認　証　報　告　書

東京都文京区本駒込2丁目28番8号
独立行政法人情報処理推進機構
理事長　齊藤　裕

原紙押印済

プロテクションプロファイル（PP）

申請受付日（受付番号）	令和7年8月4日（IT認証5919）
認証識別	JISEC-C0859
プロテクションプロファイル名称／識別	JPKI Applet Protection Profile
プロテクションプロファイルバージョン番号	1.10
プロテクションプロファイル開発者	デジタル庁
プロテクションプロファイルスポンサー	デジタル庁
保証要件適合	EAL4 及び追加の保証コンポーネントALC_DVS.2、AVA_VAN.5 COMP
ITセキュリティ評価機関の名称	株式会社ECSEC Laboratory 評価センター

上記のPPについての評価は、以下のとおりであることを認証したので報告します。
令和8年2月25日

セキュリティセンター 技術評価部
技術管理者　橋本 徹

評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。

① Common Criteria for Information Technology Security Evaluation CC:2022 Release 1
② Common Methodology for Information Technology Security Evaluation CEM:2022 Release 1
③ Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1) Version 1.1

評価結果：合格

「JPKI Applet Protection Profile、バージョン 1.10」は、独立行政法人情報処理推進機構が定めるITセキュリティ認証等に関する要求事項に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

この認証報告書は、デジタル庁が開発した「JPKI Applet Protection Profile、バージョン 1.10」（以下「PP[11]」という。）について株式会社 ECSEC Laboratory 評価センター（以下「評価機関」という。）が令和 8 年 1 月 30 日に完了した IT セキュリティ評価に対し、その内容の認証結果を申請者であるデジタル庁に報告するとともに、PP[11]に関心を持つ調達者や消費者に対しセキュリティ情報を提供するものである。

本認証報告書の読者は、本書と共に、対応する PP[11]を併読されたい。特に PP[11]に適合する TOE のセキュリティ機能要件、保証要件及びその十分性の根拠は、PP[11]において詳述されている。

本認証報告書は、PP[11]に適合した製品開発を行う開発者及び製品調達者を読者と想定している。本認証報告書は、PP[11]に対する保証要件に基づいた認証結果を示すものであり、個別の IT 製品そのものを保証するものではないことに留意されたい。

1.1 評価PP

PP[11]が要求するセキュリティ機能の概要を以下に示す。詳細は 2 章以降を参照のこと。

1.1.1 保証パッケージ

PP[11]において要求される保証パッケージは、EAL4 及び追加の保証コンポーネント ALC_DVS.2、AVA_VAN.5 と COMP である。

また、PP[11]への適合を主張する PP、及び ST は正確適合を主張しなければならない。

1.1.2 PP概要

PP[11]において、TOE は携帯電話（Mobile Phone）内の組込みセキュアエレメント（eSE）である。

TOE は、署名生成とユーザ認証のための、鍵生成機能つきの Secure signature creation device (SSCD) を提供する Java Card システムとして動作する。TOE は JPKI Applet、Java Card platform、及び Integrated Ciruit (IC) から構成される。IC と platform は別個に認証される。IC と Java Card platform 上で動作する JPKI Applet はコンポジット認証の対象となる。

図 1-1 に TOE の構成を示す。TOE は図の黄色の部分である。

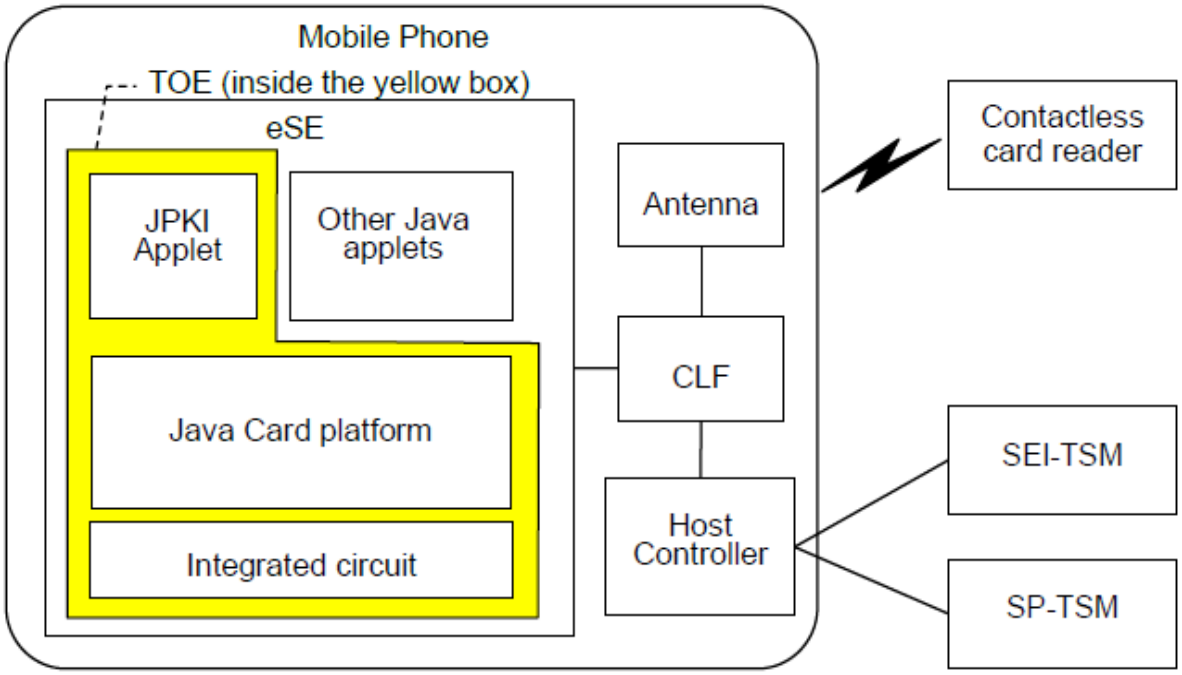

図 1-1 TOE Physical Scope

TOE のコンポーネントは以下のものである。

- JPKI Applet は、署名生成とユーザ認証のための鍵ペア生成を担う TOE の部分を構成する。これは署名生成機能の使用のアクセスコントロールと、署名生成のための暗号演算実行のアクセスコントロールを管理する。JPKI applet は運用環境において post-issuance としてインストールされる。
- Java card platform は applet を管理及び実行する。Java Card 仕様に従って API を開発するための API を提供する。Java card platform は GlobalPlatform 仕様[14]に従ってセキュアな方法でスマートカードとの通信及びアプリケーションを管理する共通のインタフェースを提供する GlobalPlatform パッケージを持つ。
- IC は TOE のハードウェアプラットフォームである。ハードウェアプラットフォームは基本的な暗号機能と、TOE を防御するためのセキュリティに関する検出器、センサー、回路を提供する。

非 TOE コンポーネントは以下のものである。

- 他の Java applet は JPKI Applet と共存できるが、互いに独立している。
- アンテナは非接触カードリーダとの通信のため電波を送受信するために使用される。

- CLF (Contactless Front-end) はアンテナと Host Controller の間のルーティングを管理し、アンテナの搬送波の伝送を制御し、カードの機能として、衝突を防止してカードを取得する。
- TOE は携帯電話上で動作することが想定されている。したがって、上記の非 TOE コンポーネントも携帯電話の一部である。

1.1.2.1 セキュリティ機能概要

PP[11]では、JPKI Applet を搭載する eSE に求められるセキュリティ機能と、IC として標準的に求められる機能を TOE に要求する。その主要なものを以下に示す。

(1) 通信データ保護

TOE と Certificate generation application (CGA) との間の通信に対してセキュアメッセージング機能を適用し、通信データの機密性及び完全性を保護する。

(2) 利用者認証とアクセス制御

TOE は、利用者の役割に応じた機能を提供するため、利用者の識別・認証を行い、アクセス制御を実施する。

(3) 暗号演算

TOE は、ハッシュ関数、Secret Key (SK) / Public Key (PK) の生成、署名生成/検証の暗号機能を提供する。

(4) 物理的攻撃への対抗

TOE のセキュリティ機能は、自身のハードウェア部分への物理的攻撃にも対抗する。想定される攻撃は、一般の IC と同様である。

1.1.2.2 脅威とセキュリティ目標

PP[11]に適合する TOE は、以下のとおりのセキュリティ機能によりそれぞれの脅威に対抗する。

攻撃者は TOE 内部のデータの開示や改変や、TOE の機能を不正に使用するための不正アクセスを試みるかもしれない。そこで、TOE は、利用者を識別・認証した上で、その利用者の役割に対応した権限の範囲で TOE 内部への論理的アクセスを許可する。

また、TOE と外部端末との通信において、外部認証に対応した通信内容を傍受・記録し、その内容を再利用することで、正規の外部端末になりすます脅威が考えられる。そこで、この脅威に対抗するため、外部認証に使用する認証データ（この生成を TOE が担う）を再利用せず、毎回異なるデータを使用することを要求する。

IC チップのハードウェアは、その物理形態の特性上、内部で処理している情報を、消費電力や放射電磁波を通じて漏えいする可能性がある。また、物理的なプロービングによる IC チップ内部の情報の暴露、IC チップ上の回路の物理的な改ざん、環境ストレスの印加による誤動作を考慮する必要がある。そこで、こういった物理攻撃から TSF を保護する機能を要求する。

1.1.3 免責事項

なし。

1.2 評価の実施

認証機関が運営する IT セキュリティ評価及び認証制度に基づき、公表文書「IT セキュリティ評価及び認証制度の基本規程」[1]、「IT セキュリティ認証等に関する要求事項」[2]、「IT セキュリティ評価機関承認等に関する要求事項」[3]に規定された内容に従い、評価機関によって PP[11]に関わる機能要件及び保証要件に基づいて IT セキュリティ評価が実施され、令和 8 年 1 月に完了した。

1.3 評価の認証

認証機関は、評価機関が作成した評価報告書[12]、所見報告書、及び関連する評価証拠資料を検証し、PP[11]の評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。認証機関が指摘した問題点は、すべて解決され、かつ、PP[11]の評価が CC（[4][5][6][7][8]）及び CEM（[9]）、及び補助文書（[10]）に照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

2 PP識別

PP[11]は、以下のとおり識別される。

PP名称：	JPKI Applet Protection Profile
バージョン：	Version. 1.10
開発者：	デジタル庁

3 セキュリティ方針

本章では、PP に適合する TOE が脅威に対抗するために採用したセキュリティ機能方針や組織のセキュリティ方針を説明する。

PP[11]では、JPKI applet が提供するサービスに求められるセキュリティ機能と、IC として標準的に求められるセキュリティ機能を TOE に要求する。TOE に要求されるセキュリティ機能は、大きく次の 4 つである。

- 通信データ保護
- 利用者認証とアクセス制御
- 暗号演算
- 物理的攻撃への抵抗

3.1 セキュリティ機能方針

PP[11]では、3.1.1.1 に示す脅威に対抗し、3.1.2.1 に示す組織のセキュリティ方針を満たすセキュリティ機能を具備する。

3.1.1 脅威とセキュリティ機能方針

3.1.1.1 脅威

PP[11]は、表 3-1 に示す脅威を想定し、これに対抗する機能を TOE に要求する。

表3-1　脅威

識別子	脅威
T.Illegal_Attack	認証されていないユーザがTOEに外部インタフェースを介してアクセスし、TOEの内部データの開示または変更を行う、またはTOEの処理機能を使用することを試みる。認証されていないユーザとは、TOEの資産にアクセスするための認証データを持っていないエンティティを意味する。
T.Replay	攻撃者が、TOEと外部端末の間の認証手順をモニタリングして記録し、それを再現することによって正当な外部端末になりすまし、TOEの認証を通過させようとする。この攻撃はTOEのユーザデータの開示または変更、TOEの処理機能の不正な利用を引き起こす。

識別子	脅威
T.Phys_Attack	攻撃者はTOEのコンポーネント（ハードウェア、ファームウェア、ソフトウェア）を物理的手段で攻撃する。この攻撃はTOEのユーザデータの開示または変更、TOEの処理機能の不正な利用を引き起こす。

3.1.1.2 脅威に対するセキュリティ機能方針

PP[11]に適合する TOE は、表 3-1 に示す脅威に対し、以下のセキュリティ機能方針で対抗する。

⑴ 脅威「T.Illegal_Attack」及び「T.Replay」への対抗

脅威「T.Illegal_Attack」は、TOE のインタフェース経由で TOE 内部のデータ、及び機能に不正アクセスされることを想定している。また、「T.Replay」は外部端末との通信における認証手順を再利用して TOE に不正アクセスすることを想定している。

これらの脅威に対して、TOE ではユーザの識別・認証を行い、認証に成功した場合に、ユーザの役割に応じた操作を許可する。また、認証データの再利用を防止する機能を提供する。

⑵ 脅威「T.Phys_Attack」への対抗

脅威「T.Phys_Attack」は、IC という物理形態という特性上、物理的な改ざん（観察、分析、あるいは改変）にさらされる。また、TOE の振る舞いは、電圧、周波数、温度といった動作条件からの影響を受ける。

この脅威に対して、TOE は、IC カード及び類似デバイスに関する必須技術文書[13]に記載された攻撃に耐えるべく、TSF に対する保護機能を提供する。

3.1.2 組織のセキュリティ方針とセキュリティ機能方針

3.1.2.1 組織のセキュリティ方針

PP[11]に適合する TOE の利用に当たって要求される組織のセキュリティ方針を表 3-2 に示す。

表 3-2　組織のセキュリティ方針

識別子	組織のセキュリティ方針
P.Multiple_authentication	TOEはユーザ認証のための複数の認証手段を提供する。パスワード認証に加えて、ユーザは暗号鍵ベースの認証も選択する。
P.Secure_messaging	TOEとCGAの間の通信にはセキュアメッセージングを適用する。
P.Cryptography	TOEはデータのハッシュ、データ保護、SK/PK生成、署名生成及び認証のために使用される暗号機能を提供する。
P.RND	TSFはTSF自身のために使用される乱数を生成する。乱数は攻撃者による予測を防ぐために十分な品質を持つ。

表 3-3 暗号機能方針

機能	鍵長、仕様など
鍵ペア生成	RSA 2048 ビット以上 [TOE 認証時に ST 作者が指定] （DTBS への署名生成のために本機能を使用）
署名生成	RSA2048 ビット以上 [TOE 認証時に ST 作者が指定] （DTBS への署名生成のために本機能を使用）
署名検証	RSA2048 ビット以上 [RSASSA-PKCS1-v1_5, PKCS #1] （PK-EA を使用した外部認証のために本機能を使用）
ハッシュ	SHA-256 [FIPS180-4]
乱数生成	物理、ハイブリッド物理、またはハイブリッド決定論的乱数生成器
鍵破棄	SK/PK pair、PK-EA が不要になったときに破棄

3.1.2.2 組織のセキュリティ方針に対するセキュリティ機能方針

TOE は、3.1.2.1 に示す組織のセキュリティ方針を満たす機能を具備する。

(1) 組織のセキュリティ方針「P.Multiple_authentication」への対応

表 3-4 に挙げる認証メカニズムを提供する。

表 3-4 Multiple authentication mechanisms

認証メカニズム	ルール
GlobalPlatform Card Specification – Amendment D[15]に記載された相互認証	GlobalPlatform Card Specification – Amendment D[15]に記載された相互認証は管理者としてのユーザの認証に使用される。
パスワード認証	署名者のデフォルトの認証メカニズムとして使用される。
PK-EA を使用した外部認証	署名者としてのユーザの代替認証手段として使用される。この手段の有効化には、個々の署名者に対応する PK-EA の登録が必要。

(2) 組織のセキュリティ方針「P.Secure_messaging」への対応

TOE が TSF 間高信頼チャネルを提供することで対応する。

(3) 組織のセキュリティ方針「P.Cryptography」「P.RND」への対応

TOE が表 3-3 に挙げる暗号機能を提供することで対応する。

4 前提条件と評価範囲の明確化

本章では、想定する読者が PP[11]に適合する TOE の利用の判断に有用な情報として、PP[11]に適合する TOE を運用するための前提条件及び運用環境について記述する。

4.1 使用及び環境に関する前提条件

PP[11]に適合する TOE を運用する際の前提条件を**表 4-1** に示す。これらの前提条件が満たされない場合、PP[11]に適合する TOE のセキュリティ機能が有効に動作することは保証されない。

表 4-1 前提条件

識別子	前提条件
A.PKI	TSFの効果的な運用のため、TOEの、公開鍵暗号の公開鍵が有効であることを保証するPKI環境が提供される。
A.Administrator	TOEのデータを作成、変更、削除する管理者は信頼できるユーザであり、特権に基づいてTOEを適切に操作する
A.Protect_VAD	Verification authentication data (VAD) が外部装置からTOEにインポートされるときに、VADの機密性と完全性が保証されている。

5 評価機関による評価実施及び結果

5.1 評価機関

評価を実施した株式会社 ECSEC Laboratory 評価センターは、IT セキュリティ評価及び認証制度により承認されるとともに、ILAC（国際試験所認定協力機構）の相互承認に加盟している認定機関（独立行政法人製品評価技術基盤機構認定センター）により認定を受けており、評価品質維持のためのマネジメント及び要員等の適切性についての要求事項を満たしていることが定期的に確認されている。

5.2 評価方法

評価は、CC パート 3 の保証要件について、CEM に規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告された。評価報告書では、PP[11]の概要と、CEM のワークユニットごとの評価内容及び判断結果を説明する。

5.3 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、令和 7 年 8 月に始まり、令和 8 年 1 月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。

評価作業中に発見された問題点は、所見報告書として発行され、開発者に報告された。それらの問題点は、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

また、認証機関が見つけた評価の問題点は、認証レビューとして記述されて、評価機関へ渡された。これらの指摘は、評価機関及び開発者が検討したのち、評価報告書に反映された。

5.4 評価結果

評価者は、評価報告書をもって PP[11]が CEM のワークユニットすべてを満たしていると判断した。

評価の結果として、以下の保証コンポーネントについて「合格」判定がなされた。

・APE_INT.1、APE_CCL.1、APE_SPD.1、APE_OBJ.2、APE_ECD.1、APE_REQ.2

5.5 評価者コメント/勧告

調達者に喚起すべき評価者勧告は、特にない。

6 認証実施

認証機関は、評価の過程で評価機関より提出される各資料をもとに、以下の観点で認証を実施した。

① 所見報告書でなされた指摘内容が妥当であること。

② 所見報告書でなされた指摘内容が解決されていること。

③ 提出された証拠資料を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。

④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。

⑤ 評価報告書に示された評価者の評価方法がCEMに適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。認証機関は、PP[11]及び評価報告書において、認証レビューで指摘された問題点が解決されていることを確認し、本認証報告書を発行した。

6.1 認証結果

評価機関より提出された評価報告書、所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、PP[11]の評価が CC パート 3 の APE_INT.1、APE_CCL.1、APE_SPD.1、APE_OBJ.2、APE_ECD.1、及び APE_REQ.2 に対する保証要件を満たすものと判断する。

6.2 注意事項

PP[11]に適合する TOE は Java Card システムを搭載するハードウェアであるため、TOE のセキュリティ評価を行う場合は、PP[11]で規定する脅威だけでなく、Java Card 特有の攻撃への耐性を含む、IC カード及び類似デバイスに関する必須技術文書[13]に記載された攻撃への耐性の評価も必要である。PP[11]に準拠した ST の作者は、Java Card システムの PP にも適合させるなどの手段で、それらの脅威にも対応したセキュリティ課題、対策方針、機能要件等の定義が必要になることに注意する必要がある。

7 附属書

特になし。

8 用語

本報告書で使用された CC に関する略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation（セキュリティ評価基準）
CEM	Common Methodology for Information Technology Security Evaluation（セキュリティ評価方法）
COMP	Composite Product Package（コンポジット製品パッケージ）
EAL	Evaluation Assurance Level（評価保証レベル）
PP	Protection Profile（プロテクションプロファイル）
ST	Security Target（セキュリティターゲット）
TOE	Target of Evaluation（評価対象）
TSF	TOE Security Functionality（TOEセキュリティ機能）

本報告書で使用された用語の定義及び略語を以下に示す。

Certificate generation application (CGA)	collection of application components that receive the PK from the SSCD to generate a certificate obtaining data to be included in the certificate and to create a digital signature of the certificate
Data to be signed (DTBS)	all electronic data to be signed including a user message and additional information that is signed together with a user message
Data to be signed or its unique representation (DTBS/R)	data received by a SSCD as input in a single signature creation operation
Japanese Public Key Infrastructure (JPKI)	a safe and secure identity verification service that uses electronic certification installed in My Number Card's IC chips (My Number is not used) to officially authenticate users and confirm that documents such as contracts have not been tampered with online.
JPKI Applet	A Java Card applet that is responsible for generating a key pair for digital signature and for user certification
JPKI Application	a mobile phone application responsible for CGA and Signature Creation Application (SCA).
Public Key (PK)	public cryptographic key that can be used to verify a digital signature. JPKI Applet has two PKs, which are “the public key for digital signature” and “the public key for user certification”.
PK-EA	Public Key for external authentication
Secure	hardware or software that is used in creating a digital

Signature Creation Device (SSCD)	signature
Secure Element Issuer Trusted Service Manager (SEI-TSM)	responsible for managing the end-to-end security of the SE, including the deployment of applications and services.
Service Provide Trusted Service Manager (SP-TSM)	entity that issues certificates or provides other services related to digital signatures
Signature creation application (SCA)	application complementing a SSCD with a user interface with the purpose to create a digital signature
Secret Key (SK)	secret cryptographic key stored in the SSCD under exclusive control by the signatory to create a digital signature. JPKI Applet has two SKs, which are “the secret key for digital signature” and “the private key for user certification”.
Verification authentication data (VAD)	data provided as input to a SSCD for authentication

9 参照

[1] ITセキュリティ評価及び認証制度の基本規程, 令和7年8月, 独立行政法人情報処理推進機構, CCS-01

[2] ITセキュリティ認証等に関する要求事項, 令和5年12月, 独立行政法人情報処理推進機構, CCM-02

[3] ITセキュリティ評価機関承認等に関する要求事項, 令和3年10月, 独立行政法人情報処理推進機構, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version CC:2022 Revision 1, November 2021, CCMB-2022-11-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version CC:2022 Revision 1, November 2021, CCMB-2022-11-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version CC:2022 Revision 1, November 2021, CCMB-2022-11-003

[7] Common Criteria for Information Technology Security Evaluation Part4: Framework for the specification of evaluation methods and activities Version CC:2022 Revision 1, November 2021, CCMB-2022-11-004

[8] Common Criteria for Information Technology Security Evaluation Part5: Pre-defined packages of security requirements Version CC:2022 Revision 1, November 2021, CCMB-2022-11-005

[9] Common Methodology for Information Technology Security Evaluation : Evaluation methodology Version CEM:2022 Revision 1, November 2021, CCMB-2022-11-006

[10] Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.1, 2024-07-22

[11] JPKI Applet Protection Profile, バージョン 1.10, 2026年1月, Digital Agency, Government of Japan

[12] PP評価報告書 JPU-ETRPP-0001-05, 第1.5版, 2026年1月30日, 株式会社 ECSEC Laboratory 評価センター

[13] Joint Interpretation Library - Application of Attack Potential to Smartcards and Similar Devices, Version 3.2.1, February 2024

[14] GlobalPlatform Card Specification v2.3.1

[15] GlobalPlatform Card Specification – Amendment D v1.2, Secure Channel Protocol '03'

[16] 所見報告書 JPU-EOR-0001-00, 2025年9月17日, 株式会社ECSEC Laboratory評価センター

[17] 所見報告書 JPU-EOR-0002-00, 2025年10月3日, 株式会社ECSEC Laboratory評価センター