FCS_COP.1 暗号操作

下位階層 :なし

依存性 :[FDP_ITC.1 セキュリティ属性なし利用者データインポート、または
FDP_ITC.2 セキュリティ属性を伴う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

FCS_COP.1.1 **TSF** は、**[割付: 標準のリスト]**に合致する、特定された暗号アルゴリズム**[割付: 暗号アルゴリズム]**と暗号鍵長**[割付: 暗号鍵長]**に従って、**[割付: 暗号操作のリスト]**を実行しなければならない。

- [割付: 標準のリスト] : CRYPTREC暗号リスト
- [割付: 暗号アルゴリズム] : RSA
- [割付: 暗号鍵長] : 2048
- [割付: 暗号操作のリスト] : データの暗号化

FIA_AFL.1 認証失敗時の取り扱い

下位階層 : なし

依存性 : FIA_UAU.1 認証のタイミング

FIA_AFL.1.1 **TSF** は、**[割付: 認証事象のリスト]**に関して、[選択: [割付: 正の整数値]、[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値**]**回の不成功認証試行が生じたときを検出しなければならない。

- [割付: 認証事象のリスト] : 暗証番号の入力
- [選択: [割付: 正の整数値]、[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値] : 3

FIA_AFL.1.2 不成功の認証試行が定義した回数[選択：に達する、を上回った]とき、TSF は、[割付: アクションのリスト]をしなければならない。

- [選択：に達する、を上回った] : 3に達する
- [割付: アクションのリスト] : 1時間 当該ICカードによる認証の拒否

FIA_SOS.1 秘密の検証

下位階層 : なし

依存性 : なし

FIA_SOS.1.1 **TSF** は、秘密が[割付: 定義された品質尺度]に合致することを検証するメカニズムを提供しなければならない。

- [割付: 定義された品質尺度] : 6文字以上で同一の番号および連番ではない

FIA_UAU.2 アクション前の利用者認証

下位階層 : FIA_UAU.1 認証のタイミング

依存性 : FIA_UID.1 識別のタイミング

FIA_UAU.2.1 TSF は、その利用者を代行する他のTSF 仲介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。

FIA_UID.2 アクション前の利用者識別

下位階層 : FIA_UID.1 識別のタイミング

依存性 : なし

FIA_UID.2.1 TSF は、その利用者を代行する他のTSF 仲介アクションを許可する前に、各利用者に識別が成功することを要求しなければならない。

FMT_MTD.1 **TSF** データの管理

下位階層：なし

依存性： FMT_SMR.1 セキュリティの役割
FMT_SMF.1 管理機能の特定

FMT_MTD.1.1 **TSF** は、**[割付: TSF** データのリスト**]**を**[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]**する能力を**[割付: 許可された識別された役割]**に制限しなければならない。

- [割付: TSF データのリスト] : 暗証番号
- [選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]する能力を[割付: 許可された識別された役割] : 改変
- [割付: 許可された識別された役割] : カード所有者

FMT_SMF.1 管理機能の特定

下位階層：なし

依存性： なし

FMT_SMF.1.1 **TSF** は、以下の管理機能を実行することができなければならない。 : **[割付: TSF** によって提供される管理機能のリスト**]**

- [割付: TSF によって提供される管理機能のリスト] : 下表に示す

機能要件	予見される管理アクティビティ	必要な管理項目
FCS_COP.1	—	—
FIA_AFL.1	不成功の認証試行に対する閾値の管理 認証失敗の事象においてとられるアクションの管理	なし(閾値およびアクションは固定である)
FIA_SOS.1	秘密の検証に使用される尺度の管理。	なし(品質の尺度は固定である)
FIA_UAU.2	管理者による認証データの管理	なし(認証データを管理する役割は存在しない)
FIA_UAU.2	関係する利用者による認証データの管理	なし(利用者識別情報は固定である)
FIA_UID.2	利用者識別情報の管理	なし(利用者識別情報は固定である)
FMT_MTD.1	TSFデータと相互に影響を及ぼしうる役割のグループの管理	なし(役割のグループはない)
FMT_SMF.1	—	—
FMT_SMR.1	役割の一部をなす利用者のグループの管理	なし(利用者のグループは固定である)

FDP_ITC.1	インポートに対して使用される追加の制御規則の改変	なし(制御規則は固定である)
FTP_PHP.3	物理的改ざんに対する自動応答の管理	なし(自動応答は固定である)

FMT_SMR.1 セキュリティの役割

下位階層:なし

依存性: FIA_UID.1 識別のタイミング

FMT_SMR.1.1 **TSF** は、役割[割付**:** 許可された識別された役割]を維持しなければならない。

- [割付: 許可された識別された役割]：カード利用者、カード発行専用端末

FMT_SMR.1.2 **TSF** は、利用者を役割に関連付けなければならない。

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

下位階層: なし

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_MSA.3 静的属性初期化

FDP_ITC.1.1 **TSF** は、**SFP** 制御下にある利用者データを**TOE** の外部からインポートするとき、[割付:アクセス制御SFP 及び/または情報フロー制御SFP]を実施しなければならない。

- [割付:アクセス制御SFP 及び/または情報フロー制御SFP]：改竄の検知

FDP_ITC.1.2 **TSF** は、**TOE** 外からインポートされるとき、利用者データに関連付けられたいかなるセキュリティ属性も無視しなければならない。

FDP_ITC.1.3 **TSF** は、**TOE** 外部から**SFP** の下で制御される利用者データをインポートするとき、**[**割付**:**追加のインポート制御規則**]**の規則を実施しなければならない。

- [割付:追加のインポート制御規則]：改竄の検知

FPT_PHP.3 物理的攻撃への抵抗

下位階層:なし

依存性: なし

FPT_PHP.3.1 **TSF** は、**SFR** が常に実施されるよう自動的に対応することによって、**[**割付**: TSF** 装置/エレメントのリスト**]**への**[**割付**:** 物理的な改ざんのシナリオ**]**に抵抗しなければならない。

- [割付: TSF 装置/エレメントのリスト]：紅電ICカード内の回路

適用箇所	内容
物理的な改竄のシナリオ	紅電ICカードを分解し回路内のデータを直接改竄する攻撃 サイドチャネル攻撃

FIA_AFL.1	認証失敗時の取り扱い
FIA_SOS.1	秘密の検証
FIA_UAU.2	アクション前の利用者認証
FIA_UID.2	アクション前の利用者識別
FMT_MTD.1	TSF データ管理
FMT_SMF.1	管理機能の特定
FMT_SMR.1	セキュリティの役割
FPT_ITC.1	送信中の TSF 間機密性
FPT_PHP.3	物理的攻撃への抵抗