様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　６　月　　５　日現在

機関番号：　１２６０８
研究種目：　挑戦的萌芽研究
研究期間：　2015～2016
課題番号：　１５Ｋ１２４５８

研究課題名（和文）次世代公的認証サービスのプライバシー及び安全性向上に関する研究

研究課題名（英文）A study on safety and privacy improvement of JPKI services

研究代表者
小尾　高史（Obi, Takashi）

東京工業大学・科学技術創成研究院・准教授

研究者番号：４０２８０９９５

交付決定額（研究期間全体）：（直接経費）　　2,600,000円

研究成果の概要（和文）：公的個人認証サービス（ＪＰＫＩ）に対して，新たに電子利用者証明サービスが追加されたが，　1つの公開鍵証明書を利用することによるプライバシーの侵害につながる可能性や，不正にインストールされたマルウエアによりサービス利用時のデータ書き換えなどが発生する可能性が指摘されている．本研究では，JPKIを安全安心に民間分野のサービスで利用可能とするために必要となる，利用者のプライバシーに配慮した利用者を識別するＩＤ番号をサービス機関が個別に発行する仕組みの提案，マルウエア等からのＪＰＫＩ利用端末で受けるサービスの保護について検討及びプロトタイプ開発を行った．

研究成果の概要（英文）：A user authentication service was added to the new JPKI. However, it is pointed out that there is a possibility of invasion of privacy by using one public key certificate, and the possibility that data rewriting etc. at the time of using the service may occur due to malware installed to a web browser. In my research, I proposed a mechanism that service provider issue an individual ID numbers that identify users who take into consideration the privacy of users and protection method of services using JPKI from malware etc..

研究分野：　社会情報システム

キーワード：　公的個人認証サービス　電子認証　プライバシー保護　ＴＥＥ

１．研究開始当初の背景

税・社会保障に関わる番号制度で設置されるポータルサイトでの利用を目的とし，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（JPKI）には，新たに電子認証（電子利用者証明）機能が追加された．「世界最先端 IT 国家創造宣言」に記載されるように，電子認証機能は，行政機関での利用にとどまらず，多くの民間事業者に広がることが想定されているが，その反面，様々な場面で１つの公開鍵証明書を利用することによるプライバシーの侵害につながる可能性や，ブラウザ内に不正にインストールされたマルウェアにより電子認証利用後のサービス利用時のデータの書き換えなどが発生する可能性が指摘されている．

２．研究の目的

新たに発行される JPKI の電子認証用公開鍵証明書は，必要以上に個人情報を与えないよう証明書内に，氏名，生年月日，性別，現住所などの個人の特定が可能な情報を記載せず，証明書のシリアル番号の告知要求なども制度として禁じている．これら対策はプライバシー保護に対して一定の効果を上げると想定されるが，海外からの攻撃など，国内の制度では十分に機能しない面も予想される．また，電子認証用公開鍵証明書には生年月日などが記載されないため，例えば成人を対象としたサービス提供時の年齢確認などには利用できない．さらに，近年，金融決済などをターゲットとして，Web ブラウザから正規の認証プロセスを経てログインした後に，マルウェアがブラウザを乗っ取り，サーバに送信される決済データを書き換えることで不正な送金等を行う Man in the browser（MITB）という攻撃が確認されている．この攻撃では，Web ブラウザを不正に操るため，PKI を用いた安全性の高い認証手段を利用してもブラウザ上に表示される情報の正当性担保や，クライアントとサーバ間でやり取りされる情報の正確性を担保することができず，今後，JPKI の利用分野が民間，特に金融分野，医療分野へ拡大された場合には，提供されるサービスの安全性を十分確保できない可能性がある．

これに対して，本研究では，JPKI の新たな機能として，プライバシーに配慮したアイデンティティ（個人識別番号だけでなく，住所、年齢などの情報や資格情報などの本人と結びつく属性を指す）の管理・利用の仕組みを開発するとともに，現在多くのプロセッサが有しているセキュア実行領域を利用する Trusted Execution Environment(TEE)機能を用いることで JPKI を利用する端末の安全性を担保する仕組みを開発し，マイナンバーカードのみで安全かつ安心して民間分野のサービスを利用可能とする仕組みの検討を目的とする．

３．研究の方法

(1)プライバシーに配慮したカード ID の生成

マイナンバーカードに搭載されている JPKI には，以前我々が開発した機関認証に基いて電子利用者証明機能を利用する仕組みが搭載されている．機関認証後の利用者証明時には，地方公共団体情報システム機構が発行する機関認証用証明書に記載された機関コードを用いた署名コード生成が行われるため，サービス機関固有の ID との組み合わせで署名コードを生成すれば，当該機関コードを有している機関のみが一意に利用者を特定可能な ID の生成が可能となる．

ID の生成には機関毎に異なる証明書記載の機関コードが必要であることから，ID を利用する機関の特定機関認証用公開鍵証明書との組み合わせでのみ，同一の ID を生成することができる．このため，JPKI 利用機関では，利用者との紐づけに，証明書記載のシリアル番号や CommonName ではなく，この ID を利用することにより仮にデータベース等が漏えいした場合でも，利用者の特定を困難にすることが可能となる．

(2)JPKI 利用時の安全性確保

本研究では JPKI のさらなる利用の拡大のために，スマートフォン１台でトランザクション認証を行うシステムを提案した．一般に，外部デバイスを用いずに，１つのデバイスでトランザクション認証を行うにはハードウェアトークン(外部デバイス)の代わりにソフトウェアトークンが必要となる．外部デバイスを用いる場合には，使用している端末がマルウェアに感染していてもその影響を受けることはないが，ソフトウェアトークンの場合には，マルウェアの影響を受ける可能性がある．そこで，同一デバイスでもマルウェアの影響を受けないようにするために，機密な情報を扱うアプリケーションと，そうでない情報を扱うアプリケーションを用意する必要があり，本研究では TEE 技術を用いることとしている．

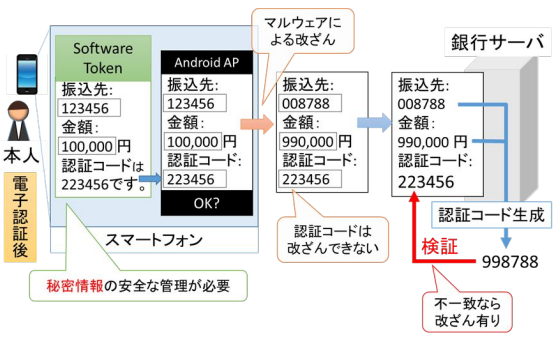

図１．ソフトウェアトークンによるトランザクション認証

図１は JPKI による利用者証明を終えた本人が，スマートフォン単体でオンラインバンキングを利用して，振込を行う様子を表している．利用者のスマートフォンにはオンライン

バンキング用の Android アプリケーションがダウンロードされており，振込を行う際にソフトウェアトークンとなるアプリケーションを呼び出している．本研究では，このソフトウェアトークンを TEE 内で動作する Trusted Application(TA)にょり実装する．例えば，利用者が振込先の口座番号と振込金額を Android アプリケーションへ入力すると，Android アプリケーションが TA を呼び出し，口座番号と振込金額を引数として渡す．これらを受け取った TA は事前に共有しておいた秘密情報を基に認証コードを生成して Android アプリケーションへ返す．そして，Android アプリケーションは振込先の口座番号と振込金額，認証コードを銀行サーバへ送信する．最後に，銀行サーバは，送られた認証コードが改ざんされていないことを確認する．この時，仮に使用しているスマートフォンがマルウェアに感染しており入力内容(口座番号と金額)が改ざんされた場合でも，TA により生成する認証コードの改ざんは行えない．

このようなトランザクション認証では，認証コードを生成するために利用者と銀行が共有する秘密情報の共有方法が重要となる．例えば，銀行が秘密情報を生成して利用者と共有する場合，ハードウェアトークンを用いる場合は郵送によって安全に共有することができるが，ソフトウェアトークンを用いる場合は電子的な手段での共有が望ましい．一方で利用者が秘密情報を生成し，銀行と共有する場合は，秘密情報の正当性が問題となる．

本研究では TEE 内の TA を用いて利用者側で秘密情報を生成する．その際，悪意のあるソフトウェアが正当な TA のように振る舞い，偽の秘密情報を生成できないよう，アプリケーション利用登録時に別端末を用いる手法を提案した．

4．研究成果

本章では，本研究で提案するシステムの具体的な処理フロー及び実装結果を示す．

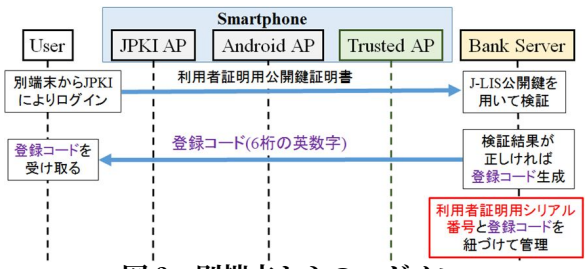

図 2．別端末からのログイン

(1)初期設定

提案システムでは初期設定時に別端末からログインを行い，利用者は，登録コードを入手する．なお，図 2 の User は，オンラインバンキングの利用者を意味し，JPKI AP はマイナンバーカード又は SIM カード内に格納されている電子利用者証明機能を持った JPKI アプリケーションを意味し，Android AP は Android アプリケーション，Trusted AP は TEE 内にある TA をそれぞれ意味する．登録コードは銀行が生成し，利用者へ別端末に送信することで共有する．この登録コードは利用者が目視で確認し，入力する必要があるので，6 桁程度の英数字を想定する．また，利用者証明用の公開鍵証明書に含まれている利用者証明用シリアル番号と登録コードを紐づけて管理することで，銀行は登録コードがどの利用者のものであるか知ることができる．

(2)秘密情報の共有

利用者証明完了後は，登録コードの検証及び秘密情報の共有を実施する．

最初に，アプリケーションをインストールする． アプリケーション内には銀行の公開鍵証明書が入っており、アプリケーションインストール後に TA が銀行の公開鍵を使用できるものとする。アプリケーションを起動し、まず JPKI による利用者証明を実施する．利用者のスマートフォンによる JPKI を利用したオンラインバンキング利用の為の本人確認が完了すると，秘密情報の共有処理に移る．

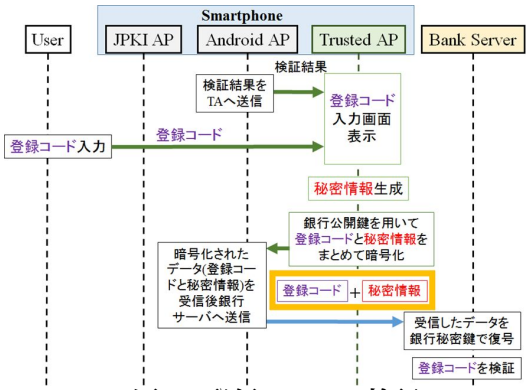

図 3．登録コードの検証

まず，図 3 に示す様に，TA は登録コード入力画面を Secure Display に表示し，利用者に入力を要求する．登録コードは使用端末がマルウェアに感染している場合でも，利用者が TA に直接入力を行うことで盗聴される危険性を無くすことができる．そして，登録コードが入力されると，TA はトランザクション認証で用いる認証コードを生成する為の秘密情報を生成する．認証コード生成のために HMAC-SHA256 を用いるので，TA が生成する秘密情報は，利用者と銀行サーバの間で「共有する鍵」になる．

次に，TA により，登録コードと秘密情報を合わせて銀行の公開鍵で暗号化し，Android アプリケーションを介して銀行サーバへ送信する．銀行サーバは，銀行の秘密鍵でそれを復号し，登録コード及び秘密情報を得る．また，登録コードから利用者を特定する．

次に，この登録コードの検証結果を Android アプリケーションへ返すことにより，秘密情報の共有処理を終了する．

まず，銀行サーバで登録コードの検証結果

をメッセージ本体として，先に入手した秘密情報を基に，HMAC-SHA256 を用いて認証コードを生成し，この認証コードと検証結果を Android アプリケーションへ送信する．
Android アプリケーションは，これを TA へ渡し，TA は受け取った認証コードを検証する．検証成功した場合には，銀行サーバと TA の間で秘密情報が共有できたことになる．

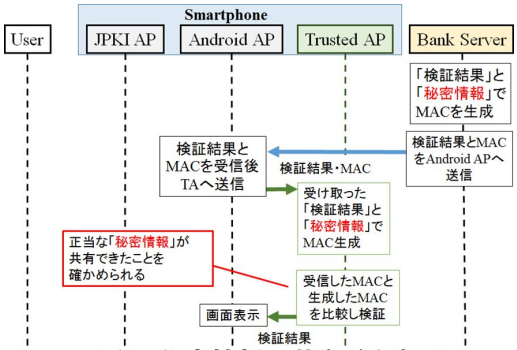

図 4 秘密情報の共有確認処理

(3)利用時処理
利用者のログインは，Android アプリケーションがログイン画面を表示し，利用者が PIN を入力することで利用者証明を行う．そして，正当に利用者証明が完了すると銀行サーバから利用者証明書に紐づいたサービス情報(預金残高等)が提供される．

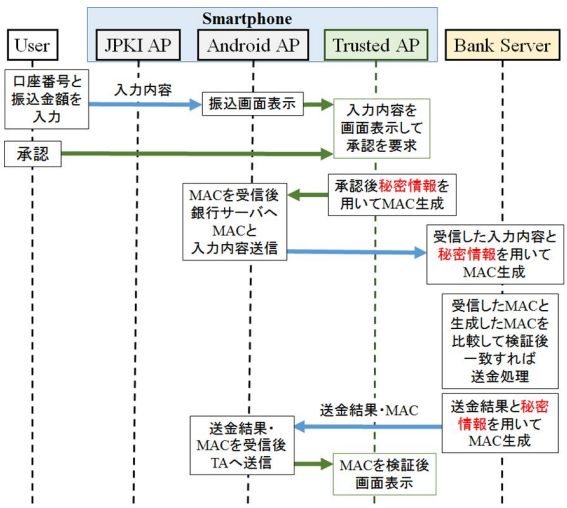

図 5 振込時の処理

振込処理時には，まず Android アプリケーションが振込画面を表示し，利用者が振込先口座番号と振込金額を入力すると，これら情報は Android アプリケーションから TA へ渡される．TA は Android アプリケーションから受け取った入力内容(振込先口座番号と振込金額)を Secure Display に表示し，利用者に確認を求める．利用者に入力内容が承認されると，TA は秘密情報を用いて入力内容に基づいた認証コードを生成する．そして，その認証コードを Android アプリケーション経由で銀行サーバへ送信する．
銀行サーバは受け取った入力内容をもとに，認証コードを検証する．検証が成功すれば，送金処理を行う．送金処理の結果についても，秘密情報を用いて認証コード生成し，Android アプリケーションを経由して TA へ返すことで，利用者へ確実に正しい結果を伝えることができる．

(4) システムの実装と評価
提案システムの実現可能性を評価するために，デモシステムを Linux 上の ARM のエミュレータである QEMU 及び Linaro が公開する ARM 用 TEE である OP-TEE を用いて実装した．また，各アプリケーションで用いる TEE 用のコマンドは GlobalPlatform の仕様を用いて実装した．
具体的には，提案システムの一部であるトランザクション認証を，TEE を用いて安全に実行できることを確かめる為のデモシステムを構築した．具体的には，オンラインバンキングにおいて送金する際の，送金先の口座番号と送金額を TA へ送り，TA がそれらの入力内容を基に HMAC を生成して表示するアプリケーションを作成した．以下に，実験システムの流れを述べる．
まず，アプリケーションを起動させ，送金先の 6 桁の口座番号と 3 桁の送金金額の入力を利用者に求める（図 6）．

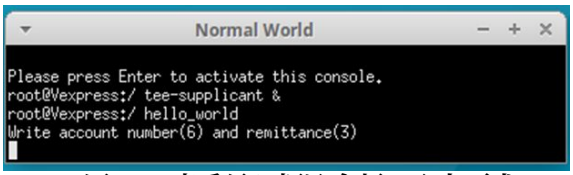

図 6 口座番号と振込金額の入力要求

口座番号と送金金額を入力すると，その情報が認証コードを生成するために TA に送られる．(図 7)

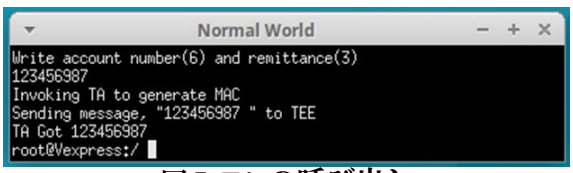

図 7 TA の呼び出し

そして TA は，入力情報を受け取り，認証コードを生成する．

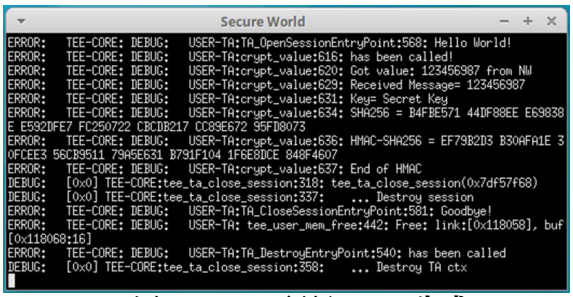

図 8 TA での認証コード生成

図 8 の上から 3 行目と 4 行目から，アプリケ

ーションに入力された数値を TA が受け取っていることが分かる．TA は数値を受け取った後，そして，受け取った情報に対して秘密情報を用いて HMAC-SHA256 の鍵付きハッシュ関数を適用し，認証コードを生成する．今回は実験のため，秘密情報に何を用いたかが分かるように，コンソール画面の上から 5 行目に示すように秘密情報を画面表示している．
このように，オンラインバンキングにおける送金時を想定し，提案システムの一部であるトランザクション認証を，TEE を用いて安全に実行できることを確認した．これにより，JPKI 利用時の安全性を向上できた．
　現時点では，実現が難しいが，TA が直接マイナンバーカード（JPKI アプリケーション）と通信できる場合には，TA に直接，利用者証明機能を利用するための PIN 入力を行うことができるため，TA の正当性を容易に確認できる可能性がある．この場合，初期登録時のシーケンスにおいて，別端末が不要になると考えられるため，更なる利便性の向上の為に，TA と JPKI アプリケーションが直接通信できる可能性や他の手法についても検討していく必要がある．

５．主な発表論文等

〔学会発表〕（計２件）

① Takashi Obi, Japan e-ID Card go to the next stage, World e-ID and Cybersecurity, 2016.9.27, Marseille (France).
② 山根拓人，鈴木裕之，大山永昭，小尾高史，トラステッド実行環境を用いた公的個人認証サービス利用時の安全性向上に関する研究，2017.3.23，2017 電子情報通信学会総合大会，名城大学（名古屋市）.

〔その他〕
第 7 回社会情報流通基盤研究センター・シンポジウムホームページ
http://asist.ssr.titech.ac.jp/wp-content/uploads/699471b4910b56e4ad3469b8f786b814.pdf

６．研究組織

(1)研究代表者
小尾 高史（OBI, Takashi）
東京工業大学・科学技術創成研究院・准教授
研究者番号：40280995