ＳＴ確認報告書

評価対象

申請受付年月日(受付番号)	**平成14年6月14日（ST確認2010）**
確認番号	V024
ＳＴ確認申請者	**日本電信電話株式会社**
ＳＴの名称	Trust-KMS v6.1 Security Target
ＳＴのバージョン	**第3.4版**
ＰＰ適合	**なし**
適合する保証要件	ASE（ST評価）クラス （TOEの保証パッケージはEAL3）
ＳＴ開発者	**日本電信電話株式会社**
評価実施機関の名称	**株式会社電子商取引安全技術研究所評価センター**

上記のSTについての評価は、以下のとおりであることを確認したので報告します。
平成17年3月9日

独立行政法人 情報処理推進機構
セキュリティセンター情報セキュリティ認証室
技術管理者　田渕　治樹

評価基準等：「セキュリティターゲットの確認業務実施規程」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 2.1
② Common Methodology for Information Technology Security Evaluation Version 1.0

評価結果：合格

「Trust-KMSセキュリティターゲット」は、独立行政法人 情報処理推進機構が定めるセキュリティターゲットの確認業務実施規程に従い、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

1.1 はじめに

このST確認報告書は、「Trust-KMSセキュリティターゲット　第3.4版」（以下「本ST」という。）について株式会社電子商取引安全技術研究所評価センター（以下「評価実施機関」という。）が行ったセキュリティ評価に対し、その内容の確認結果を申請者である日本電信電話株式会社に報告するものである。

本ST確認報告書の読者は、本書とともに、対応する本ST[1]を併読されたい。前提となる環境条件、対応するセキュリティ対策方針とその実施のためのセキュリティ機能要件、保証要件及びそれらの要約仕様は、本STにおいて詳述されている。

本ST確認報告書は、本STに対する確認結果を示すものであり、対応するTOEのいかなる実装についても言及していないことに留意されたい。

注：本ＳＴ確認報告書では、ＩＴセキュリティ評価及び認証制度が定めるＩＴセキュリティ評価基準、ＩＴセキュリティ評価方法の各々をＣＣ、ＣＥＭと総称する

1.2 評価製品

1.2.1 製品名称

本STが対象とする製品は、以下のとおりである。なお、TOEの正確な範囲は、1.2.3節で定義される。

・名称:　　Trust-KMS
・バージョン　6.1
・開発者:　　日本電信電話株式会社

1.2.2 製品概要

本製品は、PKIにおける利用者登録局（RA）である。RA管理者・申請者・審査者によって運営されるもので、一般利用者の鍵対の生成と認証局（CA）への証明書発行の申請手続きを行うソフトウェア製品である。 CAと連携することで、公開鍵暗号方式を基盤とした電子認証システムの役割を果たす。

1.2.3 TOEの範囲

本TOEは、図1-1 に示す環境下において動作する。RAサーバとRAクライアント（RA管理者端末、審査者端末、申請者端末）に、Trust-KMSがインストールされる。RAクライアントには、ICカードリーダが接続される。また、RAサーバはCAサーバとファイアウォールを介して接続される。

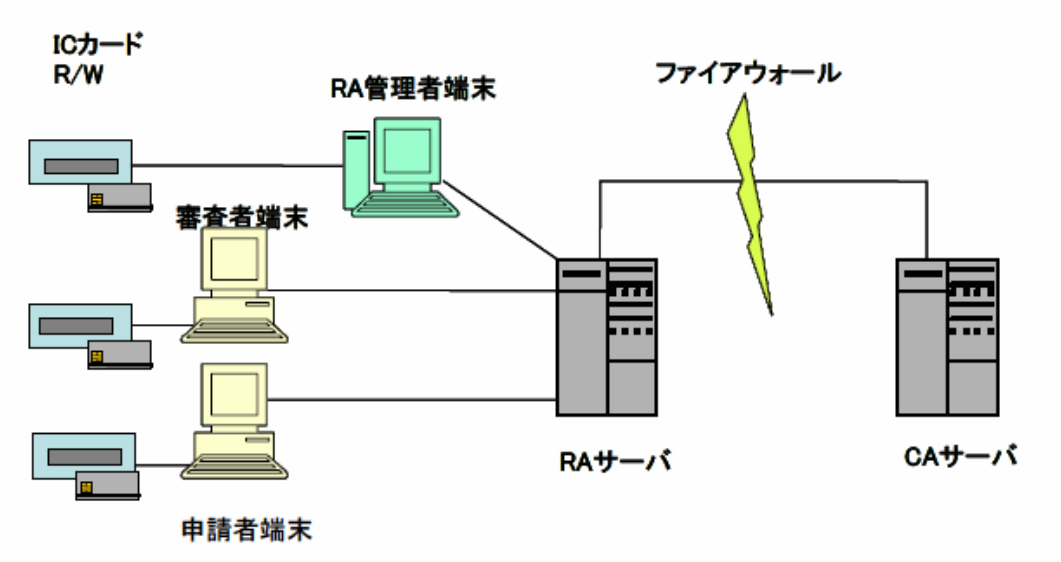

図1-1 TOEの動作環境

図中に示す構成要素は、次の通りである。

・RAサーバ
登録局としてのコア機能を行う。Trust-KMSがインストールされる。

・RAクライアント（RA管理者端末）
RA管理者向けに提供され、システム管理や初期設定、RA管理者または申請者または審査者の登録や削除に使用する。Trust-KMSがインストールされる。

・RAクライアント（申請者端末、審査者端末）
一般利用者の管理や証明書申請等に使用する。Trust-KMSがインストールされる。

・ICカード
RA管理者、審査者、申請者あるいは一般利用者の証明書の格納に使用する。

・ICカードR/W(リーダライタ)
RA管理者、申請者、審査者、一般利用者のICカードを読み書きするためのハードウェア。

・CAサーバ
認証局として、証明書の発行等を行う。

・ファイアウォール
RAサーバが外部のCAサーバと安全に接続するために使用する。

TOEの範囲を図1-2 に示す。下図のTOEと記述された部分がTOEの範囲である。

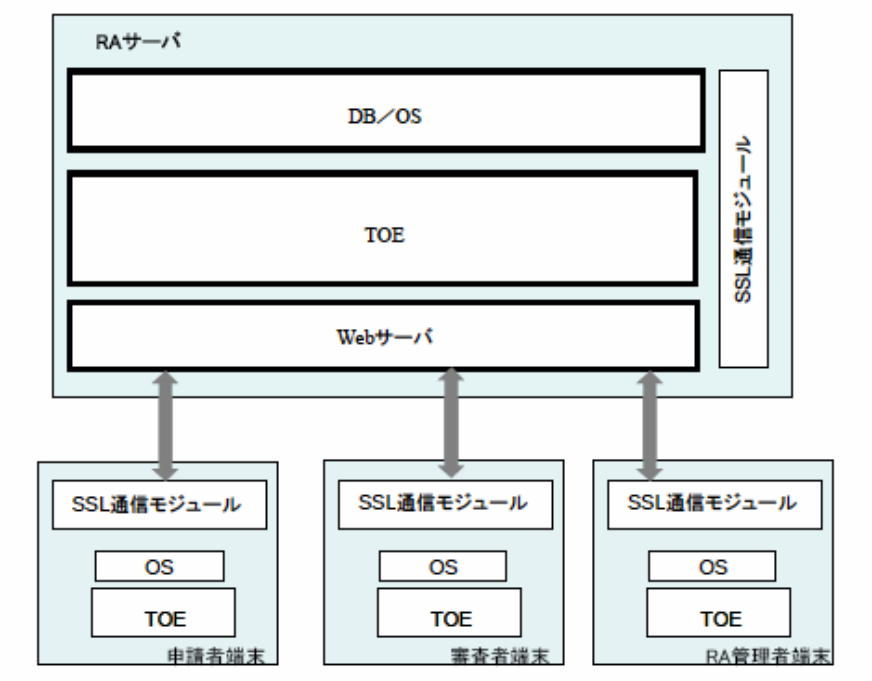

図1-2 TOEの範囲

1.2.4 TOEの動作概要

Trust-KMSは、公開鍵暗号方式を利用してネットワーク上における本人性の確認を実現するPKI（Public Key Infrastructure）を構成する製品のうち、登録局(RA)としての機能を提供する。

(1) TOEの利用方法

TOEが行うRAサービスの流れを説明する。なお、RAサービスとは一般利用者管理や証明書発行など登録局として行うサービスに対する総称である。

1)構築
RA管理者はTOEインストール時に、まずRAサーバ上でRAサーバの鍵対の生成を行う。この鍵はRAサーバで生成される申請書や登録書へ署名を付与するために用いられ、これによってCAにて申請書や登録書の真正性の確認を行うことが可能となる。次にRA管理者は、操作者の役割に応じた実行可能な操作のリスト（SNI及びSVP）の定義を行う。TOEはこのリストを使って申請書や報告書に対するアクセス制御を実施する。

2)運用

①一般利用者サービス

一般利用者の証明書発行の申請手続きは以下の通りに行われる。

申請者は、申請者端末を用いて証明書発行を希望する一般利用者の登録と鍵対の生成を行う（一般利用者自身が鍵対を用意する場合はその鍵対をRAサーバへ登録する）。生成された一般利用者の秘密鍵は、一般利用者が入力したパスワードを元に暗号化され、証明書の配付完了まで安全にRAサーバに保管される。

次に、申請者は証明書発行依頼のための申請書を作成し、CAサーバへ送付する。このとき審査者が役割として存在する場合は、証明書発行依頼のチェックを行い、申請の可否を決定することも可能である。

RAサーバは、CAサーバから証明書を報告書として受け取り、一般利用者用のICカードへ秘密鍵と共に格納する。一般利用者の秘密鍵はこのときRAサーバから削除される。

一般利用者の申請依頼では、証明書の発行以外に証明書の失効も行う。

②管理

RA管理者はTOEの操作者であるRA管理者・申請者・審査者をRAサーバに対して登録し、鍵対を生成する。以後、一般利用者の証明書発行と同様の流れで、操作者の証明書が発行され、各々のICカードに格納される。TOEの操作者は自身のICカードを用いて、RAクライアントから識別･認証を行ってログインし、サービスの運営を行う（RA管理者・申請者・審査者については「(3)TOE関与者」を参照のこと）。

また、TOEはサービス運用中に発生した事象のログを生成し運営側の管理者・操作者に提供する事で、不正な操作を追跡することが可能である。また、ログ自体の改ざんを検出する機能も有している。

(2) TOEの機能

1)RAサーバの鍵対の生成

RAサーバでRAサーバの鍵対（公開鍵、及び秘密鍵）を生成し、TOE内に保存する。ただし、公開鍵はCAへ登録しCAの署名が付けられた後、保存する。

2)RA管理者、申請者、審査者の鍵対の生成

RAサーバでRA管理者、申請者、審査者の鍵対を生成し、TOE内へ保存する。ただし、公開鍵は（登録書として）CAで署名を付けられた後、TOE内に保存する。その後、RAクライアントを経由しPINによる本人確認が成功したICカードに上述の鍵対を格納する。

3)RA管理者、申請者、審査者の認証機能

RA管理者、申請者、審査者の認証は、上記2)のICカードをPINにより本人確認後、TC（時刻情報）、UID（ユーザID)、及びUIDC（ユーザ確認情報）の情報をICカー

ド内の秘密鍵で署名し、RAサーバで検証することで行う。

4)一般利用者の鍵対の生成

一般利用者の鍵対を生成し、秘密鍵とCA署名が付けられた公開鍵を一般利用者本人が確認されたICカードに格納する。

5)アクセス制御機能

サービス要求に対して操作のリストを確認し、役割に応じて申請書や報告書に対する操作を制御する。

6)登録書や申請書への署名生成機能

RA鍵による登録書や申請書への署名生成を行う。

7)ログ管理機能

サービス運用中の事象のログを生成し、ログ管理を行う。ログには署名を付与し、改ざん検出を可能とする。

8)RA管理者・申請者・審査者の秘密鍵の暗号化機能

RA鍵、RA管理者・申請者・審査者の秘密鍵、及び一般利用者の秘密鍵を暗号化し、DBに保存する。

(3) TOE関与者

本TOEに関与する人物と利用方法を以下に定義する。

・ RA管理者

システム管理者としての立場も兼ねている。RA管理者端末を使用しシステム管理や、RAの各サービスの管理、初期設定（各ポリシー設定や権限確認するためのもの（SVP）設定など）を行う。権限を持つRA管理者はRA管理者・申請者・審査者を登録あるいは削除を行うことができる。

・申請者

申請者端末を使用し一般利用者登録、証明書発行、一般利用者削除、証明書失効等の申請書を作成し、RAサーバへ送信する。

・ 審査者

審査者端末を使用し申請書をチェックし、申請者による証明書の発行申請を許すか否かを審査する。

・利用者

RAの提供するサービスを実際に受ける者である。RAシステムの運営側として操作を行う申請者とは別個の存在として考える。一般利用者からの情報は申請者が扱い、TOEは役割として識別しない。

1.3 評価実施

「Trust-KMS V6.1 セキュリティターゲット　第3.4版」のセキュリティ評価は、認証機関が運営するITセキュリティ評価・認証プログラムに基づき、「セキュリティターゲットの評価・確認申請等の手引き」[2]、「セキュリティターゲット 評価実施機関に対する要求事項」[3]、「セキュリティターゲットの確認申請者・登録者に対する要求事項」[4]に規定された内容に従い、評価実施機関によって実施された。

本評価の目的は、申請者から提出された本ST[1]が、CCパート1([5][8][11][14]のいずれか）附属書C、CCパート2([6][9][12][15]のいずれか)の機能要件及びCCパート3([7][10][13][16]のいずれか)のASEクラスの規定を満たしており、セキュリティ機能設計の基本文書として技術的に妥当なものであるかどうかを評価することである。ただし、ASEクラスの規定の中で、TOE評価と関連する要求事項については、評価の項目に含まれていない。なお、評価方法は、CEMパート2([17] [18][19]のいずれか)に準拠する。

認証機関は、評価実施機関が実施するSTの評価を監督し、ST評価が所定の手続きに沿って行われたことを確認した。評価は、平成17年2月の評価実施機関による「Trust-KMS V6.1セキュリティターゲット評価報告書」の提出をもって完了し、同報告書に基づき、認証機関は本ST確認報告書を作成した。

1.4 報告概要

1.4.1 PP適合

適合するPPはない。

1.4.2 EAL

本STが規定するTOEの評価保証レベルは、EAL3である。

1.4.3 セキュリティ機能強度

本STにおいてTOEに要求される最小機能強度レベルは、SOF-基本である。

1.4.4 セキュリティ機能

本STで扱うTOEのセキュリティ機能は以下のとおりである。

- 本人認証機能
  各アクション前に各端末においてICカード内にある鍵を利用して、RA サーバへアクセスするRA 管理者、申請者、審査者を認証する。

- ログ管理機能
  ログを適切に生成し、閲覧に適した形での読み出しが可能で、不正な改ざんを検出する。

- 暗号処理機能
  RA 管理者・申請者・審査者の秘密鍵と一般利用者の秘密鍵に対して、入力パスワードに対するMD5を用いた演算結果を鍵としてDES暗号（CBCモード）により暗号化や復号を行う。

- 鍵管理機能
  大きく分けて2つの鍵管理機能を有している。鍵の生成・配付・破棄機能及びRA 鍵署名生成機能である。

- アクセス制御機能
  アクセス制御ポリシーに従い、管理者によって維持されたセキュリティ属性のリストを元にアクセス制御を行う。アクセス制御ポリシーには、RAサービスを行う際にセキュリティ属性に基づいてあらかじめ決められたRA管理者・審査者・申請者がアクセス可能なオブジェクト（登録書・報告書・鍵対のテーブル、通信ポート）や実行可能な操作（読み出し、書き込み、消去）のリストが規定され、これに基づいて操作要求の承認が行われる。

1.4.5 脅威

TOEは、表1に示す脅威を想定し、本製品は、これに対抗する機能を備える。

表1　想定する脅威

識別子	内容
T.LOGIN	RA管理者、申請者、審査者以外の入室を許可された者が、不正なICカードを用いてTOEにログインし、登録書や申請書の作成等を行うかもしれない。

T.PRIVILEGES	申請者や審査者が、権限外の操作（不正な登録書や申請書の作成、各鍵対に対する不正な操作）を実行しようとするかもしれない。
T.CA_TRANSFER	RA管理者以外の者がIT機器を用いて、RAサーバとCAサーバとの間で転送中の保護資産に対し、改ざん、暴露を行うかもしれない。

1.4.6 組織のセキュリティ方針

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2に示す。

表2　組織のセキュリティ方針

識別子	内容
P.KEY	TOEが生成するRA管理者、申請者、審査者の認証に用いる秘密鍵と一般利用者の秘密鍵は、TOE内に安全に保管されなければならない。また、これらの秘密鍵がICカードに格納された後はTOEから削除しなければならない。
P.AUDIT_DATA	TOEはログの不正な改ざんや消去を検出しなければならない。

1.4.7 構成条件

本TOEをセキュアに使用するためには、TOE (ソフトウェア) をインストールするコンピュータ、TOEに接続される各種機器、ネットワーク、協働するサーバの構成などが特定の条件を満たしたものでなければならない。詳細については、2章を参照のこと。

1.4.8 動作環境の前提条件

TOEを使用する環境において有する前提条件を表3に示す。

これらの前提条件が満たされない場合、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3　TOE使用の前提条件

識別子	内容
A.ADMIN	RA管理者は信頼されており、ガイダンス文書に従って操作を実施し、１）他人にICカードを使わせない ２）ログイン中、他人にRA管理者端末を操作させない ３）RAサーバのOSやDBのパスワード、RA管理者端末のOSのパスワードを漏洩しない ものと想定される。
A.USER	TOEのサービスを受ける一般利用者は、秘密鍵の暗号化のためのパスワードを漏洩させたりしないものと想定される。 また、申請者、審査者は、OSのパスワードやICカードのPINを漏洩しないと想定され

	る。
A.PHYSICAL_PROTECT	TOEが動作するために必要なハードウェアは入退管理されている場所に設置され、物理的な攻撃から保護されていると想定される。
A.LAN	RAサーバとRAクライアント間の通信路において、申請情報などの通信情報が暴露されないものと想定する。
A.NETWORK	TOEはCAと接続する際、適切に設定されたファイアウォールを介して行うものと想定される。
A.PLATFORM	TOEを動作させるために必要なソフトウェア（OS、DBMS）やハードウェア（PC、ICカード、R/W）の動作は信頼できるものとする。

1.5 ST確認に関わる注意事項

ST確認は、CCで規定された評価の全過程から、ST評価の部分だけを抜き出した評価に基づいて行われるものである。したがって、ST評価を規定したASEクラスの要件の中で、TOE評価と関連する事項についてはST評価の対象になっていない。また、ASEクラス以外の保証クラスに属する事項、例えば、STの記載事項がそのとおりに設計されTOEに実装されているかどうか、TOEに悪用可能な脆弱性が残っていないかどうか、あるいはTOEの製造・配付が安全な手続きに基づいて行われているかなども評価の範囲外である。これら評価対象外の事項については確認も行われていないことに、本報告書の読者は留意すべきである。

ST確認は、TOEに対する、潜在的なものを含めたあらゆるセキュリティ上の脅威が完全に対策されていることを保証するものではない。評価完了後にTOEやそのIT環境にあらたな脅威が発見される可能性は常に考慮されるべきであり、TOE利用者は、TOEに関わる最新のセキュリティ関連情報に継続的な注意を払うことが必要である。

STの中で前提条件として記述されたものは、TOEを安全に使用する上での必須事項である。これらの条件が満たされないと、TOEのセキュリティ機能は、期待される効果を発揮することができない。前提条件を満たすためのTOEの安全な運用管理は、TOE利用者の責務である。

本ST確認報告書は、認証機関が該当するTOEを保証し、その使用を推奨することを意図したものではない。

2 TOE構成

本TOEは、RAサーバとRAクライアントに搭載されるソフトウェアであり、前述の図1-1に示すIT環境のコンポーネント及び他の装置と共に使用される。TOEを構成するソフトウェア、ハードウェア、及び関連する他の装置のリストと構成条件を以下に示す。

(1) TOEを構成するソフトウェアコンポーネント

・Trust-KMS v6.1 (RAサーバ内)

・Trust-KMSP v6.1 (RAクライアント内：RA管理者端末内、審査者端末内、及び申請者端末内)

(2) IT環境のソフトウェア/ハードウェアコンポーネント

・DBMS：データベース Oracle 8.1.7.3。RAサーバにインストールされる。

・OS：RAサーバのOS(Solaris8)及びRAクライアントのOS(Windows2000)

・Webサーバ：Appach 1.3.x。RAサーバにインストールされる。

・SSL通信モジュール：SSLを利用する通信（TOE内部のRAクライアントとRAサーバ間、RAサーバとTOE外であるCAサーバ間）に利用される。

・RAサーバハードウェア：Sun SPARCマシンを推奨。CPU: UltraSPARCⅡ 300MHz 以上 Memory: 512MB以上 HDD: 1GB以上の空き (データ量によりさらに増加)

・RAクライアントハードウェア：以下のPCを推奨。CPU: Pentium 300MHz以上、Memory: 128MB以上、 HDD: 100MB以上の空き。

・ICカード及びICカードR/W：Cryptoflex（Schlumberger社）

・CAサーバ：Trust-CANP v6.1 がインストールされている。

3 評価実施機関による評価結果

評価は、CCパート3のASEクラスの規定に基づき、CEMパート2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、ST評価報告書[20]において報告されている。ST評価報告書には、TOEの概要説明、CEMパート2のワークユニットごとの評価内容及び判断が記載されている。各ワークユニットの評価作業において発見された問題点及びその対処の経過・結果も記載されている。

評価実施機関が評価中に発見した問題点は、すべて、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。

総合判定は、「合格」である。

4 結論

4.1 ST確認実施

認証機関は、評価の過程で評価実施機関より提出される各資料をもとに、以下の確認を実施した。

① 評価実施機関が評価作業中に指摘した所見報告書の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正しくSTに反映されていること。

③ 提出されたSTの内容を確認し、関連する評価者アクションエレメントが本評価報告書で示されたように評価されていること。

④ 本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 本評価報告書に示された評価者の評価方法がCEMに準拠していること。

これらの確認において発見された問題事項を認証レビューとして記載し、評価実施機関に送付した。

認証機関は、本STにおいて、所見報告書及び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た。

4.2 ST確認結果

提出されたST評価報告書及び所見報告書を調査した結果、認証機関は、本STがCCパート3に規定されたASEクラスの保証要件を満たしていることを確認した。

評価実施機関の実施した各評価者アクションエレメントについての調査結果を表4にまとめる。

表4　評価者アクションエレメント調査結果

評価者アクションエレメント	調査結果
セキュリティターゲット評価	**適切な評価が実施された。**
ASE_DES.1.1E	評価はワークユニットに沿って行われ、TOE種別、境界の記述が明瞭であることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ASE_DES.1.2E	評価はワークユニットに沿って行われ、TOE記述が理路整然と一貫性のあることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ASE_DES.1.3E	評価はワークユニットに沿って行われ、TOE記述がST全体の内容と一貫していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ASE_ENV.1.1E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が前提条件、脅威、組織のセキュリティ方針を漏れなく識別していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ASE_ENV.1.2E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が理路整然とし一貫していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ASE_INT.1.1E	評価はワークユニットに沿って行われ、ST及びTOEの識別、概要及びCC適合が明確に述べられていることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ASE_INT.1.2E	評価はワークユニットに沿って行われ、ST概説の記述が理路整然とし一貫していることを確認している。
ASE_INT.1.3E	評価はワークユニットに沿って行われ、ST概説の記述がST全体の内容と一貫していることを確認している。
ASE_OBJ.1.1E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述にTOE及び環境のセキュリティ対策方針が明記され、それらが脅威、組織のセキュリティ、前提条件へ遡れ、その対策方針の正当性をセキュリティ対策方針根拠が示していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ASE_OBJ.1.2E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述が理路整然とし、完結しており、かつ一貫していることを確認している。
ASE_PPC.1.1E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_PPC.1.2E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。

ASE_REQ.1.1E	評価はワークユニットに沿って行われ、TOE及びIT環境の要件の記述、操作がCCに準拠していること、要件の依存性、機能強度が適切であること、各要件がそれぞれの対策方針に遡れ、それらを満たす根拠が示されていること、要件のセットが内部的に一貫し、相互サポート可能な構造となっていることを根拠が示していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ASE_REQ.1.2E	評価はワークユニットに沿って行われ、ITセキュリティ要件の記述が理路整然とし、完結しており、かつ一貫していることを確認している。
ASE_SRE.1.1E	評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。
ASE_SRE.1.2E	評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。
ASE_TSS.1.1E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が適切なセキュリティ機能及び保証手段を示していること、それらが機能要件や保証要件を満たす根拠が示されていること、ITセキュリティ機能に対する機能強度主張が機能要件に対する機能強度と一貫していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ASE_TSS.1.2E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が完結しており、理路整然とし、かつ一貫していることを確認している。

4.3 注意事項

鍵の暗号化において、入力パスワードに対してハッシュ関数を用いた演算結果を鍵として暗号処理を行っている。この処理では、電子政府推奨暗号リスト[21]にないMD5、DESが使われているが、現在では、標準から削除されているアルゴリズムもある。電子政府推奨暗号リストに登録されているアルゴリズム、または、信頼できる機関で、その暗号強度が検証されているものを利用することを勧める。

5 用語

本報告書で使用された略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation

本報告書で使用された用語の定義を以下に示す。

CA	Certification Authorityの略で、認証局。 電子商取引などで使用される電子証明書を発行する機関。 認証局は、公開鍵が間違いなく本人のものであると証明可能な第三者機関で、公正、中立な立場にあり信頼できなければならない。
ICカード	Integrated Circuit Card の略で、ICチップが埋め込まれたカード状デバイス。 証明書や鍵対の保管に使用する。
PKI	Public Key Infrastructureの略で、公開鍵基盤。 公開鍵暗号化方式という暗号技術を基に成り立っており、秘密鍵、公開鍵、電子証明書の3要素で構成される。
RA	Registration Authorityの略で、登録局。 電子証明書発行の申請者の本人を審査・確認し、主として登録業務を行う機関。
RA鍵	RAサーバ自身が持つ鍵対のうち本STでは秘密鍵を指す。
RAサービス	本STでは一般利用者管理や証明書発行などの登録局としてのサービスの総称である。
SNI	Trust-KMSにアクセスする者がどの役割にあたるかという、付与される役割を示す、役割確認に用いられるもの。
SVI	RA管理者・申請者・審査者がTrust-KMSに要求する各サービスを表すもの。

SVP	Trust-KMSアクセス制御ポリシーに基づいて、RA管理者・申請者・審査者が、それぞれの役割がどのサービスが実現可能な権限を有しているかを記録した権限確認に用いられるもの。あらかじめRA管理者によってRAの初期設定時に決定され、安全に設定されているものである。
Trust-KMS アクセス制御ポリシー	RAサービスを行う際に、適用する原則、方針、ルール、設定内容が規定されている。また、セキュリティ属性に基づいてそれぞれの役割（RA管理者・申請者・審査者）がアクセス可能なオブジェクトの種類や実行可能な操作のリストが規定されている。
Tc	信頼できるOSが供給する時刻情報。
Ts	RAサーバが供給する認証時刻。
UID	RA管理者・申請者・審査者に割り当てられているユーザのIDとなるもの。
UIDC	RA管理者・申請者・審査者がTrust-KMSにアクセスする際の本人認証に用いるユーザ確認情報。
公開鍵	秘密鍵と対になる鍵で、誰でも入手可能な状態に公開されている。
公開鍵証明書（証明書）	公開鍵の所有者の身分を示す証明書で、印鑑証明に相当する。デジタル証明書あるいは単に証明書ともいう。 公開鍵証明書は、公開鍵の持ち主情報、公開鍵、CAの情報、CAの署名からなる。
申請書	申請者によって作成される、申請内容が記述されたデータ。審査者は、申請書を参照し、審査を行う。
電子署名	電子文書の正当性を保証するために付けられる署名情報。公開鍵暗号などを利用し、相手が本人であることを確認するとともに、情報が送信途中に改竄されていないことを証明することができる。 デジタル署名ともいう。
登録書	RA管理者、申請者、審査者の登録、削除を行う際にRA管理者が作成するデータ。申請書と同一のフォーマットでありサーバにおける処理方法も同じ。
秘密鍵	公開鍵と対になる鍵。 公開せず、他人に漏れないように鍵の所有者だけが管理する鍵。 秘密鍵で署名したものは、それに対応する公開鍵でのみ検証が可能である。
報告書	申請内容の結果が記述されたデータ。 申請者は、報告書を受信することによりRAサービスの結果を受け取ることができる。サービスの結果には、サーバで生成した秘密鍵や公開鍵、発行した証明書などが含まれる。

6 参照

[1] Trust-KMS v6.1セキュリティターゲット 第3.4版 2005年2月14日 日本電信電話株式会社

[2] セキュリティターゲットの評価・確認申請等の手引き 平成16年4月 独立行政法人 情報処理推進機構 ITQM-21

[3] セキュリティターゲット 評価実施機関に対する要求事項 平成16年4月 独立行政法人 情報処理推進機構 ITQM-13

[4] セキュリティターゲットの確認申請者・登録者に対する要求事項 平成16年4月 独立行政法人 情報処理推進機構 ITQM-12

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.1 August 1999 CCIMB-99-031

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033

[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1: 概説と一般モデル バージョン2.1 1999年8月 CCIMB-99-031

[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2: セキュリティ機能要件 バージョン2.1 1999年8月 CCIMB-99-032

[10] 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: セキュリティ保証要件 バージョン2.1 1999年8月 CCIMB-99-033

[11] ISO/IEC 15408-1 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model ISO/IEC15408-1: 1999(E)

[12] ISO/IEC 15408-2 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements ISO/IEC15408-2: 1999(E)

[13] ISO/IEC 15408-3 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements ISO/IEC15408-3: 1999(E)

[14] JIS X 5070-1: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第1部: 総則及び一般モデル

[15] JIS X 5070-2: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第2部: セキュリティ機能要件

[16] JIS X 5070-3: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第3部: セキュリティ保証要件

[17] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part2: Evaluation Methodology Version 1.0 August 1999

[18] 情報技術セキュリティ評価のための共通方法論 CEM-99/045 パート2: 評価方法論 バージョン1.0 1999年8月

[19] JIS TR X 0049: 2001 情報技術セキュリティ評価のための共通方法

[20] Trust-KMS v6.1セキュリティターゲット　評価報告書 第3.0版　2005年2月18日 ATL-ETRST-0003-00　株式会社電子商取引安全技術研究所 評価センター

[21] 電子政府推奨暗号リスト 平成15年2月20日 総務省／経済産業省