなりすまし通信	・SP-TSMの構築先を既存の公的個人認証サービスと同一とする、または閉域網で繋ぐことで、外部からの侵入を物理的に防ぐ。 ・SP-TSMと公的個人認証サービスの通信は全てHTTPSとする。	○
6		別端末との通信	・マイナンバーカードによる署名処理を実施したスマホとは別のスマホのGP-SEに鍵ペア生成/鍵登録/SE識別ID認識　等を行う	・マイナンバーカードによる署名生成時にGP-SEでコミットメントSを発生させ、SE識別ID読出し時に前記Sを確認する方式とし、マイナンバーカードの署名生成とSE識別IDが同一スマホであることを確認する方式とする。 ・SE識別ID読出し時のコミットメントS確認を実施したセッションを維持することで、他の後続段階においても署名処理を実施したスマホと同一スマホでの実施が担保できている。	○
7		(偽)スマホアプリへのなりすまし	・(偽)スマホアプリになりすましてフィッシング等を行う	・スマホアプリからのGP-SEへのアクセス制御の仕組みにより、GP-SEとの通信を事前に行うことでスマホアプリの正当性が担保されている。 ・不正なアプリに関してはGP-SEにアクセスできないため実害が発生しない	○

各段階における攻撃可能性に紐づく対策の整理(2/3)

攻撃可能性に紐づく対策案について、以下に整理した。

パターン番号	分類	攻撃可能性	具体的な脅威	対策	評価
8	窃取	マイナンバーカードの不正利用	・他人のマイナンバーカードでスマホJPKIの初期設定を行う。 ・マイナンバーカード内の秘密鍵を取り出し複製を行う。	・マイナンバーカードはPINにより本人にしか利用できない。 ・マイナンバーカードはPINは連続して所定回数失敗するとロックする。 ・マイナンバーカードのICチップは耐タンパ性があるため、秘密鍵を取り出し複製することは困難。	○
9		他人によるスマホ操作	・他人の端末でPIN設定等の操作を行う	・端末自体のロック操作等により他人によるスマホ操作を防ぐことができる。	○
10	盗聴	通信の盗聴	・スマホアプリとGP-SEとの間の通信を盗聴される	・SCP03通信については盗聴が困難なため攻撃についても困難。 ・上記以外の通信でやり取りされる情報は、コミットメント生成コマンドと乱数ハッシュSのみであり、これらが取得されてもコミットメント照合の安全性に影響はない。	○
11			・スマホアプリとSP-TSMとの間の通信を盗聴される	・SCP03通信については盗聴が困難なため攻撃についても困難。 ・HTTPS通信については盗聴が困難なため攻撃についても困難。 ・上記以外の通信は発生しない。	○
12			・SP-TSMと公的個人認証サービスとの間の通信を盗聴される	・SP-TSMの構築先を既存の公的個人認証サービスと同一とする、または、閉域網で繋ぐことで、外部からの侵入を物理的に防ぐ。 ・SP-TSMと公的個人認証サービスの通信は全てHTTPSとする。	○

各段階における攻撃可能性に紐づく対策の整理(3/3)

攻撃可能性に紐づく対策案について、以下に整理した。

パターン番号	分類	攻撃可能性	具体的な脅威	対策	評価
13	改ざん	操作の改ざん	・利用者が意図していない操作が行われる。 （利用者が承認していないのに承認の返信を行う等）	・スマホアプリからのGP-SEへのアクセス制御の仕組みにより、GP-SEとの事前通信によりとでスマホアプリの正当性が担保されている。 ・上記により、スマホアプリは正常であり、利用者の失効承認等の各種操作は正しく機能すると考える。	○
14		通信の改ざん	・通信データの改ざんが行われる	・HTTPS通信/SCP03通信は改ざんが困難・SP-TSMと公的個人認証サービスの通信についてもHTTPSとする。 ・コミットメント生成コマンドと戻り値である乱数ハッシュSが改ざんされても、コミットメント照合時にエラーとなり、後続のフローは動作しない。	○
15		業務処理の改ざん	・SP-TSMやGP-SE、公的個人認証サービスの中で実施している業務処理の改ざんが行われる ・SP-TSMの業務処理遷移において改ざんが行われる	・GP-SEの処理はチップ内で閉じているため改ざんは困難 ・SP-TSMの業務処理はサーバ内に閉じているため改ざんは困難 ・公的個人認証サービスの業務処理はサーバ内に閉じているため改ざんは困難 ・SP-TSMの業務処理遷移は単一サーバ内に閉じており外部通信ではないため改ざんは困難	○
16		アプリ処理の改ざん	・スマホアプリ内処理の改ざんが行われる ・スマホアプリ内遷移の改ざんが行われる	・業務処理実行前および完了後の処理および遷移については、業務処理に影響しないため実害が発生しない。 ・失効処理においても業務処理が改ざんされアプレットの残存が考えられるが、実害は発生しない。	○

発行業務における攻撃可能性と対策の一覧表(1/5)

【凡例】
■：フロー番号がパターンに該当する
－：フロー番号がパターンに該当しない

P5-7の攻撃可能性と対策一覧に基づいて、発行フローの攻撃可能性について一覧表として整理した。
その他のフローについても同様に整理/評価を行っている。

フロー番号	アクター	概要	攻撃可能性	具体的な脅威	脅威と対策パターン番号																評価
					なりすまし							窃取		盗聴			改ざん				
					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
①	スマホ	初期設定フェーズ開始	※	別フローにて検討	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	※
①-②間	－	遷移	○	GP-SEへのなりすまし通信 GP-SEへの通信の改ざん/盗聴	■	－	－	－	－	－	－	－	－	■	－	－	－	■	－	－	○
②	スマホ	GP-SE内で乱数Rとそのコミットメント S=H[R]を生成	○	GP-SE内処理の改ざん	－	－	－	－	－	－	－	－	－	－	－	－	－	－	■	－	○
②-③間	－	遷移	○	GP-SEからのなりすまし通信 GP-SEからの通信の改ざん/盗聴	■	－	－	－	－	－	－	－	－	■	－	－	－	■	－	－	○
③	スマホ	スマホ用JPKI更新申請	○	スマホアプリになりすましての更新申請	－	■	－	－	－	－	－	－	－	－	－	－	－	－	－	－	○
③-④間（TSM側）	－	通信	○	SP-TSMとの通信の傍受 スマホアプリから出力されるデータの改ざん	－	－	－	－	－	－	－	－	－	－	■	－	－	■	－	－	○
③-④間（カード側）	－	マイナンバーカード読込	○	他人のマイナンバーカードでスマホJPKIの初期設定を行う マイナンバーカードの複製	－	－	－	－	－	－	－	■	－	－	－	－	－	－	－	－	○
④	TSM	署名検証&申請受理、S一時保持	○	公的個人認証へのなりすまし通信	－	－	－	■	－	－	－	－	－	－	－	－	－	－	－	－	○
④-⑤間	－	公的個人認証との通信	○	公的個人認証サービスとの通信盗聴/改ざん	－	－	－	－	－	－	－	－	－	－	－	■	－	■	－	－	○
⑤	JPKI	カード用電子証明書の 有効性確認	○	公的個人認証サービス内処理の改ざん	－	－	－	－	－	－	－	－	－	－	－	－	－	－	■	－	○

発行業務における攻撃可能性と対策の一覧表(2/5)

【凡例】
■：フロー番号がパターンに該当する
－：フロー番号がパターンに該当しない

P5-7の攻撃可能性と対策一覧に基づいて、発行フローの攻撃可能性について一覧表として整理した。
その他のフローについても同様に整理/評価を行っている。

フロー番号	アクター	概要	攻撃可能性	具体的な脅威	脅威と対策パターン番号																評価
					なりすまし							窃取		盗聴			改ざん				
					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
⑤–⑥間	－	遷移	○	SP–TSM内処理遷移の改ざん	－	－	－	－	－	－	－	－	－	－	－	－	－	－	■	－	○
⑥	TSM	SE識別ID読出し要求	○	スマホアプリへのなりすまし通信	－	－	■	－	－	－	－	－	－	－	－	－	－	－	－	－	○
⑥–⑦間	－	通信	○	通信の盗聴/改ざん	－	－	－	－	－	－	－	－	－	－	■	－	－	■	－	－	○
⑦	スマホ	SE識別ID読出し実行	○	GP–SEとのなりすまし通信 SP–TSMへのなりすまし通信 異なる端末とのSE識別ID読出し	■	■	－	－	－	■	－	－	－	－	－	－	－	－	－	－	○
⑦–⑧間	－	遷移	○	SP–TSM内処理遷移の改ざん	－	－	－	－	－	－	－	－	－	－	－	－	－	－	■	－	○
⑧	TSM	スマホ用電子証明書の状態チェック	○	公的個人認証へのなりすまし通信	－	－	－	■	－	－	－	－	－	－	－	－	－	－	－	－	○
⑧–⑨間	－	公的個人認証との通信	○	公的個人認証サービスとの通信盗聴/通信改ざん	－	－	－	－	－	－	－	－	－	－	－	■	－	■	－	－	○
⑨	JPKI	スマホ用電子証明書の状態確認	○	公的個人認証サービス内処理の改ざん	－	－	－	－	－	－	－	－	－	－	－	－	－	－	■	－	○
⑨–⑩間	－	遷移	○	SP–TSM内処理遷移の改ざん	－	－	－	－	－	－	－	－	－	－	－	－	－	－	■	－	○
⑩	TSM	状態遷移による処理選択	○	SP–TSM内処理分岐の改ざん	－	－	－	－	－	－	－	－	－	－	－	－	－	－	■	－	○
⑩–⑪間	－	遷移	○	SP–TSM内処理遷移の改ざん	－	－	－	－	－	－	－	－	－	－	－	－	－	－	■	－	○

発行業務における攻撃可能性と対策の一覧表(3/5)

【凡例】
■：フロー番号がパターンに該当する
－：フロー番号がパターンに該当しない

P5-7の攻撃可能性と対策一覧に基づいて、発行フローの攻撃可能性について一覧表として整理した。
その他のフローについても同様に整理/評価を行っている。

フロー番号	アクター	概要	攻撃可能性	具体的な脅威	脅威と対策パターン番号																評価
					なりすまし							窃取		盗聴			改ざん				
					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
⑩–⑯間	–	遷移	○	SP–TSM内処理遷移の改ざん	–	–	–	–	–	–	–	–	–	–	–	–	–	–	■	–	○
⑪	TSM	(旧端末)利用者に失効確認	○	スマホアプリへのなりすまし通信	–	–	■	–	–	–	–	–	–	–	–	–	–	–	–	–	○
⑪–⑫間	–	通信	○	スマホアプリとの通信の傍受 SP–TSMから出力されるデータの改ざん	–	–	–	–	–	–	–	–	–	–	■	–	–	■	–	–	○
⑫	スマホ	利用者による失効承認	○	異なる端末による失効承認 他人による失効承認 失効承認操作の改ざん	–	–	–	–	–	■	–	–	■	–	–	–	■	–	–	–	○
⑫–⑬間	–	通信	○	SP–TSMとの通信の傍受 スマホアプリから出力されるデータの改ざん	–	–	–	–	–	–	–	–	–	–	■	–	–	■	–	–	○
⑬	TSM	(旧端末)失効依頼	○	公的個人認証へのなりすまし通信	–	–	–	■	–	–	–	–	–	–	–	–	–	–	–	–	○
⑬–⑭間	–	公的個人認証との通信	○	公的個人認証サービスとの通信盗聴/通信改ざん	–	–	–	–	–	–	–	–	–	–	–	■	–	■	–	–	○
⑭	JPKI	スマホ用電子証明書の失効処置(旧端末の失効)	○	SP–TSMへのなりすまし通信	–	–	–	–	■	–	–	–	–	–	–	–	–	–	–	–	○
⑭–⑮間	–	公的個人認証との通信	○	公的個人認証サービスとの通信盗聴/通信改ざん	–	–	–	–	–	–	–	–	–	–	–	■	–	■	–	–	○
⑮	TSM	失効完了	○	SP–TSM内処理の改ざん	–	–	–	–	–	–	–	–	–	–	–	–	–	–	■	–	○

発行業務における攻撃可能性と対策の一覧表(4/5)

【凡例】
■：フロー番号がパターンに該当する
－：フロー番号がパターンに該当しない

P5-7の攻撃可能性と対策一覧に基づいて、発行フローの攻撃可能性について一覧表として整理した。
その他のフローについても同様に整理/評価を行っている。

フロー番号	アクター	概要	攻撃可能性	具体的な脅威	脅威と対策パターン番号																評価
					なりすまし							窃取		盗聴			改ざん				
					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
⑮–⑯間	–	遷移	○	SP–TSM内処理遷移の改ざん	–	–	–	–	–	–	–	–	–	–	–	–	–	–	■	–	○
⑯	TSM	鍵ペア生成要求	○	SP–TSMになりすましての通信	–	–	■	–	–	–	–	–	–	–	–	–	–	–	–	–	○
⑯–⑰間	–	通信	○	スマホアプリとの通信の傍受 SP–TSMから出力されるデータの改ざん	–	–	–	–	–	–	–	–	–	–	■	–	–	■	–	–	○
⑰	スマホ	GP–SE内で鍵ペアを生成し、秘密鍵を保存。 公開鍵とRをアップロード	○	スマホアプリになりすましての鍵ペア生成、アップロード 異なる端末での鍵ペア生成	■	–	–	–	–	■	–	–	–	–	–	–	–	–	–	–	○
⑰–⑱間	–	通信	○	SP–TSMとの通信の傍受 スマホアプリから出力されるデータの改ざん	–	–	–	–	–	–	–	–	–	–	■	–	–	■	–	–	○
⑱	TSM	スマホ用公開鍵取得 H[R]=Sをチェック	○	SP–TSM内処理の改ざん	–	–	–	–	–	–	–	–	–	–	–	–	–	–	■	–	○
⑱–⑲間	–	遷移	○	SP–TSM内処理遷移の改ざん	–	–	–	–	–	–	–	–	–	–	–	–	–	–	■	–	○
⑲	TSM	スマホ用電子証明書発行依頼	○	SP–TSMになりすましての通信	–	–	■	–	–	–	–	–	–	–	–	–	–	–	–	–	○
⑲–⑳間	–	公的個人認証との通信	○	公的個人認証サービスとの通信 盗聴/改ざん	–	–	–	–	–	–	–	–	–	–	–	■	–	■	–	–	○

発行業務における攻撃可能性と対策の一覧表(5/5)

【凡例】
■：フロー番号がパターンに該当する
－：フロー番号がパターンに該当しない

P5-7の攻撃可能性と対策一覧に基づいて、発行フローの攻撃可能性について一覧表として整理した。
その他のフローについても同様に整理/評価を行っている。

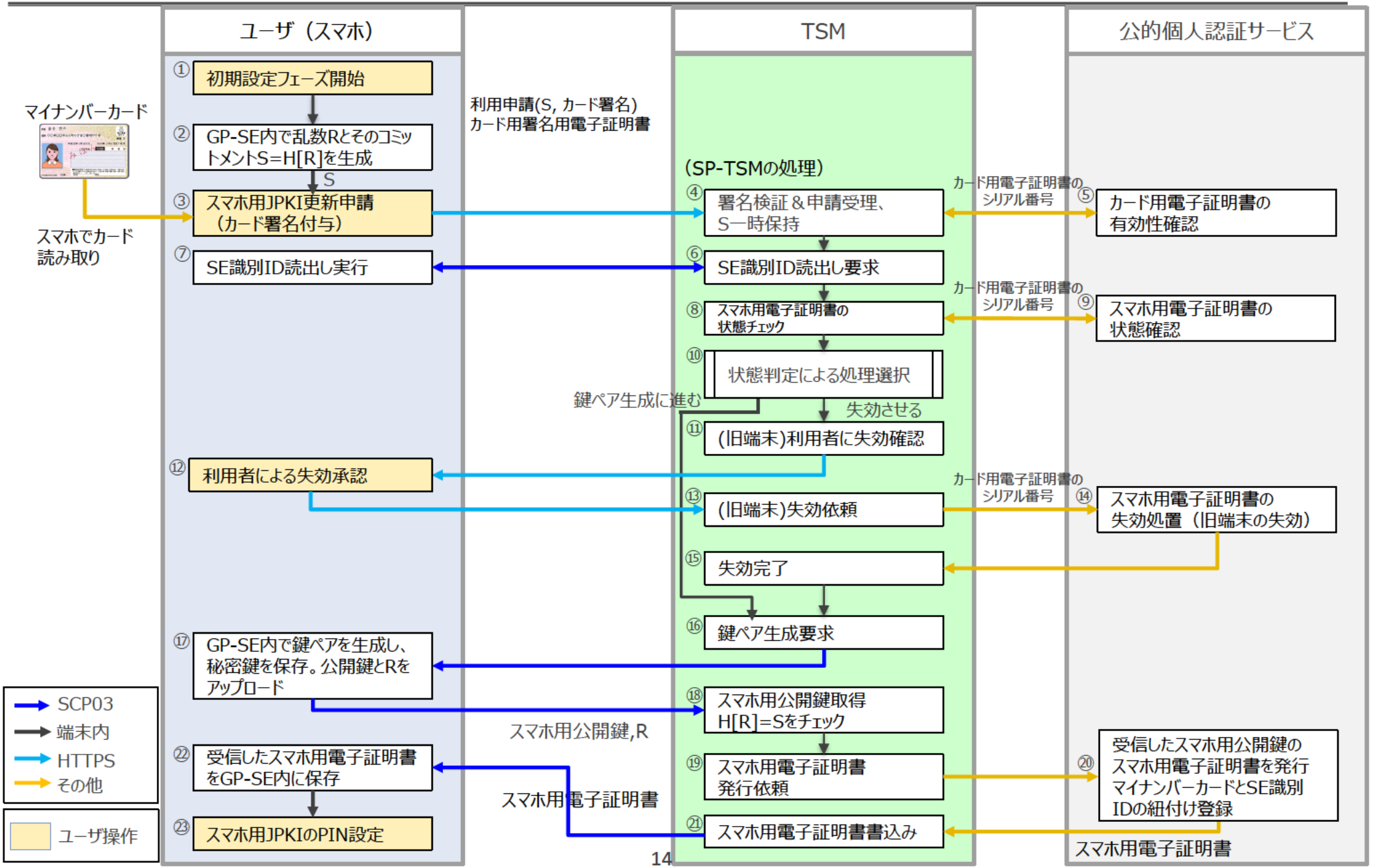
フロー番号	アクター	概要	攻撃可能性	具体的な脅威	脅威と対策パターン番号																評価
					なりすまし							窃取		盗聴			改ざん				
					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
⑳	JPKI	受信したスマホ用公開鍵のスマホ用電子証明書を発行 マイナンバーカードとSE識別IDの紐づけ登録	○	公的個人認証サービス内処理の改ざん	－	－	－	－	－	－	－	－	－	－	－	－	－	－	■	－	○
⑳-㉑間	－	公的個人認証との通信	○	公的個人認証サービスとの通信盗聴/改ざん	－	－	－	－	－	－	－	－	－	－	－	■	－	■	－	－	○
㉑	TSM	スマホ用電子証明書書込み	○	スマホアプリへのなりすまし通信	－	－	■	－	－	－	－	－	－	－	－	－	－	－	－	－	○
㉑-㉒間	－	通信	○	スマホアプリとの通信の傍受 SP-TSMから出力されるデータの改ざん	－	－	－	－	－	－	－	－	－	－	■	－	－	■	－	－	○
㉒	スマホ	受信したスマホ用電子証明書をGP-SE内に保存	○	スマホアプリになりすましての証明書格納 異なる端末への証明書格納 GP-SEへの通信の改ざん./盗聴	■	－	－	－	－	■	－	－	－	■	－	－	－	■	－	－	○
㉒-㉓間	－	遷移	○	スマホアプリ内処理遷移の改ざん	－	－	－	－	－	－	－	－	－	－	－	－	－	－	■	－	○
㉓	スマホ	スマホ用JPKIのPIN設定	※	別フローにて検証	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－	※

参考資料

参考

スマホ用電子証明書発行の概略フロー

第一次とりまとめから引用

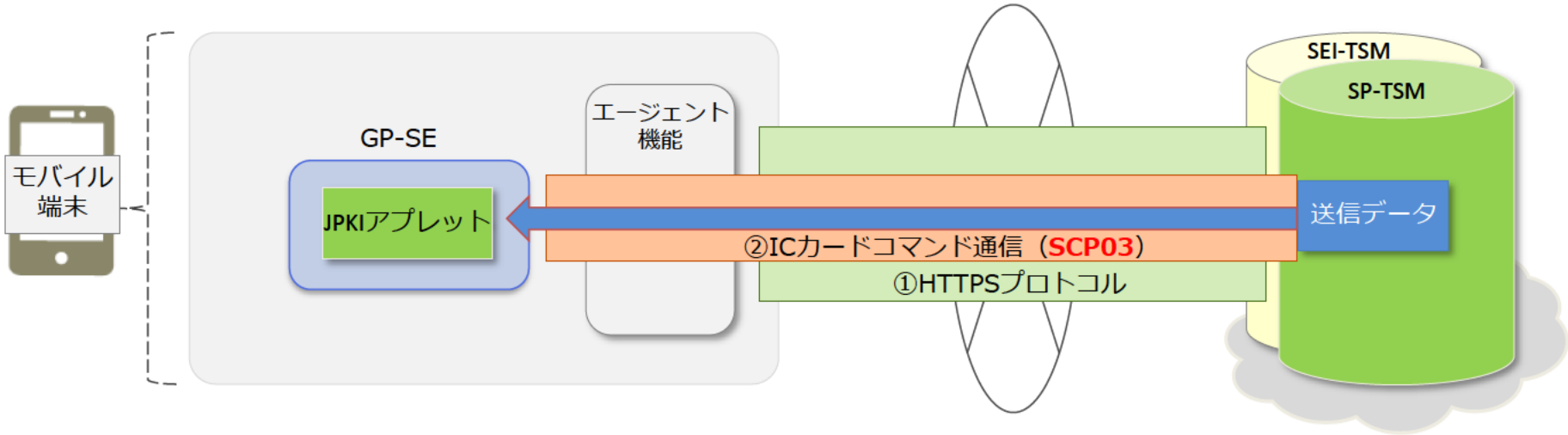


参考

GP-SEのセキュリティ機能①

（1）セキュアチャネルプロトコル

GP-SEとTSMとの間は、セキュアチャネルプロトコル（SCP03）によってデータ通信が実施される。SCP03は、GlobalPlatformによって定めれた暗号通信プロトコルであり、GP-SEとTSMの2者間での鍵共有と暗号化されたデータを送受信するため、経路途中のデータがスキミングされたとしても解読、改ざんが極めて困難。



（2）GP-SEの暗号機能

GP-SEは、公的個人認証サービスで要求される以下の暗号アルゴリズムに対応している。また、RSA2048bitの鍵ペア生成も可能となっている。

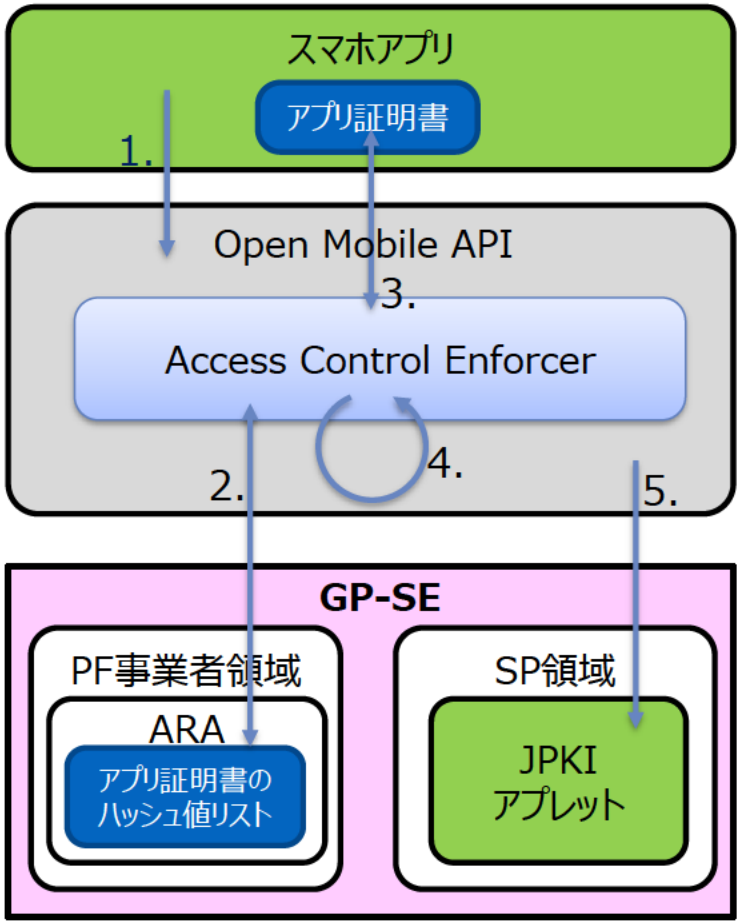
No.	暗号アルゴリズム	サポート状況	備考
1	RSA2048bit	○	署名はRSASSA-PKCS#1_v1.5に対応
2	AES128bit	○	SCP03の暗号化プロトコル
3	乱数生成	○	SCPで使用

参考

GP-SEのセキュリティ機能②

（3）スマホアプリからのアクセスに関するセキュリティ機能

GP-SE内に格納されたアプレット（JPKIアプレット）は、下図の仕組みによりアクセス元アプリケーションの認証を行なうことで、正当なAndroidアプリケーション（スマホアプリ）のみがアクセス可能となっている。この仕組みにより、第三者がGP-SEにアクセス可能なスマホアプリを作ることは極めて困難である。



【参考】GlobalPlatform, Secure Element Access Control v1.0

■アプレットにアクセスできるアプリケーションリストの登録方法

1. SPは、JPKIアプレットにアクセスできるアプリケーションのホワイトリスト（Androidアプリケーションの証明書ハッシュ値リスト）を作成し、SEI-TSMに登録しておく。
2. SEI-TSMがJPKIアプレットをGP-SEに格納する際に、上記のリストをARA（Access Rule Application）に格納する。

■認証手順（番号は左図に対応）

1. スマホアプリがOpen Mobile APIにアクセスする。
   Open Mobile API： GP仕様に準拠したGP-SE内のセキュアな領域にアクセスするために提供されているAndroid用API
2. Open Mobile API内部のACE（Access Control Enforcer）がPF事業者領域内のARA（Access Rule Application）から、アクセスルールを取得する。
3. ACEは、アクセス元のAndroidアプリケーションに付与されている公開鍵証明書のハッシュ値を算出する。
4. ACEは、手順2と手順3で取得したハッシュ値を比較する。一致した場合は、正しいアプリケーションからのアクセスであると判断する。
5. 手順4で一致した場合は、手順1で要求されたOpen Mobile API処理が実行される。