資料1

第2回検討会における指摘事項

令和2年12月23日

総務省　情報流通行政局　デジタル企業行動室

「カード機能のスマホへの搭載」に関する指摘事項

◆システム構成と初期発行フロー

① 格納媒体の名称は、Android-SEではなく、例えばGP-SEのように、より汎用的なものを提案したい。Android OSにおいてSEには2つの方法でアクセスすることができ、Androidのアプリ開発で従来から利用されてきたKeymasterをSEとする方法（StrongBox）と、GP準拠のOpen Mobile APIによってSEを扱う方法がある。本検討会の議論で指しているSEは後者で「Global platform-supported Secure Element」とも呼ばれるものであり、また「Android」はGoogle LLCの商標であることからも、分かりやすい名称の方がよい。

② スマホに搭載する証明書に設定するPINは、カードの署名用・利用者証明用パスワードと異なる値とするものか。また、PINの格納領域・フォーマットはどのようになっているか。

③ PINの設定フローにおいて仮PINが必要な理由は何か。それがTSMの管理者のみがPIN設定を管理できるようにするためであれば、TSM側からPINの閉塞解除のためにSCP03による接続を確立するので、仮PINは不要ではないか。仮PINがどのような脅威に対応するためのものか不明。

④ 今後PINロック解除のフローを設計すると思うが、その見通しを教えてほしい。

⑤ TSMの運用主体はどのような事業者で、どのように認定していくのかについて、検討状況を教えてほしい。例えば、J-LISが何らかの認定や監査を行うのか。

⑥ 現在の議論の方向性は全てマイナンバーカードを既に所持していることを前提として証明書をスマホに搭載していくというものだが、今後の流れとして、マイナンバーカードを持っていない人がスマホのみでJPKIを利用する方法は検討するのか。

⑦ 現在のマイナンバーカードだけで4種類のPINがあり、これらを十分に理解できてない利用者が大半。今回、途中で使う仮PINも含めて、新しくユーザーが意識するPINとパスワードはいくつあるのか、これらは全く別の値を設定しなければならないのか、それとも同じ値のものがあっても構わないという整理をするのかについて、それら名称の呼び分けも含めて、利用者から見て十分に理解できるような整理ができるのか、まとめて検討する必要がある。

⑧ 他者参入ついては、恐らくJ-LISが何らかの形で委託する形になると思うが、競争性を発揮できるような形での調達が行われないのは問題であるので、ベンダーロックインとならないように十分配慮してほしい。

⑨ CC認証について、以前はICカードやOSといったプラットフォームの部分とアプリの認証を別々に取得することを検討していたと思うが、今回はJPKIで使用するSEに関してトータルでコンポジットの認証を取得するということか。もしそうであれば、非常に好ましい。

⑩ CC認証の扱い方は産業分野によって違うものと理解している。ICカードなどの部品という意味ではCC認証を取得していることが多い。一方、モバイルのエコシステムは非常に速いスピード感があり、装置に組み込むことについてCC認証を取るというケースは実態として非常に少ないが、現状ではモバイルのエコシステムは機能している状況。そのため、どの部分についてコンポジットでCC認証を取得することが必須なのかについては、確認した方がよい。

⑪ 行政手続のオンライン化については、昨今のパンデミックによって海外動向への国民の関心が高いと思う。よく比較対象となるエストニアでは、SIMカード方式のモバイルIDの後にスマートIDが登場し、全てのスマートフォンで利用できるほか、マルチデバイスにも対応しており、とても使い勝手がよく見える。これらは当然eIDAS規則に準拠しており、QSCDについても最高レベルとなっているが、一方でなぜ日本では利用できるスマホが限定されるのかについて説明できるようにしておいた方がよい。様々なユースケースをスマホで実現したいというニーズがあり、高齢者も8割はスマホを保有しているので、今後健康保険証や運転免許証の実現が求められた時、非対応端末があることには様々な意見が出ると思う。

◆スマホ特有のライフサイクルへの対応

① PINの設定時にはTSMに接続してPINの閉塞を行うのに対して、PINの変更時にはTSMに接続する必要がない理由は何か。

② データ消去の方法は、完全に上書きしてデータの断片も残らないような消去をしているのか、WindowsにおけるFATの削除相当のことを行っているのみか。

③ PINの初期化フローが他人のスマホのPINを初期化できるようなものになっている。PINの初期化機能は本当に必要なのかという論点もあり、いたずらで何回も証明書を発行される可能性はあるが、PINを忘れたら再発行することでよいのではないか。

④ 紛失時の対応について、利用者証明用電子証明書はオンライン利用が前提なので、証明書が失効すると即時利用できなくなるが、署名用電子証明書についてはオフラインの利用が考えられており、失効管理だけでは何かトラブルになる可能性があるのではないか。ただ、証明書をスマホに搭載する場合、完全にオフラインで使うという場面があまり考えられない。例えば、署名を付与する前にJ-LISで証明書の有効性を確認し、その後J-LISからアプリケーションに対して外部認証することを必須とし、外部認証がなければ署名を付与できないという仕組みとすれば、証明書失効後に署名が付与できないことを技術的に担保できるのではないか。

「生体認証の活用・FIDO認証の適用」に関する指摘事項

◆生体認証の活用

① 現在のJPKIの機能はマイナンバーカードに搭載されているが、そのチップの中のOSやアプレットについて、J-LISが定めたPPに対するCC認証を受けたチップをJ-LISが調達している。今と同じような形でJ-LISが責任を持って運用できるようにするには、J-LISが生体認証のロジックの部分のみならず、そのロジックがどこで動いているかなども含めて、それぞれのスマートフォンでどう第三者評価を受けているのかという情報を開示してもらうことが必要ではないか。

② 現在のマイナンバーカードやSEについて、J-LISが第三者評価を受けたチップ等を調達するという形になっており、J-LISの責任において運用管理することになっている。一方、パスワードの管理については、JPKIの運用管理規定（CP/CPS）において利用者に適切な管理を求めることとされている。そのため、何か問題が生じた時に、J-LISと利用者の間で責任を切り分けることは現実的には可能。しかし、生体認証の場合にはスプーフィング攻撃のようななりすまし攻撃の可能性が考えられ、認証が成功してしまった場合の責任の所在については難しい課題。なりすましが発生した時に端末メーカーに責任を負わせたり、生体情報の適切な管理を利用者に義務づけたりすることは難しく、誰がどう責任を取るのかという責任分界について議論しなければならない。

③ 生体認証の導入は、パスワードがたくさんある状態をどのように便利にできるかというところから始まった取組であり、品質を担保すべきなのか、より多くの利用者が便利に利用できるためにどうしたらよいか、という課題に対する1つの答えが、グローバルなアライアンスの中でスマホのエコシステムを主導している者との協調であった。そのため、マイナンバーカードが積み上げてきたことは尊重すべきであるが、既存の運用管理の方法だけで、例えばスマホに搭載する証明書用に新たなPINを設けるといった課題を解決できるのか、それともスマホのエコシステムと調和すべき部分があるか、という点について議論すべき。その議論ができると、責任分界についても少しずつ整理整頓できるのではないか。

④ スマホの生体認証ではSARが7%以下と高く、本人が知らないうちに電子署名を付与されてしまう可能性は一定程度あるため、生体認証を利用した場合のデジタル署名は、電子署名法第3条の固有性の要件を満たさず、法的な裏付けのある電子署名としては認められないのではないか。日本ではEUのように保証レベルがきちんと議論されていないため、生体認証を使う場合には、例えばEUにおける認証レベルや適格電子署名・先進電子署名のうちどれに当たるかといった議論をした上で、電子認証・電子署名に対して生体認証をどう使うのかを時間をかけて議論した方がよい。

⑤ 電子署名法第3条の固有性の要件というのは、実際に「符号及び物件を適正に管理する」ということではなく、仮にこれらを安全に管理していれば他人が署名することはできないということであると考えられている。生体情報で鍵のロックを解除することは利用者における鍵管理の問題になるので、固有性の要件とは切り離して考えた方がよく、利用者が秘密鍵を適正に管理していなかった時・管理できなかった時については、電子署名法第3条では言及されていない。

⑥ FARが0.002%の時、FRRはどの程度か。

⑦ 生体認証の導入当初は、FRRの目標値は1%前後の値であったと記憶する。これは生体認証装置の部品としての性能だけでなく、装置として組み込んだ場所の問題があり、コーティング・カラーリングの影響も受ける。最近では改善が図られ、大きな議論にはなっていない。

◆FIDO認証の適用

① FIDO認証は金融業界でも大幅に導入が進んでいるが、FIDO認証を起因とした不正送金等については聞いておらず、従前のワンタイムパスワード等と比べても大幅にユーザビリティが改善され、アプリのアクティブユーザーは非常に増えている。特に国が提供するサービスではユニバーサルアクセス、誰からでも利用できることは非常に重要な点であるので、検討する必要がある。本検討会の最初のマイルストーンが公的個人認証法の改正内容を年内に固めることである一方、マイナポータルをはじめとした政府のウェブサイトのユーザビリティの改善については菅首相や平井デジタル改革担当相からも非常に強く求められているため、年明け速やかに、可能であれば次期IT戦略が決定されるまでの来年前半の早い時期へ向けてしっかりとした整理が必要。既に世界では台湾、韓国、エストニアにおいて類似のものが利用されており、EUのeIDAS規則における整理によっては署名への利用はハードルが高く、リモート署名との組合せ等の議論になると思うが、スマートフォンの中に認証器として搭載する場合の技術要件等も含めて、諸外国を参考とした整理が必要。

② 現在、市役所の窓口等で一番問題になっているのは、電子証明書の期限が切れて来訪した高齢者のほとんどがPINを忘れている状況であると聞いている。これを踏まえて、提案のあったFIDO認証などをうまく活用することによって、マイナンバーカードの持っている機能を補完することができるのではないか。前回の検討会でもサービスモデル戦略を並行して考えていくべきと発言したが、やはり、今後利用者がより使いやすいモデルを使っていく中で様々な認証方式を並行して議論をしてほしい。