スマートフォンのセキュリティ機構

～マイナンバーカードのスマホ搭載における論点を参考に～

"On the Internet, nobody knows you're a dog."

Image from *The New Yorker* cartoon by Peter Steiner, 1993.

情報セキュリティ大学院大学 教授
日本銀行金融研究所 客員研究員
デジタルアイデンティティ推進コンソーシアム理事
大塚　玲

目次

1.マイナンバーカード

1.2 法改正

デジタル社会の形成を図るための関係法律の整備に関する法律案の概要 ＜予算関連法案＞

趣旨

デジタル社会形成基本法に基づき**デジタル社会の形成に関する施策を実施するため、**個人情報の保護に関する法律、行政手続における特定の個人を識別するための番号の利用等に関する法律等の**関係法律について所要の整備を行う。**

概要

個人情報保護制度の見直し（個人情報保護法の改正等）

① 個人情報保護法、行政機関個人情報保護法、独立行政法人等個人情報保護法の3本の法律を1本の法律に統合するとともに、地方公共団体の個人情報保護制度についても統合後の法律において全国的な共通ルールを規定し、全体の所管を個人情報保護委員会に一元化。
② 医療分野・学術分野の規制を統一するため、国公立の病院、大学等には原則として民間の病院、大学等と同等の規律を適用。
③ 学術研究分野を含めたGDPR（EU一般データ保護規則）の十分性認定への対応を目指し、学術研究に係る適用除外規定について、一律の適用除外ではなく、義務ごとの例外規定として精緻化。
④ 個人情報の定義等を国・民間・地方で統一するとともに、行政機関等での匿名加工情報の取扱いに関する規律を明確化。

施行日：公布から１年以内（地方公共団体関係は公布から２年以内）

マイナンバーを活用した情報連携の拡大等による行政手続の効率化（マイナンバー法等の改正）

① 国家資格に関する事務等におけるマイナンバーの利用及び情報連携を可能とする。
② 従業員本人の同意があった場合における転職時等の使用者間での特定個人情報の提供を可能とする。

施行日：公布日（①のうち国家資格関係事務以外(健康増進事業、高等学校等就学支援金、知的障害者など)）、公布から４年以内（①のうち国家資格関係事務関連）、令和３年９月１日（②）

マイナンバーカードの利便性の抜本的向上、発行・運営体制の抜本的強化（郵便局事務取扱法、公的個人認証法、住民基本台帳法、マイナンバー法、J-LIS法等の改正）

＜マイナンバーカードの利便性の抜本的向上＞

① 住所地市区町村が指定した郵便局において、公的個人認証サービスの電子証明書の発行・更新等を可能とする。
② 公的個人認証サービスにおいて、本人同意に基づき、基本４情報（氏名、生年月日、性別及び住所）の提供を可能とする。
③ マイナンバーカード所持者について、電子証明書のスマートフォン（移動端末設備）への搭載を可能とする。
④ マイナンバーカード所持者の転出届に関する情報を、転入地に事前通知する制度を設ける。 等

Duplication

施行日：公布日（①）、公布から２年以内（①以外）

＜マイナンバーカードの発行・運営体制の抜本的強化＞

① 地方公共団体情報システム機構（J-LIS）による個人番号カード関係事務について、国による目標設定、計画認可、財源措置等の規定を整備。
② J-LISの代表者会議の委員に国の選定した者を追加するとともに、理事長及び監事の任免に国の認可を必要とする等、国によるガバナンスを強化。
③ 電子証明書の発行に係る市町村の事務を法定受託事務化。 等

施行日：令和３年９月１日

押印・書面の交付等を求める手続の見直し（48法律の改正）

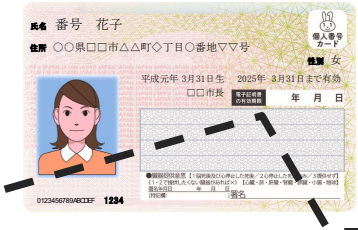
○ 押印を求める各種手続についてその押印を不要とするとともに、書面の交付等を求める手続について電磁的方法により行うことを可能とする。

施行日：令和３年９月１日（施行までに一定の準備期間が必要なものを除く。）

出所)内閣官房「デジタル社会の形成を図るための関係法律の整備に関する法律案」2021.3.9.

1.3 マイナンバーカードの概要①

マイナンバーカードに格納される公的個人認証サービスについて



公開鍵暗号方式

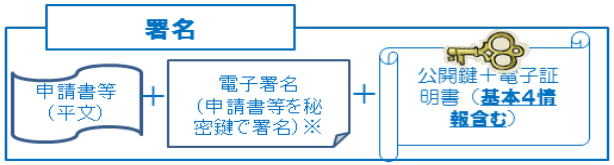
公的個人認証サービスが採用する暗号方式。秘密鍵と公開鍵はペアとなっており、片方の鍵で暗号化されたものは、もう一方の鍵でしか復号できない性質をもつ。

署名用電子証明書

（性質）
インターネットで電子文書を送信する際などに、署名用電子証明書を用いて、文書が改ざんされていないかどうか等を確認することができる仕組み

（利用局面）
e-Taxの確定申告等、文書を伴う電子申請等に利用される。

（利用されるデータの概要）



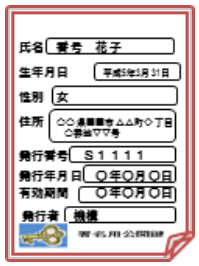
※電子署名法（平成12年法律第102号）の「電子署名」に該当し、同法第3条による「真正な成立の推定」の対象になり得る。

署名用秘密鍵

※ カードの中の格納された領域から外に出ることがない

※ 秘密鍵を無理に読みだそうとすると、ICチップが壊れる仕組み

電子証明書のイメージ



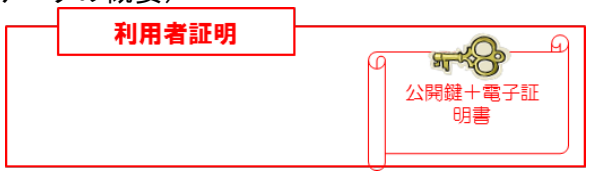
※基本4情報を記録

利用者証明用電子証明書

（性質）
インターネットを閲覧する際などに、利用者証明用電子証明書（基本4情報の記載なし）を用いて、利用者本人であることのみを証明する仕組み

（利用局面）
マイナポータルのログイン等、本人であることの認証手段として利用される。

（利用されるデータの概要）



利用者証明用秘密鍵

※ カードの中の格納された領域から外に出ることがない

※ 秘密鍵を無理に読みだそうとすると、ICチップが壊れる仕組み

電子証明書のイメージ

※基本4情報の記録なし

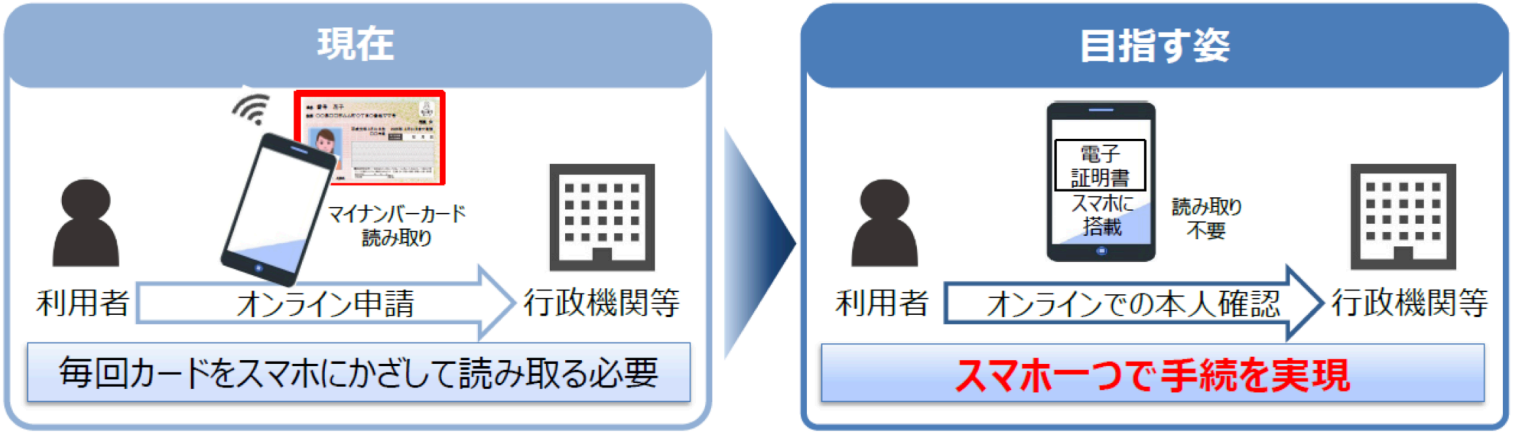
出所)総務省 マイナンバーカードの機能のスマートフォン搭載等に関する検討会 第1回資料.

1.3 マイナンバーカードの概要②

出所)総務省 「第1次とりまとめ ～電子証明書のスマートフォン搭載の実現に向けて～」2020.12.25.

2. ICカードとスマホ搭載SEの本質的な違い

2.1 スマートフォン＝カード＋UI＋通信機能



出所)総務省 「マイナンバーカードの機能のスマートフォン搭載等に関する検討会（第7回）資料2」2021.7.28.

	セキュアエレメント (耐タンパ性)	UI	通信機能
ICカード 	○ NFC通信可能な セキュアエレメント	タッチ動作	NFC タッチ時のみON
スマートフォン 	○ NFC通信可能かつ **アプリ連携可能な** セキュアエレメント	タッチ動作 ＋ 表示機能 ＋ 入力機能 WYSIWYS可能	NFC ＋ インターネット (紛失時リモート消去可) 常にON ⇒ 高いマルウェア耐性が求められる

2.2 WYSIWYS(What You See Is What You Sign)の達成

不正アプリを用いて、**表示内容およびサーバーへの送信内容を不正に制御する**トロイの木馬型のウイルス。(MitMo: Man in the Mobile攻撃)

利用者が画面で確認した文書(SEE)＝署名される文書(SIGN)が重要！

(マイナンバーカード搭載スマホではWYSIWYSの達成を目標にセキュリティ機構を設計)

補足：Androidマルウェアの実態（感染ルート）

ノースカロライナ州立大学の調査

*Android*マルウェアの全体の*83%*（*1083*件）は*Repackaging*

Repackaging:

有名なアプリにマルウェアを同梱した偽アプリを配布

Update:

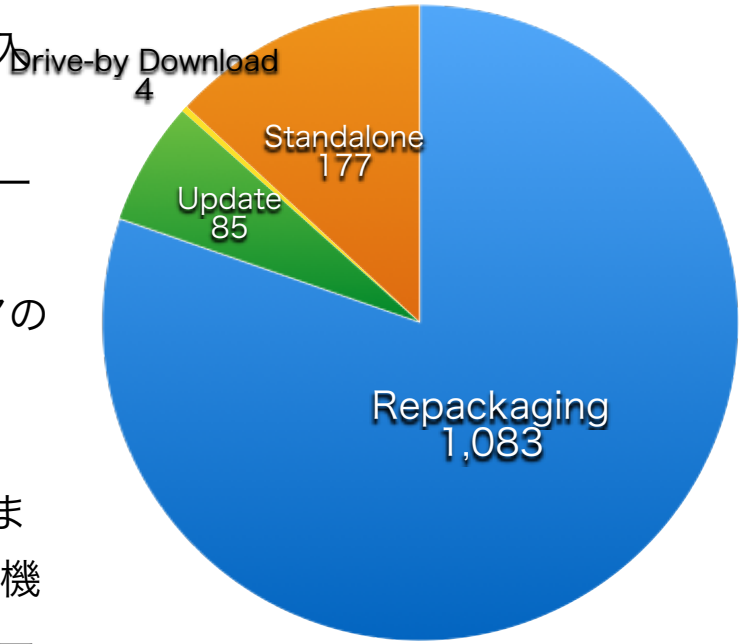
*Repackage*と同じく有名なアプリにアップデートプログラムを同梱し，ソフトウェアアップデートでマルウェアを導入

Drive-by Download:

ブラウザの脆弱性を利用してダウンロードで感染させる*PC*版とは異なり，*Android*版は利用者を騙してマルウェアの導入を促すことが多い

Standalone:（その他）

スパイウェア，有名アプリの見かけをまねた偽アプリ，自作アプリに*SMS*窃取機能を持たせたもの，脆弱性を使ったルート化ツール等



調査対象のマルウェアの概要

Malware	Samples	Markets		Discovered Month
		O†	A‡	
FakePlayer	6		√	2010-08
GPSSMSSpy	6		√	2010-08
TapSnake	2	√		2010-08
SMSReplicator	1	√		2010-11
Geinimi	69		√	2010-12
ADRD	22		√	2011-02
Pjapps	58		√	2011-02
BgServ	9		√	2011-03
DroidDream	16	√	√	2011-03
Walkinwat	1		√	2011-03
zHash	11	√	√	2011-03
DroidDreamLight	46	√	√	2011-05
Endofday	1		√	2011-05
Zsone	12	√	√	2011-05
BaseBridge	122		√	2011-06
DroidKungFu1	34		√	2011-06
GGTracker	1		√	2011-06
jSMSHider	16		√	2011-06
Plankton	11	√		2011-06
YZHC	22	√	√	2011-06
Crusewin	2		√	2011-07
DroidKungFu2	30		√	2011-07
GamblerSMS	1		√	2011-07
GoldDream	47		√	2011-07
HippoSMS	4		√	2011-07
Lovetrap	1		√	2011-07
Nickyspy	2		√	2011-07
SndApps	10	√		2011-07
Zitmo	1	√	√	2011-07
CoinPirate	1		√	2011-08
DogWars	1		√	2011-08
DroidKungFu3	309		√	2011-08
GingerMaster	4		√	2011-08
NickyBot	1		√	2011-08
RogueSPPush	9		√	2011-08
AnserverBot	187		√	2011-09
Asroot	8	√	√	2011-09
DroidCoupon	1		√	2011-09
DroidDeluxe	1		√	2011-09
Gone60	9	√		2011-09
Spitmo	1		√	2011-09
BeanBot	8		√	2011-10
DroidKungFu4	96	√	√	2011-10
DroidKungFuSapp	3		√	2011-10
DroidKungFuUpdate	1	√	√	2011-10
FakeNetflix	1		√	2011-10
Jifake	1		√	2011-10
KMin	52		√	2011-10
RogueLemon	2		√	2011-10
Total	*1260*	*14*	*44*	

Source) Y. Zhou and X. Jiang, “Dissecting android malware: Characterization and evolution,” IEEE S&P 2012, pp. 95–109.

(O†: OFFICAL ANDROID MARKET; A‡: ALTERNATIVE ANDROID MARKETS)

3. スマートフォンのセキュリティ機構

3.1 セキュアエレメント (GP-SE)の機能① 耐タンパー性

【補足資料4】セキュリティ評価（マイナンバーカードとの比較）

・FeliCa-SEのプラットフォーム（HW+OS）は、FASTというフェリカネットワークス（FN）社で定めたセキュリティルールに基づいて、CC認証、もしくは、EMV認定の取得に加えて、FeliCa機能に関するセキュリティ要件を満たすことが条件となっている。マイナンバーカードにおけるCC認証とは、以下のような相違がある。

項目	マイナンバーカードのセキュリティ評価（CC認証）	FeliCa-SEプラットフォームのセキュリティ評価		
		FAST認定（FeliCa機能観点）		
		CC認証（HW＋OS）	EMV認定（HW+OS）	
セキュリティ要件	ISO15408に基づいて作成されたプロテクションプロファイル（公開）EAL4+（AVA_VAN.5）	ISO15408に基づいて作成されたプロテクションプロファイル（公開）EAL4+（AVA_VAN.5）	EMVCoが定めるSecurity Guideline（非公開）EAL4+（AVA_VAN.5）	FNが定めるSecurity Guideline（非公開）EAL4+（AVA_VAN.5）
評価の範囲	製品の評価及びその開発プロセスを含んだ評価	製品の評価及びその開発プロセスを含んだ評価		
脆弱性評価	JIWG文書（※1）で示される攻撃への対抗	JIWG文書（※1）で示される攻撃への対抗		
有効期間	認証取得国による	認証取得国による	1年（再評価後1年、最長6年）	3年（再評価後1.5年）
評価機関	認証機関が認定した評価機関	認証機関が認定した評価機関	EMVCoが認定した評価機関	FNが認定した評価機関
認証機関	認証制度に基づく認証機関（公的機関）	認証制度に基づく認証機関（公的機関）	EMVCo	FNが認定した認証機関

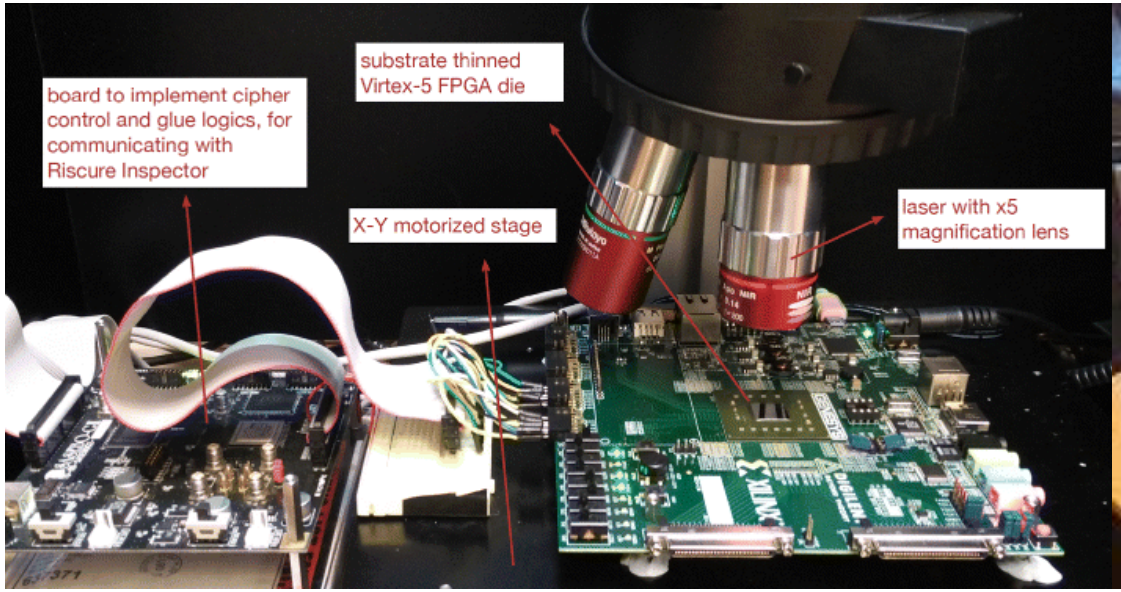
・マイナンバーカードのCC認証及びFeliCa-SEのFAST認定では、脆弱性分析においてはいずれも同一のJIWG文書を参照し、攻撃方法への対抗策が評価されている。参照するJIWG文書は、現在想定されるICカードへの攻撃方法を網羅的に記したものであり、国際的に広く参照されている文書である。

※1 JIL Application of Attack Potential to Smart Cards, version 2.9 Jan 2013

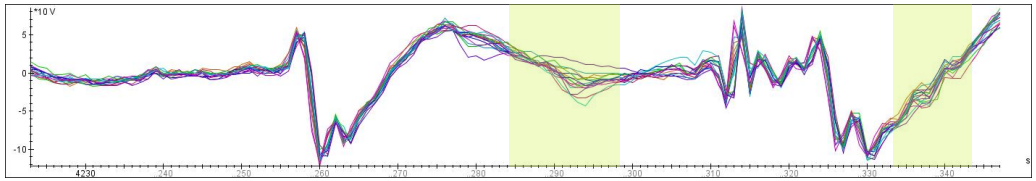
・FeliCa-SEでは、脆弱性分析においては最高レベルであるAVA_VAN.5を取得することが条件となっており、マイナンバーカードと同等の保証レベル（AVA_VAN.5）を要求していることは高く評価できるものと考えられる。

出所)総務省 マイナンバーカードの機能のスマートフォン搭載等に関する検討会 第1回資料.

AVA_VAN.5 ペネトレーションテスト

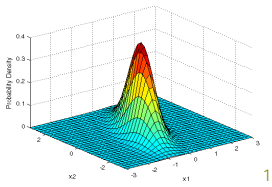


Points of interest selection



Data leakage　　Noise

Samples showing **statistical dependency** between intermediate (key-related) data and power consumption.

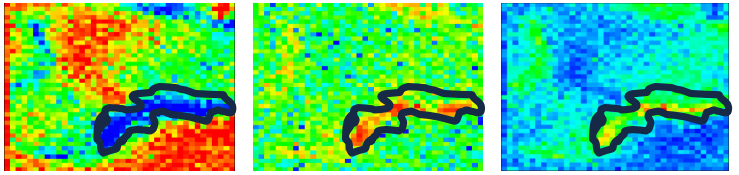


riscure　10

EM leakage location finding

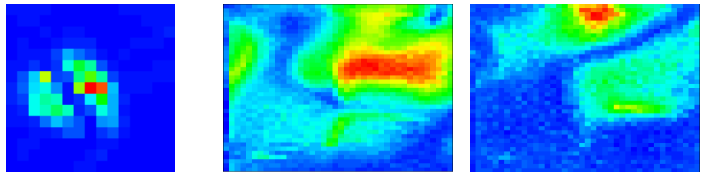
Some delivers truth but too costly

Pics origin: "EM-scanning" by Albert Spruyt



Key rank (5M)　*Ghost peak dist.(8M)*　*Intermediates corr. (3M)*

Some cheaper but misleading



Spectral intensity (1)　*Input corr. (1M)*　*Output corr. (1M)*

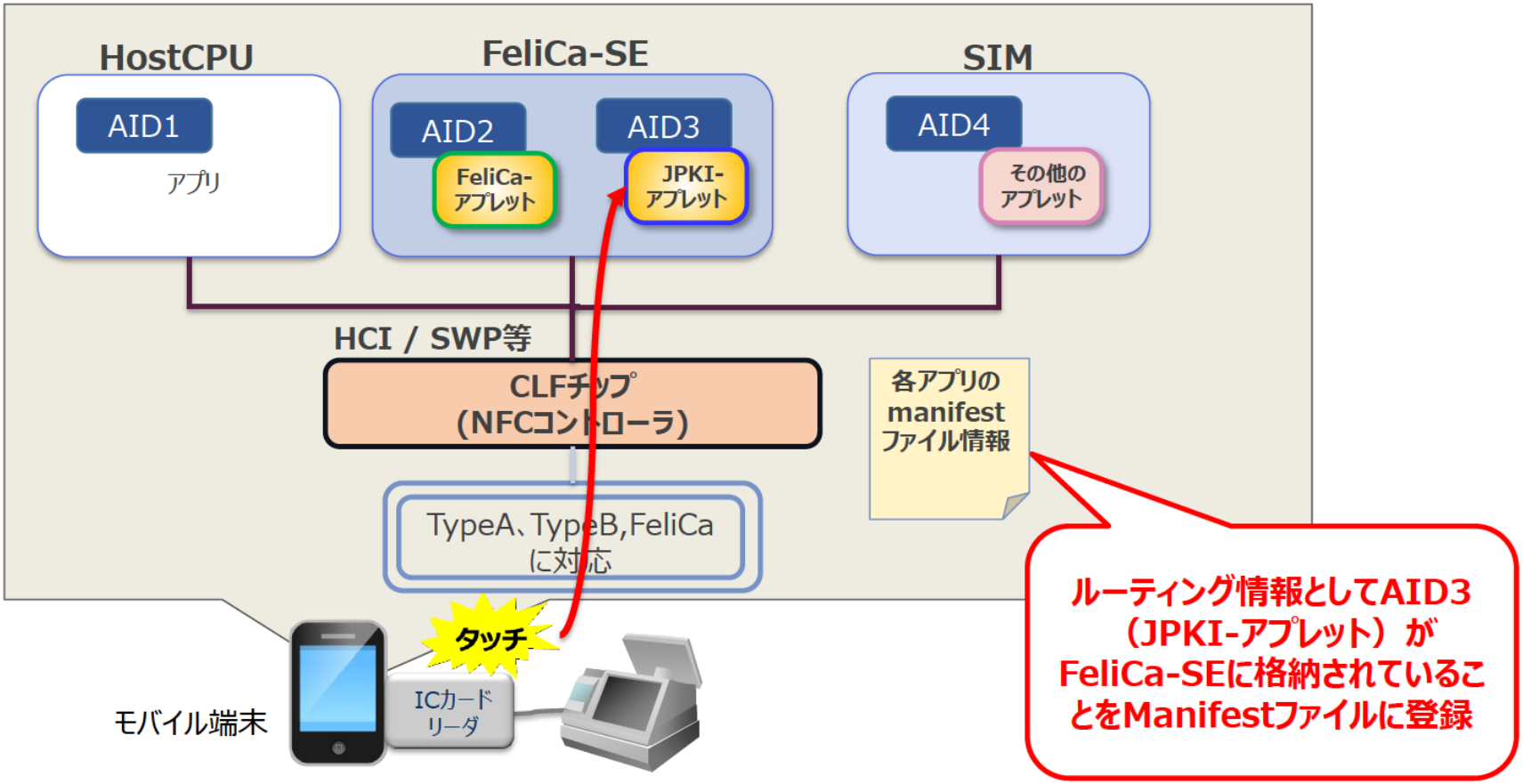
riscure

出所) Jasper van Woudenberg, "Practicing the art and science of side channel and fault attacks," Real World Crypto 2019.

3.1 セキュアエレメント (GP-SE)の機能② タッチ動作

【補足資料7】外部端末からのアクセス方式

FeliCa-SE搭載スマートフォンでは、 NFCを用いたカードエミュレーションモードが利用可能であり、カードエミュレーションを実施した際、Manifestファイルに記載されたAIDの情報に従って、FeliCa-SEにルーティングされる。



出所)総務省 マイナンバーカードの機能のスマートフォン搭載等に関する検討会 第1回資料.

3.2 セキュアブート機構

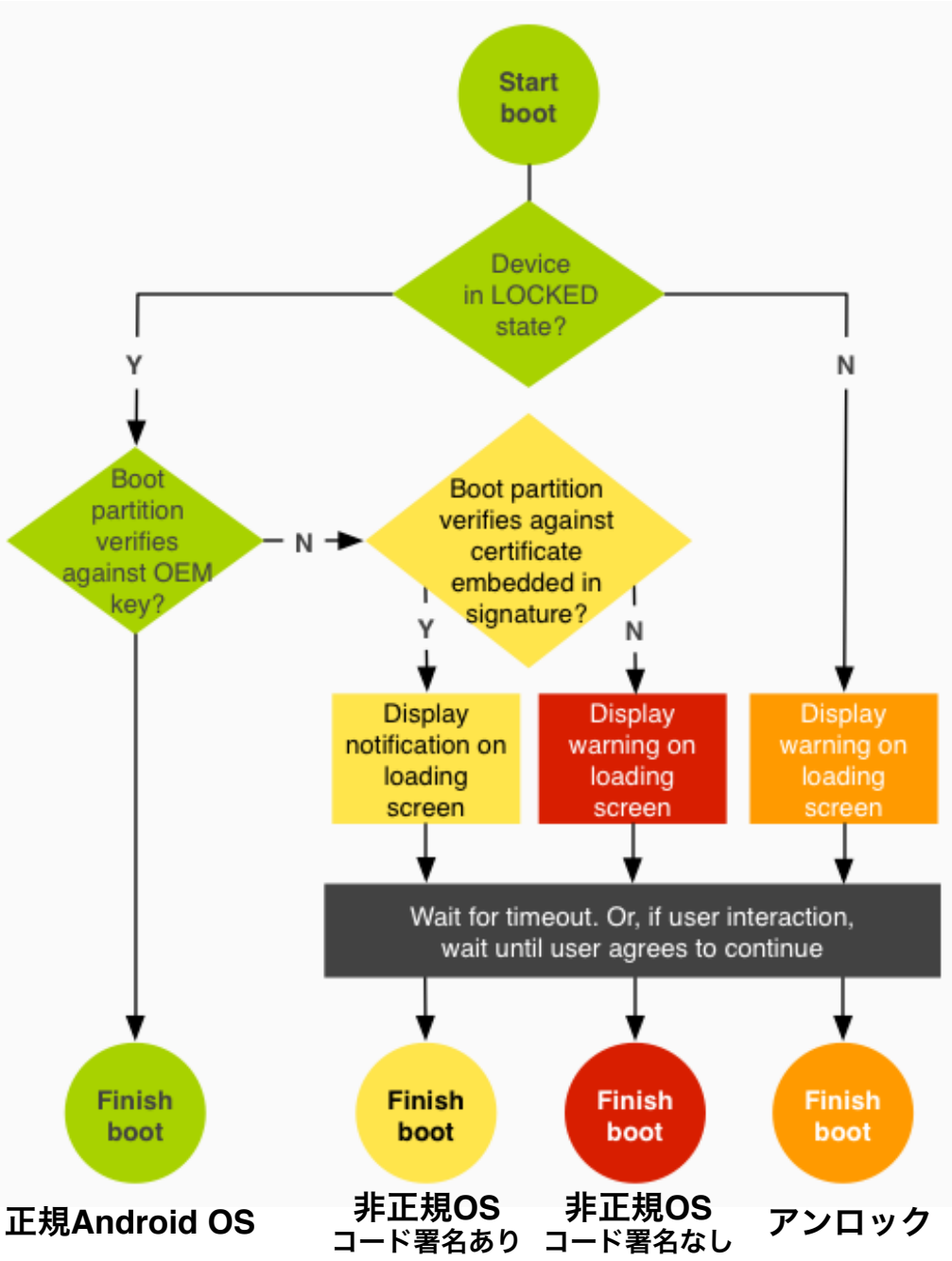
Android OSの保護機構: Verified Boot

`fastboot flashing [unlock | lock]`

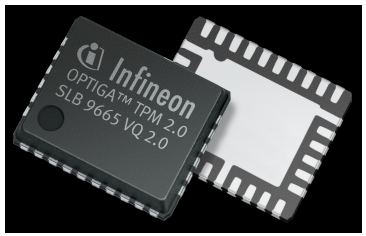
BootloaderはOSの保護機構の役割を果たしており、OEMの署名が施された正規OSだけがシステム領域にインストール&Boot可能になっている

但し、Android端末では、利用者がシステム領域を**`unlock`**する機能を提供しており、利用者が`unlock`コマンドを実行した場合には、**データ領域を全消去**（工場出荷時に戻す）した上で、システム領域の書き込み制限を解除する

`lock`状態	OEMベンダーの署名が施された正規OSのみをインストール可能（正規Android OS） システム領域は読み込み専用
`unlock`状態	所有者が好みのOSを導入可能 システム領域は書き込み可能

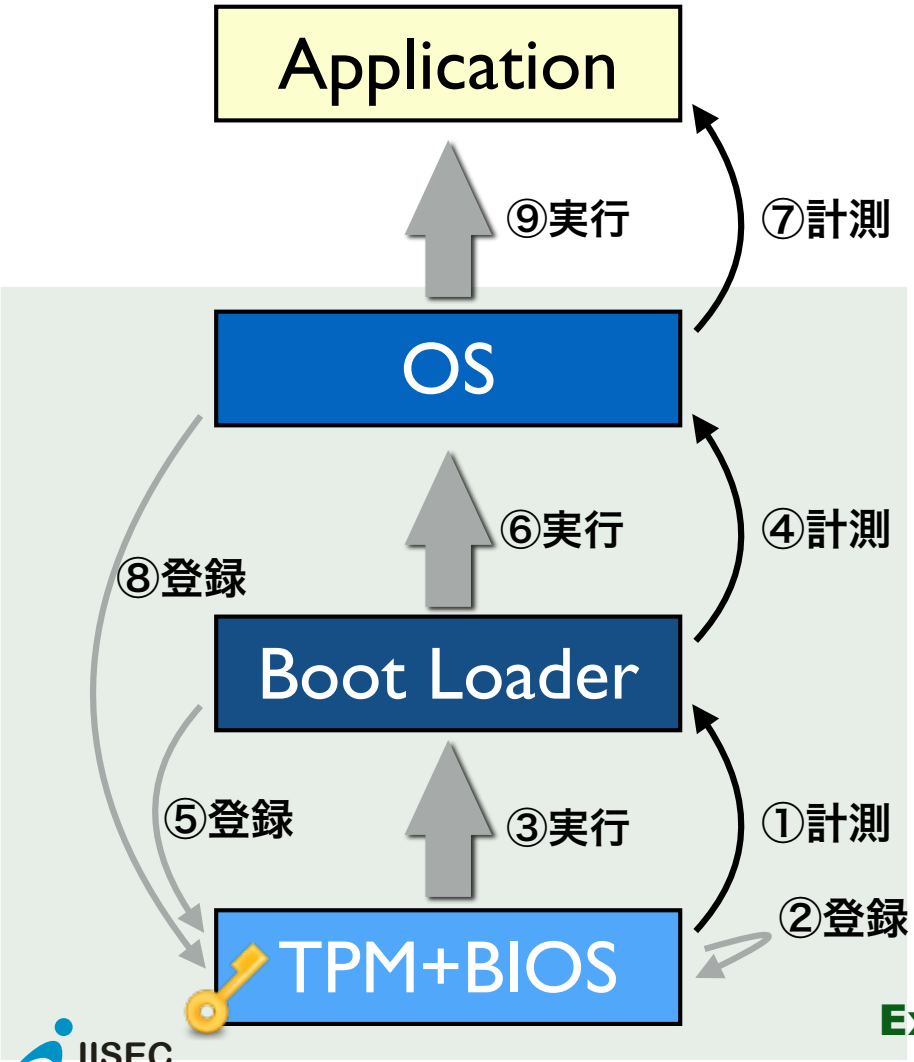


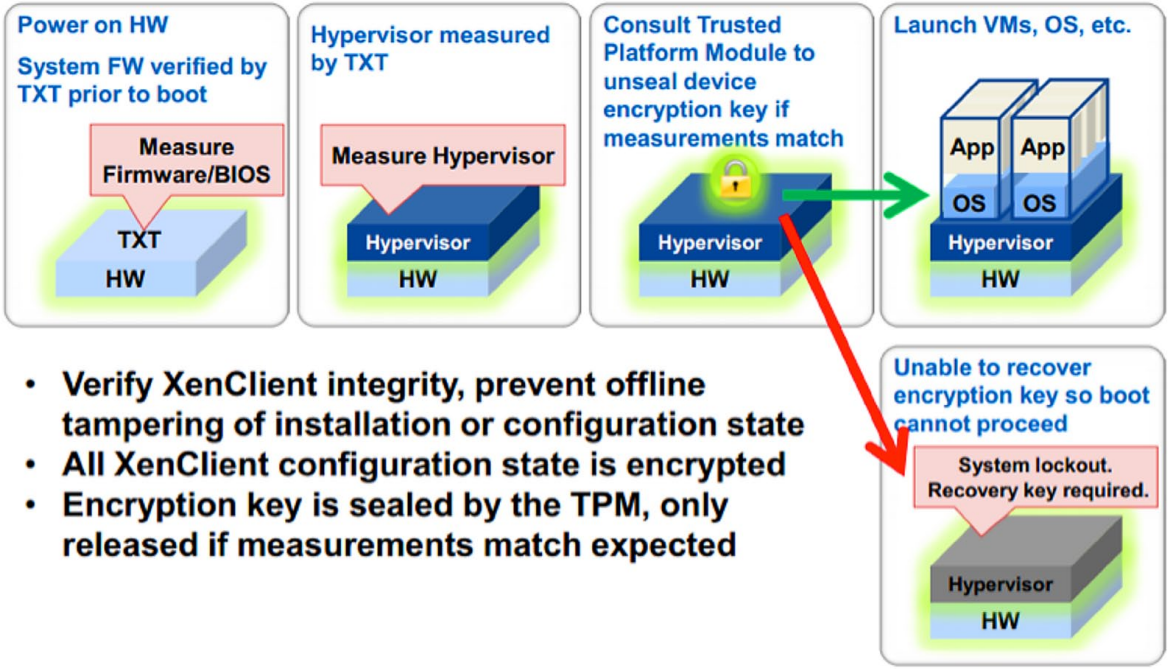
補足：セキュアブート機構 TPM (Trusted Platform Module)



Source) Infineon

ソフトウェアの真正性を検査するためのハッシュ値測定/格納機能,
およびRemote Atrtestationのための公開鍵暗号機能を有する耐タンパーチップ.





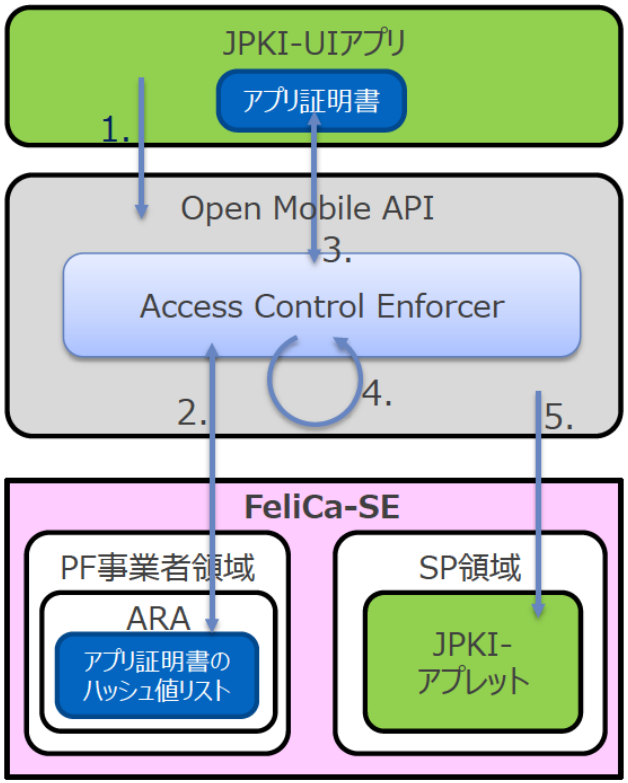
Source) Gal Sphantzer, “Implementing Hardware Roots of Trust: The Trusted Platform Module Comes of Age,” A SANS Whitepaper, June, 2013.

監視HW
Extension of Trust Chain

3.3 アクセス制御機構

【補足資料5】スマホアプリからのアクセス方式

【内容】
・FeliCa-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（JPKI-UIアプリ）のみがアクセス可能となっている。



【参考】Global Platform, 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FeliCa-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. JPKI-UI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FeliCa-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。

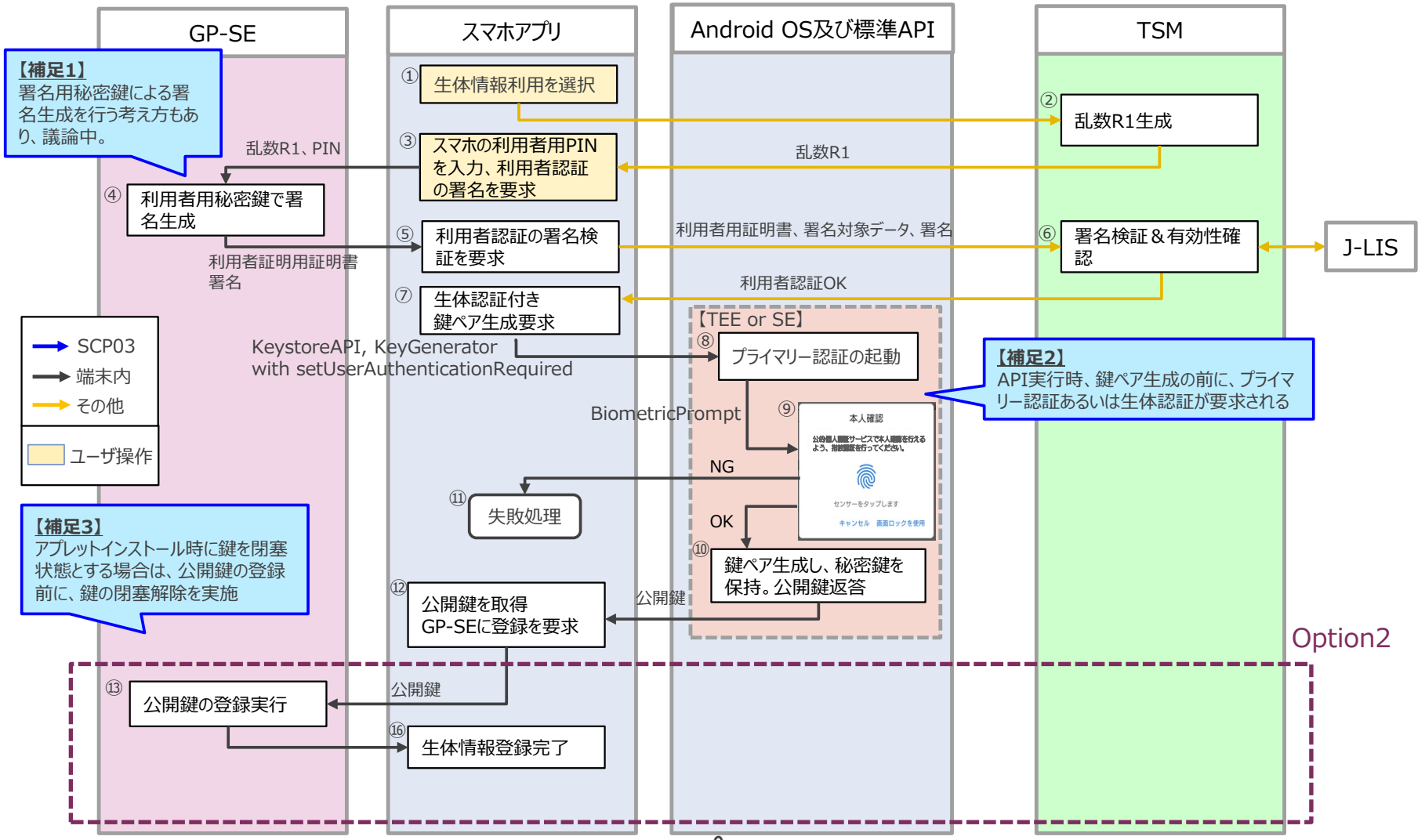
出所)総務省 マイナンバーカードの機能のスマートフォン搭載等に関する検討会 第1回資料.

- Global Platform規格により，SE(Secure Element)にアクセスできるアプリ(JPKI-UIアプリ)は，事前にARAに登録済みのアプリ証明書を持つものに限られる(=アクセス制御)
- このアクセス制御機構により，マルウェアによるSEへのアクセスを制限し，UI機能付きのSEのようにアプリとSEを連携させる.

3.4 生体認証によるPWの代替（...排除）

5. 生体認証＋外部認証（アクティベート時）の詳細フロー　Option2

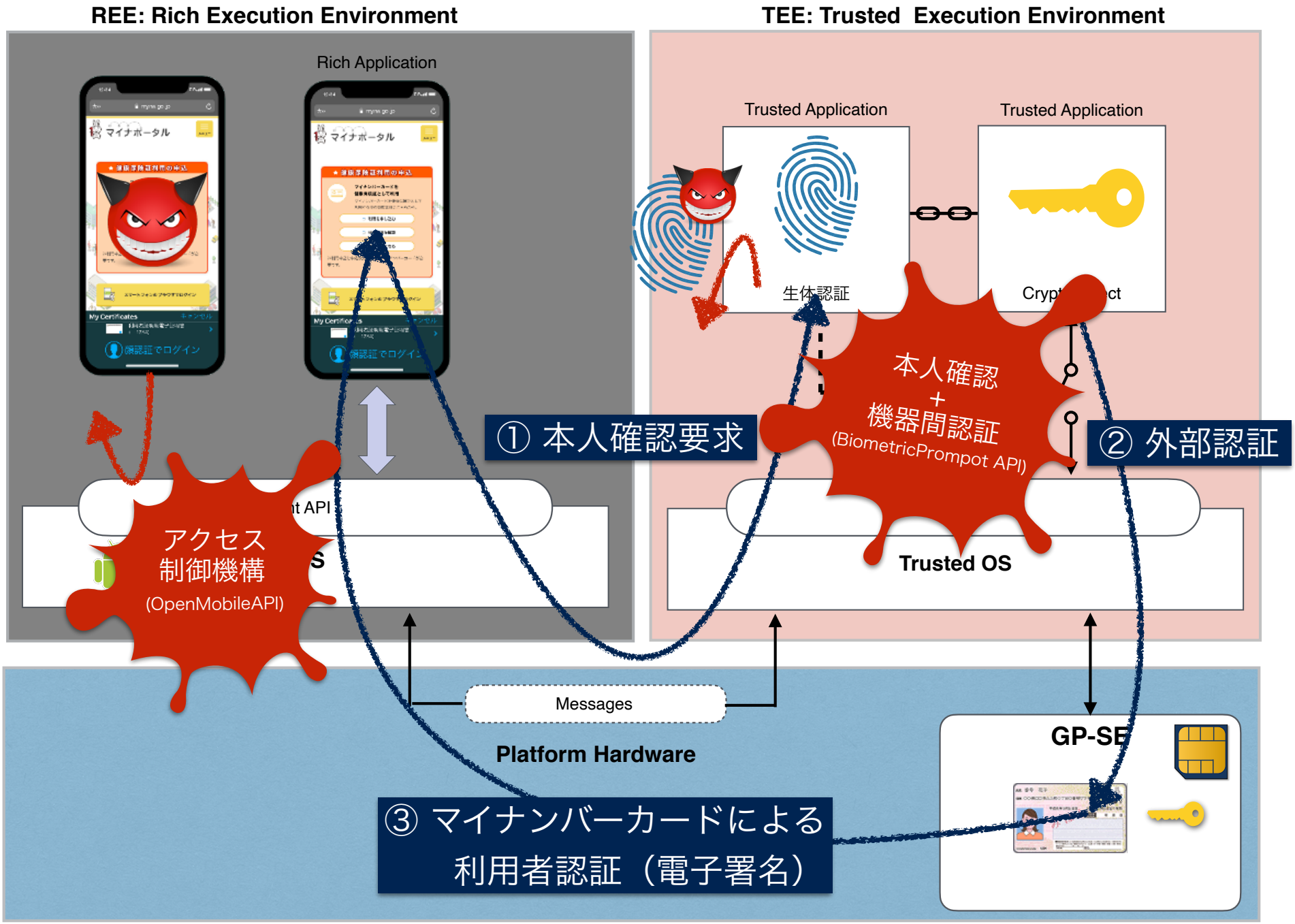
・生体認証の利用を開始するためのフローを以下に示す。



出所)総務省 マイナンバーカードの機能のスマートフォン搭載等に関する検討会 第5回資料.

- TEE内で生成した鍵ペア(Cryptographic Object)を生体認証と結びつける(BiometricPrompt API)
- GP-SEの認証／署名は，GP-SEが生体認証で起動されたCryptographic Objectの認証成功が条件

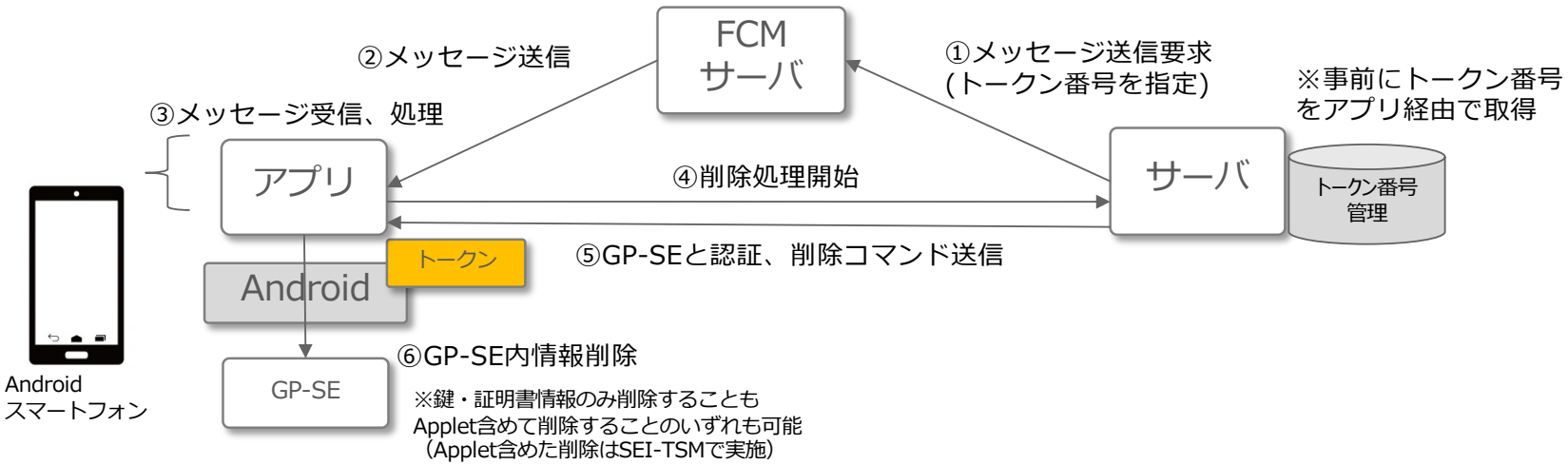
3.4 生体認証によるPWの代替（...排除）



3.5 盗難／紛失／譲渡時の対応

リモートでのGP-SE内の情報削除

- **サーバから要求を開始して、GP-SEにアクセスし、GP-SE内の情報を削除することが技術的に可能。**
- **Google社が提供するFCM（Firebase Cloud Messaging）という、サーバからスマートフォン上のアプリにメッセージを送信するサービスを利用する。**
- **スマートフォン1台毎に“トークン“と呼ばれるユニークな番号がFCMの仕組みで発番され、サーバはトークン番号をキーにメッセージを送信する。**
- **ユーザのアプリ操作なしに、サーバとアプリの通信で処理を行うことが可能。**
- **リモートでの処理が必ず成功することを保証するサービスではないため、削除ができないケースがありえる。**
  - スマートフォンがネットワーク通信できない場合はメッセージ送信が失敗する。
  - アプリの削除や端末の初期化が行われた場合や、あるいはその他の理由、トークンが削除されたり無効になった場合もメッセージ送信が失敗する。
  - その他の理由で、FCMサーバからのメッセージ送信は失敗するケースがあり得る。



出所)総務省 「第1次とりまとめ ～電子証明書のスマートフォン搭載の実現に向けて～」2020.12.25.

4. まとめと金融機関へのインプリケーション

5. まとめと金融機関へのインプリケーション

■スマートフォンのセキュリティ機能

- GP-SE = ICカード + UI + 通信機能
- 紛失時はリモート消去可能
- セキュアブート
- アクセス制御機構(OpenMobile API)
  =マルウェアによるGP-SEへのアクセスを阻止
- 生体認証でパスワードレス認証＝フィッシングリスク減

■金融機関へのインプリケーション

- マイナンバーカードのスマホ搭載で公共サービスが便利に！
- 金融機関（民間事業者）でもGP-SE領域を利用可能
  - オンラインで確実なeKYC(民間利用)
  - キャッシュカード／クレジットカードのスマホGP-SE化
  - CBDCのプラットフォーム