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　富田　達夫

原紙押印済

IT製品（TOE）

申請受付日（受付番号）	平成30年7月9日（IT認証8678）
認証識別	JISEC-C0648
製品名称	ID&Trust IDentity-J with SAC (PACE) and AA version 1.0 on IFX M7892 G12 SLJ 52G
バージョン及びリリース番号	v1.0.7052
製品製造者	ID&Trust Ltd.
評価スポンサーの名称	マクセル株式会社
機能要件適合	プロテクションプロファイル適合、CCパート2拡張
プロテクションプロファイル	旅券冊子用ICのためのプロテクションプロファイル－SAC対応(PACE) 及び能動認証対応－ 第1.00版（認証識別：JISEC-C0499）
保証パッケージ	EAL4 及び追加の保証コンポーネントALC_DVS.2、AVA_VAN.5
ITセキュリティ評価機関の名称	TÜV Informationstechnik GmbH, Evaluation Body for IT Security

上記のTOE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。
令和元年 8月28日

セキュリティセンター セキュリティ技術評価部
技術管理者　佐藤 眞司

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 Version 3.1 Release 5
② Common Methodology for Information Technology Security Evaluation Version 3.1 Release 5

評価結果：合格

「ID&Trust IDentity-J with SAC (PACE) and AA version 1.0 on IFX M7892 G12 SLJ 52G」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、ID&Trust Ltd.が開発した「ID&Trust IDentity-J with SAC (PACE) and AA version 1.0 on IFX M7892 G12 SLJ 52G」（以下「本 TOE」という。）について TÜV Informationstechnik GmbH, Evaluation Body for IT Security（以下「評価機関」という。）が令和元年 7 月 31 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マクセル株式会社に報告するとともに、本 TOE に関心を持つ調達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、11 章のセキュリティターゲット（以下「ST」という。）を併読されたい。特に本 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、ST において詳述されている。

本認証報告書は、旅券発行当局を読者と想定している。本認証報告書は、本 TOE が適合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。

本認証報告書で使用する用語については 12 章を参照されたい。

1.1 評価対象製品概要

本 TOE の機能、運用条件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 プロテクションプロファイル

本 TOE は、次のプロテクションプロファイル[16]（以下「適合 PP」という。）に適合する。

> 旅券冊子用 IC のためのプロテクションプロファイル　－SAC 対応(PACE) 及び能動認証対応－第 1.00 版（認証識別：JISEC C0499)

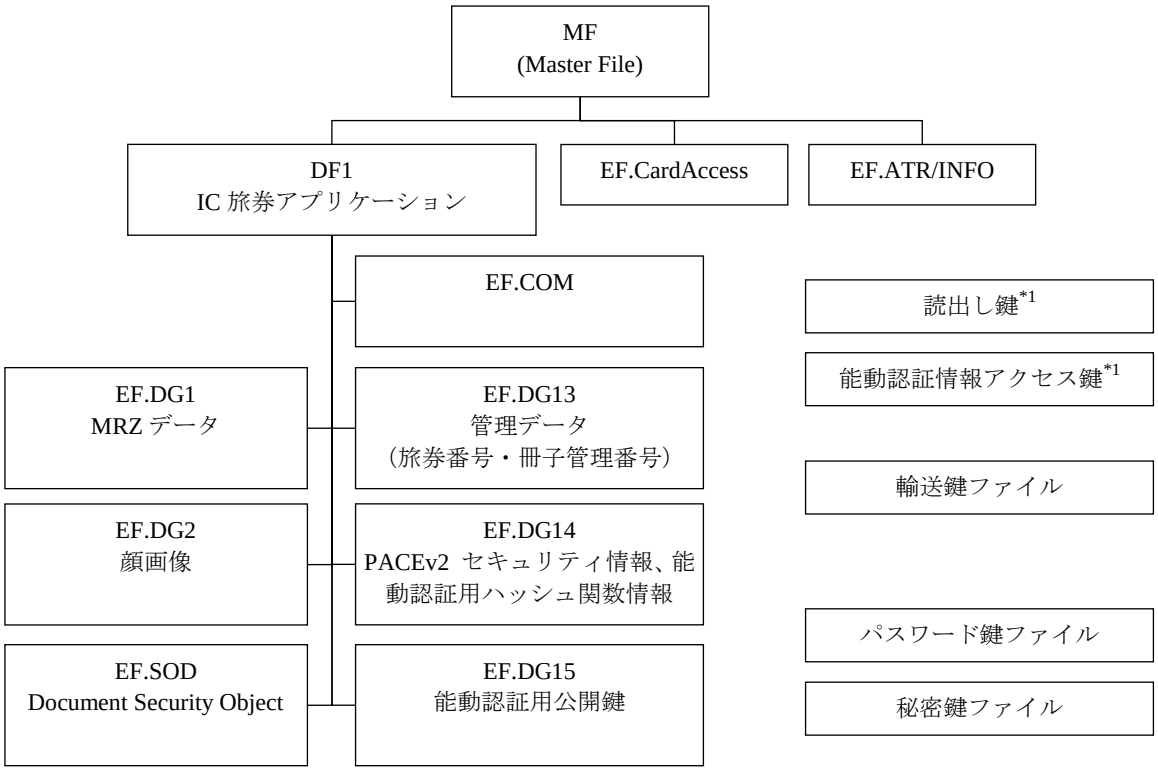
1.1.2 TOEとセキュリティ機能性

本 TOE は、旅券に綴じ込まれる旅券冊子用 IC（必要なソフトウェアを含む）である。

本 TOE は、非接触通信インタフェースを持つ IC チップハードウェア、それに搭載される基本ソフトウェア(OS)、及び IC 旅券用アプリケーションプログラムからなる。その外部に非接触通信のためのアンテナが接続され、アンテナと共にプラスチックシートに埋め込まれて旅券冊子の一部を構成する。

旅券保持者の出入国において、出入国審査官は、旅券検査用端末装置（以下、端末装置と称する）を使用して旅券を検査する。通常の文字で旅券冊子に印刷された情報は、それと同じ内容が符号化されて旅券冊子の MRZ（機械読み取り領域）に印刷され、端末装置の光学文字読み取り装置で読み取られる。なお、これらの情報はデジタルデータ[1]化され、TOE である IC チップ内に格納されている。このデジタルデータは、TOE の非接触通信インタフェース経由で端末装置によって読み出される。このデジタルデータには、顔画像も含まれる。

図 1-1 は、IC 旅券規格[24] Part 10, Figure 2 を、TOE を説明する目的で再構成したものである。



*1　PP[16]上、ファイルであるとは明示されていない。

図 1-1 旅券冊子用ICのファイル構成

適合 PP[16]では、IC 旅券アプリケーション配下のファイルの読出しに先立って、端末装置と TOE とが相互認証し、TOE と端末装置間の通信にセキュアメッセージングを適用することを要求している。IC 旅券規格[24]で規定された相互認証及びセキュアメッセージングの方式には、基本アクセス制御（BAC: Basic Access Control）

[1] デジタルデータの偽造を防ぐため、個々のデジタルデータに旅券発行者によるデジタル署名が付与される。デジタル署名の検証は、受動認証方式としてICAOによって標準化されている。受動認証に対応するため、デジタル署名付与から端末装置での検証に至るまで、全ての加盟国間で相互運用性を持つPKIが運用される。受動認証は、署名から検査に至るまで（バックグラウンドとなるPKIを含め、）TOEのセキュリティ機能が関与することなく実施されるので、TOEに対するセキュリティ要件には含まれない。

と、鍵共有利用アクセス制御（PACE: Password Authenticated Connection Establishment v2）の 2 つがあり、後者は公開鍵暗号を取り入れ、セキュアメッセージングの中で使用されるセッション鍵の暗号強度を強化した方式である。

図 1-2 は、端末装置が旅券冊子用 IC にアクセスする手順の中で、基本アクセス制御、及び鍵共有利用アクセス制御がどのように関わってくるかを示したもので、基本アクセス制御又は鍵共有利用アクセス制御のどちらか一方が適用される。

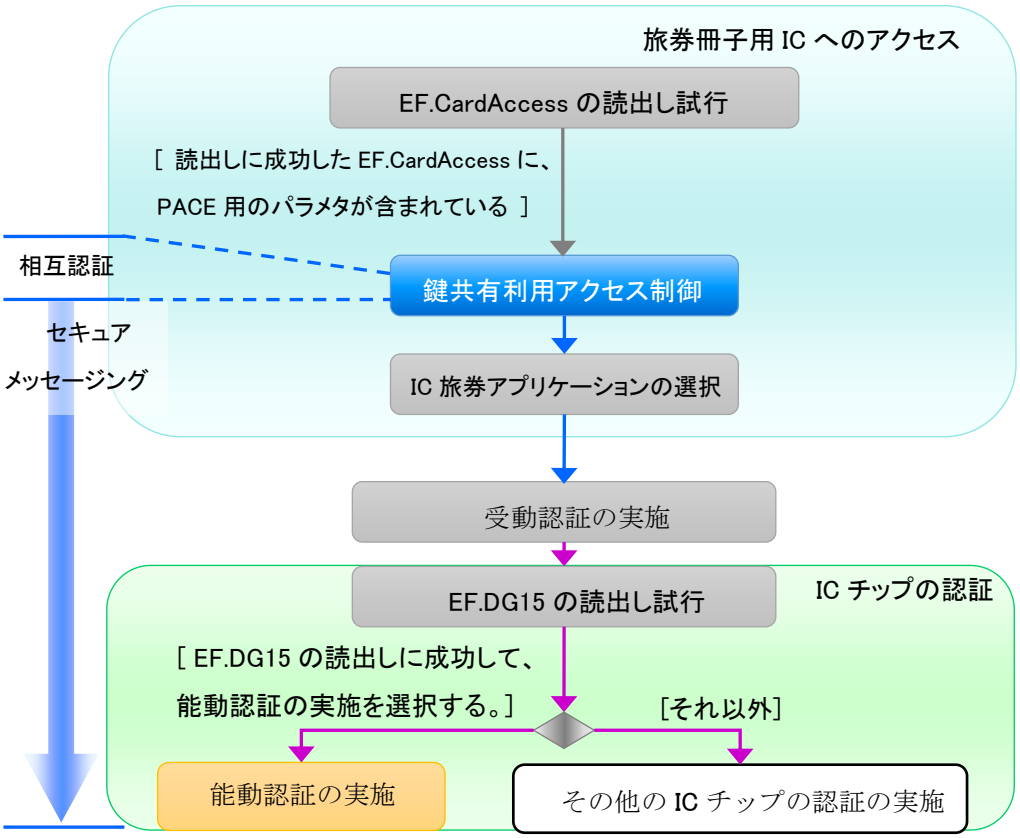


図 1-2　端末装置が旅券冊子用ICにアクセスする手順

互換性確保の観点から、2017 年末までは、基本アクセス制御機能を実装せずに鍵共有利用アクセス制御機能のみを IC チップに実装することは IC 旅券規格[24] Part 11 で禁止されていた。

TOE は、基本アクセス制御をサポートせず、鍵共有利用アクセス制御をサポートする IC チップである。

TOE は、旅券冊子用 IC の複製を防止するため、公開鍵暗号を利用したチャレンジレスポンスにより、IC チップの真正性を証明しようとする能動認証対応機能を実装している。能動認証対応機能は、過去に認証された PP[34]では RSA を使用することを要求していたが、適合 PP[16]の要求に対応して ECDSA を使用している。

TOE のライフサイクルは 4 つのフェーズに分けられ、それらを図示したものが図 1-3 である。

フェーズ 1、及びフェーズ 2 では運用環境の脅威は想定されていないが、開発データや IC チップの構成要素の機密性・完全性を保護するために適切な開発セキュリティが保たれていなければならない。フェーズ 3 では、権限を持つものだけに TOE の処理を許可するようなセキュリティ機能性が要求される。フェーズ 4 では高い攻撃能力を持つ攻撃者からの攻撃に対抗できるセキュリティ機能性が要求される。

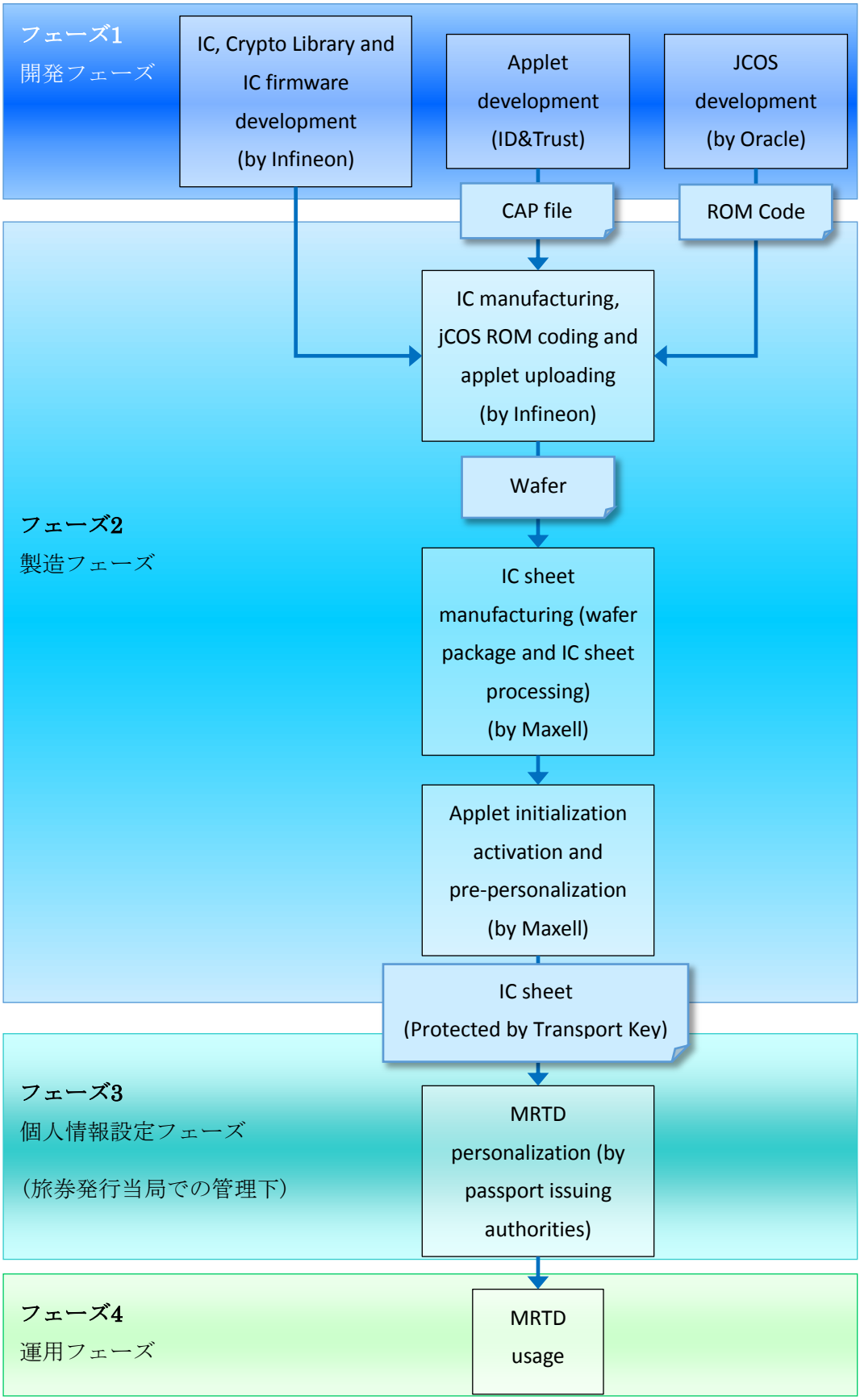


図 1-3　TOEのライフサイクル

TOE は、その内部に格納されたデータの不正な読出しや書込みから保護する機能、IC 旅券規格[24] Part 11 が規定する鍵共有利用アクセス制御機能、能動認証対応機能、輸送時の保護機能、及び物理的攻撃に備える耐タンパー機能を持つ。その概要を以下に示す。

(1)鍵共有利用アクセス制御機能

TOE は、端末装置との間で相互認証を行い、相互認証に成功した端末装置との間にセキュアメッセージングを適用して、TOE 内のアクセス制御対象のファイルの読出しを許可する。

鍵共有利用アクセス制御の相互認証及びセキュアメッセージングに使用される暗号は、公開鍵確立手法（ECDH[2]）、共通鍵暗号（AES[3]）及びハッシュ関数（SHA-1[4]、SHA-256[5]）である。

(2) 能動認証対応機能

TOE は、旅券冊子用 IC の複製を防止するため、公開鍵暗号を利用したチャレンジレスポンスにより、IC チップの真正性を証明しようとする能動認証対応機能を提供する。

能動認証に使用される暗号は、デジタル署名（ECDSA[6]）及びその中で使用されるハッシュ関数（SHA-256、SHA-384）である。

(3) 書込み禁止機能

旅券の発行後、TOE 内のファイルに対する一切の書込みを禁止する機能である。

(4) 輸送時の保護機能

TOE は、輸送途中の不正利用から IC チップを保護する目的で、輸送鍵を用いた認証に成功して初めて TOE 内の所定のファイルにアクセスできる機能を提供する。

(5) 物理攻撃に備える耐タンパー機能

---

[2] IC旅券規格[24]ではDHを使う選択肢も記載されているが、PP[16]ではECDHを選択している。

[3] IC旅券規格[24]ではTriple DESを使う選択肢も記載されているが、PP[16]ではAESを選択している。PP[16]では128ビットのAES鍵を使う場合と256ビットのAES鍵を使う場合の両方に対応できることを要求している。

[4] SHA-1は、128ビットのAES鍵を使う場合の鍵導出に使用される。

[5] SHA-256は、256ビットのAES鍵を使う場合の鍵導出に使用される。

[6] IC旅券規格[24]ではRSAを使う選択肢も記載されているが、PP[16]ではECDSAを選択している。その上で、256ビット又は384ビットの秘密鍵を用いて署名生成を行う。256ビットの秘密鍵の場合には、SHA-256が、384ビットの場合にはSHA-384が使用される。

TOE のセキュリティ機能は、自身のハードウェア部分及び TSF を構成するソフト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 カードと同様である。例えば、IC チップ内部への物理的操作やプロービングによる情報の暴露・改変、あるいは、TOE の電磁放射の観測・分析による暗号鍵暴露など、物理的手段を用いる多様な攻撃が存在する。

これらのセキュリティ機能性について、その設計方針の妥当性と実装の正確性について適合 PP[16]の要求する保証要件の範囲で評価が行われた。

本 TOE が想定する脅威及び前提については次項のとおりである。

1.1.2.1 脅威とセキュリティ目標[7]

本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。

身分証明書として必要な情報が全て紙の冊子に印刷されていた旧来の旅券については、偽造等による不正使用が懸念されていた。この課題を解決すべく旅券冊子用 IC では、IC チップ内に格納されるデジタルデータに、正規の旅券発行者によるデジタル署名を施し、旅券発行側と受け入れ側の双方が相互運用性の保証された PKI システムを用いることによって、IC チップから読み出されたデータの真正性を確認できるようにする受動認証が採用されている。

しかし､受動認証だけでは､正規のデジタル署名付き個人情報を複製して別の IC チップに格納する偽造に対抗できない。そこで TOE は、IC 旅券規格[24]で規定された、能動認証（Active Authentication）と呼ばれる公開鍵暗号を利用したチャレンジレスポンス方式を採用し、その能動認証に使う秘密鍵（以下「能動認証用秘密鍵」という。）の IC チップからの読出しを制限することによって、偽造に対抗しようとしている。

IC 旅券規格[24]では、ISO/IEC 7816-4 で規定されたファイルシステムを採用している。能動認証用秘密鍵もこのファイルシステムの中に格納されていることを想定すると、ISO/IEC 7816-4 で規定されたコマンドを用いて能動認証用秘密鍵が読み出せる可能性がある。そのような脅威に対して、TOE は、読出しアクセスを拒否することで対抗する。

旅券冊子用 IC から読み出し可能なデータには顔画像や受動認証のための情報が含まれている。出入国審査の窓口の端末装置と旅券冊子用 IC との間で通信されるデータを暴露・改ざんしようとする試みが想定される。この脅威に、TOE と端末装

---

[7] CC Part 1 [4]で定義されている"security objective"の訳語として、日本語翻訳版[7]では「セキュリティ対策方針」を割り当てているが、本認証報告書の中では、"security objective"の訳語として、「セキュリティ目標」を用いることとする。

置間の相互認証及び TOE と端末装置間のセキュアメッセージングを適用することで対抗する。

IC カードに搭載される IC チップは、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 TOE は備える。但し、脅威への対抗のほとんどは、5.1 で説明するプラットフォームによって担われている。

1.1.2.2 構成要件と前提条件

評価対象製品は、次のような構成及び前提で運用することを想定する。

本 TOE は、旅券に必要な情報が書き込まれた上で、プラスチックシートに埋め込まれ、旅券冊子に綴じ込まれる。旅券冊子は旅券保持者によって携行され、出入国手続きをはじめとする多様な局面で、旅券保持者の身元証明手段として使用される。

TOE 製造者から旅券発行当局へ納入され当局の管理下にある TOE は、旅券保持者へ発行されるまでの間、セキュアに管理され発行処理が行われなければならない。

旅券発行者によってデジタル署名され TOE に格納された情報について、その真正性を受入国の旅券審査当局が検証できるようにするため、旅券の発行国、受入国双方の PKI 環境が相互運用性を含めて適切に維持されなければならない。

1.1.3 認証に際しての免責事項

1.1.3.1 PP[16]に由来し ST[18]に引き継がれた事項

PP[16]では、鍵共有利用アクセス制御を、相互認証及びセキュアメッセージング機能であると謳っている。IC 旅券規格[24]で規定された鍵共有利用アクセス制御は、MRZ データを知らない攻撃者が、無線通信に割り込み、旅券冊子用 IC から端末装置に読み出される情報を盗聴・改ざんしようとする攻撃にのみ対抗しようとする機能である。

IC 旅券規格[24]によれば、鍵共有利用アクセス制御を突破するために必要な情報が MRZ データであるため、MRZ データを知ることができれば、正規の端末装置になりすまして、最終的に受動認証のための情報を読み出すことが可能である。したがって、MRZ データを知っている攻撃者が、鍵共有利用アクセス制御を突破して、旅券冊子用 IC のデータを読み出す、という脅威には対抗できない。しかしながら、

攻撃者が MRZ データを知ることができても、PP[16]に適合する TOE であれば能動認証用秘密鍵を論理的に読み出すことはできない。

また、PP[16]では旅券冊子用 IC の複製防止のための能動認証対応機能を TOE に要求しているが、TOE の機能だけで、旅券の偽造による悪用を防止できるわけではない。能動認証の仕組みがシステムとして適切に機能するためには、能動認証用秘密鍵の機密性及び能動認証用公開鍵の完全性・真正性が重要である。旅券発行当局の許可された利用者（読出し鍵、輸送鍵、あるいは能動認証情報アクセス鍵の照合に成功した者）は、後述する前提条件 A.Administrative_Env に対応して、次の事項をセキュアに行う必要がある。

— 能動認証用鍵ペアを生成する

— 能動認証用公開鍵にデジタル署名を付ける

— 能動認証用鍵ペアを旅券冊子用 IC に格納する

加えて、旅券発行当局の許可された利用者は、後述する前提条件 A.PKI に対応して、旅券冊子用 IC に格納するデータのデジタル署名生成に使う鍵ペアをセキュアに管理すると共に、PKI 環境を適切に維持する必要がある。

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、評価機関によって本 TOE 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、令和元年 7 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[23]、所見報告書（[27]～[33]）、及び関連する評価証拠資料を検証し、本 TOE 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、全て解決され、かつ、TOE の評価が CC（[4][5][6]または[7][8][9]）及び CEM（[10][11]のいずれか）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 TOE識別

本 TOE は、以下のとおり識別される。

TOE名称：	ID&Trust IDentity-J with SAC (PACE) and AA version 1.0 on IFX M7892 G12 SLJ 52G
バージョン：	v1.0.7052
開発者：	ID&Trust Ltd.

製品が評価･認証を受けた本 TOE であることを、利用者はユーザーズガイド[26]に記載された方法によって確認することができる。

IDentity-J-v1.0 は、個人情報設定フェーズと運用フェーズにおいて GET DATA コマンドを使用することにより識別できる。ユーザーズガイド[26]の 12.1 節の記述に従って、GET DATA コマンドを使用し、その結果を次と比較することにより、本 TOE であることを確認できる。

GET DATA コマンドの返り値：IDentity-J-v1.0.7052

3 セキュリティ方針

本章では、本 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。

TOE は、名前、生年月日、顔画像データなどの、旅券として必要な情報が書き込まれた、旅券冊子用 IC である。

TOE は、適合 PP[16]の要求を満足する以下のセキュリティ機能を提供する。

— 鍵共有利用アクセス制御機能（相互認証とセキュアメッセージング）

— 能動認証対応機能（旅券冊子用 IC の複製防止）

— 書き込み禁止機能（旅券発行後のデータ書込み禁止）

— 輸送時の保護機能（発行前 TOE を輸送時の攻撃から保護）

— 耐タンパー性（物理的攻撃による機密情報漏えい防止）

3.1 セキュリティ機能方針

TOE は、3.1.1 に示す脅威に対抗し、3.1.2 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

本 TOE は、表 3-1 に示す脅威を想定し、これに対抗する機能を備える。

表3-1 想定する脅威

識別子	脅威
T.Copy	IC旅券の偽造を意図する攻撃者がTOEからデジタル署名付きの個人情報を読み出し、その複製データをTOEと同様の機能性を持つICチップに書き込んでIC旅券を偽造しようとするかもしれない。この攻撃によって、TOEを含む旅券冊子全体に対する信用が毀損される。 [注釈] 不正なICチップに正規のTOEから取り出された情報が複製されると、デジタル署名ごとTOE内情報が複製されるので、デジタル署名の検証による偽造防止が無効になる。デジタル署名によって元情報の改ざんは防止できるため、顔画像の比較検証で旅券偽造を検出できるかもしれない。しかし、顔だちの判別だけでは、確実に旅券偽造を検出することは困難である。

識別子	脅威
T.Logical_Attack[8]	TOEを組み込んだ旅券冊子発行後の運用環境において、旅券冊子のMRZデータを読み取れる状態にある攻撃者が、TOEの非接触通信インタフェース経由でTOE内に格納された機密情報（能動認証用秘密鍵）を読み出そうとするかもしれない。 [注釈] 攻撃者が旅券冊子に物理的にアクセスできれば、攻撃者は、目視で旅券冊子に印刷された個人情報を読み取ったり、あるいはMRZの印刷データを光学的に読み取ることができる。これらの読み取りをTOEのセキュリティ機能で防止することはできないので、これらの情報は、この脅威に関わる保護資産に含まれない。つまり本脅威の趣旨は、攻撃者がMRZから読み取ったデータを利用してTOEの非接触インタフェース経由でTOEにアクセスし、内部の機密情報（能動認証用秘密鍵）を読み出そうとする攻撃である。
T.Communication_Attack[9]	TOEを組み込んだ旅券冊子発行後の運用環境において、MRZデータを知らない攻撃者が端末装置とTOE間の通信に割込み、秘匿が必要な通信データを暴露・改ざんするかもしれない。 [注釈] 端末装置と旅券冊子間の通信に割り込むような攻撃においては、攻撃者が旅券保持者や出入国審査官に気づかれずに攻撃対象の旅券冊子へ物理的にアクセスすることは不可能と考えられる。攻撃者は旅券冊子に物理的にアクセスできる場合のみ、MRZデータを知ることができるため、本脅威の想定する攻撃者はMRZデータを知らないものと考えられる。

[8] 脅威「T.Logical_Attack」は、TOEがISO/IEC 7816-4で規定されたファイルシステムを採用していることに対応して、ISO/IEC 7816-4で規定されたコマンドを用いて能動認証用秘密鍵の出力が可能かもしれないという可能性を表したものである。

[9] 脅威「T.Communication_Attack」は、顔画像などの読出し可能なデータの、攻撃者による暴露・改ざんの懸念を表したものである。対象となるデータが異なるという点で、脅威「T.Logical_Attack」とは独立である。

識別子	脅威
T.Physical_Attack[10]	TOEを組み込んだ旅券冊子発行後の運用環境において、攻撃者が物理的手段を用いてTOE内部の機密情報（能動認証用秘密鍵）を暴露しようとしたり、閉塞された鍵の閉塞状態を解除したり、無効化されたアクセス制御機能を再活性化したりするかもしれない。この物理的手段には、TOEの機能を損なわずに攻撃する非破壊攻撃と、TOEの一部を破壊して内部に機械的にアクセスする破壊攻撃の両方が含まれる。 [注釈] 攻撃者がTOEに物理的にアクセスし、内部の機密情報（能動認証用秘密鍵）を読み出したり、TOE内の情報を書き換えたりする攻撃が考えられる。このような物理的攻撃が行われると、TOEのプログラムによって動作するセキュリティ機能は本来の機能を発揮できず、SFR侵害の恐れが生じる。非破壊攻撃の例は、TOEの動作に伴う漏えい電磁波観測、動作中のTOEに環境ストレス（温度やクロックの変化、高エネルギーの電界・磁界印加など）を与えてセキュリティ機能の誤動作を誘起するものである。破壊攻撃の例は、内部回路のプロービングや操作(manipulation)によって情報を収集・分析し、機密情報を暴露するものである。内部に残されたテスト用端子や電源端子も攻撃に利用され得る。破壊攻撃を受けたTOEは、旅券用ICとして再使用できないかもしれない。しかしその場合でも、読み出された秘密鍵がTOEの偽造に悪用される恐れがある。

3.1.1.2 脅威に対するセキュリティ機能

本 TOE は、表 3-1 に示す脅威に対し、以下のセキュリティ機能で対抗する。

(1) 脅威「T.Copy」への対抗

受動認証は、デジタル署名が付与された個人情報を旅券冊子用 IC に格納し、その個人情報を端末装置が読み出して、PKI システムを用いて検証する方式である。脅威「T.Copy」は、デジタル署名を含めて個人情報を複製し、別の IC チップに書き込んで偽造した IC 旅券を用いて、受動認証による検査を突破することを想定している。

この脅威に対して、IC 旅券規格[24]は、次の手順による能動認証を規定している。

a). 端末装置は、ナンス(8 バイト)を旅券冊子用 IC に送信する。

---

[10] 脅威「T.Physical_Attack」は、TOEに物理的手段を用いるという点で、利用可能な手段が論理的な手段に限定されている脅威「T.Logical_Attack」と対比される。しかしながら、脅威「T.Physical_Attack」には、攻撃者が、差分故障利用攻撃(Differential Fault Analysis：DFA)のような、論理的な手段(非接触通信インタフェースを介したデータ出力)と物理的な手段とを組み合わせて攻撃することも含まれる。

b). 旅券冊子用 IC は、受信したナンスに旅券冊子用 IC 内で格納している能動認証用秘密鍵を用いて署名生成し、その署名文を端末装置に送信する。

c). 端末装置は、旅券冊子用 IC から別途読み取った能動認証用公開鍵を用いて、署名文を検証し、検証に成功すれば正規の旅券冊子用 IC であると判断する。なお、能動認証用公開鍵にはデジタル署名が付けられており、端末装置は PKI システムを用いることによって、能動認証用公開鍵の完全性・真正性を検証することができる。

能動認証用のデジタル署名アルゴリズムとして、適合 PP[16]では、IC 旅券規格[24]から参照される[25]で規定された ECDSA(但し、256 ビット又は 384 ビットの秘密鍵を用いる)を規定している。

関連する能動認証用秘密鍵の機密性、及び能動認証用公開鍵・能動認証用秘密鍵の完全性の観点について、適合 PP[16]では、3.1.2.1 に示す組織のセキュリティ方針 P.Data_Lock を通じて、次の 2 つが禁止された状態で旅券保持者に発行される仕組みを要求している。

— 能動認証用秘密鍵の読出し及び書込み

— 能動認証用公開鍵の書込み

(2) 脅威「T.Logical_Attack」への対抗

脅威「T.Logical_Attack」は、TOE を組み込んだ旅券冊子が旅券保持者に発行された運用環境において、非接触通信インタフェースを経由して能動認証用秘密鍵が論理的に読み出される可能性を想定している。

この脅威に対して、TOE は、旅券冊子発行後の運用環境において、能動認証用秘密鍵の論理的な読出しを禁止することで対抗する。

(3) 脅威「T.Communication_Attack」への対抗

脅威「T. Communication_Attack」は、顔画像などの読出し可能なデータの、攻撃者による暴露・改ざんを想定している。

この脅威に対して、TOE と端末装置間の相互認証及び TOE と端末装置間のセキュアメッセージングを適用することで対抗する。

適用される相互認証及びセキュアメッセージングの方式は、IC 旅券規格[24]で規定された鍵共有利用アクセス制御である。

鍵共有利用アクセス制御に用いられる暗号アルゴリズムを表 3-2 に示す。

表 3-2　鍵共有利用アクセス制御に用いられる暗号アルゴリズム

暗号アルゴリズム	暗号操作	暗号鍵長 (ビット)	用途
SHA-1[*1]	鍵共有利用アクセス制御用セッション鍵の導出	—[*3]	相互認証及び セキュアメッセージング
SHA-256[*2]	鍵共有利用アクセス制御用セッション鍵の導出	—[*3]	相互認証及び セキュアメッセージング
ECDH	鍵共有	256又は384	相互認証及び セキュアメッセージング
CMAC モード AES	認証トークンの生成および検証	128又は256	相互認証
	認証子の生成・検証	128又は256	セキュアメッセージング
CBC モード AES	ナンス[*4]の暗号化	128又は256	相互認証
	メッセージの暗号化・復号	128又は256	セキュアメッセージング

[*1] 128ビットのAESのセッション鍵を導出するために使用される。

[*2] 256ビットのAESのセッション鍵を導出するために使用される。

[*3] ハッシュ関数とみると暗号鍵は存在しないが、鍵導出関数と見た場合の入力は、ECDHで確立したShared Secretにカウンタ32ビットを連結したものである。

[*4] 能動認証に登場するナンスとは異なるもので、TOE 自身が乱数生成器を使って生成する。

(4) 脅威「T.Physical_Attack」への対抗

本 TOE は、IC という物理形態の特性上、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。

これらの脅威に対して、本 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。

例えば、この攻撃は次を含む。

— TOE 内部を流れる信号を読み取ろうとする攻撃、

— TOE 内部を流れる信号を改変しようとする攻撃、

— 故障注入攻撃(DFA を含む) 、

— サイドチャネル攻撃(DEMA を含む)、

— IC チップのテスト機能の悪用、

— 無効化されたアクセス制御機能の再活性化、

— 乱数生成器の出力乱数を予測したり、出力乱数のエントロピーを減らしたりする攻撃

3.1.2 組織のセキュリティ方針とセキュリティ機能

3.1.2.1 組織のセキュリティ方針

本 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 3-3 に示す。

表 3-3 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.PACE	TOEを組み込んだ旅券冊子発行後の運用環境において、TOEは、IC旅券規格[24]のPart11で規定される鍵共有利用アクセス制御手順に従って端末装置がTOEから所定の情報を読み出すことを許可しなければならない。この手順は、TOEと端末装置の相互認証及びTOEと端末装置間のセキュアメッセージングを含む。読出し対象となるTOEのファイルは、同規定におけるEF.DG1、EF.DG2、EF.DG13、EF.DG14、EF.DG15、EF.COM、EF.SODである。
P.Authority[11]	旅券発行当局の管理下にあるTOEは、表 3-4 に示すとおり、許可された利用者（読出し鍵、輸送鍵、あるいは能動認証情報アクセス鍵の照合に成功した者）だけにTOE内部情報へのアクセスを許可する。
P.Data_Lock[12]	TOEが輸送鍵、読出し鍵あるいは能動認証情報アクセス鍵による認証失敗を検出したとき、それぞれの鍵に関わる認証を恒久的に無効とし、それによって、その認証成功に基づくファイル読出し・書込みを禁止する。認証に用いる鍵とそれに対応するTOE 内ファイルとの関係は、表 3-4 に示される。
P.Prohibit[13]	旅券保持者への発行後、TOE内ファイルに対する一切の書込み、及び読出し鍵による認証成功に基づく読出しを禁止する。その手段として、輸送鍵、読出し鍵及び能動認証情報アクセス鍵の認証失敗による認証無効化（P.Data_Lockに示す）を利用する。

表 3-4 旅券発行当局におけるTOE内部情報アクセス制御

認証状況	アクセス制御対象となるファイル	許可される操作	参考：操作対象データ
読出し鍵*1 によ	EF.DG13*2	読出し	IC チップシリアル番号(製造者記入済

11 輸送時の保護機能に対応する。
12 書き込み禁止機能に対応する。
13 書き込み禁止機能に対応する。

認証状況	アクセス制御対象となるファイル	許可される操作	参考：操作対象データ
る照合成功			み)
輸送鍵*1による照合成功	輸送鍵ファイル	書込み	輸送鍵データ（旧データの更新）
	パスワード鍵ファイル		パスワード鍵
	EF.DG1	読出し又は書込み	MRZ データ
	EF.DG2		顔画像
	EF.DG13*2		管理データ（旅券番号・冊子管理番号）
	EF.DG14		PACEv2 セキュリティ情報 能動認証用ハッシュ関数情報
	EF.COM*3		共通情報
	EF.SOD		IC 旅券規格[24] Part10 に定められる受動認証関連セキュリティデータ
	EF.CardAccess	書込み	PACEv2 セキュリティ情報
	EF.DG15	読出し	能動認証用公開鍵
能動認証情報アクセス鍵*1による照合成功	EF.DG15	書込み	能動認証用公開鍵
	秘密鍵ファイル		能動認証用秘密鍵

*1 読出し鍵、輸送鍵、能動認証情報アクセス鍵は、製造者によって設定される。輸送鍵は、利用者が変更（更新）できる。本表に含まれるアクセス制御対象ファイルや認証状況を変化させる読出し鍵、能動認証情報アクセス鍵を格納したファイルについては、本表及び注に記載のない利用者アクセスは禁止される。(TOEを組み込んだ旅券冊子が旅券保持者へ発行された後の、端末装置からのTOE内部の情報へのアクセス制御<鍵共有利用アクセス制御>は別途規定する)

*2 EF.DG13 にはIC チップシリアル番号が製造者によって記入済みであり、旅券発行当局によって管理データが追記される。

*3 EF.COM ファイルは、旅券発行当局の指示により生成されない場合がある。

表 3-3 に示す組織のセキュリティ方針とそれが適用されるフェーズの関係を表 3-5 に示す。

表 3-5 組織のセキュリティ方針と適用されるフェーズ

	TOEのライフサイクル			
組織のセキュリティ方針	フェーズ 1	フェーズ 2	フェーズ 3	フェーズ 4
P.PACE				X
P.Authority			X	
P.Data_Lock			X	
P.Prohibit			X	X

注 'X' は、組織のセキュリティ方針が適用されることを表す。

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

TOE は、表 3-3 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.PACE」への対応（鍵共有利用アクセス制御機能）

本組織のセキュリティ方針は、TOE を組み込んだ旅券冊子発行後の運用環境において、IC 旅券規格[24]で規定される鍵共有利用アクセス制御手順に従って端末装置が TOE から所定の情報を読み出すことを規定している。

TOE が、IC 旅券規格[24] Part 11 で規定された鍵共有利用アクセス制御手順に従った機能を提供することにより、TOE からの所定の情報の読出しを鍵共有利用アクセス制御手順で意図した程度でセキュアにすることができる。

(2) 組織のセキュリティ方針「P.Authority」への対応（輸送時の保護機能）

本組織のセキュリティ方針は、旅券発行当局の管理下にある TOE に対して、TOE 内のファイルを、表 3-4 に従ってアクセス制御することを規定している。

TOE 内のファイルにアクセスするために、輸送鍵、読出し鍵、又は能動認証情報アクセス鍵を用いて利用者を認証することを TOE が要求し、認証が成功した場合のみ、それぞれの鍵の認証に基づく TOE 内のファイルへのアクセスを許可する。

(3) 組織のセキュリティ方針「P.Data_Lock」への対応（書き込み禁止機能）

本組織のセキュリティ方針は、TOE が輸送鍵、読出し鍵あるいは能動認証情報アクセス鍵による認証失敗を検出したとき、それぞれの鍵に関わる認証を恒久的に無効とし、それによって、表 3-4 に示される認証成功を必要とするファイルの読出し・書込みが禁止されることを規定している。

読出し鍵、輸送鍵あるいは能動認証情報アクセス鍵による認証失敗を TOE が検出したとき、TOE はそれぞれの鍵を用いる認証メカニズムを無効化する機能を提供する。これによって、読出し鍵、輸送鍵又は能動認証情報アクセス鍵を用いてファイルにアクセスすることが禁止される。

(4) 組織のセキュリティ方針「P.Prohibit」への対応（書き込み禁止機能）

本組織のセキュリティ方針は、旅券保持者への発行後、TOE 内ファイルに対する一切の書込み、及び読出し鍵の認証成功に基づく読出しを禁止することを規定している。

旅券保持者への発行前に、読出し鍵、輸送鍵、能動認証情報アクセス鍵による認証失敗を起こし、TOE が提供する前述(3)に示す機能を利用して、TOE 内のファイルに対する書込み、及び読出し鍵の認証に基づいた読出しを禁止する。

4 前提条件と評価範囲の明確化

本章では、想定する読者が本 TOE の利用の判断に有用な情報として、本 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

本 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、本 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.Administrative_Env	TOE製造者から旅券発行当局へ納入され当局の管理下にあるTOEは、旅券保持者へ発行されるまでの間、セキュアに管理され発行処理を受ける。
A.PKI	旅券発行者によってデジタル署名されTOEに格納された情報（能動認証用公開鍵を含む)について、その真正性を受入国の旅券審査当局が検証できるようにするため、旅券発行当局により旅券の発行国、受入国双方のPKI環境の相互運用性が保たれる。

4.2 運用環境と構成

本 TOE の形態は、IC チップであり、非接触インタフェースを有している。本 TOE を使用する際には、ISO/IEC 14443 で規定された Type-B 伝送プロトコルをサポートし、光学文字読み取り装置を備えた旅券検査用端末装置を用いる。

4.3 運用環境におけるTOE範囲

1.1.3 に記載したように、MRZ データを知っている攻撃者が、鍵共有利用アクセス制御を突破して、旅券冊子用 IC のデータを読み出す、という脅威には対抗できない。

同様に、PP[16]では旅券冊子用 IC の複製防止のための能動認証対応機能を TOE に要求しているが、TOE の機能だけで、旅券の偽造による悪用を防止できるわけではない。能動認証の仕組みがシステムとして適切に機能するためには、能動認証用秘密鍵の機密性及び能動認証用公開鍵の完全性・真正性が重要である。旅券発行当局の許可された利用者は、後述する前提条件 A.Administrative_Env に対応して、次の事項をセキュアに行う必要がある。

— 能動認証用鍵ペアを生成する

— 能動認証用公開鍵にデジタル署名を付ける

— 能動認証用鍵ペアを旅券冊子用 IC に格納する

加えて、旅券発行当局の許可された利用者は、後述する前提条件 A.PKI に対応して、旅券冊子用 IC に格納するデータのデジタル署名生成に使う鍵ペアをセキュアに管理すると共に、PKI 環境を適切に維持する必要がある。

5 アーキテクチャに関する情報

本章では、本 TOE の範囲と主要な構成（サブシステム）を説明する。

5.1 TOE境界とコンポーネント構成

TOE の構成を図 5-1 に示す。

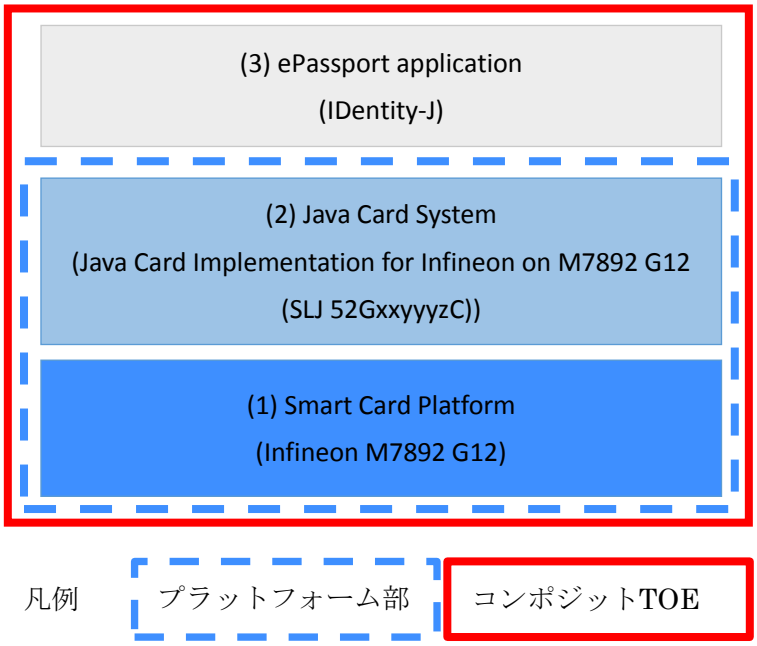


図 5-1 TOEの構成

TOE を構成するコンポーネントについて説明する。

表 5-1 TOEを構成するコンポーネントとその概要

	コンポーネント	概要
(1)	Smart Card Platform	Infineon Technology社製ICチップ及び暗号ライブラリ。 プラットフォームのST[20]で識別されるM7892 G12を用いている。
(2)	Java Card System	Java CardのAPI, Virtual Machine, Runtime Environmentを提供する。(1)及び(2)が統合された形で、Java Card Platformとして認証されている（ST[20]参照）。 (1)を利用して、旅券冊子用ICに使用される暗号アルゴリズム及びセキュアメッセージング機能を提供する。
(3)	ePassport application (IDentity-J)	Java Card System上で動作する、IC旅券規格[24]で規定された機能を提供するアプレット。

5.2 IT環境

TOE は、旅券冊子用 IC に必要な組込みソフトウェアと、そのソフトウェアが動作するハードウェアプラットフォームを一体化した IC チップである。TOE は、端末装置から送られる無線信号電力で動作する。

6 製品添付ドキュメント

本 TOE に添付されるドキュメントの識別を以下に示す。TOE の利用者は、前提条件を満たすため下記ドキュメントの十分な理解と遵守が要求される。

ユーザーズガイド [26]

ID&Trust Ltd., ID&Trust IDentity-J-v1.0 Applet for Japanese ePassport - User's Guide v1.0.12.

7 サイトセキュリティ

本 TOE の評価では、ALC_DVS.2 の評価において、Minimum Site Security Requirements[15]を適用した。評価作業中に発見された懸念は、全て所見報告書として発行され、開発者及び申請者に報告された。それらの懸念は、開発者及び申請者による見直しが行われ、最終的に、全ての懸念が解決されている。

8 評価機関による評価実施及び結果

8.1 評価機関

評価を実施した TÜV Informationstechnik GmbH, Evaluation Body for IT Security 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。

8.2 評価方法

評価は、CC パート 3 の保証要件について、CEM 及び CC サポート文書（[12][13][14][15]）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、本 TOE の概要と、CEM 及び CC サポート文書（[12][13][14][15]）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。

8.3 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、平成 30 年 7 月に始まり、令和元年 7 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。また、平成 30 年 10 月及び 11 月に開発・製造現場へ赴き、記録及びスタッフへのヒアリングにより、構成管理・配付・開発セキュリティの各ワークユニットに関するプロセスの施行状況の調査を行った。また、平成 30 年 10 月に開発者サイトで開発者のテスト環境を使用し、開発者テストのサンプリングチェック及び評価者テストを実施した。

評価作業中に発見された問題点は、全て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、全ての問題点が解決されている。

評価は、CC サポート文書([12][13][14])に基づくコンポジット評価が適用され、参照されるプラットフォームの認証報告書は、BSI-DSZ-CC-0869-V2-2019[22][14]である。

---

[14] プラットフォームのCCRAの相互承認範囲を超える部分については、プラットフォームの評価がJISEC傘下でもある評価機関で実施され、同じ評価機関がコンポジット評価を担っていることを踏まえて、コンポジット評価の中で再利用できると確認した。

8.4 製品テスト

評価者は、開発者の実施したテストの正当性を確認し、評価の過程で示された証拠と開発者のテストを検証した結果から、必要と判断された再現・追加テスト及び脆弱性評定に基づく侵入テストを実行した。

8.4.1 開発者テスト

評価者は、開発者が実施した開発者テストの完全性と実際のテスト結果の証拠資料を評価した。評価者が評価した開発者テストの内容を以下に説明する。

(1) 開発者テスト概説

開発者テストの概説は以下のとおりである。

a) テスト概要

開発者テストは大きく、(i) 機能テストと(ii) 発行テストの二種類に分類される。機能テストは、ICAO が定めるテスト仕様[35]に従った機械読み取り式旅券に対する共通のテストである。発行テストは、ICAOでカバーされていない、旅券冊子用ICの発行手順に関連するテストである。

＜開発者テスト手法＞

TOE のテストの実施に際して、IC カードリーダを用い、TOE の非接触インタフェースを介して、コマンド APDU を送信し、レスポンス APDU を受信して、TOE の振舞いの確認を行った。

＜開発者テストツール＞

ID&Trust Ltd.が機能テストに利用したツールを表 8-1 に示す。マクセル株式会社が発行テストに利用したツールを表 8-2 に示す。

表 8-1 開発者テストツール (機能テスト)

ツール名称	概要・利用目的
Gemalto Prox-DU Contactless_12400279	非接触インタフェースを備えたICカードリーダで、TOEにコマンドAPDUを送信し、レスポンスAPDUを受信する。
GlobalTester TestManager Release 2.9.0v20160509	ID&Trust Ltd.が使用した旅券冊子用ICのテストツール。 ドイツBSI及びICAOによって発行された旅券冊子用ICのテスト仕様に基づくテストが実行可能にする。

ツール名称	概要・利用目的
Windows PC	上記ICカードリーダを接続し、上記ソフトウェアが動作するPC。

表 8-2　開発者テストツール (発行テスト)

ツール名称	概要・利用目的
DUALi DE-620	非接触インタフェースを備えたICカードリーダで、TOEにコマンドAPDUを送信し、レスポンスAPDUを受信する。
ePassport Committee member of JBMIA test tool version 1.0.0.1	マクセル株式会社が使用したテストツール。
IDnT perso tool 3.7.1476	TOEの初期化及び個人情報設定に用いられたツール。
Windows PC	上記ICカードリーダを接続し、上記ソフトウェアが動作するPC。

＜開発者テストの実施内容＞

機能テストについては、ICAO が定めるテスト仕様[35]の中で、テストシナリオと期待値が明記されており、そのシナリオに沿って期待値と実際の値との比較が行われた。

発行テストについても、テストの事前条件が明記された上で、テスト手順と期待値が明記されており、そのテスト手順に沿って期待値と実際の値との比較が行われた。

b) **開発者テストの実施範囲**

開発者テストは開発者によって234項目実施された。カバレージ分析によって、機能仕様に記述された全てのセキュリティ機能と外部インタフェースがテストされたことが検証された。

カバレージ分析によって、機能仕様に記述された全てのセキュリティ機能と外部インタフェースが十分にテストされたことが検証された。プラットフォームが評価・認証されているという前提の下、深さ分析によって、TOE設計に記述された全てのサブシステムとサブシステムインタフェースが十分にテストされたことが検証された。

c) 結果

評価者は、開発者テストの実施方法、実施項目の正当性を確認し、テスト計画書に示された実施方法と実際の実施方法が一致することを確認した。評価者は、開発者が期待したテスト結果と開発者によって実施されたテスト結果が一致していることを確認した。

8.4.2 評価者独立テスト

評価者は、開発者テストから抽出したテスト項目を使用して製品のセキュリティ機能が実現されていることを再確認するサンプルテストを実施するとともに、評価の過程で示された証拠から、製品のセキュリティ機能が確実に実現されていることをより確信するための評価者独立テスト（以下「独立テスト」という。）を実施した。評価者が実施した独立テストを以下に説明する。

(1) 独立テスト構成

本 TOE には、EF.CardAccess、EF.DG14 及び EF.DG15 に埋め込まれる情報によって表 8-3の2つのバリエーションが存在し、評価者が実施した独立テストでは、両方についてテストが実施された。

表 8-3 TOEのバリエーション

識別	PACE OID[15]	楕円曲線ドメインパラメタ[16]	能動認証用のECDSAの中で使用されるハッシュ関数[17]
Config_A	id_PACE_ECDH_GM_AES_CBC_CMAC-128[18]	NIST P-256	SHA-256
Config_B	id_PACE_ECDH_GM_AES_CBC_CMAC-256[19]	NIST P-384	SHA-384

＜独立テストツール＞

独立テストにおいて利用したツールを表 8-4 に示す。

表 8-4 独立テストで使用したツール

ツール名称	概要・利用目的

[15] EF.CardAccess及びEF.DG14に情報が記録されている。
[16] PACEの中のECDH及び能動認証用のECDSAに適用される。EF.CardAccess, EF.DG14, EF.DG15に情報が記録されている。
[17] EF.DG14に情報が記録されている。
[18] TR-03111[25]の中で、OIDを定義している。
[19] TR-03111[25]の中で、OIDを定義している。

ツール名称	概要・利用目的
SDI011	非接触ICカードリーダ
WOLF v1.84 / Python v2.7	APDU scriptのためのツール。
Windows PC	上記ICカードリーダが動作し、上記ソフトウェアが動作するWindows PC

(2) 独立テスト概説

評価者の実施した独立テストは以下のとおりである。

a) 独立テストの観点

評価者が、開発者テスト及び提供された評価証拠資料から考案した独立テストの観点を以下に示す。

評価者は、インタフェースに対する開発者テストを補強し、開発者テスト方針を補うという考えのもと、独立テストを考案した。独立テストの考案にあたって、開発者テストを補強するほかに、複雑度やインタフェース及び関連する機能の脆弱性へのつながりやすさが考慮された。その上で、具体的には、次に関連するTSFIをカバーするように選択された。

- 識別・認証
- 干渉、論理的なタンパー、及びバイパスに対する保護
- セキュアメッセージング
- ガイダンスに従った準備手順

選択のプロセスは、評価機関の経験に基づき、全てのTOEセキュリティ機能がいずれかの部分集合に含まれるように選択された。全ての暗号機能はプラットフォームによって提供され、プラットフォーム評価の中で十分にテストされていることが考慮された。

＜独立テストの観点＞

① 異常系の振舞いの確認

② 基本アクセス制御(BAC)が無効化されていることの確認

③ 書込み禁止機能の正しい振舞いの確認

b) 独立テスト概要

評価者は、開発者テスト及び提供された評価証拠資料から、以下の観点で追加の独立テストを考案した。評価者が実施した独立テストの概要は以下のとおりである。

＜独立テスト手法＞

このTOEについては、APDUインタフェースが本質的であり、焦点を当ててテストを実施した。

＜独立テストの実施内容＞

独立テストは、評価者によって18項目実施された。

独立テストの観点とそれに対応したテスト内容を表 8-5 に示す。

表 8-5 実施した独立テスト(観点①～③)

観点	テスト概要
異常系の振舞い	— ファイルの読出しに先立って、PACEによる認証が必要なファイルについて、PACEによる認証を完了せずにファイル選択や読出しができないことを確認する。 — 書込み不可となっているファイルについて、PACEによる認証を経ても書込みできないことを確認する。 — 調達者から提供された仕様書で文書化されていないファイルについて、ISO/IEC 7816-4のファイルシステムを想定して、ファイル選択できないことを確認する。 — PACEによる認証を経た上で、セキュアメッセージングによるコマンドの再生攻撃が検出されることを確認する。
BACの無効化の確認	— TERMINATE BACコマンドを実行して、既にBACが無効化されており、成功しないことを確認する。 — BACによる認証に必要な、GET CHALLENGEコマンドが使えないことを確認する。
書込み禁止機能の正しい振舞いの確認	旅券冊子発行後のTOEに対して、VERIFYコマンドが適切にブロックされるか確認する。

c) 結果

評価者が実施した全ての独立テストは正しく完了し、評価者はTOEのふるまいを確認した。評価者は、全てのテスト結果と期待されるふるまいが一致していることを確認した。

8.4.3 評価者侵入テスト

評価者は、評価の過程で示された証拠から、想定される使用環境と攻撃レベルにおいて懸念される脆弱性となる可能性があるものについて、必要と思われる評価者侵入テスト（以下「侵入テスト」という。）を考案し実施した。評価者が実施した侵入テストを以下に説明する。

(1) 侵入テスト概説

評価者が実施した侵入テストの概説は以下のとおりである。

a) 懸念される脆弱性

評価者は、提供された証拠資料や公知の情報より、潜在的な脆弱性を探索し、CCサポート文書 ([13][14]) に基づいて侵入テストを必要とする脆弱性を識別した。具体的には、侵入テストを必要とする脆弱性の識別にあたっては、次の2つの背景・事実が考慮され、これらの評価における脆弱性評定が再利用できると判断され、本TOEとして最終的に必要な侵入テストが識別された。

- プラットフォームの評価を通じて、次の攻撃への耐性を確認する侵入テストが実施され、その結果、プラットフォームはEAL5+ ALC_DVS.2, AVA_VAN.5で認証されている。
  - サイドチャネル攻撃
  - 故障注入攻撃
  - メモリ内容の操作
- プラットフォームが依存するSmart Card Platformの評価を通じて、物理的なタンパー及び物理的な改変を必要としない攻撃への耐性を確認する侵入テストが実施され、その結果、Smart Card Platformは EAL6+ ALC_FLR.1で認証されている。

① まず、評価対象のTOEに関連して、共通的で、潜在的な脆弱性を探索した結果、セキュアメッセージングプロトコルの実装に、その振舞いから平文又は暗号鍵の復元を可能とするような可能性が懸念された。

② 次に、上述の背景・事実を考慮した上で、プラットフォームのガイダンスに基づいて実装された対策を確認するためのテストが実施された。

その他、CCサポート文書[13]で言及されている、ソフトウェア攻撃に分類される次の侵入テストについて、分析の結果、懸念される脆弱性は悪用できないと考えられるが、評価の確信を得るためのテストとして実施された。

③ コマンドの編集
④ 直接プロトコル攻撃
⑤ リプレイ攻撃
⑥ 認証やアクセス制御のバイパス

b) 侵入テストの概要

評価者は、潜在的な脆弱性が悪用される可能性を検出するために、以下の侵入テストを実施した。

＜侵入テスト環境＞

侵入テストの環境の構成要素、および侵入テストで使用したツールの詳細を表 8-6 に示す。

表 8-6　侵入テスト構成

構成品	概要・利用目的
TOE	ID&Trust IDentity-J with SAC (PACE) and AA version 1.0 on IFX M7892 G12 SLJ 52G v1.0.7052 表 8-3に記載したバリエーションの全てが侵入テストの対象とされた。
SDI011	非接触ICカードリーダ
WOLF v1.84 / Python v2.7	APDU scriptのためのツール。
Windows PC	上記ICカードリーダが動作するパソコンと上記ソフトウェアが動作するWindows PC

＜侵入テストの実施項目＞

懸念される脆弱性と対応する侵入テスト内容を表 8-7 に示す。

表 8-7　侵入テスト概要

脆弱性の観点	テスト概要
①セキュアメッセージングプロトコルの実装	入力コマンドを編集しても、過剰に内部の情報を提供するような振舞いをしないか確認する。
②プラットフォームのガイダンスに基づく対策の実装	PACEの相互認証の手順を試行して、TOEの振舞いを観察することにより、文書化された対策が実装されていることを確認する。
③コマンドの編集 ④直接プロトコル攻撃	パラメタを様々に加工した、能動認証のコマンドに対するTOEの振舞いが、文書化された仕様書に沿っていることを確認する。 PACEの認証手順の中で、端末装置からTOEに送信された公開鍵が楕円曲線上に無い場合の振舞いがセキュアであることを確認する。
⑤リプレイ攻撃	セキュアメッセージングが適用された後、コマンドの再生攻撃が検出され対処されること、無効なコマンドが処理されないこと又はTOEがリセットすること。

⑥ 認証やアクセス制御のバイパス	個人情報設定後のTOEに対して、PACEの認証を経た後、セキュアメッセージングを適用した上で、ファイル生成できないこと。 PACEの認証手順におけるコマンドの順序を変化させることを通じて、PACEを実現するステートマシーンが適切に実装されていることを確認する。

c) **結果**

評価者が実施した侵入テストでは、想定する攻撃能力を持つ攻撃者が悪用可能な脆弱性は確認されなかった。

8.5 評価構成について

TOE 評価において、表 8-3 に示す、調達者が旅券冊子用 IC に要求する 2 つの構成が用いられた。

TOE 評価では、「8.4.2 評価者独立テスト」に示す構成において、評価を行った。

光学文字読み取り装置を備えていない IC カードリーダが用いられ、MRZ データの情報をツール側に設定する方式を採用して評価が実施された。実際の運用においては、光学文字読み取り装置を備えた端末装置が使われるが、TOE のインタフェースは非接触インタフェースであることを踏まえて、評価者は、上記の評価構成は、適切であると判断した。

8.6 評価結果

評価者は、評価報告書をもって本 TOE が CEM 及び CC サポート文書（[12][13][14]）のワークユニット全てを満たしていると判断した。

評価では以下について確認された。

PP 適合：旅券冊子用 IC のためのプロテクションプロファイル － SAC 対応（PACE）及び能動認証対応 －, 第 1.00 版, 2016年3月8日, 外務省領事局旅券課

セキュリティ機能要件： コモンクライテリア パート2 拡張

セキュリティ保証要件： コモンクライテリア パート3 適合

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。

EAL4パッケージの全ての保証コンポーネント

追加の保証コンポーネント　AVA_VAN.5、ALC_DVS.2

評価の結果は、第 2 章に記述された識別に一致する TOE によって構成されたもののみに適用される。

8.7 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。

9 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。

提出された証拠資料をサンプリングし、その内容を検査し、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。

③ 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。

評価報告書に示された評価者の評価方法がCEM及びCCサポート文書（[12][13][14][15]）で示されている方法に適合していること。

9.1 認証結果

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、本 TOE の評価が CC パート 3 の EAL4 及び保証コンポーネント AVA_VAN.5、ALC_DVS.2 に対する保証要件を満たすものと判断する。

9.2 注意事項

本 TOE の調達者・利用者は、本 TOE が使用されるシステムのリスクマネジメントの中でこの認証結果を利用するにあたっての検討を行うべきである。例えば、攻撃方法・技術の変化を踏まえて、この認証書及び依存する認証書の有効性の確認"re-assessment"をいつまでに行うべきかを定めておくべきである。また、本 TOE の調達者・利用者は、本 TOE が使用されるシステムのリスクマネジメントの中で、暗号アルゴリズムの使用方法の有効性についても、見直さなければならない。

10 附属書

特になし。

11 セキュリティターゲット

本 TOE の ST-Lite[19]は、本報告書とは別文書として以下のとおり提供される。

Security Target Lite ID&Trust IDentity-J with SAC (PACE) and AA, v1.4, 26.07.2019, ID&Trust Ltd.

この ST-Lite は、評価された完全な ST[18]を、CC サポート文書である ST sanitising for publication [17] に従って、公開用に不適切な部分を整理したものである。

12 用語

12.1 CCに関する略語

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）
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）

12.2 本認証報告書で使用された用語及び略語

本報告書で使用された TOE に関する略語を以下に示す。

鍵共有利用アクセス制御	IC旅券規格[24]で規定された相互認証及びセキュアメッセージングの方式の一つで、PACEv2を指す。
基本アクセス制御	IC旅券規格[24]で規定された相互認証及びセキュアメッセージングの方式の一つで、BACを指す。
受動認証	TOEに格納する個人情報データに旅券発行者のデジタル署名を施し、旅券発行側と受け入れ側の双方が相互運用性の保証されたPKIシステムを用いることによって、TOEから読み出されたデータの真正性を確認できるようにする方式。 ICAOにおいて、手順が標準化されている。
セキュアメッセージング	コマンド及びその応答に対して、その一部又は全体を暗号によって保護するための方法 ([JIS X 6320-4:2017, 定義3.50]を参照)
能動認証	TOEのパーツであるICチップ内に公開鍵暗号方式に基づく公開鍵・秘密鍵ペアを格納し、秘密鍵を秘匿する。TOEを認証しようとする外部装置に公開鍵を渡し、TOE内に秘匿された秘密鍵を用いたチャレンジレスポンス方式による暗号演算によってTOE認証を実施する。 ICAOにおいて、手順が標準化されている。
能動認証情報アクセス鍵	能動認証用鍵ペアを書き込むための認証データ。
パスワード鍵ファイル	MRZ データから導出され、鍵共有利用アクセス制御手続きにおいてナンスの暗号化に使われる鍵が格納されるファイル。

発行	法的にその効力を有する状態におくこと。旅券そのものを作成，旅券として使用できる状態にすること。
輸送鍵	輸送途中の不正利用からICチップを保護するための認証データ。
読出し鍵	ICチップシリアル番号を読み出すための認証データ。
旅券	各国の政府あるいはそれに相当する公的機関が発行する国外渡航者のための身分証明書のこと。旅券は1冊の文書(旅券冊子)形式をとるのが一般的である。
旅券事務所	TOEを含む旅券冊子に旅券保持者の個人情報を設定し、旅券発行を行う。各地に設置され、旅券保持者に旅券冊子を交付する窓口となる。
旅券製造業者	旅券冊子を作成し、TOEに基本的データ(旅券番号等の管理データ、能動認証用公開鍵・秘密鍵ペア等)を設定する。
旅券発行当局	外務省とその指示下にある旅券製造業者及び各地の旅券事務所が該当する。旅券製造業者は、TOEを埋め込んだプラスチックシートを旅券冊子に綴じ込み、個人情報（生年月日や顔画像データ、それらのデータに関わるセキュリティ上のデータなど）以外の必要データを設定する。旅券事務所では、個人情報に関わる旅券データを設定する。
AES	Advanced Encryption Standard
ATR	Answer To Reset。リセット応答
BAC	Basic Access Control
CBC	Cipher Block Chaining
CMAC	Cipher-based MAC
DEMA	Differential Electro-Magnetic Analysis
DES	Data Encryption Standard
DF	専用ファイル。ファイル制御情報と任意選択として割付け利用可能なメモリとを含んでいる構造。 ([JIS X 6320-4:2017, 定義3.19]を参照)
DFA	Differential Fault Analysis
DG	Data Group
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EF	基礎ファイル。同一ファイル識別子を共有するデータオブジェクト、レコード、又はデータ単位の集合 ([JIS X 6320-4:2017, 定義3.23]を参照)
EF.ATR/INFO	Answer-to-Reset file, or Information file ([ISO/IEC 7816-4:2013, 4]を参照)
EF.CardAccess	MF直下に配置されるEFで、PACEv2セキュリティ情報を格納する。
EF.COM	旅券冊子用ICにどのようなフォーマットでデータを格納するかを規定する論理データ構造(Logical Data Structure：LDS)のバージョン情報、及び旅券用アプリケーションプログラムが格納され

	るDF配下に格納されるData Groupの一覧を提供する。
EF.DG1	MRZデータを格納するEF
EF.DG2	顔画像を格納するEF
EF.DG13	管理データ（旅券番号・冊子管理番号）を格納するEF
EF.DG14	PACEv2 セキュリティ情報、能動認証用ハッシュ関数情報を格納するEF
EF.DG15	能動認証用公開鍵を格納するEF
EF.SOD	他のData Groupのハッシュ値と受動認証用のデジタル署名を格納している。
ICAO	International Civil Aviation Organization (国際民間航空機関)
JCOS	Java Card Operating System
MAC	Message Authentication Code
MF	主ファイル。DFの階層構造を用いているカードでファイル構成の根幹となる唯一のDF。 ([JIS X 6320-4:2017, 定義3.33]を参照)
MRTD	Machine Readable Travel Document (機械読み取り式旅券)
MRZ	Machine Readable Zone (機械読み取り領域) IC旅券の身分事項ページに印刷されたデジタル顔画像、身分事項ページ下部の88文字の機械読み取り領域のこと。姓名、国籍、性別、生年月日、旅券番号、有効期間満了日等が記載される。
MRZデータ	IC旅券券面に印字され、端末装置によって読み取られる情報。
OID	Object Identifier (オブジェクト識別子)
PACE	Password Authenticated Connection Establishment
PACEv2	Password Authenticated Connection Establishment v2
PACEv2セキュリティ情報	PACEv2で使用する暗号アルゴリズムやドメインパラメタ等の情報。
PKI	Public Key Infrastructure
SAC	Supplemental Access Control [36] 1.1.3 Supplemental Access Controlでは次のように説明されている。 “This Technical Report specifies PACE v2 as an access control mechanism that is supplemental to Basic Access Control. PACE MAY be implemented in addition to Basic Access Control, i.e. ・States MUST NOT implement PACE without implementing Basic Access Control if global interoperability is required. ・Inspection Systems SHOULD implement and use PACE if provided by the MRTD chip.”
SHA	Secure Hash Algorithm
SOD	Document Security Object

13 参照

[1] ITセキュリティ評価及び認証制度の基本規程, 平成30年7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, 平成30年9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, 平成30年9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 3.1 Revision 5, April 2017, CCMB-2017-04-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 5, April 2017, CCMB-2017-04-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 5, April 2017, CCMB-2017-04-003

[7] 情報技術セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル バージョン3.1 改訂第5版, 2017年4月, CCMB-2017-04-001 (平成29年7月翻訳第1.0版)

[8] 情報技術セキュリティ評価のためのコモンクライテリア パート2: セキュリティ機能コンポーネント バージョン3.1 改訂第5版, 2017年4月, CCMB-2017-04-002 (平成29年7月翻訳第1.0版)

[9] 情報技術セキュリティ評価のためのコモンクライテリア パート3: セキュリティ保証コンポーネント バージョン3.1 改訂第5版, 2017年4月, CCMB-2017-04-003 (平成29年7月翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology Version 3.1 Revision 5, April 2017, CCMB-2017-04-004

[11] 情報技術セキュリティ評価のための共通方法: 評価方法 バージョン3.1 改訂第5版, 2017年4月, CCMB-2017-04-004 (平成29年7月翻訳第1.0版)

[12] Application Notes and interpretation of the Scheme(AIS34), Version 3, September 2009, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[13] Joint Interpretation Library - Application of Attack Potential to Smartcards, Version 2.9, January 2013

[14] Joint Interpretation Library - Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018

[15] Joint Interpretation Library – Minimum Site Security Requirements, Version 2.1 (for trial use), December 2017

[16] 旅券冊子用 IC のためのプロテクションプロファイル　－SAC 対応(PACE) 及び能動認証対応－第 1.00 版（認証識別：JISEC C0499)

[17] ST sanitising for publication, April 2006, CCDB-2006-04-004

[18] Security Target ID&Trust IDentity-J with SAC (PACE) and AA, v1.3, 26.07.2019, ID&Trust Ltd.

[19] Security Target Lite ID&Trust IDentity-J with SAC (PACE) and AA, v1.4, 26.07.2019, ID&Trust Ltd.

[20] Security Target Lite for BSI-DSZ-CC-0869-V2-2019, “Security Target Lite Java Card Platform Implementation for Infineon on M7892 G12 (SLJ52GxxyyyzC) v2.0”, Version 3.6, May 2019, Oracle Corporation

[21] Security Target Lite for BSI-DSZ-CC-0891-V3-2018, “Security Target Lite Common Criteria EAL6 augmented / EAL6+ M7892 Design Steps D11 and G12”, Version 1.2, 2017-11-21, Infineon Technologies AG

[22] Certification Report BSI-DSZ-CC-0869-V2-209 for Java Card Platform Implementation for Infineon on M7892 G12 (SLJ 52GxxyyyzC) V2.0, 13 June 2019, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[23] ID&Trust IDentity-J with SAC (PACE) and AA version 1.0 on IFX M7892 G12 SLJ 52G EVALUATION TECHNICAL REPORT SUMMARY, Version 5, 2019-07-29, TÜV Informationstechnik GmbH – Evaluation Body for IT Security

[24] DOC 9303 Machine Readable Travel Documents Seventh Edition, ICAO, 2015

[25] Technical Guideline TR-03111, Elliptic Curve Cryptography, Version 2.0, 2012, Bundesamt für Sicherheit in der Informationstechnik

[26] ID&Trust IDentity-J-v1.0 Applet for Japanese e-Passport User’s Guide, Version 1.0.12, 2019-07-21

[27] OBSERVATION REPORT (OR) AGD and FSP, Version 7, 2019-06-11, Evaluation Body for IT-Security of TÜV Informationstechnik GmbH (TÜViT)

[28] OBSERVATION REPORT (OR) ALC ID&T, Version 3, 2019-02-26, Evaluation Body for IT-Security of TÜV Informationstechnik GmbH (TÜViT)

[29] OBSERVATION REPORT (OR) ASE, Version 9, 2019-07-19, Evaluation Body for IT-Security of TÜV Informationstechnik GmbH (TÜViT)

[30] OBSERVATION REPORT (OR) ADV (TDS & ARC), Version 6, 2019-04-24, Evaluation Body for IT-Security of TÜV Informationstechnik GmbH (TÜViT)

[31] OBSERVATION REPORT (OR) NPB, Version 3, 2018-11-20, Evaluation Body for IT-Security of TÜV Informationstechnik GmbH (TÜViT)

[32] OBSERVATION REPORT (OR) ALC MAXELL, Version 4, 2019-03-04, Evaluation Body for IT-Security of TÜV Informationstechnik GmbH (TÜViT)

[33] OBSERVATION REPORT (OR) ATE, Version 3, 2019-05-21, Evaluation Body

for IT-Security of TÜV Informationstechnik GmbH (TÜViT)

[34] 旅券冊子用ICのためのプロテクションプロファイル －能動認証対応－ 第1.00版 2010年2月15日 外務省領事局旅券課（認証識別：JISEC-C0247）

[35] RF protocol and application test standard for eMRTD – part 3, tests for application protocol and logical data structure, Version: V2.07, October 10, 2014, ICAO.

[36] International Civil Aviation Organization, ICAO MACHINE READABLE TRAVEL DOCUMENTS, TECHNICAL REPORT, Supplemental Access Control for Machine Readable Travel Documents, Version 1.1, 15 April 2014