NTT

Trust-KMS v6.1

Security Target

NTT 情報流通ﾌﾟﾗｯﾄﾌｫｰﾑ研究所 Copyright NTT 2005

No part of the contents of this document may be reproduced or distributed in any means without the prior written permission of NTT Corporation.

Table of Contents

1 ST Introduction 6

1.1 ST identification 6

1.2 TOE identification 6

1.3 CC conformance claims 6

1.4 ST overview 6

1.5 Assurance level 6

1.6 Conformance to a PP 7

2 TOE description 8

2.1 TOE 概説 8

2.1.1 TOE 概要 8

2.1.2 TOE サービスの流れ 8

2.2 関与する人と役割 10

2.2.1 関与する人の区分 10

2.3 TOE の環境 11

2.3.1 ハードウェア構成 11

2.3.2 設置環境 12

2.3.3 ソフトウェアの構成 13

2.3.4 セキュリティ機能 14

3 TOE security enviroment 16

3.1 Assets 16

3.2 Assumption 16

3.3 Threats 17

3.4 Organizational security policies 17

4 Security objectives 18

4.1 Security objectives for the TOE 18

4.2 Security objectives for the environment 18

4.2.1 IT 環境 19

4.2.2 非 IT 環境 19

5 IT Security requirements 21

5.1 TOE security requirements 21
5.1.1 TOE Security functional requirements 21
5.1.2 Minimum strength of function claim 33
5.1.3 TOE assurance requirements 33
5.2 Security requirements for the IT enviroment 34
6 TOE summary specification 35
6.1 TOE Security functions 35
6.1.1 SF.Auth 本人認証機能 35
6.1.2 SF.Audit ログ管理機能 36
6.1.3 SF.Crypto 暗号処理機能 38
6.1.4 SF.KeyManagement 鍵管理機能 38
6.1.5 SF.AccessControl アクセス制御機能 41
6.2 Strength of funtion claims 44
6.3 Assurance measures 44
7 PP claims 46
8 Rationale 47
8.1 Security objective rationale 47
8.2 Security requirements rationale 50
8.2.1 Security requirements rationale 50
8.2.2 Dependency analysis 53
8.2.3 Demonstration of mutual support between security requirements 55
8.2.4 Security audit data generation rationale 56
8.2.5 Appropriateness of assurance requirements 57
8.2.6 Minimum strength of function(SOF) claim rationale 57
8.3 TOE summary specification rationale 58
8.3.1 Security functions rationale 58
8.3.2 Demonstration of mutual support between security functions 63
8.3.3 Strength of function claims rationale 63
8.3.4 Assurance measures rationals 64
8.4 PP claims rationale 65
＜付録 A＞ 参考文献 66
＜付録 B＞ 用語説明 67

＜付録 C＞　ESIGN について.....68

1 ST Introduction

1.1 ST identification

ST 名称:「Trust-KMS v6.1 Security Target」
日付: 2005-02.14
バージョン: 3.4
著者: NTT 情報流通プラットフォーム研究所 情報セキュリティプロジェクト 藤村 明子
ST の開発に使用した CC のバージョン：CC Ver.2.1
ただし、各要件の日本語訳は、IPA（情報処理推進機構）セキュリティセンターが訳した Ver.2.1 の Part2、Part3 を使用している。

1.2 TOE identification

本 ST の TOE 名称: 「Trust-KMS」（以下、文中では Trust-KMS とする。）
本製品 Trust-KMS の製品バージョンは v6.1 である。

1.3 CC conformance claims

本 TOE は
・機能要件は、ISO/IEC15408-2：1999(E)（CC Ver.2.1 part2）に適合。
・保証要件は、ISO/IEC15408-3：1999(E)（CC Ver.2.1 part3）に適合。

1.4 ST overview

Trust-KMS は PKI における利用者登録局（RA…Registration Authority）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…Certification Authority）への証明書発行の申請手続きを行うものである。

CA としての機能を持つ「Trust-CANP v6.1」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。こうした電子認証システムはネットワークを介した電子政府や電子商取引などの実現に役立つ。

1.5 Assurance level

選択された評価保証レベルは EAL3 である。

1.6 Conformance to a PP

この ST が適合している PP はない。

2 TOE description

このセクションでは対象となる TOE について、製品の背景、運用される環境および提供される機能、関与する人と役割について記述する。

2.1 TOE 概説

2.1.1 TOE 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、RA としての機能を提供する製品である。

・Trust-KMS は、PKI の利用者の登録、審査、CA への申請依頼と証明書の取得などのサービスを提供する。
・Trust-KMS は、PKI 利用者の鍵や CA から発行された証明書の管理機能を備えている。
・Trust-KMS は、RA サーバと RA クライアントから構成される。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る。本 ST で RA サーバ、RA クライアントと表現する場合は、それぞれのハードウェアおよび TOE から構成された製品を指している。

2.1.2 TOE サービスの流れ

Trust-KMS が行う RA サービスの流れを記述する。本 ST でいう 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。

2.1.2.1 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。

2.1.2.2 運用

2.1.2.2.1 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。

2.1.2.2.2 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 2.2「関与する人と役割」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。

2.2 関与する人と役割

2.2.1 関与する人の区分

関与する人は以下のように分けられる。

○RA 管理者
○申請者
○審査者
○一般利用者

関与する人と TOE が認識する役割は以下の通りである。なお、それぞれの役割には複数人ずついる場合がある。

表 2-2.1： 関与する人の区分とその役割

区分		役割	役割に許可された操作内容
運営側	管理者	RA 管理者	本 ST でいう RA 管理者とは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。
	操作者	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。
一般利用者		—	RA の提供するサービスを実際に受ける者である。本 ST では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。

2.3 TOEの環境

2.3.1 ハードウェア構成

TOE である Trust-KMS は RA サーバ、RA クライアント（RA 管理者端末、申請者端末、審査者端末）上で動作するアプリケーションソフトウェアである。
図 2-3.1 に Trust-KMS がインストールされる物理的なハードウェアと、そのほかのハードウェア（周辺機器および CA サーバ）の構成を示し、表 2-3.1 にその内容を記述し、表 2-3.2 には Trust-KMS がインストールされるハードウェアの仕様を記述する。

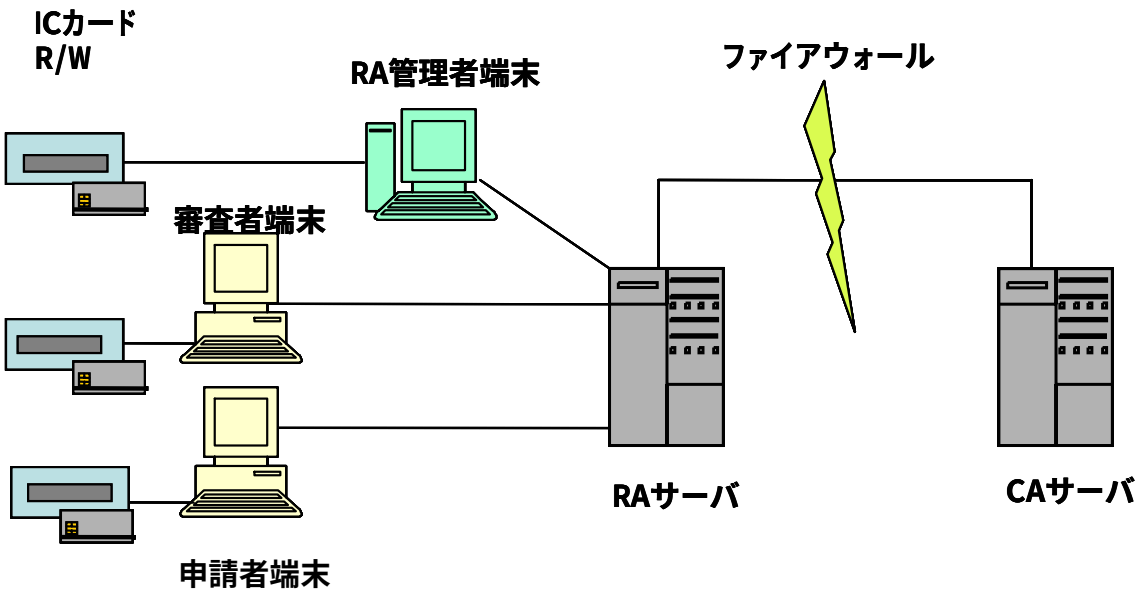

図 2-3.1：ハードウェア構成

表 2-3.1： Trust-KMS がインストールされるハードウェアと、そのほかのハードウェアの構成要素

構成要素		概要
RA サーバ		登録局としてのコア機能を行う。
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。
	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。
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。

表 2-3.2：Trust-KMS がインストールされるハードウェア及び周辺機器の仕様

構成要素	スペック
RA 管理者端末、申請者端末、審査者端末	以下のスペックを満たす PC を推奨 CPU: Pentium 300MHz 以上 Memory: 128MB 以上 HDD: 100MB 以上の空き
RA サーバ	以下のスペックを満たす 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)
IC カード及び IC カード R/W	Cryptoflex（Schlumberger 社）＊これらは端末との通信を安全に行う機能を有している IC カードおよび R/W である。
CA サーバ	「Trust-CANP v6.1 Security Target」を参照のこと

2.3.2 設置環境

RA サーバと RA クライアントは物理的に入退管理された場所に設置される。
RA サーバと RA クライアントは LAN で接続され、その間の通信は SSL のみが許可される。
また、RA サーバと外部に設置された CA サーバとはファイアウォールを介して接続され、その間の通信は SSL のみが許可される。

2.3.3 ソフトウェアの構成

下記の図 2-3.2 にソフトウェア構成を示し、表 2-3.3 にその内容を記述する。

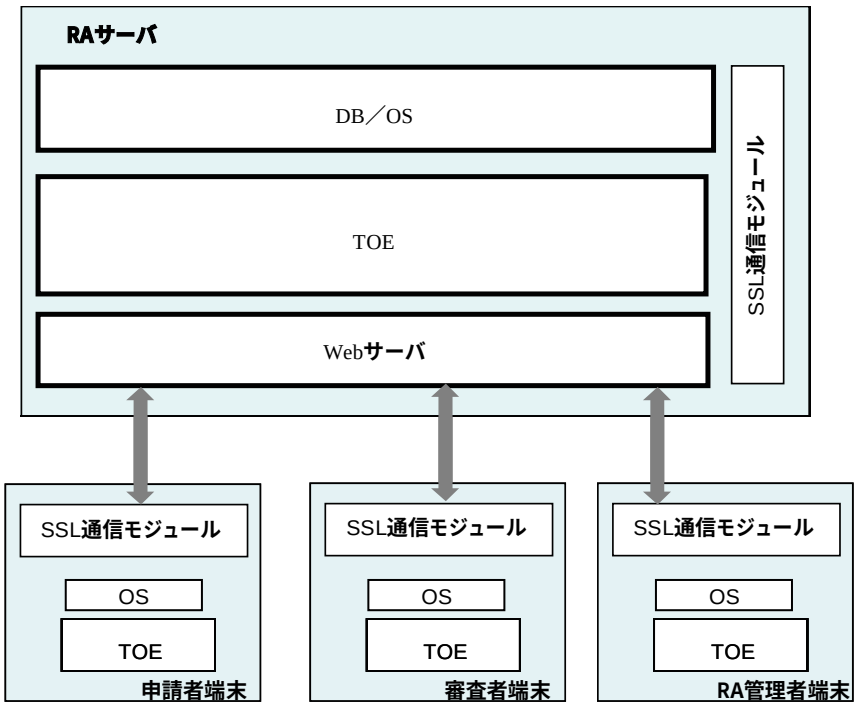

図 2-3.2：ソフトウェア構成

表 2-3.3： ソフトウェア構成
（網掛け部分は TOE 範囲内）

構成要素	概要
DBMS（TOE 範囲外）	RA サーバ内のデータベース。Oracle 8.1.7.3
OS（TOE 範囲外）	RA サーバ：Solaris8、RA クライアント：Windows2000
Web サーバ（TOE 範囲外）	RA サーバ内の Web サーバ。Apache 1.3.x
SSL 通信モジュール （TOE 範囲外）	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）に利用されるものであり、クライアント側の SSL 通信モジュールから通信の相手先にある web サーバに対して SSL 通信を実行する。RA クライアント内の当該モジュールでブラウザを使用する場合には、Internet Explorer 5.5 SP2 が利用される。
Trust-KMS（RA サーバ用）	RA サーバにインストールする TOE。
Trust-KMS（RA クライアント用）	RA クライアントにインストールする TOE。

2.3.4 セキュリティ機能

以下の説明において Tc は時刻情報、UID はユーザ ID、UIDC はユーザ確認情報を指す。
保護資産は論理的にはすべて TOE 内にある。

1. RA サーバの鍵対の生成
   TOE のインストール時に、RA サーバで RA 管理者は RA サーバの鍵対（RSA、ESIGN、DSA から指定）を生成後、RA の公開鍵を RA サーバのコマンド機能を使用しオンラインで CA に登録し CA の署名を付けて RA 秘密鍵とともに TOE（DB のファイル）に保存する。（以下、本 ST で RA 鍵といえばすべてこの RA 秘密鍵を指す。）

2. RA 管理者、申請者、審査者の鍵対の生成
   権限を持つ RA 管理者は RA 管理者端末から RA サーバ内で鍵対を生成する。生成した RA 管理者、申請者、審査者の鍵対のうち、公開鍵は権限を持つ RA 管理者の操作により登録書として CA での署名を求め CA の署名のついた公開鍵を TOE 内に保存し RA 管理者、申請者、審査者の認証（IC カードで生成された署名の検証）に使用する。
   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 カードに鍵対を格納する。TOE で生成した秘密鍵は TOE には残さない。鍵の生成や格納は TOE の機能であるが、IC カードの鍵を使った署名生成機能は TOE 範囲外である。

3. RA 管理者、申請者、審査者の認証機能
   上記 2 において RA 管理者、申請者、審査者の秘密鍵と CA 署名が付与された公開鍵の格納された IC カードを PIN により本人確認後 Tc、UID および、UIDC の情報を IC カード内の秘密鍵にて署名を付与し RA サーバで検証することで RA 管理者、申請者、審査者の認証をおこなう。

4.一般利用者の鍵対の生成
   TOE にて鍵対を生成する場合と、一般利用者が自分で鍵を持ち込んでくる場合がある。TOE にて生成する場合は権限を持つ申請者が申請者端末を操作し TOE で鍵対を生成する。一般利用者の公開鍵は権限を持つ申請者の操作により CA での署名を求め一般利用者の秘密鍵と CA の署名のついた公開鍵を PIN による本人確認がされた IC カードに格納する。TOE で生成した秘密鍵は TOE には残さない。このように鍵の生成や格納は TOE の機能である。

5.アクセス制御機能
   「Trust-KMS アクセス制御ポリシー」に従いアクセス制御をおこなう。「Trust-KMS ア

クセス制御ポリシー」には、サービス要求に対する役割が実行可能な操作のリスト（付与される役割(SNI)/役割ごとの権限(SVP)）が規定されている。RA 管理者のみがこのリストを新規登録、削除、変更、参照できる。TOE は本人認証に成功した者の識別情報から役割を確認し役割から権限を確認し申請書や報告書に対する操作を制御する。また、RA サーバと CA サーバ間で送受信されるデータには RA サーバ、CA サーバの秘密鍵による署名が付与され、データの改ざんを検出することが可能である

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おこなう。

7.ログ管理機能

サービス運用中に発生した事象のログを生成し、閲覧に適した形での読み出しが可能で、不正な改竄を検出できるログ管理をおこなう。

生成したログには以下の方法で署名を付与し、その署名を検証することで改竄を検出可能とする。

ログファイルが更新されるたびに Keyed-hash 方式による署名をログに付与

1 世代前となって更新されないログファイルに対して RA 鍵で署名を付与

ログ管理機能の開始、停止の操作は RA 管理者のみに制限されている。

ログファイルは、許可された RA 管理者、申請者、審査者のみが閲覧可能である。

8. RA 管理者・申請者・審査者の秘密鍵の暗号化機能

RA 鍵と、RA 管理者・申請者・審査者の秘密鍵、一般利用者の秘密鍵を安全に保管するために、一般利用者、RA 管理者・申請者・審査者の秘密鍵を入力パスワードに対する MD5 を用いた演算結果を鍵とする DES 暗号 (CBC モード) を用いて暗号化して DB に保存する。

3 TOE security enviroment

3.1 Assets

TOE で保護される資産は以下である。

（1）RA 管理者に操作を許可されたユーザデータ
登録書（RA 管理者、申請者、審査者の登録、削除用）
報告書 （CA より受信）
RA 管理者、申請者、審査者の鍵対

（2）申請者に操作を許可されたユーザデータ
申請書 （一般利用者の登録、削除、証明書発行、失効用）
報告書 （CA より受信）
一般利用者の鍵対

（3）審査者に操作を許可されたユーザデータ
申請書 （審査時使用）

（4）TSF データ
ログ
セキュリティ属性および Trust-KMS アクセス制御ポリシーのリスト

3.2 Assumption

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。

3.3 Threats

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。

3.4 Organizational security policies

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 はログの不正な改竄や消去を検出しなければならない。

4 Security objectives

この章では、TOE 及び TOE（をとりまく）環境に対する「セキュリティ目標」を定義する。ここで挙げた「Security objective」はすべて、前章で記述した「Assumption」「Threats」「Organizational security policy」に対応している。

4.1 Security objectives for the TOE

SO.AUTH
TOE は、ログインしてきた者の正当性を確認するために正しく本人認証を行わなければならない。

SO.PRIVILEGES
TOE は、本人認証の後に RA 管理者、申請者、審査者それぞれどの役割かの役割確認と役割ごとに許可された操作の権限確認を行ない、登録書や申請書の作成、各鍵対に対する操作を許可しなければならない。

SO.RA_SIGN
RA サーバと CA サーバ間を転送中の保護資産が、改ざんから保護されなければならない。

SO.LOGGEN
TOE は、不正なアクセス行為などがあった場合に、後から正しく分析することができるようにするために、操作記録としてログを生成、閲覧できなくてはならない。

SO.AUDIT_DATA
TOE は、ログに対して改ざんなどの不正な加工が行われた場合には、そのような不正な加工が行われたことを事後に検出することが可能でなければならない。

SO.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 内に暗号化されて安全に保管されなければならない。また、これらの鍵が TOE 外にエクスポートされた場合は、TOE 内に秘密鍵の情報を残してはならない。

4.2 Security objectives for the environment

4.2.1 IT 環境

SOE.SSL
RA サーバと CA サーバ間の通信は SSL で行い、通信データの暴露を防止しなければならない。

SOE.LAN
RA サーバと RA クライアント間の通信は SSL で行い、通信データの暴露を防止しなければならない。

4.2.2 非 IT 環境

SOEN.ADMIN
RA 管理者はガイダンス文書に基づいて操作を実施しなければならない。自己の所有する IC カードの紛失、PIN の漏洩に注意し離席時には他者に RA 管理者端末を操作されないよう、必ずログアウトしなければならない。
また、RA 管理者は、RA サーバの OS や DB 及び RA 管理者端末の OS のパスワードには推測されにくいパスワードを設定し、他人に漏洩しないよう管理し、定期的に変更しなければならない。

SOEN.USER
TOE のサービスを受ける一般利用者は、自己の所有する秘密鍵の暗号化のためのパスワードや IC カードの PIN には推測されにくいパスワードを設定し、他人に漏洩しないよう管理し、定期的に変更しなければならない。
また、申請者、審査者は、申請者端末、審査者端末の OS のパスワードや IC カードの PIN には推測されにくいパスワードを設定し、他人に漏洩しないよう管理し、定期的に変更しなければならない。

SOEN.PHYSICAL_PROTECT
TOE が動作するハードウェアおよび IC カードは、サービス運用元によって入退管理が可能な安全な場所に設置、管理されなければならない。

SOEN.NETWORK
TOE が、外部に設置された CA サーバと接続する場合には、必ず適切に設定されたファイアウォールを介して接続しなければならない。

SOEN.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）は、正しく動作する信頼できる製品を使用しなければならない。

5 IT Security requirements

5.1 TOE security requirements

この章では、TOE が持つセキュリティ要件を記述する。

5.1.1 TOE Security functional requirements

FAU_GEN.1 監査データ生成

下位階層: なし

FAU_GEN.1.1

TSF は、以下の監査対象事象の監査記録を生成できなければならない:

a) 監査機能の起動と終了;

b) 監査の[選択: 指定なし]レベルのすべての監査対象事象; 及び

c) [割付: 表 5-1 の監査対象事象]。

FAU_GEN.1.2

TSF は、各監査記録において少なくとも以下の情報を記録しなければならない:

a) 事象の日付・時刻、事象の種別、サブジェクト識別情報、事象の結果(成功または失敗); 及び

b) 各監査事象種別に対して、PP/ST の機能コンポーネントの監査対象事象の定義に基づいた、[割付: 以下の＜監査関連情報のリスト＞]

依存性: FPT_STM.1 高信頼タイムスタンプ

＜監査関連情報のリスト＞

・ログ種別番号…ログの種類ごとに割り当てられる番号

・メッセージ詳細番号…出力されるログに関するメッセージやそれに付随する番号

・付与される役割…操作した者の役割の種別などを示す番号や記号

・ユーザ ID…RA 管理者、申請者、審査者ごとに割り振られる記号や番号

・拡張情報…申請書関連処理の場合は申請書 ID、またはエラー時には内容の詳細

表 5-1 監査対象とすべきアクションと関連する監査対象事象

機能要件	監査対象とすべきアクション	監査対象事象
FAU_GEN.1	—	—
FAU_GEN.2	—	—
FAU_SAR.1	a) 基本：監査記録からの情報の読み出し	a) ログの取得／参照
FAU_SAR.2	a) 基本:監査記録からの成功しなかった情報読み出し	a) RA で発生したエラー

FAU_STG.1	—	—
FAU_STG.3	a) 基本:閾値を超えたためにとられるアクション	表 8-2-4 参照
FCS_CKM.1	a) 最小: 動作の成功と失敗。 b) 基本: オブジェクト属性及び機密情報(例えば共通あるいは秘密鍵)を除くオブジェクトの値。	a) RA で発生したエラー a) CA サーバ情報の登録 a) RA 管理者の登録 a) 申請者と審査者の登録 a）一般利用者の登録
FCS_CKM.4	a) 最小: 動作の成功と失敗。 b) 基本: オブジェクト属性及び機密情報(例えば共通あるいは秘密鍵)を除くオブジェクトの値。	a) RA で発生したエラー a) CA サーバ情報の削除 a) RA 管理者の削除 a) 申請者と審査者の削除 a)申請者と審査者の証明書失効 a) 一般利用者の削除 a) 一般利用者の証明書失効
FCS_COP.1 その 1	a) 最小: 成功と失敗及び暗号操作の種別。 b) 基本: すべての適用可能な暗号操作のモード、サブジェクト属性、オブジェクト属性。	a)署名検証処理の失敗 （表 8.2.4 参照）
FCS_COP.1 その 2	a) 最小: 成功と失敗及び暗号操作の種別。 b) 基本: すべての適用可能な暗号操作のモード、サブジェクト属性、オブジェクト属性。	a) RA 管理者の登録 a) 申請者と審査者の登録 a) 一般利用者の登録
FCS_COP.1 その 3	a) 最小: 成功と失敗及び暗号操作の種別。 b) 基本: すべての適用可能な暗号操作のモード、サブジェクト属性、オブジェクト属性。	a) ログに対する署名及び署名検証操作
FDP_ACC.1	—	—
FDP_ACF.1	a) 最小: SFP で扱われるオブジェクトに対する操作の実行における成功した要求。 b) 基本: SFP で扱われるオブジェクトに対する操作の実行におけるすべての要求。 c) 詳細: アクセスチェック時に用いられる特定のセキュリティ属性	a) b) RA で発生したエラー a) b) RA サービス環境情報の取得／状態表示／状態変更 a) b) ポリシー情報の取得／登録／削除／参照 a) b) 申請処理の状況参照／取消 a) b) ログの取得／参照 a) b) 報告書返却 a) b) 申請審査処理 a) b) RA 管理者の登録／削除／検索 a) b) 申請者と審査者の登録／削除／検索 a) b) 申請者と審査者の証明書発行／失効 a) b) 一般利用者の登録／削除 a) b) 一般利用者の証明書発

		行／失効
FDP_UIT.1	a) 最小: データ交換メカニズムを使用する利用者あるいはサブジェクトの識別情報。 b) 基本: データ交換メカニズムの使用を試みる、不当な利用者あるいはサブジェクト の識別情報。 c) 基本: 送信あるいは受信された利用者データの識別に利用できる名前、あるいはそ れ以外のインデックス情報の参照。これは利用者データに関連するセキュリティ属性を含むことができる。 d) 基本: 利用者データの送信を妨害する識別された試み。 e) 詳細: 送信された利用者データに対する、検出された改変の種別及び/あるいは影響。	a) 署名検証を行った RA 管理者 a) 署名検証の成功/失敗
FIA_ATD.1	—	—
FIA_UAU.2	a) 最小: 認証メカニズムの不成功になった使用; b) 基本: 認証メカニズムのすべての使用。	a) ログイン／ログアウト
FIA_UID.2	a) 最小: 提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用; b) 基本: 提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用。	a) ログイン／ログアウト
FIA_USB.1	a) 最小: 利用者セキュリティ属性のサブジェクトに対する不成功結合(例えば、サブジェクトの生成)。 b) 基本: 利用者セキュリティ属性のサブジェクトに対する結合の成功及び失敗(例えば、サブジェクトの生成の成功及び失敗)。	a)b) RA 管理者・申請者・審査者の役割確認び成功/失敗
FMT_MOF.1	a) 基本: TSF の機能のふるまいにおけるすべての改変。	a) RA サーバの開始・停止 a) ログイン／ログアウト a) RA サービスの状態変更 a) ポリシ情報の登録・削除 a) CA サーバ情報の登録・削除 a) RA 管理者の登録／削除 a) 申請者と審査者の登録／削除
FMT_MSA.1	a) 基本: セキュリティ属性の値の改変すべて	a) ポリシー情報の取得／登録／削除 a) RA 管理者の登録／削除 a) 申請者と審査者の登録／削除

		a) 一般利用者の登録／削除
FMT_MSA.2	a) 最小: セキュリティ属性に対して提示され、拒否された値すべて; b) 詳細: セキュリティ属性に対して提示され、受け入れられたセキュアな値すべて。	a) RA 管理者の登録／削除 a) 申請者と審査者の登録／削除 a) 一般利用者の登録／削除 a) 一般利用者の証明書発行／失効
FMT_SMR.1	a) 最小: 役割の一部をなす利用者のグループに対する改変； b) 詳細: 役割の権限の使用すべて	a) ポリシ情報の登録 b) RA で発生したエラー
FPT_SEP.1	—	—
FPT_RVM.1	—	—
FPT_STM.1	a) 最小: 時間の変更; b) 詳細: タイムスタンプの提供。	表 8-2.4 参照

＊アンダーラインは本 ST で対象とするアクションを示している

FAU_GEN.2 利用者識別情報の関連付け

下位階層: なし

FAU_GEN.2.1

TSF は、各監査対象事象を、その原因となった利用者の識別情報に関連付けられなければならない。

依存性: FAU_GEN.1 監査データ生成

FIA_UID.1 識別のタイミング

FAU_SAR.1 監査レビュー

下位階層: なし

FAU_SAR.1.1

TSF は、[割付: RA 管理者、申請者、審査者]が、[割付: 以下の＜監査情報のリスト＞]を監査記録から読み出せるようにしなければならない。

FAU_SAR.1.2

TSF は、利用者に対し、その情報を解釈するのに適した形式で監査記録を提供しなければならない。

依存性: FAU_GEN.1 監査データ生成

＜監査情報のリスト＞

{ログ種別番号、メッセージ詳細番号、事象の結果、付与される役割、ユーザ ID、拡張情報
事象の日付・時刻}

FAU_SAR.2 限定監査レビュー

下位階層: なし

FAU_SAR.2.1

TSF は、明示的な読み出しアクセスを承認された利用者を除き、すべての利用者に監査記録への読み出しアクセスを禁止しなければならない。

依存性: FAU_SAR.1 監査レビュー

FAU_STG.1 保護された監査証跡格納

下位階層: なし

FAU_STG.1.1

TSF は、格納された監査記録を不正な削除から保護しなければならない。

FAU_STG.1.2

TSF は、監査記録の改変を[選択: 検出]できねばならない。

依存性: FAU_GEN.1 監査データ生成

FAU_STG.3 監査データ損失の恐れ発生時のアクション

下位階層: なし

FAU_STG.3.1

TSFは、監査証跡が[割付: TOE構築時に設定した量]を超えた場合、[割付: 警告表示が出され、RAとしてのサービスを停止する措置]をとらなければならない。

依存性: FAU_STG.1 保護された監査証跡格納

FCS_CKM.1 暗号鍵生成

下位階層: なし

FCS_CKM.1.1

TSF は、以下の[割付: 表 5-2 の標準]に合致する、指定された暗号鍵生成アルゴリズム[割付: 表 5-2 のアルゴリズム]と指定された暗号鍵長[割付: 表 5-2 の鍵長]に従って、暗号鍵を生成しなければならない。

依存性: [FCS_CKM.2 暗号鍵配付

または

FCS_COP.1 暗号操作]

FCS_CKM.4 暗号鍵破棄

FMT_MSA.2 セキュアなセキュリティ属性

表 5-2：鍵生成アルゴリズムと鍵長

アルゴリズム（標準）	使用場面	鍵長 （bit）
RSA（PKCS#1）	・IC カードに格納する鍵の生成（RA 管理者、申請者、審査者の鍵、一般利用者の鍵） ・RA サーバの鍵対の生成	512~2048
ESIGN（ISO14888-3）	・RA サーバの鍵対の生成	576~2304
DSA（公開鍵部分 ANSI X9.57）	・RA サーバの鍵対の生成	512~1024
MD5（PKCS#5）	・RA 管理者、申請者、審査者、一般利用者の秘密鍵を一時的に暗号化するための鍵の生成	56

FCS_CKM.4 暗号鍵破棄

下位階層: なし

FCS_CKM.4.1

TSF は、以下の[割付: なし]に合致する、指定された暗号鍵破棄方法[割付: 表 5-3]に従って、暗号鍵を破棄しなければならない。

依存性: [FDP_ITC.1 セキュリティ属性なし利用者データのインポート

または

FCS_CKM.1 暗号鍵生成]

FMT_MSA.2 セキュアなセキュリティ属性

表 5-3：鍵破棄の方法

鍵の種類	保存場所	破棄方法
◎ＲＡ鍵（RA サーバの秘密鍵）	ＤＢ	0 値化
◎一般利用者の秘密鍵 ◎RA 管理者・申請者・審査者の秘密鍵	ＤＢ	0 値化
◎ＲＡサーバの公開鍵 ◎一般利用者の公開鍵 ◎RA 管理者・申請者・審査者の公開鍵	DB	0 値化
◎RA 管理者、申請者、審査者、一般利用者の秘密鍵を一時的に暗号化するための鍵	メモリ	電源オフによりクリア

FCS_COP.1 その１ 暗号操作

下位階層: なし

FCS_COP.1.1 その１

TSF は、[割付: RSA:PKCS#１、ESIGN:ISO14888-3、DSA:FIPS186-2]に合致する、特定された暗号アルゴリズム[割付: 表 5-4 のアルゴリズム]と暗号鍵長[割付: 表 5-4 の鍵長]に従って、[割付: 表 5-4 で示す署名生成、署名検証]を実行しなければならない。

依存性: [FDP_ITC.1 セキュリティ属性なし利用者データのインポート

または

FCS_CKM.1 暗号鍵生成

FCS_CKM.4 暗号鍵破棄

FMT_MSA.2 セキュアなセキュリティ属性

表 5-4 署名生成、署名検証の実現方法

暗号操作	使用場面および方法	アルゴリズム	鍵長
RA 管理者・申請者・審査者の鍵によって生成された署名の検証	本人認証、役割確認・権限確認	RSA	512~2048 (bit)
RA 鍵による署名生成、	登録書、申請書への署名生成、RA クライアントから送られた認証データへの署名生成、ログへの RA 鍵ログ署名の生成（長期的改竄防止）	RSA ESIGN DSA	RSA: 512~2048 ESIGN: 576~2304 DSA: 512~1024 (bit)
RA 公開鍵による署名検証	SNI の署名検証、ログに付けられた署名の検証	RSA ESIGN DSA	RSA: 512~2048 ESIGN: 576~2304 DSA: 512~1024 (bit)

FCS_COP.1 その２ 暗号操作

下位階層: なし

FCS_COP.1.1 その２

TSF は、[割付: 表 5-5 で示した標準]に合致する、特定された暗号アルゴリズム[割付: DES]と暗号鍵長[割付: 56bit]に従って、[割付: 暗号化、復号]を実行しなければならない。

依存性: [FDP_ITC.1 セキュリティ属性なし利用者データのインポート
または
FCS_CKM.1 暗号鍵生成
FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

表 5-5 暗号操作

暗号操作	使用場面および方法	標準
秘密鍵の暗号化・復号	一般利用者・RA 管理者・申請者・審査者の秘密鍵を暗号化、復号	PKCS#5

FCS_COP.1 その３ 暗号操作

下位階層: なし
FCS_COP.1.1 その 3
TSF は、[割付: FIPS PUB 180-1]に合致する、特定された暗号アルゴリズム[割付: 表 5-6 のアルゴリズム]と暗号鍵長[割付: なし]に従って、[割付: 表 5-6 で示す署名生成]を実行しなければならない。
依存性: [FDP_ITC.1 セキュリティ属性なし利用者データのインポート
または
FCS_CKM.1 暗号鍵生成
FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

表 5-6 ログへ署名生成の実現方法

暗号操作	使用場面および方法	アルゴリズム
ハッシュ値による署名生成	ログへのハッシュ値ログ署名の生成（短期的改竄防止）	SHA-1

FDP_ACC.1 サブセットアクセス制御

下位階層: なし
FDP_ACC.1.1
TSFは、[割付: 表5-7に示すサブジェクト、オブジェクト、およびサブジェクトとオブジェクト間で許可される操作]に対して[割付: 「Trust-KMSアクセス制御ポリシー」]を実施しなければならない。
依存性: FDP_ACF.1 セキュリティ属性によるアクセス制御

FDP_ACF.1 セキュリティ属性によるアクセス制御

下位階層: なし

FDP_ACF.1.1

TSF は、[割付: サブジェクト属性である「付与される役割(SNI)/役割ごとの権限(SVP)」]に基づいて、オブジェクトに対して、[割付: 「Trust-KMS アクセス制御ポリシー」]を実施しなければならない。

FDP_ACF.1.2

TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうか決定するために、次の規則を実施しなければならない: [割付:表 5-7 が表す規則]。

FDP_ACF.1.3

TSF は、以下の追加規則に基づいて、オブジェクトに対するサブジェクトのアクセスを明示的に承認しなければならない: [割付: なし]。

FDP_ACF.1.4

TSF は、[割付:なし]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。

依存性: FDP_ACC.1 サブセットアクセス制御

FMT_MSA.3 静的属性初期化

表5-7　各サブジェクトがオブジェクトに対し許可される操作

サブジェクト	オブジェクト	許可される操作
RA管理者プロセス	登録書テーブル（RA管理者、申請者、審査者の登録、削除）	読み出し、書き込み、消去
	報告書テーブル	読み出し、消去
	RA管理者、申請者、審査者の鍵対テーブル	読み出し、書き込み、消去
	通信ポート	読み出し、書き込み
申請者プロセス	申請書（一般利用者の登録、削除、証明書発行、失効）テーブル	読み出し、書き込み、消去
	一般利用者の鍵対（内部生成）テーブル	読み出し、書き込み、消去
	一般利用者の鍵対（持ち込み）ファイル	読み出し、書き込み、消去
	報告書テーブル	読み出し、書き込み
	通信ポート	読み出し、書き込み
審査者プロセス	申請書テーブル	読み出し、書き込み

FDP_UIT.1 データ交換完全性

下位階層: なし

FDP_UIT.1.1

TSF は、利用者データを[選択: 改変]誤りから保護した形で[選択: 送信、受信]できるようにするために、[割付: Trust-KMSアクセス制御ポリシー]を実施しなければならない。

FDP_UIT.1.2

TSF は、利用者データ受信において、[選択:改変]が生じたかどうかを判定できなければならない。

依存性: [FDP_ACC.1 サブセットアクセス制御、または
FDP_IFC.1 サブセット情報フロー制御]
[FTP_ITC.1 TSF 間高信頼チャネル、または
FTP_TRP.1 高信頼パス]

FIA_ATD.1 利用者属性定義

下位階層: なし

FIA_ATD.1.1

TSF は、個々の利用者に属する以下のセキュリティ属性のリスト[割付:「ユーザ ID（UID）/付与される役割(SNI)/役割ごとの権限(SVP)」]を維持しなければならない。

依存性: なし

FIA_UAU.2　アクション前の利用者認証

下位階層: FIA_UAU.1

FIA_UAU.2.1 その 1

TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

依存性: FIA_UID.1 識別のタイミング

FIA_UID.2　アクション前の利用者識別

下位階層: FIA_UID.1

FIA_UID.2.1

TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

依存性: なし

FIA_USB.1 利用者・サブジェクト結合

下位階層: なし

FIA_USB.1.1

TSFは、適切な利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない。

依存性: FIA_ATD.1 利用者属性定義

FMT_MOF.1 セキュリティ機能のふるまいの管理

下位階層: なし

FMT_MOF.1.1

TSF は、機能[割付:表 5-8 のリスト][選択: を動作させる]能力を[割付: RA 管理者]に制限しなければならない。

依存性: FMT_SMR.1 セキュリティ役割

表 5-8　権限のリスト

機能
RA サーバ本体の開始・停止 RA サービス（機能そのもの）開始・停止 ログ管理機能の起動・停止 CA サーバに関する情報の登録・削除 RA 鍵対の生成・破棄、RA 管理者・申請者・審査者の鍵対の生成・破棄

FMT_MSA.1 セキュリティ属性の管理

下位階層: なし

FMT_MSA.1.1

TSF は、セキュリティ属性[割付: ユーザ ID（UID）]に対し[選択: 改変 [割付: 新規登録]、削除、参照]をする能力を[割付: RA 管理者]に制限するために[割付: 「Trust-KMS アクセス制御ポリシー」]を実施しなければならない。

依存性: [FDP_ACC.1 サブセットアクセス制御または
FDP_IFC.1 サブセット情報フロー制御]
FMT_SMR.1 セキュリティ役割

FMT_MSA.2 セキュアなセキュリティ属性

下位階層: なし

FMT_MSA.2.1

TSF は、セキュアな値だけがセキュリティ属性として受け入れられることを保証しなければならない。

依存性: ADV_SPM.1 非形式的TOEセキュリティ方針モデル
[FDP_ACC.1 サブセットアクセス制御または
FDP_IFC.1 サブセット情報フロー制御]
FMT_MSA.1 セキュリティ属性の管理
FMT_SMR.1 セキュリティ役割

FMT_SMR.1 セキュリティ役割

下位階層: なし
FMT_SMR.1.1
TSF は、役割[割付: RA 管理者、申請者、審査者]を維持しなければならない。
FMT_SMR.1.2
TSF は、利用者を役割に関連づけなければならない。
依存性: FIA_UID.1 識別のタイミング

FPT_SEP.1 TSFドメイン分離

下位階層: なし
FPT_SEP.1.1
TSF は、それ自身の実行のため、信頼できないサブジェクトによる干渉と改ざんからそれを保護するためのセキュリティドメインを維持しなければならない。
FPT_SEP.1.2
TSF は、TSC 内でサブジェクトのセキュリティドメイン間の分離を実施しなければならない。
依存性: なし

FPT_RVM.1　TSPの非バイパス性

下位階層: なし
FPT_RVM.1.1
TSFは、TSC内の各機能の動作進行が許可される前に、TSP実施機能が呼び出され成功することを保証しなければならない。
依存性: なし

FPT_STM.1 高信頼タイムスタンプ

下位階層: なし
FPT_STM.1.1
TSFは、それ自身の使用のために、高信頼タイムスタンプを提供できなければならない。

依存性: なし

5.1.2 Minimum strength of function claim

本 TOE における Minimum strength of function レベルを、SOF-basic としてクレームする。

5.1.3 TOE assurance requirements

本 TOE の保証要件は **EAL3** からなる。これらは CC part3 から選択されている ACM_CAP.3、ACM_SCP.1、ADO_DEL.1、ADO_IGS.1、ADV_FSP.1、ADV_HLD.2、ADV_RCR.1、AGD_ADM.1、AGD_USR.1、ALC_DVS.1、ATE_COV.2 、 ATE_DPT.1 、 ATE_IND.2 、 ATE_FUN.1 、 AVA_MSU.1 、 AVA_SOF.1,AVA_VLA.1

5.2 Security requirements for the IT enviroment

◎SSL通信対象

FTP_ITC.1 TSF間高信頼チャネル

下位階層: なし

FTP_ITC.1.1

TSFは、それ自身とリモート高信頼IT製品間に、他の通信チャネルと論理的に区別され、その端点の保証された識別及び改変や暴露からのチャネルデータの保護を提供する通信チャネルを提供しなければならない。

FTP_ITC.1.2

TSFは、[選択: TSF]が、高信頼チャネルを介して通信を開始するのを許可しなければならない。

FTP_ITC.1.3

TSFは、[割付: TOEとCAサーバ間における登録書、申請書、報告書の送受信]のために、高信頼チャネルを介して通信を開始しなければならない。

依存性: なし

注釈：TSFはSSL機能を指す。

6 TOE summary specification

6.1 TOE Security functions

本章では、TOE である Trust-KMS によって提供される IT セキュリティ機能について記述する。

6.1.1 SF.Auth 本人認証機能

Trust-KMS は、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、審査者を認証する本人認証機能を提供している。この識別・認証が成功するまでは、アクセスする者はいかなるアクションも行うことができない。

Trust-KMS では IC カードに格納できる鍵は RSA アルゴリズムを使用して生成されたものに限られるため、本機能では、RSA (512～2048bit) を使用して署名検証を行う。署名検証時には、鍵のセキュリティ属性として公開鍵証明書に記述してある以下の３つをチェックしている(FMT_MSA.2)。

・鍵の有効期間（検証日時が鍵の有効期間内かどうか）
・鍵種別（許可された鍵のアルゴリズムと鍵長が一致するかどうか）
・公開鍵証明書の失効情報（公開鍵証明書が失効されているかどうか）

本人認証は、RA 管理者、申請者、審査者の IC カードで生成した署名を RA サーバが検証することによって行われる。検証により送受信されるデータの改ざんも検出できる。これらは表 5-4 に示された署名アルゴリズムと暗号鍵長に従って（FCS_COP.1 その１）行われる。タイムアウトが発生するかログアウトするまではログインセッションが維持され、RA サーバへのアクセスのために IC カードを使って認証をする必要はない。この本人認証機能は、RA 管理者・申請者・審査者が RA クライアントから RA サーバへアクセスを行う際には必ず呼び出される。（FIA_UAU.2、FIA_UID.2、FPT_RVM.1）。これにより、信頼できないサブジェクトによる干渉と改ざんからそれを保護するためのセキュリティドメインを維持、分離している。（FPT_SEP.1）

対応する機能要件：FCS_COP.1 その１、FIA_UAU.2、FIA_UID.2、FMT_MSA.2、FPT_SEP.1、FPT_RVM.1

＜参考＞表 5-4 署名生成、署名検証の実現方法

暗号操作	使用場面および方法	アルゴリズム	鍵長
RA 管理者・申請者・審査者の鍵によって生成された署名の検証	本人認証、役割確認・権限確認	RSA	512~2048 (bit)
RA 鍵による署名生成、	登録書、申請書への署名生成、RA クライアントから送られた認証データへの署名生成、ログへの RA 鍵ログ署名の生成（長期的改竄防止）	RSA ESIGN DSA	RSA: 512~2048 ESIGN: 576~2304 DSA: 512~1024 (bit)
RA 公開鍵による署名検証	SNI の署名検証、ログに付けられた署名の検証	RSA ESIGN DSA	RSA: 512~2048 ESIGN: 576~2304 DSA: 512~1024 (bit)

6.1.2 SF.Audit　ログ管理機能

Trust-KMS は、ログを適切に生成し（FAU_GEN.1）、閲覧に適した形での読み出しが可能で、不正な改竄を検出できるログ管理機能を提供する。

（1）ログ管理機能の開始、停止

ログ管理機能の開始、停止の操作が可能なのは RA 管理者のみに制限されており（6.1.4SF.AccessControl にて後述）、RA サービスそのものの起動時にはログ管理機能を持つプログラムを先に起動し、次に他のサービスを起動させる。ログ管理機能が先に起動していない場合、他のサービスは起動させることはできない。

また、RA 管理者は、ログ管理機能起動時に RA の運用中に取得できるログの量を規定する。RA の運用中にログが規定量に達した場合には、ログ管理機能は RA クライアントに警告メッセージを発信し、他のサービスを自動停止する（FAU_STG.3）。

（2）ログの生成

ログ管理機能は、Trust-KMS のサービス運用中に発生した事象の開始や終了を以下のような形のログファイルとして記録する。

・事象の発生した日付・時刻（OS の時刻データを用いたタイムスタンプ（FPT_STM.1））
・ログ種別番号、メッセージ詳細番号、拡張情報といった事象の種別や結果を表す情報
・付与される役割、ユーザ ID といった識別情報を表す情報（FAU_GEN.2）

ログ生成時に記録の対象となる事象は以下の通りである。

・ RA で発生したエラー

・ RA サーバ開始／停止
・ログイン／ログアウト
・ RA の提供するサービス環境情報取得／状態表示／状態変更
・ポリシー情報の取得／登録／削除／参照
・CA サーバ情報の登録／削除／検索
・ 一般利用者の情報取得／情報変更／検索
・ 申請処理の状況参照／取消
・ ログの取得／参照
・ 監査機能の起動と終了
・ 報告書返却
・ 申請審査処理
・ RA 管理者の登録／削除／検索
・ 申請者と審査者の登録／削除／検索
・ 申請者と審査者の証明書発行／失効
・ 一般利用者の登録／削除
・ 一般利用者の証明書発行／失効
・証明書の検索／検証処理

（3）ログファイルの出力・閲覧

ログ管理機能によって生成されたログファイルは RA 管理者、申請者、審査者が閲覧可能であり（FAU_SAR.1）、閲覧しやすい状態のテキストファイル形式として外部出力することが可能である。

（4）ログの完全性保護

ログ管理機能は、Trust-KMS の動作中に生成されるすべてのログに対して以下の 2 種類の電子署名を付与し、ログに対する不正な加工を事後検出する（FAU_STG.1）。ログの保護のために施される署名は二種類ある。

①Keyed-hash 方式を使った署名（名前：ハッシュ値ログ署名）は、記録する操作が動作中でまだ更新途中のログファイルに対して、更新されるたびにハッシュを取ることで、少ないマシン負荷で短期的に改竄を検出可能とすることを目的としている（FCS_COP.1 その３）。
②RA 鍵によって施される署名（名前：RA 鍵ログ署名）は、1 世代前となって更新されないログファイルに対して RA 鍵で署名を付与することで（FCS_COP.1 その１）、長期的に改竄を検出可能とすることを目的としている。②は RA 鍵によって署名を付与されログサブシステム機能により保護される。
ただし、このハッシュ値署名の操作に関しては、処理の際には暗号鍵を利用しないためこの

処理に関して鍵の生成及び破棄はない。

以上により Trust-KMS は、生成したログに署名を付与し、その署名を検証することで不正な加工が行われたとしても事後検出が可能になり、すべてのログを正確な操作記録として保持することができるようになった。 上記②の場合には、鍵のセキュリティ属性として公開鍵証明書に記述してある以下の３つをチェックしている(FMT_MSA.2)。
・鍵の有効期間（検証日時が鍵の有効期間内かどうか）
・鍵種別（許可された鍵のアルゴリズムと鍵長が一致するかどうか）
・公開鍵証明書の失効情報（公開鍵証明書が失効されているかどうか）
これにより、動作中にどのような操作が Trust-KMS に対して行われたかについて、保存されているログを事後分析することで正確に知ることが可能である。
対応する機能要件：FAU_GEN.1、FAU_GEN.2、FAU_SAR.１、FAU_STG.1、FAU_STG.3、FCS_COP.1 その１、FCS_COP.1 その３、FMT_MSA.2 、FPT_STM.1、

6.1.3 SF.Crypto　暗号処理機能

Trust-KMS は、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ことで安全に保管する機能を提供している。

具体的には、

・一般利用者、RA 管理者・申請者・審査者の秘密鍵を暗号化して DB に保存

することである（FCS_COP.1 その 2）。

対応する機能要件：FCS_COP.1 その 2

6.1.4 SF.KeyManagement　鍵管理機能

Trust-KMS は、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・破棄機能および RA 鍵署名生成機能である。

（１）鍵の生成・破棄機能

Trust-KMS は、下記の 3 種類の鍵対を安全に生成（FCS_CKM.1）・破棄（FCS_CKM.4）する機能を提供している。

①RA 管理者・申請者・審査者の鍵対

②一般利用者の鍵対

③RA サーバの鍵対

次におのおのの処理について詳述する。

①RA 管理者・申請者・審査者の鍵対

◎生成・破棄について：

表 5-2 で規定している標準、アルゴリズム、鍵長に基づき RA 管理者が他の RA 管理者・申請者・審査者の登録を行う際に RA サーバで生成され、各人の本人認証等に用いられる。また、登録されていた者を削除する際に鍵が破棄される。

◎配付方法について：

RA 管理者・申請者・審査者の秘密鍵は各人の IC カードに格納される。対となる公開鍵は、RA 管理者によって登録書とともに CA サーバへ送られ CA サーバから証明書に格納されて報告書として戻ってくる。公開鍵を含んだ証明書は標準 PKCS#7 に基づいて DB へ格納される。

②一般利用者の鍵対

◎生成・破棄について：

表 5-2 で規定している標準、アルゴリズム、鍵長に基づき、電子認証サービスを受ける一般利用者のうち自分で鍵を持ち込んでいない一般利用者の申請を行う。その際に一般利用者の鍵対が申請者によって RA サーバで生成される。一般利用者の鍵は一時的に TOE 内にあっても報告書を RA 管理者端末から IC カードに出力した後に破棄される。

◎配付方法について：

一般利用者の秘密鍵は IC カードに格納される。対となる公開鍵は、申請者によって申請書とともに CA サーバへ送られて CA サーバから証明書に格納されて報告書として戻ってくる。公開鍵を含んだ証明書は標準 PKCS#7 に基づいて DB へ格納される。

③RA サーバの鍵対

◎生成・破棄について：

表 5-2 に基づき RA 管理者によって RA サーバで生成される。鍵変更時には古い鍵は破棄する。

◎配付方法について：

対となる公開鍵は RA サーバのコマンド機能を使用しオンラインであらかじめ CA 側に登録される。秘密鍵は生成後、いずれにも配付されない。

なお、上記①から③の 3 種類の鍵の破棄の具体的な方法は、表 5-3 に示す手段で行われる。なお、上記鍵の生成時には、登録を行う者の鍵と対を成す公開鍵証明書に、鍵の配付、破棄時には、鍵のセキュリティ属性として公開鍵証明書に記述してある以下の３つをチェックしている(FMT_MSA.2)。

・鍵の有効期間（検証日時が鍵の有効期間内かどうか）

・鍵種別（許可された鍵のアルゴリズムと鍵長が一致するかどうか）
・公開鍵証明書の失効情報（公開鍵証明書が失効されているかどうか）

（２）パスワードによる秘密鍵の一時的な暗号化

RA 管理者、申請者、審査者、一般利用者の秘密鍵を一時的に暗号化するために、パスワードを用いる。ここでの暗号化は、入力パスワードに対する MD5 を用いた演算結果による DES 暗号 (CBC モード) を利用することで行われる。これらは電源オフにより破棄される。また、これらはいずれにも配付されない。

（３）RA 鍵署名生成機能

Trust-KMS は、RA 鍵による登録書や申請書への署名生成機能も提供している。

RA 鍵は表 5-4 に基づいて登録書や申請書への署名生成を行う。（なお、RA 鍵はログへの署名生成に用いられるがそれは SF.Audit の機能である。また RA 鍵は役割確認・権限確認の際にも署名生成を行うがそれは SF.AccessControl の機能である。）表 5-4 に示された署名アルゴリズムと暗号鍵長に従って RA 鍵によって署名生成（FCS_COP.1 その１）を行う際には、公開鍵証明書に記述してある以下の３つをチェックする(FMT_MSA.2)。

・鍵の有効期間（検証日時が鍵の有効期間内かどうか）
・鍵種別（許可された鍵のアルゴリズムと鍵長が一致するかどうか）
・公開鍵証明書の失効情報（公開鍵証明書が失効されているかどうか）

対応する機能要件：FCS_CKM.1、FCS_CKM.4、FCS_COP.1 その１、FMT_MSA.2

＜参照＞表 5-2：鍵生成アルゴリズムと鍵長

アルゴリズム（標準）	使用場面	鍵長 （bit）
RSA（PKCS#1）	・IC カードに格納する鍵の生成（RA 管理者、申請者、審査者の鍵、一般利用者の鍵） ・RA サーバの鍵対の生成	512~2048
ESIGN（ISO14888-3）	・RA サーバの鍵対の生成	576~2304
DSA（公開鍵部分 ANSI X9.57）	・RA サーバの鍵対の生成	512~1024
MD5（PKCS#5）	・RA 管理者、申請者、審査者、一般利用者の秘密鍵を一時的に暗号化するための鍵の生成	56

＜参照＞表 5-3：鍵破棄の方法

鍵の種類	保存場所	破棄方法
◎ＲＡ鍵（RA サーバの秘密鍵）	ＤＢ	0 値化
◎一般利用者の秘密鍵 ◎RA 管理者・申請者・審査者の秘密鍵	ＤＢ	0 値化
◎ＲＡサーバの公開鍵 ◎一般利用者の公開鍵 ◎RA 管理者・申請者・審査者の公開鍵	DB	0 値化
◎RA 管理者、申請者、審査者、一般利用者の秘密鍵を一時的に暗号化するための鍵	メモリ	電源オフによりクリア

＜参考＞表 5-4 署名生成、署名検証の実現方法

暗号操作	使用場面および方法	アルゴリズム	鍵長
RA 管理者・申請者・審査者の鍵によって生成された署名の検証	本人認証、役割確認・権限確認	RSA	512~2048 (bit)
RA 鍵による署名生成、	登録書、申請書への署名生成、RA クライアントから送られた認証データへの署名生成、ログへの RA 鍵ログ署名の生成（長期的改竄防止）	RSA ESIGN DSA	RSA: 512~2048 ESIGN: 576~2304 DSA: 512~1024 (bit)
RA 公開鍵による署名検証	SNI の署名検証、ログに付けられた署名の検証	RSA ESIGN DSA	RSA: 512~2048 ESIGN: 576~2304 DSA: 512~1024 (bit)

6.1.5 SF.AccessControl　アクセス制御機能

Trust-KMS は Trust-KMS 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を元にアクセス制御が行われている(FIA_ATD.1)。表 6-1 のリストに基づいてサブジェクト（RA 管理者プロセス・申請者プロセス・審査者プロセス）とオブジェクト

間の全ての操作に対して行われる（FDP_ACC.1、FDP_ACF.1 ）。また、セキュリティドメインを分離および維持しており、信頼できないサブジェクトから干渉や改竄などから保護されている。（FPT_SEP.1)。RA サーバと CA サーバ間で送受信されるデータには RA サーバ、CA サーバの秘密鍵による署名が付与され、データの改ざんを検出することが可能である（FDP_UIT.1）

「Trust-KMS アクセス制御ポリシー」には、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（FMT_SMR.1）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、これに基づいて操作要求の承認が行われる。このセキュリティ属性の定義を新規登録、削除、変更、参照できるのは RA 管理者のみに制限している（FMT_MSA.1)。

アクセス制御の具体的な手段について説明する。SF.Auth で規定された本人認証機能による認証の後、アクセスしたすべての者に対して以下の役割確認と権限確認を行うことで、その操作要求を承認する。大きくわけて下記の二つの段階を踏む。
①役割確認機能
表 6-1 に示された役割ごとのサブジェクトと本人認証に成功した者の関連付けを本人認証に成功した者の識別情報に応じて行う。（FIA_USB.1)。
②権限確認機能
セキュリティ属性に基づきその役割に与えられた権限の範囲内で、各端末から RA サーバに対し操作要求を行う。

次に、この 2 つの機能を実現する流れを示す。
1.SF.Auth による本人認証後、端末からサービス情報（SVI）と SNI を RA サーバに送信する。
2．RA サーバは受信した SNI を検証しその Ts が有効であることを確認し、SNI を更新する。
3．権限を確認するために、RA サーバは受信した SVI に含まれるサービス内容をその者に提供可能かを DB 内に保存されている役割ごとの権限確認をするためのもの（SVP）から確認する。
（ここで参照される DB 内の SVP はあらかじめ RA 管理者により初期設定の段階で正しく設定されている）
4. RA サーバは SVI を元にサービスを実行しその結果（SVR）と、更新した SNI を返信する。端末は SVR を受信しサービス結果を得る。

以上の手順でアクセス制御を実行することにより、以下のことが実現できる。

・ログ閲覧が可能な権限を RA 管理者、申請者、審査者のみに限定し、それ以外の者が閲覧することはできない（FAU_SAR.2）。また、ログの削除はどの役割にも許可しない（FAU_STG.1）。
・RA サーバの開始・停止、RA サービスそのものの開始・停止、ログ管理機能の起動・停止、CA サーバ情報の登録・削除といった操作の動作や停止、またポリシー情報の登録・削除、RA 鍵対の生成・破棄、RA 管理者・申請者・審査者の鍵対の生成・破棄、RA 管理者と申請者と審査者の登録・削除といったふるまいの決定も RA 管理者のみに限定する（FMT_MOF1）。
・RA 管理者・申請者・審査者・一般利用者の秘密鍵と証明書、申請書、登録書、報告書をインポートする。

以上により Trust-KMS は、操作要求の前には必ず本人認証が必要となり、操作要求する者が操作要求を行う際には必ず役割確認や権限確認が呼び出され（FPT_RVM.1）、操作要求を承認された者だけが、サービスを執り行うことができるようになる。役割確認・権限確認の SNI などの検証時には公開鍵証明書に記述してある以下の３つをチェックする(FMT_MSA.2)。
・有効期間（検証日時がそれらの鍵の有効期間内かどうか）
・鍵種別（許可された鍵のアルゴリズムと鍵長が一致するかどうか）
・公開鍵証明書の失効情報（公開鍵証明書が失効されているかどうか）

対応する機能要件：FAU_SAR.2、FAU_STG.1、FDP_ACC.1、FDP_ACF.1、FDP_UIT.1、FIA_ATD.1、FIA_USB.1、FMT_MOF1、FMT_MSA.1、FMT_MSA.2、FMT_SMR.1、FPT_RVM.1、FPT_SEP.1

表 6-1　各サブジェクトがオブジェクトに対し許可される操作

サブジェクト	オブジェクト	許可される操作
RA管理者プロセス	登録書テーブル（RA管理者、申請者、審査者の登録、削除）	読み出し、書き込み、消去
	報告書テーブル	読み出し、消去
	RA管理者、申請者、審査者の鍵対テーブル	読み出し、書き込み、消去
	通信ポート	読み出し、書き込み
申請者プロセス	申請書（一般利用者の登録、削除、証明書発行、失効）テーブル	読み出し、書き込み、消去
	一般利用者の鍵対（内部生成）テーブル	読み出し、書き込み、消去
	一般利用者の鍵対（持ち込み）ファイル	読み出し、書き込み、消去
	報告書テーブル	読み出し、書き込み
	通信ポート	読み出し、書き込み

審査者プロセス	申請書テーブル	読み出し、書き込み

6.2 Strength of funtion claims

確率的あるいは順列的メカニズムに基づくセキュリティ機能として、SF.Auth、SF.Audit、SF.Crypto、SF.KeyManagement がある。しかし、これらのメカニズムの内、SF.Audit のハッシュ署名生成アルゴリズム以外は暗号アルゴリズムに基づいており、CC の適用範囲外である。そのため本 TOE では、SF.Audit のハッシュ署名生成アルゴリズムについて SOF-basic を claim する。

6.3 Assurance measures

EAL3 からなる保証要件と、それぞれのコンポーネントの要件を満たす保証手段とを以下に示す。

表 6-3.1 保証要件とコンポーネントの要件を満たす保証手段

保証クラス	保証要件コンポーネント	保証手段
ACM：構成管理	ACM_CAP.3 ACM_SCP.1	Trust-KMS,構成管理仕様書
ADO：配付と運用	ADO_DEL.1	Trust-KMS,配付手順マニュアル
	ADO_IGS.1	Trust-KMS,構築マニュアル
ADV：開発	ADV_FSP.1	Trust-KMS,機能仕様書 Trust-KMS,外部インタフェース仕様書
	ADV_HLD.2	Trust-KMS,構成設計書
	ADV_RCR.1	Trust-KMS,機能仕様及び上位レベル設計間対応分析書 Trust-KMS,TOE 要約仕様及び機能仕様間対応分析書
AGD：ガイダンス文書	AGD_ADM.1	Trust-KMS,管理者マニュアル
	AGD_USR.1	Trust-KMS,利用者マニュアル
ALC：ライフサイクルサポート	ALC_DVS.1	Trust-KMS,開発セキュリティに関する開発文書 Trust-KMS,保守マニュアル
ATE：テスト	ATE_COV.2 ATE_DPT.1 ATE_FUN.1	Trust-KMS,テストカバレージ分析書 Trust-KMS,テスト深さ分析書 Trust-KMS,テスト手順書 Trust-KMS,テスト結果一覧
	ATE_IND.2	TOE

AVA：脆弱性評定	AVA_MSU.1 AVA_SOF.1 AVA_VLA.1	 Trust-KMS セキュリティ機能強度分析書 Trust-KMS,脆弱性分析書

7　PP claims

この ST で参照される PP はない。

8 Rationale

8.1 Security objective rationale

表 8-1.1 Assumption,Threats,Organisational security policy と Security objective の根拠

	SO.AUTH	SO.PRIVILEGES	SO.RA_SIGN	SO.LOGGEN	SO.AUDIT_DATA	SO.KEY	SOE.LAN	SOE.SSL	SOEN.ADMIN	SOEN.USER	SOEN.PHYSICAL_PROTECT	SOEN.NETWORK	SOEN.PLATFORM
A.ADMIN									○				
A.USER										○			
A.PHYSICAL_PROTECT											○		
A.LAN							○						
A.NETWORK												○	
A.PLATFORM													○
T.LOGIN	○			○									
T.PRIVILEGES		○		○									
T.CA_TRANSFER			○					○					
P.KEY						○							
P.AUDIT_DATA					○								

A.ADMIN

A.ADMIN は SOEN.ADMIN によって達成される。何故ならこの Objective によって、RA 管理者はガイダンス文書に従い操作を行い、自己の所有する IC カードの紛失を防止し、PIN やパスワードの漏洩に注意を払い、離席時にログアウトすることを利用者に知らせることで他者に RA 管理者端末を操作されることを防ぐことができるからである。

A.USER

A.USER は、SOEN.USER によって達成される。何故ならこの Objective によって、TOE のサービスを受ける一般利用者の秘密鍵暗号化のためのパスワードや IC カードの PIN や、申請者、審査者のそれぞれの申請者端末、審査者端末の OS のパスワードや IC カードの PIN の安全性が保たれ、パスワードの漏洩や推測を防ぐことができるからである。

A.PHYSICAL_PROTECT

A.PHYSICAL_PROTECT は、SOEN.PHYSICAL_PROTECT によって達成される。何故ならこの Objective によって、TOE が動作するハードウェアおよび IC カードがサービス運用元によって入退管理が可能な安全な場所に設置、管理されるからである。

A.LAN

A.LAN は、SOE.LAN によって達成される。何故ならこの Objective によって、RA サーバと RA クライアント間の通信が SSL で行われることで通信データの暴露を防止されるからである。

A.NETWORK

A.NETWORK は、SOEN.NETWORK によって達成される。何故ならこの Objective によって、TOE は正しく設定されたファイアウォールを介してのみ、外部に設置された CA と接続されるからである。

A.PLATFORM

A.PLATFORM は、SOEN.PLATFORM によって達成される。何故ならこの Objective によって、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）は、正しく動作する信頼できる製品が使用されるからである。

T.LOGIN

・T.LOGIN は、SO.AUTH によって対抗される。何故ならこの Objective によって、
外部の攻撃者が不正にログインすることを防止できるからである。
・T.LOGIN は、SO.LOGGEN によって対抗される。なぜならこの Objective によって、

不正なアクセスがあった場合にログの分析によって不正なアクセスの存在を知ることが出来るからである。

T.PRIVILEGES

・T.PRIVILEGES は、SO.PRIVILEGES によって対抗される。何故ならこの Objective によって、TOE は、RA 管理者、申請者、審査者の役割確認を正しく行うことができる。さらに各役割にの操作要求に対して権限確認を正しく行うことで、申請者や審査者（RA 管理者は信頼が前提）が、ログイン後も自分の権限の範囲を超えた操作を行うことを防止でき、TOE の適正な動作を確保することができるからである。

・T.PRIVILEGES は、SO.LOGGEN によって対抗される。なぜならこの Objective によって、不正なアクセスがあった場合にログの分析によって不正なアクセスの存在を知ることが出来るからである。

T.CA_TRANSFER

・T.CA_TRANSFER は、SO.RA_SIGN によって対抗される。何故なら、この Objective によって、RA 鍵によって保護資産に署名が付与されることで RA サーバと CA サーバ間で転送される保護資産が不当に改ざんされることが防げるからである。

・T.CA_TRANSFER は、SOE.SSL によって対抗される。何故なら、この Objective によって、Web サーバを介した SSL を通信に 利用することで、RA サーバと CA サーバ間で転送される保護資産が不当に暴露されることが防げるからである。

P.KEY

P.KEY は SO.KEY によって実現される。何故なら、この Objective によって、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が、TOE 内に暗号化されて保管されることで、安全性、機密性の高い形で管理されるからである。また、これらが TOE 外にエクスポートされた場合は、TOE 内に秘密鍵の情報を残さないようにできるからである。

P.AUDIT_DATA

P.AUDIT_DATA は、SO.AUDIT_DATA によって対抗される。何故ならこの Objective によって、ログに対して改ざんなど不正な加工が行われた事実を検出可能にする手段があることでログが完全性を維持しているのかそうでないのか保証できるからである。

8.2 Security requirements rationale

8.2.1 Security requirements rationale

表 8-2.1 Security objective と Security requirements の根拠

	FAU_GEN.1	FAU_GEN.2	FAU_SAR.1	FAU_SAR.2	FAU_STG.1	FAU_STG.3	FCS_CKM.1	FCS_CKM.4	FCS_COP.1 その１	FCS_COP.1 その２	FCS_COP.1 その３	FDP_ACC.1	FDP_ACF.1	FDP_UIT.1	FIA_ATD.1	FIA_UAU.2	FIA_UID.2	FIA_USB.1	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_SMR.1	FPT_SEP.1	FPT_RVM.1	FPT_STM.1	FTP_ITC.1
SO.AUDIT_DATA					○	○			○		○															
SO.AUTH									○						○	○	○				○		○	○		
SO.PRIVILEGES									○			○	○					○	○	○	○	○	○	○		
SO.LOGGEN	○	○	○	○																					○	
SO.RA_SIGN									○					○												
SO.KEY							○	○		○																
SOE.SSL																										○

SO.AUDIT_DATA は、FAU_STG.1、FAU_STG.3、FCS_COP.1 その１、FCS_COP.1 その 3 によって実現される。なぜならこれらの機能要件によって以下のことが保証されるからである。

・FAU_STG.1：監査記録に対する不正な削除からの保護と改変の検出が可能である。
・FAU_STG.3：運用中にログが規定量に達した場合には警告が出てサービスが停止される。
・FCS_COP.1 その１および FCS_COP.1 その 3：ログに対し署名を生成し付与する。

SO.AUTH は、FCS_COP.1 その１、FIA_ATD.1、FIA_UAU.2、FIA_UID.2、FMT_MSA.2、FPT_SEP.1、FTP_RVM.1 によって実現される。なぜならこれらの機能要件によって以下が保証されるからである。

・FCS_COP.1 その１：利用者の識別認証時に IC カード内にある鍵対を使用して生成した署名の検証を行う。また FMT_MSA.2 によって使用された鍵対のセキュリティ属性をチェックする。
・FIA_ATD.1：識別認証される利用者に関わるセキュリティ属性のリストを維持する。
・FIA_UID.2：利用者が TOE にアクセスしてアクションを行う前に自分自身を識別する
・FIA_UAU.2：利用者が TOE にアクセスしてアクションを行う前に本人認証を

正しく行う。
・FPT_RVM.1 ：TOE にアクセスする者に対して必ず本人認証機能を呼び出し、他の機能要件がバイパスされることを防ぐ。
・FPT_SEP.1 ：本人認証機能によりセキュリティドメインを分離および維持し、他の信頼できないサブジェクトによる干渉や改ざんから保護する。

SO.PRIVILEGES は、FCS_COP.1 その１、FDP_ACC.1、FDP_ACF.1、FIA_USB.1、FMT_MOF.1、FMT_MSA.1、FMT_MSA.2、FMT_SMR.1、FPT_SEP.1、FTP_RVM.1 によって実現される。なぜならこれらの機能要件によって以下が保証されるからである。
・FCS_COP.1 その１：表 5-4 に基づき RA 鍵によって署名生成と署名検証を行う。
また、RA 管理者・申請者・審査者の役割確認・権限確認を行う際の署名検証を行う。また FMT_MSA.2 によって使用された鍵対のセキュリティ属性をチェックする。
・FDP_ACC.1：サブジェクトとオブジェクト間で行われる操作において「Trust-KMS アクセス制御ポリシー」が適用される。
・FDP_ACF.1：セキュリティ属性によって操作要求を承認された者だけがあらかじめ役割ごとに決められた操作を可能になる。
・FIA_USB.1：RA 管理者、申請者、審査者といった役割確認の際に各セキュリティ属性に応じたサブジェクトの関連付けを行う。
・FMT_MOF.1：TOE セキュリティ機能の動作管理に関わる操作を RA 管理者に制限する
・FMT_MSA.1： UID の改変は RA 管理者のみが行うことができる。
・FMT_SMR.1：RA 管理者、申請者、審査者といった役割についてあらかじめ定義を行う。
・FPT_SEP.1： セキュリティドメインを分離および維持しており、信頼できないサブジェクトから干渉や改竄などから保護されている。
・FPT_RVM.1 ：アクセスするすべての者に対して本人認証を行い、操作要求を行う際には必ず役割確認や権限確認が呼び出され、これらの機能をバイパスすることができない。

SO.LOGGEN は、FAU_GEN.1、FAU_GEN.2、FAU_SAR.1、FAU_SAR.2、FPT_STM.1 によって実現される。なぜならこれらの機能要件によって以下のことが保証されるからである。
・FAU_GEN.1：表 5－1 の事象が発生した際にログは、事象の日時、事象の種別、事象の成功や失敗を関連付けた形で生成、格納される。
・FAU_GEN.2：上記のログとタイムスタンプが操作した者の識別情報と関連付けられる。
・FAU_SAR.1：上記のログを閲覧に適した形で読み出しが可能になる
・FAU_SAR.2：許可された者以外のログへのアクセスは禁止される
・FPT_STM.1：ログに対して高信頼なタイムスタンプが付与される。

SO.RA_SIGN は FCS_COP.1 その１、FDP_UIT.1 によって実現される。なぜならこれらの機能要件によって以下が保証されるからである。
・FCS_COP.1 その１：登録書、申請書に RA 鍵による署名を付与することで改ざんを防げる。
・FDP_UIT.1：RA と CA 間を流れる保護資産に改変が生じたかを確認することができるからである。

SO.KEY は FCS_COP.1 その 2、FCS_CKM.1、FCS_CKM.4 によって実現される。なぜならこれらの機能要件によって以下が保証されるからである。
・FCS_COP.1 その 2：これにより秘密鍵は、特定された暗号アルゴリズムと鍵長に従い暗号化される。
・FCS_CKM.1：表 5-2 にのっとった方法で RA 管理者・申請者・審査者の鍵対、
　一般利用者の鍵対、RA サーバの鍵対、および、RA 管理者、申請者、審査者、一般利用者の秘密鍵を一時的に暗号化するための鍵が生成される。
・FCS_CKM.4：DB 内で保存されてきた鍵対で不用となったものを表 5-3 にのっとった方法で廃棄を行う。

SOE.SSL は、FTP_ITC.1 によって実現される。なぜならこの機能によって以下のことが保証されるからである。
FTP_ITC.1 ： TOE と CA サーバ間の通信において、IT 環境が持つ暗号機能によって保護資産の暴露を防ぐことができる。

8.2.2 Dependency analysis

Security Reqirements とその依存性の関係を表 8-2.2.1 にまとめる。
依存性を満たしていないものに関しては下線で表記している。なお、依存性を満たしていない理由については表の後で述べている。また、網掛け部分は本 ST で選択したコンポーネントを指している。

表 8-2.2.1 Security requirements と依存性の関係

Component	Name	Hierarchical to	dependencies
FAU_GEN.1	監査データ生成	—	FPT_STM.1
FAU_GEN.2	利用者識別情報の関連付け	—	FAU_GEN.1 FIA_UID.1*
FAU_SAR.1	監査レビュー	—	FAU_GEN.1
FAU_SAR.2	限定監査レビュー	—	FAU_SAR.1
FAU_STG.1	保護された監査証跡格納	—	FAU_GEN.1
FAU_STG.3	監査データ損失の恐れ発生時のアクション	—	FAU_STG.1
FCS_CKM.1	暗号鍵生成		[FCS_CKM.2 または FCS_COP.1] FCS_CKM.4 FMT_MSA.2
FCS_CKM.4	暗号鍵破棄		[FDP_ITC.1 または FCS_CKM.1] FMT_MSA.2
FCS_COP.1 その 1	暗号操作	—	[FDP_ITC.1 または FCS_CKM.1] FCS_CKM.4 FMT_MSA.2
FCS_COP.1 その 2	暗号操作	—	[FDP_ITC.1 または FCS_CKM.1] FCS_CKM.4 **FMT_MSA.2**
FCS_COP.1 その 3	暗号操作	—	[FDP_ITC.1 または **FCS_CKM.1**] **FCS_CKM.4** **FMT_MSA.2**
FDP_ACC.1	サブセットアクセス制御	—	FDP_ACF.1
FDP_ACF.1	セキュリティ属性によるアクセス制御	—	FDP_ACC.1 **FMT_MSA.3**

FDP_UIT.1	データ交換完全性	—	[FDP_ACC.1 または FDP_IFC.1] [FTP_ITC.1 または FTP_TRP.1]
FIA_ATD.1	利用者属性定義	—	—
FIA_UAU.2	アクション前の利用者認証	FIA_UAU.1	FIA_UID.1*
FIA_UID.2	アクション前の利用者識別	FIA_UID.1	—
FIA_USB.1	利用者・サブジェクト結合	—	FIA_ATD.1
FMT_MOF.1	セキュリティ機能のふるまいの管理		FMT_SMR.1
FMT_MSA.1	セキュリティ属性の管理	—	[FDP_ACC.1または FDP_IFC.1] FMT_SMR.1
FMT_MSA.2	セキュアなセキュリティ属性	FMT_MSA.1	ADV_SPM.1 [FDP_ACC.1 または FDP_IFC.1] FMT_MSA.1 FMT_SMR.1
FPT_RVM.1	TSP の非バイパス性	—	—
FPT_STM.1	高信頼タイムスタンプ	—	—
FMT_SMR.1	セキュリティ役割	—	FIA_UID.1*

注： *が付与されている機能要件 FIA_UID.1 の依存性について：
CC Part2 によると、FIA_UAU.2 に対しては FIA_UID.1 に依存関係が与えられているが、FIA_UID.1 と FIA_UID.2 はそれぞれ階層関係があるので依存性は満たしている。

表 8-2.2.1 で下線を引いた機能要件が、依存性を満たす必要がない理由はそれぞれ以下である。

・FCS_COP.1 その 2 では、一般利用者または RA 管理者、申請者、審査者のパスワードを用いて暗号処理するため FCS_CKM.1 は必要。
ただし TOE 内に鍵対を保存する必要はなく復号する場合パスワードの入力を TOE は求め、復号鍵を生成し暗号処理する。暗号処理は一般利用者または RA 管理者、申請者、審査者それぞれの秘密鍵ごとにおこない、使用する秘密鍵はユーザが入力したパスワードから生成されたものを使用し、その際属性値によって鍵がセキュアかどうかをチェックしていないが、鍵生成にハッシュアルゴリズムを使用しており、セキュアな鍵が生成されることが保証される。そのため FMT_MSA.2 への依存性は満たさなくても問題はない。

・FCS_COP.1 その 3 では、ハッシュアルゴリズムには暗号鍵が使われないため、鍵の生成・破棄、及び暗号鍵のセキュリティ属性は存在しない。FCS_CKM.1、FCS_CKM.4、FMT_MSA.2 との依存性は満たさなくても問題はない。

・FDP_ACF.1 のアクセス制御で扱われるセキュリティ属性はデフォルト値の改変を許可していないため FMT_MSA.3　との依存性は必要ない。

・FMT_MSA.2 から依存する ADV_SPM.1 を満たさなくても問題は発生しない理由を以下にあげる。

表 8-2.2.2　FMT_MSA.2 で扱うセキュアなセキュリティ属性のセキュリティポリシモデル

目的	RA 管理者、申請者、審査者の秘密鍵の署名検証	一般利用者の秘密鍵の署名検証
セキュリティ属性	RA 管理者、申請者、審査者の証明書の有効期限、種別、失効情報	一般利用者の証明書の有効期限、種別、失効情報
説明	TOE は RA 管理者、申請者、審査者の秘密鍵による署名を検証する際に、対となる公開鍵証明書の有効期限、種別、失効情報を確認する。条件を満たさない場合は署名の検証がエラーとなり、TOE はその署名を受け入れない。このため、使用する鍵のセキュリティ属性はセキュアなものだけを受け入れることが保証される。	TOE は一般利用者の秘密鍵による署名を検証する際に、対となる公開鍵証明書の有効期限、種別、失効情報を確認する。条件を満たさない場合は署名の検証がエラーとなり、TOE はその署名を受け入れない。このため、使用する鍵のセキュリティ属性はセキュアなものだけを受け入れることが保証される。

以上により、依存関係を満足している。

8.2.3　Demonstration of mutual support between security requirements

以下に記述する通り、本 ST で選択された機能要件は相互にサポートしあっている。

○依存性

前節 8.2.2 のとおり、本 ST で選択された機能要件の依存関係は、その依存関係を満たす必要がないことが明確であるもの以外はすべて満たされている。

○内部一貫性

本 ST では、要件間で相反する要求により矛盾が生じるような機能要件は選択されていない。

○SFR（機能要件）の保護

・＜バイパス防止＞TOE は、FPT_RVM.1 によって、識別認証やアクセス制御に関わる機能要件がバイパスされることを防ぐ。

・＜不正干渉防止＞FPT_SEP.1 により、信頼できないサブジェクトからの TSF に対する不正な干渉が防止され、外部の信頼できないサブジェクトからの不正な干渉が阻止される。

・＜非活性化防止＞FMT_MOF.1 により TOE のセキュリティ機能の動作管理を RA 管理者のみに許可しているので、セキュリティ機能要件の非活性化は防止される。

・＜無効化攻撃の検出＞FAU_GEN.1, FAU_GEN.2 によって RA 管理者・申請者・審査者の識別情報と共に監査記録を生成され、また、FAU_SAR.1, FAU_SAR.2 によって定められた役割である RA 管理者・申請者・審査者が監査記録をレビューすることで TOE セキュリティ機能の無効化を狙った攻撃の試みを検出することが可能である。また、FAU_STG.1 により監査記録は不正な改竄を事後に検出することが可能である。

8.2.4 Security audit data generation rationale

FAU_GEN.1 において、最小レベルのアクションを採用しなかった機能要件の根拠について以下で述べる。

表 8-2.4　最小レベルのアクション除外の根拠

機能要件	監査対象レベルとすべき最小レベルのアクション	根拠
FAU_STG.3	a) 基本：閾値を超えたためにとられるアクション	TOE は、ログの容量が規定量を超えた場合、ログ管理機能が停止し同時に RA 自体のサービスも停止するため、監査対象事象に含まなくてもセキュリティ対策方針上問題はない。
FCS_COP.1 その１	a) 最小: 成功と失敗及び暗号操作の種別。	TOE では、署名生成/検証を呼び出した機能が成功の場合は特にログは記録されず、不成功だった

		場合に「失敗」のログが記録される。ゆえに失敗した場合にはその旨の記録が検出できるため、結果的に不正な利用が発生した事実を検出することが可能となる。ゆえにセキュリティ方針上問題はない。
FPT_STM.1	a) 最小: 時間の変更;	TOE には OS の時刻を変更する機能が存在せず、また、サーバの OS のパスワードは RA 管理者が行っており、勝手に変更することはできないため、セキュリティ対策方針上問題はない。

8.2.5 Appropriateness of assurance requirements

本製品は、PKI の中で一般利用者管理や証明書発行申請を担当する製品であり、開発環境や構成管理の評価を通じて製品の一定以上の品質が要求されるものであるが、CA に対する基盤製品であるため安価な製品価格を実現する必要がある。

そこで、主なターゲットである一般的な民間企業または一般的な公的機関が本製品を導入する際に、可能な限り開発側として求めたい物理環境や利用環境や人的条件や接続性に関する前提条件をセキュリティ環境と対策方針にて設置した。また低レベルの攻撃者によるなりすましや不正アクセスといった脅威を想定してそれに対し低レベルの本製品の対策方針を講じている。また本製品で claim する機能強度は SOF-basic である。

以上の点を考慮すると、保証レベルとして EAL3 が妥当である。

8.2.6 Minimum strength of function(SOF) claim rationale

TOE は 3.2 Assumptions で述べたように物理的および接続的に安全に保たれているため、過度に保護される必要はない。このためセキュリティ機能は攻撃に対し低レベルの攻撃に対する防御を備えればよい。本 TOE では 3.3 Threats で述べたように、攻撃レベルが低レベルの脅威エージェントを想定したセキュリティ対策方針で施している。従って、Minimum strength of function レベルは SOF-basic が妥当であるといえる。

8.3 TOE summary specification rationale

8.3.1 Security functions rationale

表 8-3.1 Security requirements と Security functions の根拠

	SF.Auth	SF.Audit	SF.Crypto	SF.KeyManagement	SF.AccessControl
FAU_GEN.1		○			
FAU_GEN.2		○			
FAU_SAR.1		○			
FAU_SAR.2					○
FAU_STG.1		○			○
FAU_STG.3		○			
FCS_COP.1 その 1	○	○		○	
FCS_COP.1 その 2			○		
FCS_COP.1 その 3		○			
FCS_CKM.1				○	
FCS_CKM.4				○	
FDP_ACC.1					○
FDP_ACF.1					○
FDP_UIT.1					○
FIA_ATD.1					○
FIA_UAU.2	○				
FIA_UID.2	○				
FIA_USB.1					○
FMT_MOF1					○
FMT_MSA.1					○
FMT_MSA.2	○	○		○	○
FMT_SMR.1					○
FPT_SEP.1	○				○
FPT_RVM.1	○				○
FPT_STM.1		○			

FAU_GEN.1 監査データ生成 （SF.Audit）
TOE は、5 章 FAU_GEN.1 における表 5－1 に基づき、発生した事象を、「ログ種別番号、メッセージ詳細番号、付与される役割、ユーザ ID、拡張情報」と関連付けてログの生成を行うことで実現している。

FAU_GEN.2 利用者識別情報の関連付け （SF.Audit）
TOE は、ログをその原因となった操作を行った者の識別情報の、付与される役割、ユーザ ID と関連付けていることで実現している。

FAU_SAR.1 監査レビュー （SF.Audit）
SF.Audit：
TOE では、ログは監査情報のリストに基づいた形で出力される。これら（ログ種別番号、メッセージ詳細番号、事象の結果、付与される役割、ユーザ ID、拡張情報、事象の日付・時刻）は、許可された役割である RA 管理者、申請者、審査者が閲覧可能である。また、閲覧しやすいようテキストファイルの形で出力されることで実現している。

FAU_SAR.2 限定監査レビュー （SF.AccessControl）
SF.AccessControl：
TOE では、役割確認と権限確認によって、許可された役割である RA 管理者、申請者、審査者に対してのみログの読み出しが許可され､許可された役割以外の者に対しログの読み出しを禁止することで実現している。

FAU_STG.1 保護された監査証跡格納
SF.Audit：
TOE は、ログに対して署名が生成されるため、その署名を検証することで、ログの改竄が行われても検出が可能であることで実現している。
SF.AccessControl：
TOE は、本人認証の後に役割確認・権限確認を行うことでアクセスを制御することでき、これにより外部の者がログにアクセスしてログに対して不正な加工を行うことを防止することを実現している｡またログの削除はすべての役割に対して許可しないことで機能要件を実現している。

FAU_STG.3 監査データ損失の恐れ発生時のアクション （SF.Audit）
TOE は、運用中にログが RA 管理者があらかじめ規定した量に達した場合には、警告を表示して業務としての RA サービスそのものを停止することで実現している。

FCS_CKM.1 暗号鍵生成 (SF.KeyManagement)
TOE は表 5-2 で定める標準と種類、鍵長に基づいて、鍵対を生成することで実現している。

FCS_CKM.4 暗号鍵破棄 (SF.KeyManagement)
TOE は、表 5-3 に基づいて 0 値化することで鍵対を破棄できることで実現している。

FCS_COP.1 その１ 暗号操作　(SF.Auth, SF.Audit, SF.KeyManagement)
SF.Auth：
TOE は本人認証を行う際、RA サーバへアクセス時に受信する電子署名の署名検証を行う場合、表 5-4 に示された署名アルゴリズムと暗号鍵長に従って、署名検証という暗号操作を行うことで実現している。
SF.Audit：
TOE は、ログは RA 鍵によって署名生成されるため、改竄が行われたとしてもその署名を検証することで検出可能であることで実現している。
SF.KeyManagement:
TOE は RA 鍵によって申請書および登録書への署名生成を行う場合、表 5-4 に示された署名アルゴリズムと暗号鍵長に従うことで実現している。
　以上、これら３つの SF によって、TOE は特定された暗号アルゴリズムと鍵長に従って、表 5-4 で示された使用場所にて署名生成、署名検証を行うことにより、FCS_COP.1 その１を実現している。

FCS_COP.1 その 2 暗号操作　（SF.Crypto）
TOE は、一般利用者、RA 管理者・申請者・審査者の秘密鍵を暗号化して DB に保存したりすることで、秘密鍵を安全に管理している。これらの暗号化は『入力パスワードに対する MD5 を用いて導出された DES 暗号 (CBC モード)』によって行われていることで実現している。

FCS_COP.1 その 3 暗号操作　（SF.Audit）
TOE は、ログに対してハッシュ値署名操作を行うことで署名生成されるため、改竄が行われたとしてもその署名を検証することで事後に検出可能であることで実現している。

FDP_ACC.1 サブセットアクセス制御 (SF.AccessControl)
TOE はサブジェクト（RA 管理者プロセス、申請者プロセス、審査者プロセス）とオブジェクト間の全ての操作に対して『Trust-KMS アクセス制御ポリシー』に基づいてアクセス制御を行われることで実現している。

FDP_ACF.1 セキュリティ属性によるアクセス制御 (SF.AccessControl)
TOE は『Trust-KMS アクセス制御ポリシー』によって維持されているセキュリティ属性に基づいて、サブジェクト（RA 管理者・申請者・審査者）とオブジェクト間の操作が許可される。これによりセキュリティ属性で識別された者のうち、事前に権限が与えられた者に対してのみ、アクセスすることが可能となることで実現している。

FDP_UIT.1 データ交換完全性 (SF.AccessControl)
TOE は『Trust-KMS アクセス制御ポリシー』を実施することで RA サーバと CA サーバ間で送受信されるデータには RA サーバ、CA サーバの秘密鍵による署名が付与され、データの改ざんを検出することを可能とすることで実現している。

FIA_ATD.1 利用者属性定義(SF.AccessControl)
TOE は、TOE 内のセキュリティ属性である「ユーザ ID（UID）/付与される役割(SNI)/役割ごとの権限(SVP)」は TOE の中に維持されており、それらを使ってアクセスする者のアクセス制御を行うことで実現している。

FIA_UAU.2 アクション前の利用者認証(SF.Auth)
TOE は RA 管理者・申請者・審査者がアクションを行う前に、本人認証によって自分自身の認証に成功しなくてはならず､本人認証に成功しなかった場合にはその後のいかなるアクションも実行することができないことで実現している。

FIA_UID.2 アクション前の利用者識別(SF.Auth)
TOE は RA 管理者、申請者、審査者がアクションを行う前に、本人認証によって自分自身の識別に成功しなくてはならず､本人認証に成功しなかった場合にはその後のいかなるアクションも実行することができないことで実現している。

FIA_USB.1 利用者・サブジェクト結合(SF.AccessControl)
TOE は本人認証後、セキュリティ属性に応じたサブジェクトを関連付けることで、各人に対して維持されている役割（RA 管理者・申請者・審査者）を付与する役割確認を実現している。

FMT_MOF.1 セキュリティ機能のふるまいの管理(SF.AccessControl)
TOE の RA サーバ本体の開始・停止、RA サービス（機能そのもの）開始・停止
ログ管理機能の起動・停止、CA サーバに関する情報の登録・削除、RA 鍵対の生成・破棄、RA 管理者・申請者・審査者の鍵対の生成・破棄除といった操作の動作は RA 管理者のみが行うことと限定することで実現している。

FMT_MSA.1 セキュリティ属性の管理(SF.AccessControl)
TOE がセキュリティ属性に対し、新規登録、改変、削除、参照する能力を『Trust-KMS アクセス制御ポリシー』に基づいて、RA 管理者に制限することで実現している。

FMT_MSA.2 セキュアなセキュリティ属性(SF.Auth、、SF.Audit、 SF.KeyManagement、SF.AccessControl)

SF.Auth

本人認証を行う際、IC カード内の秘密鍵を用いて生成された電子署名を検証する際に、公開鍵証明書に記述してある、鍵対の有効期間、鍵種別及び公開鍵証明書の失効情報をチェックすることで実現している。

SF.Audit

ログに対して署名生成の時、RA 鍵と対を成す公開鍵証明書に記述してある、鍵対の有効期間、鍵種別及び公開鍵証明書の失効情報をチェックすることで実現している。また署名検証する際に、公開鍵証明書に記述してある、鍵対の有効期間、鍵種別及び公開鍵証明書の失効情報をチェックすることで実現している。

SF.KeyManagement

鍵対を生成する際に、登録を行う者の秘密鍵と対を成す公開鍵証明書に記述してある、鍵対の有効期間、鍵種別及び公開鍵証明書の失効情報をチェックすることで実現している。

また、鍵対を配付、破棄する際に、鍵対が誤って配付、破棄されないように公開鍵証明書に記述してある、鍵対の有効期間、鍵種別及び公開鍵証明書の失効情報をチェックすることで実現している。

また RA 鍵によって署名生成する際に、公開鍵証明書に記述してある、鍵対の有効期間、鍵対種別及び公開鍵証明書の失効情報をチェックすることで実現している。

SF.AccessControl

本人認証後に、役割確認・権限確認する際に SNI などを検証する際に、公開鍵証明書に記述してある、鍵対の有効期間、鍵種別及び公開鍵証明書の失効情報をチェックすることで実現している。

FMT_SMR.1 セキュリティ役割 (SF.AccessControl)
TOE は、TOE 内部で役割確認や権限確認に必要な情報を管理することでそれぞれの役割（RA 管理者、申請者、審査者）を維持することで実現している。

FPT_STM.1 高信頼タイムスタンプ(SF.Audit)
TOE は OS から時刻情報を取得してきてログに対してタイムスタンプを施すことで実現している。

FPT_SEP.1　TSF ドメイン分離
SF.Auth：
TOE は、信頼できないサブジェクトによる干渉と改ざんからそれを保護するためのセキュリティドメインを維持し、TSC 内でサブジェクトのセキュリティドメインを分離することにより実現している。
SF.AccessControl：
TOE は、セキュリティドメインを分離および維持することで、他の信頼できないサブジェクトによる干渉や改ざんから保護することにより実現している。

FPT_RVM.1 TSP の非バイパス性（SF.Auth ,SF.AccessControl）
SF.Auth：
TOE は、アクセスするすべての者に対して本人認証を行うことで識別・認証していることで実現している。
SF.AccessControl：
TOE は、本人認証後に TSC 内の各機能の動作進行を許可する前に、アクセスしたすべての者に対して役割確認と権限確認を行うことで、その操作要求を承認する」ことで実現している。
以上、これら２つの SF が確実に呼び出され、識別認証やアクセス制御機能が実行され、これらの機能をバイパスすることができないことにより FPT_RVM.1 が実現されている。

8.3.2 Demonstration of mutual support between security functions

前節 8.3.1 で記述した通り、Security functions はすべての機能要件を実現しており、機能要件同士は相互にサポートしあっている。本 TOE では不正な利用者による TOE の利用を SF.Auth と SF.AccessControl のセキュリティ機能により防止している。また、利用者データや TSF データを保護するために、SF.Crypto による暗号化や SF.KeyManagement による暗号鍵の管理を行っている。さらに、SF.Audit により監査記録を取ることで不正なアクセスを検出することが可能となっている。これらのセキュリティ機能は、全体として相互にサポートするような構造を実現している。

8.3.3 Strength of function claims rationale

本 TOE において、ハッシュ署名の生成アルゴリズムが確率的または順列的メカニズムに含まれる。strength of function は 6.2 節では「SOF-basic」と宣言している。一方、5.3 節において「SOF-basic」と宣言している。これらが矛盾しないことは明らかである。

8.3.4 Assurance measures rationals

EAL3 からなる保証要件と、それぞれのコンポーネントに対応する保証手段とを表 8-3.2 に示す。以下の ASE クラス及び EAL3 からなる保証要件が満たされていることを確認する手段として、関連する文書を分析するという方法はきわめて妥当である。従って、各 ASE クラス及び EAL3 からなる保証要件に関連ある文書名を保証手段として引用する。なお、これらの保証手段が実際に保証要件を満たしていることは評価過程を経て明らかにしていく。（カッコ内は各保証手段の概要）

表 8-3.2　保証要件と保証手段

保証クラス	保証要件 コンポーネント	保証手段
ACM：構成管理	ACM_CAP.3 ACM_SCP.1	Trust-KMS,構成管理仕様書 （ソフトウェアの更新など構成管理に必要な項目【ACM_CAP.3】及び製品開発の際に実践した構成管理の記録【ACM_SCP.1】）
ADO：配付と運用	ADO_DEL.1	Trust-KMS,配付手順マニュアル （製品や変更された製品情報などをユーザに配付する際のルールの記述【ADO_DEL.1】）
	ADO_IGS.1	Trust-KMS,構築マニュアル （セットアップ方法やパラメータの説明などの操作手順【ADO_IGS.1】）
ADV：開発	ADV_FSP.1	Trust-KMS,機能仕様書 Trust-KMS,外部インタフェース仕様書 （前者は製品の持つ機能の使用方法や効果やエラー情報。後者は外部インタフェースにおけるセキュリティ機能【ADV_FSP.1】）
	ADV_HLD.2	Trust-KMS,構成設計書 （製品内の各サブシステム基本構成【ADV_HLD.2】）
	ADV_RCR.1	Trust-KMS,機能仕様及び上位レベル設計間対応分析書 Trust-KMS,TOE 要約仕様及び機能仕様間対応分析書 （前者は ST5 章で定義した機能と実製品間の分析結果、後者は ST6 章で定義した要約仕様と実製品間の分析結果【ADV_RCR.1】）
AGD：ガイダンス文書	AGD_ADM.1	Trust-KMS,管理者マニュアル （管理者が利用できる機能や運営管理する方法や行動指針等【AGD_ADM.1】）
	AGD_USR.1	Trust-KMS,利用者マニュアル （利用者が利用できる機能や守るべき行動指針など【AGD_USR.1】）

ALC：ライフサイクルサポート	ALC_DVS.1	Trust-KMS,開発セキュリティに関する開発文書 Trust-KMS,保守マニュアル （前者は、開発環境の物理的セキュリティ対策、規則、人的管理について。後者は製品を運用していく上で求められる保守内容【ALC_DVS.1】）
ATE：テスト	ATE_COV.2	Trust-KMS,テストカバレージ分析書 （開発者が行ったテストの完全さ。試験の方法結果テスト証跡【ATE_COV.2】）
	ATE_DPT.1	Trust-KMS,テスト深さ分析書 （開発者が行ったテストの詳細さ（規模や範囲）分析。【ATE_DPT.1】）
	ATE_IND.2	TOE
	ATE_FUN.1	Trust-KMS,テスト結果一覧 （開発者によるテスト。開発者がテスト証跡として出してきた文書検証内容【ATE_FUN.1】）
AVA：脆弱性評定	AVA_MSU.1 AVA_SOF.1 AVA_VLA.1	Trust-KMS セキュリティ機能強度分析書 [AVASOF.1] Trust-KMS,脆弱性分析書 （管理者、利用者が保障手段通りの操作をしてセキュリティ機能が実現するかガイダンス文書の検証【AVA_MSU.1】及び ST で設定した脅威に対するセキュリティ機能の検証【AVA_VLA.1】）

8.4 PP claims rationale

この ST で参照される PP はない。

＜付録A＞ 参考文献

＜DES＞ FIPS PUB 47, *Data Encryption Standard, November 23, 1976.*

＜RSA＞ RSA Laboratories, *PKCS #1: RSA Encryption Standard, Version 1.5 Revised November 1, 1993.*

＜ESIGN＞ NTT 情報流通プラットフォーム研究所, *“デジタル署名ESIGN技術仕様書”, 2002年3月26日 http://info.isl.ntt.co.jp/esign/NKCS/nttdoc-esign1.0.pdf*

＜SHA-1＞ FIPS PUB 180-1, *Secure Hash Standard, April 17,1995.*

＜FEAL＞ ISO/IEC 9979, *Information technology - Security Techniques -Procedures for the registration of cryptographic algorithms,ISO entry name; {iso standard 9979 feal (10)},Date registered; 14 November 1994.*

＜MD5＞ R.L.Rivest, *The MD5 Message Digest Algorithm, RFC 1321 April 1992.*

＜FIPS140-2＞ NIST FIPS PUB 140-2, *Security Requirements for Cryptographic Modules, May 25,2001.*

＜PKCS#７＞ RSA Laboratories, *PKCS#7 – Cryptographic Message Syntax Standard, Version 1.5, November 1993.*

＜PKCS#8＞ RSA Laboratories, *PKCS#8 – Private-Key Information Syntax Standard, Version 1.2, November 1993.*

＜PKCS#10＞ RSA Laboratories, *PKCS#10 – Private-Key Information Syntax Standard, Version 1.2, November 1993.*

＜SSLv2＞ Hickman, Kipp, *"The SSL Protocol", Netscape Communications Corp., Feb 9, 1995.*

＜SSLv3＞ A. Frier, P. Karlton, and P. Kocher, *"The SSL 3.0 Protocol", Netscape Communications Corp., Nov 18, 1996.*

＜付録B＞ 用語説明

用語	説明
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
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。
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。
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。
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
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。

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。
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。
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。
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。
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。

＜付録C＞ ESIGNについて

ESIGN の安全性を証明するものとして、ESIGN-D と ESIGN-R (ESIGN-TSHv2)に関する NESSIE の自己評価レポートを参考文献として以下に提示する。

NESSIE, Security Evaluation. Version 2.0 ,February 19, 2003

https://www.cosic.esat.kuleuven.ac.be/nessie/deliverables/D20-v2.pdf

該当部分は同資料の257ページ 7.4.2 ESIGN の章を参照されたい。