参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
3. フレームワーク要件					
	3.1 登録・認定要件				
	R 3.1.0.1 カード供給者、カード発行者、サービス提供者は、それぞれの役割に対応したサービスを提供する前に2.5 の手順に従い登録認定機関に登録し、識別子（ID）と公開鍵証明書を得なければならない（カード供給者は識別子のみ取得）。（仕様要件・必須）				
	R 3.1.0.2 登録認定機関はカード発行者およびサービス提供者の公開鍵に対する認証サービスと登録情報の検索サービスを提供しなければならない。（仕様要件・必須）				
	R 3.1.0.3 カード供給者は2.5 の手順に従いカード登録認定を受けたカードをカード発行者に供給しなければならない。（運用要件・必須）				
	R 3.1.0.4 カード発行者は登録されたカード供給者およびサービス提供者のみと取引しなければならない。（運用要件・必須）				
	R 3.1.0.5 カード発行者は発行するICカードに一意なカードIDを付与しなければならない。（仕様要件・必須）				
	R 3.1.0.6 登録認定機関はAP登録の際にアプリケーションプログラムの実体を識別できるAP 識別子(AP_ID)を払い出し、その一意性を保証しなければならない。（運用要件・必須）				
	R 3.1.0.7 IC カードへのAP 搭載に関する取引をカード発行者とする前に、サービス提供者は登録認定機関にAP 登録を行わなければならない。（運用要件・必須）				
	R 3.1.0.8 登録認定機関はIC カードがカード発行者やサービス提供者の外部プレーヤを認証処理するのに適した公開鍵証明書（簡易証明書）をカード発行者やサービス提供者に発行しなければならない。（仕様要件・必須）				
	3.2 セキュリティ要件				
	R 3.2.0.1 カード発行者は登録認定されたカード供給者からIC カードを入手しなければならない				
	、IC カードの輸送に伴う盗難、改ざんを防ぐための対策を施したほうがよい。（運用要件・オプション）				
	R 3.2.0.2 カード発行者は、カードに設定する公開鍵証明書に対するカード証明書の検索やCRL（証明書失効リスト）の管理などの認証サービスを提供しなければならない。（仕様要件・必須）				
	R 3.2.0.3 カード発行時にカード発行者はカードへのアクセス制御機能（カードにアクセスできる主体や利用できる機能を制御する機能）を有効にしなければならない。（機能要件・必須）				
	R 3.2.0.4 カード発行者はカード保有者に安全にカードを渡さなければならない				
	カード保有者に渡る前にカードが紛失・改ざんされる可能性がある場合は、カード保有者以外の者がカードへアクセスできないような対策を施したほうがよい。（運用要件・オプション）				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	R 3.2.0.5 カード発行者は搭載を許可したAP がカードにダウンロードされることを、AP 搭載許可証により保証しなければならない。(仕様要件・必須)				
	R 3.2.0.6 AP ダウンロード時のカードによるダウンロード主体の認証(外部認証)行う場合には、カード内の登録認定機関の公開鍵を用いてサービス提供者の公開鍵証明書を認証しなければならない。(仕様要件・オプション)				
	R 3.2.0.7 ネットワーク経由のAP ダウンロードにおいて、AP ファイルの暗号化および通信路の暗号化、鍵配送処理はできた方が良い。(仕様要件・オプション)				
	R 3.2.0.8 カード発行者は、カードのアクセス制御に使用する暗号鍵(カード秘密鍵)が漏洩した可能性を検知したら、サービス提供者に通知すると共に、カードにロック機能がある場合には速やかにカードをロック状態にしたほうがよい。(運用要件・オプション)				
	R 3.2.0.9 カード保有者は、カードマネジャ機能を有効にするためのPIN 情報を他人に漏洩しないほうがよい				
	定期的にPIN を変更して漏洩の可能性を低く抑えたほうがよい。(運用要件・オプション)				
	R 3.2.0.10 カード保有者はカードを紛失した場合、速やかにカード発行者(あるいはサービス提供者)に報告したほうがよい。(運用要件・オプション)				
	R 3.2.0.11 ユーザインタフェース上でカード保有者の投入したPIN 情報やパスワード情報などを端末サブシステム上の他ソフトや端末サブシステム外に漏洩しない工夫を、端末サブシステムの所有者は施さなければならない。(機能要件・必須)				
	R 3.2.0.12 カード発行時に、登録認定機関の公開鍵によりカード発行者の公開鍵証明書を検証し、正しい場合のみカード発行者の公開鍵(あるいは公開鍵証明書)の設定を行わなければならない。				
	たカード発行者はこの鍵が設定されない状態でカードの発行処理を実施してはならない。(機能要件・必須)				
	R 3.2.0.13 カードは、定された公開鍵(カード発行者の公開鍵を利用するかどうかはカード発行者の自由)を用いてAP 搭載許可証およびAP 削除許可証の正当性を検証する機能を有していなければならない。(仕様要件・必須)				
	R 3.2.0.14 カードの権限設定により、カードは認証した主体が権限のある主体(例えばカード発行者)であると認知した場合には、AP搭載許可証およびAP削除許可証の検証は省略しても良い。(機能要件・オプション)				
	3.3 コストシェア要件				
	(直接的に関係がないと判断し、割愛する)				
4 カード発行者の個別要件					
	4.1 登録認定機関への登録				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	R 4.1.0.1 カード発行者自身の秘密鍵、公開鍵を作成し、システム内で安全に保持・管理しなければならない。(機能要件・必須)				
	R 4.1.0.2 登録認定機関へ登録認定機関が定めた情報(カード発行者の公開鍵を含む)を登録することにより、カード発行者ID(CI_ID)、登録認定機関の公開鍵、X.509 公開鍵証明書および簡易証明書を受けなければならない。(R 3.1.0.1 に同じ)(仕様要件・必須)				
	R 4.1.0.3 カード発行者ID(CI_ID)、登録認定機関の公開鍵X.509 公開鍵証明書および簡易証明書はシステム内で保持・管理しなければならない。(機能要件・必須)				
	R 4.1.0.4 公開鍵の有効性をチェックするために、登録認定機関に対しCRL(無効証明書リスト)を参照しなければならない。(機能要件・必須)				
	4.2 サービス提供者との契約				
	R 4.2.0.1 サービス提供者情報(事業者名、住所、代表者名、サービス提供者ID など)をシステムの内で保持・管理を行わなければならない。(機能要件・必須)				
	R 4.2.0.2 サービス提供者と契約するAPについて、登録認定機関が発行したAPのAP 証明書をチェックし、正当なAPであることを確認しなければならない。(仕様要件・必須)				
	R 4.2.0.3 正当なAPの情報(AP名、AP 識別子(AP_ID)、バージョン、およびAP 証明書など)をシステムの内で保持・管理を行う方が良い。(機能要件・オプション)				
	R 4.2.0.4 ダウンロードするAPの利用メモリサイズを元にサービスの割り当てを行う方が良い。(機能要件・オプション)				
	4.3 カード保有者の決定				
	R 4.3.0.1 カード発行を決定した利用者の利用者情報(住所、氏名)をシステムの内で保持・管理しなければならない。(機能要件・必須)				
	R 4.3.0.2 カード発行を決定した利用者に対する課金情報をシステムの内で保持・管理を行う方が良い。(機能要件・オプション)				
	4.4 カード発行処理				
	R 4.4.0.1 カードに関する情報(カードプラットフォーム種別、バージョン、メモリ容量、カード種別など)をシステムの内で保持・管理を行わなければならない。(仕様要件・必須)				
	R 4.4.0.2 新たに発行されるカードに対し、ユニークなカードID(CID)を払い出し管理しなければならない。(運用要件・必須)				
	R 4.4.0.3 カードに格納する鍵ペア(カード秘密鍵、カード公開鍵)を作成しなければならない。(機能要件・必須)				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	R 4.4.0.4 カード公開鍵およびカードID に対しカード発行者の署名した公開鍵証明書（カード証明書）を作成し、カードの鍵ペアと共にカードに設定しなければならない。（仕様要件・必須）				
	R 4.4.0.5 カードの有効期限を設定した方が良い。（運用要件・オプション）				
	R 4.4.0.6 上記のカードID、カード公開鍵、公開鍵証明書（カード証明書）管理およびカード有効期限の情報をシステムの内で保持・管理した方が良い。（機能要件・オプション）				
	R 4.4.0.7 カードにカード管理情報（①カード発行者ID、②カードID、③カード種別情報など）を設定しなければならない。（仕様化要件・必須）				
	R 4.4.0.8 個々のカードと利用者との対応付けをシステムの内で保持・管理を行わなければならない。（機能要件・必須）				
	R 4.4.0.9 カードに各利用者の個人情報を設定した方が良い。（運用要件・オプション）				
	R 4.4.0.10 カード発行時にAPを搭載できた方が良い。（運用要件・オプション）				
	R 4.4.0.11 カード券面にカード保有者の個人情報を印刷した方が良い。（運用要件・オプション）				
	R 4.4.0.12 カード券面にカードID（CID）を印刷した方が良い。（運用要件・オプション）				
	R 4.4.0.13 カード券面にカード発行者の組織名を印刷したほうがよい。（運用要件・オプション）				
	R 4.4.0.14 カード発行者は、カードを輸送する際の輸送途中におけるカード改ざん防止、盗難後の偽造防止のために、カード供給者がカードに埋め込んだ輸送鍵あるいはPIN情報を、カード供給者から安全に入手しなければならない。（運用要件・必須）				
	R 4.4.0.15 カード発行者は、カード発行処理において、輸送鍵あるいはPIN 情報により、カードのアクセス制御やカードの認証を有効な状態にしなければならない。（運用要件・必須）				
	R 4.4.0.16 カード発行者は、利用者の本人認証のためのPIN（カード管理PIN）をカードに設定した方が良い。（仕様要件・オプション）				
	4.5 サービス提供者間の処理				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	R 4.5.0.1 サービス提供者からのAPのダウンロードの申請を受け、少なくとも以下の情報を含んだAP 搭載許可証を発行しなければならない。(仕様要件・必須) AP搭載許可証 ① 許可証ID ② AP 識別子(AP_ID) ③ AID ④ APハッシュ値: ダウンロード対象APファイルのハッシュ値 ⑤ CID: 許可したカードID ⑥ AP 搭載許可証のハッシュ値に対するカード発行者の署名				
	R 4.5.0.2 サービス提供者からのAPの削除許可申請を受け、少なくとも以下の情報を含んだAP 削除許可証を発行しなければならない。(仕様要件・必須) AP削除許可証 ① 許可証ID ② AID ③ CID: 許可したカードID ④ AP 削除許可証のハッシュ値に対するカード発行者の署名				
	R 4.5.0.3 個々のカードに発行したAP 搭載許可証／AP 削除許可証の情報をシステムの内で保持・管理した方が良い。(機能要件・オプション)				
	R 4.5.0.4 カードがレシート情報生成機能をもっている場合は、サービス提供者が取得したレシート情報を取得したほうがよい。レシート情報には、少なくとも以下の情報を含まなければならない。(仕様要件・オプション) レシート情報 ① 許可証情報 ② レシート情報のハッシュ値に対するカードの署名				
	R 4.5.0.5 レシート情報を受け取った場合は、システムの内で保持・管理しなければならない。(機能要件・オプション)				
	R 4.5.0.6 カード発行者は、サービス提供者からのカードID をキーにしたカードの有効性(盗難・紛失・破損などの異常状態でないこと)問合せに対し応答しなければならない。(仕様要件・必須)				
	R 4.5.0.8 サービス提供者からのホットリスト情報問合せに対し応答しなければならない。(仕様要件・必須)				
	R 4.5.0.9 サービス提供者からのホットリスト情報の通知を受信した方が良い。(運用要件・オプション)				
	4.6 カード運用処理				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	R 4.6.0.1 カード発行者の判断により、個々のカード保有者のカードに対し一時利用停止（ロック）、停止解除（ロック解除）処理を行う機能があった方が良い。（仕様要件・オプション）				
	R 4.6.0.2 カード保有者との契約切れ、あるいはカード保有者からカード廃止（終了）申請があった場合、カード保有者のカードに対し廃止処理（終了）を行わなければならない。（仕様要件・必須）				
	R 4.6.0.3 カード管理PIN の機能があるカードに対して、PIN の投入ミスでロック状態になったカードをロック解除することができた方が良い。（仕様要件・オプション）				
	R 4.6.0.4 個々のカードのライフサイクル状態をシステムで保持・管理を行う方が良い。（機能要件・オプション）				
	4.7 利用者との対応				
	R 4.7.0.1 利用者からの問合せに従い、AIDからAPに関する情報（AP名、サービス提供者名、AP製造者など）を返す方が良い。（機能要件・オプション）				
	R 4.7.0.2 利用者からの問合せに従い、利用者のカードに搭載されているAPのAID 一覧を返す方が良い。（機能要件・オプション）				
	R 4.7.0.3 利用者から、カードの破損、紛失、盗難の申請を受付けなければならない。（運用要件・必須）				
	R 4.7.0.4 個々のカードの盗難・紛失・破損などの異常状態をシステムの内で保持・管理を行える方が良い。（機能要件・オプション）				
	R 4.7.0.5 利用者からの利用者氏名あるいはカードID をキーにしたカード有効性やライフサイクル状態のカード情報問合せに対し応答する方が良い。（機能要件・オプション）				
	4.8 セキュリティ要件				
	R 4.8.0.1 2.4.3 節で記述された方式によりサービス提供者の認証を行わなければならない。（仕様要件・必須				
	R 4.8.0.2 2.5.5 節で記述された方式によりカードの認証を行わなければならない。（仕様要件・必須）				
	R 4.8.0.3 カード発行者は、秘密鍵、公開鍵を生成する手段を持たなければならない。（機能要件・必須）				
	R 4.8.0.4 カードへの公開鍵証明書発行に伴う、証明書失効リスト（CRL）の管理など認証（CA）局の機能を持たなければならない。（機能要件・必須）				
	R 4.8.0.5 生成した暗号鍵の漏洩を防ぐ為、セキュアに保管しなければならない。（運用要件・必須）				
	R 4.8.0.6 カード間およびサービス提供者間の通信路の暗号化や鍵配送処理は行えた方が良い。（仕様要件・オプション）				
	R 4.8.0.7 カード発行者が偽造カードなどの不審なカードを検出した場合は、即座にサービス提供者に通知しなければならない。（運用要件・必須）				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
5 サービス提供者の個別要件					
	5.1 登録認定機関への登録				
	R 5.1.0.1サ ービス提供者自身の秘密鍵、公開鍵を作成し、システム内で保持・管理しなければならない。(機能要件・必須)				
	R 5.1.0.2登 録認定機関へ登録認定機関が定めた情報(サービス提供者の公開鍵やRID:AID の先頭5 バイト部分)を登録することにより、ユニークなサービス提供者ID(SP_ID)、登録認定機関の公開鍵およびX.509 公開鍵証明書を取得しなければならない。(仕様要件・必須)				
	R 5.1.0.3サ ービス提供者ID(SP_ID)、登録認定機関の公開鍵およびX.509 公開鍵証明書はシステム内で保持・管理できなければならない。(機能要件・必須)				
	R 5.1.0.4 公開鍵の有効性をチェックするために、登録認定機関に対しCRL(無効証明書リスト)を参照しなければならない。(機能要件・必須)				
	R 5.1.0.5サ ービス提供者は事前にRID(AIDの先頭5バイト部分)を取得しなければならない。(運用要件・必須)				
	R 5.1.0.6カ ードにダウンロードするAP毎にアプリケーション識別子(AID)を付与しなければならない。(運用要件・必須)				
	R 5.1.0.7登 録認定機関が定めたAP情報(AP名、AID、AP 識別子(AP_ID)、バージョン、およびAPのハッシュ値)を登録認定機関へ登録することにより、少なくとも以下の情報を含むAP 証明書を取得しなければならない。(仕様要件・必須) AP 証明書 (1) AID (2) AP 識別子(AP_ID) (3) AP ファイルのハッシュ値 (4) SP_ID: サービス提供者ID (5) 登録認定機関による署名				
	R 5.1.0.8 ダウンロード対象となるAP ファイルおよびAP情報とAP 証明書はシステム内で保持・管理する方が良い。(機能要件・オプション)				
	R 5.1.0.9サ ービス提供者は、カードダウンロードするAPを登録認定機関に登録する。(運用要件・必須)				
	5.2 カード発行者との契約				
	R 5.2.0.1 カード発行者情報(事業者名、住所、代表者名、カード発行者ID など)を受け取り、システムの内で保持・管理する方が良い。(機能要件・オプション)				
	R 5.2.0.2 正当なカード発行者に対し、サービス提供者の情報(事業者名、住所、代表者名、サービス提供者ID など)を登録申請しなければならない。(仕様要件・必須)				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	R 5.2.0.3 カードへダウンロードしたいAPの情報（AP名、AP 識別子(AP_ID)、バージョン、および登録・認定機関が発行したAP 証明書）を登録申請しなければならない。（仕様要件・必須）				
	R 5.2.0.4 申請するAPは登録認定機関に登録され、AP 証明書を受け取ったAPでなければならない。（運用要件・必須）				
	R 5.2.0.5 登録されたAP情報によりカード発行者との間でカード資源（メモリ）の割り当ての契約を行い、その情報をシステムの内で保持・管理した方が良い。（機能要件・オプション）				
	5.3 サービス利用者の決定				
	R 5.3.0.1 利用者の利用者情報（住所、氏名）をシステムの内で保持・管理した方が良い。（機能要件・オプション）				
	R 5.3.0.2 利用者のカードの識別情報（カード発行者ID、カードID、有効期限等）をシステムの内で保持・管理した方が良い。（機能要件・オプション）				
	5.4 APのダウンロード				
	R 5.4.0.1 カード発行者に対し、カード保有者のカードIDとダウンロードさせたいAPのAP 識別子(AP_ID)の情報によるAP搭載の申請を行わなければならない。（仕様要件・必須）				
	R 5.4.0.2 AP搭載の申請を行うAPは、カード発行者と契約を行った、つまりカード発行者に登録されたAPでなければならない。（運用要件・必須）				
	R 5.4.0.3 カード発行者からAP 搭載申請に対応するAP 搭載許可証(R 4.5.0.1 参照)を取得しなければならない。（仕様要件・必須）				
	R 5.4.0.4 個々のカードに発行したAP 搭載許可証の情報をシステムの内で保持・管理した方が良い。カード発行者の方針で許可証を再利用させたくない場合には、再利用ができない仕組みが必要。（機能要件・オプション）				
	R 5.4.0.5 アプリケーション利用の申請を行ったカード保有者のカードに対し、APダウンロードコマンドと共に、APファイルと、該当するAP搭載許可証を送信しなければならない。（仕様要件・必須）				
	R 5.4.0.6 カードがレシート生成機能をもっている場合、レシート通知情報(R 4.5.0.4 参照)を受け取り、システムの内で保持・管理した方が良い。（仕様要件・オプション）				
	R 5.4.0.7 レシート通知情報を受け取った場合にはカード発行者に通知しなければならない。（仕様要件・必須）				
	5.5 APの削除				
	R 5.5.0.1 カード発行者に、カード保有者のカードIDに対する当該APのAP 削除の申請を行わなければならない。（仕様要件・必須）				
	R 5.5.0.2 カード発行者からAP 削除申請に対応するAP 削除許可証(R 4.5.0.2 参照)を取得しなければならない。（仕様要件・必須）				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	R 5.5.0.3　個々のカードに発行したAP 削除許可証の情報をシステムの内で保持・管理した方が良い。（機能要件・オプション）				
	R 5.5.0.4 AP削除の申請を行ったカード保有者のカードに対し、AP削除コマンドと共に、該当するAP 削除許可証を送信しなければならない。（仕様要件・必須）				
	R 5.5.0.5 カードがレシート生成機能をもっている場合は、レシート通知情報(R 4.5.0.4 参照)を受け取り、システムの内で保持・管理しなければならない。（仕様要件・オプション）				
	R 5.5.0.6 レシート通知情報を受け取った場合には、カード発行者に通知しなければならない。（仕様要件・必須）				
	5.6 ホットリスト処理				
	R 5.6.0.1 カード発行者から通知されるホットリスト情報（破損・紛失・盗難および廃止になったカードID 情報）を受け取り、システムの内で保持・管理しなければならない。（仕様要件・必須）				
	R 5.6.0.2 ホットリスト情報に従い該当のカードIDに対するサービスの停止を行うほうがよい。（運用要件・オプション）				
	R 5.6.0.3 ホットリスト情報で通知された、盗難カードからサービスの要求を受けた場合には、カード発行者に通知した方が良い。（運用要件・オプション）				
	R 5.6.0.4 利用者からカードの紛失・盗難の申告を受付けた場合には、カード発行者に通知した方が良い。（運用要件・オプション）				
	5.7 サービス実施				
	R 5.7.0.1 サービスの提供に先立ち、APを初期化およびパーソナライズした方が良い。（運用要件・オプション）				
	R 5.7.0.2 サービスの実施中に、APの一時利用停止（ロック）、停止解除（ロック解除）などのAPライフサイクル状態の管理、設定を行えた方が良い。（機能要件・オプション）				
	5.8 セキュリティ要件				
	R 5.8.0.1 サービス提供者は2.4.3 節で記述された方式によりカード発行者の認証を行わなければならない。（仕様要件・必須）				
	R 5.8.0.2 2.5.5 節で記述された方式によりカードの認証を行った方が良い。（仕様要件・オプション）				
	R 5.8.0.3 サービス提供者は、秘密鍵や公開鍵を生成する手段を持たなければならない。（機能要件・必須）				
	R 5.8.0.4 生成した暗号鍵の漏洩を防ぐ為、セキュアに保管しなければならない。（運用要件・必須）				
	R 5.8.0.5 APのダウンロード／削除時にはカード利用者の本人認証を行う方が良い。（運用要件・オプション）				
6 登録認定機関の個別要件					
	6.1 カード登録認定機関（CR: Card Registry）				
	R 6.1.0.2 オンラインでの申請、発行、問合せについて、できたほうがよい。（仕様要件・オプション）				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	R 6.1.0.3 カード供給者の登録申請を受付けて、内容が適正かどうか審査しなければならない。(運用要件・必須)				
	R 6.1.0.4 申請に対し、ユニークなカード供給者識別子(CS_ID)を払い出さなければならない。(仕様要件・必須)				
	R 6.1.0.5 CS_ID によるカード供給者に関する問合せがあったとき、これに答えなければならない。(運用要件・必須)				
	R 6.1.0.6 カードを認定する基準を持っていなければならない。(運用要件・必須)				
	R 6.1.0.7 基準に準拠していることを確認する手段をもっていなければならない。(機能要件・必須)				
	R 6.1.0.8 認定したカードに対してユニークなカード登録ID(CR_ID)を払い出さなければならない。(仕様要件・必須)				
	R 6.1.0.9 基準に準拠しているカードに対してカード登録ID とカード種別を表すカードタイプID(CT_ID)が記載された認定証を発行しなければならない。(運用要件・必須)				
	R 6.1.0.10 カード登録ID によるカードが認定されているかの問合せに答えられなければならない。(運用要件・必須)				
	R 6.1.0.11 カードのセキュリティ評価基準についてセキュリティ評価機関の認定を受けている方が良い。(運用要件・オプション)				
	R 6.1.0.12 基準に準拠しなくなった場合、認定を取り消さなければならない。(運用要件・必須)				
	R 6.1.0.13 カードおよびリーダライタの互換性を確保するために、評価用カード／リーダライタによる所定の認定を行う必要がある。(運用要件・必須)				
	6.2 発行者登録機関(CIR: Card Issuer Registry)				
	R 6.2.0.1 新規申請に対し、ユニークなカード発行者ID(CI_ID)を払い出さなければならない。(仕様要件、必須)				
	R 6.2.0.2 CI_IDによりカード発行者に関する問合せがあったとき、これに答えられなければならない。(運用要件・必須)				
	R 6.2.0.3 登録内容の変更・削除ができなければならない。(機能要件・必須)				
	R 6.2.0.4 カード発行者にX.509 に準拠した公開鍵証明情報および簡易証明書を発行しなければならない。(仕様要件・必須				
	R 6.2.0.5 不正なカード発行者に対しては、登録を削除する責任を持たなければならない(運用要件・必須)。				
	R 6.2.0.7 ID をキーにして公開鍵証明書を要求された時に、それを発行しなければならない。(機能要件・必須)				
	R 6.2.0.8 公開鍵証明書の有効性の問合せがあったとき、これに答えなければならない(仕様要件・必須)				
	R 6.2.0.9 機関自身の公開鍵証明書を要求された時に、それを発行しなければならない。(仕様要件・必須)				
	R 6.2.0.10 要求はネットワーク経由で行える方が良い。(機能要件・オプション)				
	R 6.2.0.11 機関自身の秘密鍵と公開鍵を生成し、管理しなければならない。(機能要件・必須)				
	R 6.2.0.12 無効証明書リストを管理しなければならない。(機能要件・必須)				
	6.3 サービス登録機関(SR: Service Registry)				
	■サービス提供者登録				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	R 6.3.0.1 サービス提供者の登録申請情報（サービス提供者の公開鍵およびAID 登録センタから取得したRID を含む）を受付けて、内容を審査しなければならない。（運用要件・必須）				
	R 6.3.0.2 サービス提供者の申請に対し、ユニークなサービス提供者ID（SP_ID）を払い出さなければならない。（仕様要件・必須）				
	R 6.3.0.3 サービス提供者にX.509 に準拠した公開鍵証明情報と簡易証明書を発行しなければならない。（仕様要件・必須）				
	R 6.3.0.4 サービス提供者ID（SP_ID）による問合せがあったとき、これに答えなければならない。（仕様要件・必須）				
	R 6.3.0.5 登録内容の変更・削除ができなければならない。（機能要件・必須）				
	R 6.3.0.6 不正なサービス提供者に対しては、登録を削除する責任を持たなければならない。（運用要件・必須）				
	■アプリケーション登録				
	R 6.3.0.8 サービス提供者からのアプリケーションの登録申請情報（アプリケーション名、AID、AP ファイルのハッシュ値、APファイルサイズ、SP_IDなど）を受付けて、登録しなければならない。（機能要件・必須）				
	R 6.3.0.9 アプリケーション登録申請毎にユニークなアプリケーションプログラム識別子（AP_ID）を払い出さなければならない。（仕様要件・必須）				
	R 6.3.0.10 アプリケーションの登録の後、サービス提供者にAP 証明書を発行しなければならない。（運用要件・必須）				
	R 6.3.0.11 AIDあるいはAP識別子(AP_ID)による登録に関する問合せがあったとき、これに答えなければならない。（仕様要件・必須）				
	R 6.3.0.12 アプリケーションの登録内容の変更・削除を行わなければならない。（機能要件・必須）				
	R 6.3.0.13 アプリケーションの登録申請要求はネットワーク経由でも行えたほうがよい。（仕様要件・オプション）				
	■その他				
	R 6.3.0.15 ID をキーにして公開鍵証明書を要求された時に、それを返信しなければならない。（仕様要件・必須）				
	R 6.3.0.16 公開鍵証明書の有効性の問合せがあったとき、これに答えられなければならない（仕様要件・必須）				
	R 6.3.0.17 機関自身の公開鍵証明書を要求された時に、それを返信しなければならない。（仕様要件・必須）				
	R 6.3.0.18 機関自身の秘密鍵と公開鍵を生成し、管理しなければならない。（機能要件・必須）				
	R 6.3.0.19 無効証明書リストを管理しなければならない。（機能要件・必須）				
7 IC カードの個別要件					
	7.1 カード物理／論理インタフェース				
	R 7.1.0.1 カードはカード保有者の利便性、カードの耐久性および適用分野の拡大を考慮し、①非接触型か、②接触/非接触の両方のインタフェースを持ったコンビ型あるいはハイブリッドでなければならない。（機能要件・必須）				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	R 7.1.0.2 接触インタフェースは、ISO/IEC 7816 に準拠しなければならない。(仕様要件・必須)				
	R 7.1.0.3 非接触のインタフェース仕様はISO/IEC 14443 に準拠しなければならない。(仕様要件・必須)				
	R 7.1.0.4 曲げ、ねじれ強度等の信頼性に関しては、ISO/IEC 10373 に準拠しなければならない。(仕様要件・必須)				
	R 7.1.0.5 非接触の場合、日本国内の電波法等に準拠しなければならない。(仕様要件・必須)				
	R 7.1.0.6 カードおよびリーダライタ間の互換性確保のため、別途規定するカード／リーダライタ仕様に準拠しなければならない。(仕様要件・必須)				
	7.2 マルチアプリケーション対応				
	R 7.2.0.1 カード内に複数のAPがダウンロードされ、複数のサービスを提供できなければならない。(機能要件・必須)				
	R 7.2.0.2 カード発行後にAPがダウンロードでき、ダウンロードされたAPは削除できなければならない。(機能要件・必須)				
	R 7.2.0.3 既存サービスで使用しているコマンドはアプリケーション等により実現できること。(機能要件・オプション)				
	R 7.2.0.4 ダウンロードされたAPが、他のAP(プログラムおよびデータ)に対し、他のAPの許可無しに読み込み、書き込み、変更が行えないような機構を実装しなければならない。(機能要件・必須)				
	7.3 カードの保持情報				
	R 7.3.0.1 カードの認証および暗号化通信のため、①カードの秘密鍵、②カード公開鍵証明書を保持しなければならない。(仕様要件・必須)(その他、サービス提供者の認証に必要な登録機関の公開鍵の必要性や鍵長については仕様化において整理)				
	R 7.3.0.2 NICSS において一意にカードを識別させるために、カード発行者ID(CI_ID)を保持しなければならない。(仕様要件・必須)				
	R 7.3.0.3 カード発行者がカード毎にユニークに払い出すカードID(CID)を保持しなければならない。(仕様要件・必須)				
	R 7.3.0.4 カード製造者、カードプラットフォーム種別、バージョンなどを保持しなければならない。(仕様要件・必須)				
	7.4 APのダウンロード				
	R 7.4.0.1 カードは、APのダウンロードに関わるコマンドを処理する時にコマンドを起動しようとするサービス提供者の公開鍵証明書を取得し、登録認定機関の公開鍵を用いて相手の正当性をチェックした方が良い。(仕様要件・オプション)				
	R 7.4.0.2 サービス提供者にリソースの割り当てが行われているかどうかチェックした方が良い。				
	(機能要件・オプション)				
	R 7.4.0.3 カードはAPダウンロード時に、①AP本体と、カード発行者が発行した②AP 搭載許可証(R 4.5.0.1 参照)を受け取らなければならない。(仕様要件・必須)				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	R 7.4.0.4 AP 搭載許可証のAP 情報、AID の重複、ハッシュ値をチェックし、合格した場合のみAPのダウンロード・インストール処理を行わなければならない。(仕様要件・必須)				
	R 7.4.0.5 カードにリソース割り当て管理機能がある場合には、サービス提供者に割り当てたリソース(メモリ領域)以外に、該サービス提供者のAPをダウンロードしてはならない。(機能要件・必須)				
	R 7.4.0.6 割り当てられたリソースとダウンロードしたサービス提供者のAPの対応を管理した方が良い。(機能要件・オプション)				
	R 7.4.0.7 APのダウンロードが完了した場合、サービス提供者に以下の情報を含むレシート情報(R4.5.0.4 を参照)を通知した方が良い。(仕様要件・オプション)				
	R 7.4.0.8 コマンドのパラメータおよびAP本体を通信で暗号化する場合は、共通鍵を利用した方が良い。(仕様要件・オプション)				
	R 7.4.0.9 共通鍵をサービス提供者と安全に共有するためにはPKI ベースの手法を用いる方が良い。(仕様要件・オプション)				
	7.5 APの削除				
	R 7.5.0.1 APの削除に関わるコマンドを処理する時にコマンドを起動しようとするサービス提供者の公開鍵証明書を取得し、登録認定機関の公開鍵を用いて相手の正当性をチェックした方が良い。(仕様要件・オプション)				
	R 7.5.0.2 カードはAP削除時に、サービス提供者からカード発行者が発行したAP削除許可証(R 4.5.0.2 参照)を受け取らなければならない。(仕様要件・必須)				
	R 7.5.0.3 AP 削除許可証の中のAID を、カード内に搭載されているAIDでチェックし、合格した場合のみAPの削除処理を行わなければならない。(仕様要件・必須)				
	R 7.5.0.4 APを削除した場合割り当てられたリソースを開放したほうがよい。(機能要件・オプション)				
	R 7.5.0.5 APの削除が完了した場合、サービス提供者に以下の情報を含むレシート情報(R4.5.0.4 を参照)を通知した方が良い。(仕様要件・オプション)				
	7.6 カード管理				
	R 7.6.0.1 カード上に搭載されているAPの起動(選択)はISO7816-4で規定されるSELECTFILEコマンド仕様に従わなければならない。(仕様要件・必須)				
	R 7.6.0.2 カードに搭載されているAPの領域管理および、AP実行時のメモリ管理などリソース管理機能を有していなければならない。(機能要件・必須)				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	R 7.6.0.3 カード発行後の①カード一時停止状態／停止解除状態、②カード終了　など、カードのライフサイクル状態を管理した方が良い。（仕様要件・オプション）				
	R 7.6.0.4 APダウンロード後の①アプリケーションの一時停止状態／停止解除状態　などアプリケーションのライフサイクル状態を管理した方が良い。（仕様要件・オプション）				
	R 7.6.0.5 カード保有者の本人性を確認するためにPIN認証機能を持った方が良い。（仕様要件・オプション）				
	R 7.6.0.6 カードがPINを管理している場合、カード保有者によるPINの変更機能を持っている方が良い。（仕様要件・オプション）				
	R 7.6.0.7 PIN投入ミスの上限回数を設定し上限値を越えたらPINまたはカードをカード一時停止状態にできた方が良い。（機能要件・オプション）				
	7.7 カード状態検索				
	R 7.7.0.1 カード属性に関する情報（①カードプラットフォーム種別、②カードの識別、③カード発行者ID 等）を返却するコマンドを有しなければならない。（仕様要件・必須：返却情情報については仕様書にて明確化）				
	R 7.7.0.3 カード認証のためにカード公開鍵またはカード公開鍵証明書を取得するためのコマンドを有すること。（仕様要件・必須：相互認証方式については仕様化において再整理）				
	R 7.7.0.4 外部から送信されたメッセージをカード秘密鍵で暗号化して返却する内部認証機能を有すること。（仕様要件・必須：相互認証方式については仕様化において再整理）				
	R 7.7.0.5 カードは7.6.0.3 で規定するカードのライフサイクルを返却する機能を有すること。（仕様要件・オプション）				
	R 7.7.0.6 カード内にダウンロードされているAP(AID)のリストを返却するAIDリストの問合せコマンドをサポートしなければならない。（仕様要件・オプション）				
	R 7.7.0.7 AIDリストの問合せコマンドは、実行制限がかけられた方がよい。（機能要件・オプショ				
	ン）				
	R 7.7.0.8 AID に対応するAP ラベル（サービス内容の簡易表記）を、表示したほうが良い。（仕様要件・オプション）				
	7.8 カードのセキュリティ機能				
	R 7.8.0.1 カードはセキュリティ評価機関の認定を受けている方が良い。（運用要件・オプション）				
	R 7.8.0.2 APのダウンロード時に、公開鍵あるいは公開鍵証明書を使用してサービス提供者の認証を行う方が良い。（仕様要件・オプション）				
	R 7.8.0.3 回線上での暗号化によるセキュア通信ができる方が良い（仕様要件・オプション）				
	R 7.8.0.4 アクセス制御のためのPIN認証を有している方が良い。（仕様要件・オプション）				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	R 7.8.0.5 次の基本的な暗号処理はIC カード内で行えた方が良い。(機能要件・オプション) 共通鍵アルゴリズム:①DES 暗号／復号、②TripleDES 暗号／復号 公開鍵アルゴリズム:③RSA 暗号/復号、④楕円暗号／復号				
8 カード リーダライタの要件					
	8.1 カード リーダライタの基本要件				
	R 8.1.0.1 卓上型のカード リーダライタは、微弱無線局扱いとしたほうがよい。(機能要件・オプション)				
	R 8.1.0.2 リーダライタは電波法に準拠すること。(機能要件・必須)				
	R 8.1.0.3 カードおよびリーダライタ間の互換性確保のため、別途規定されるRW の実装規約に準拠しなければならない。(仕様要件・必須)				
	R 8.1.0.5 R8.1.0.3における互換性を検証するために、評価用カード／リーダライタによる所定の認定を受けなければならない。(運用要件・必須)				
	8.2 カード リーダライタの機能、性能				
	R 8.2.0.2 ISO/IEC14443-2 で規定されるタイプAとタイプB の両方にアクセスできた方が良い(タイプA,B 以外については今後検討)(機能要件・オプション)。				
	R 8.2.0.3 スロットイン型のリーダライタにおいては、スロット当たり1枚の動作を基本とし、単一スロットの2枚挿し動作はオプションとする。(機能要件・オプション)				
	R 8.2.0.4 データ通信中は状態を示す表示を行う方が良い。(機能要件・オプション)				
	8.3 カード リーダライタと上位システムとの互換性確保				
	R 8.3.0.1 端末システムへの接続ポートとしては、業界(全銀協、ICPA、JCCA)に準じた方が良い。(機能要件・オプション)				
	R 8.3.0.2 端末システムからリーダライタを制御するドライバーは別途、規定する仕様に準拠することが望ましい(現在検討中)。(仕様要件・オプション)				
9 端末システムの要件					
	9.1 端末基本要件				
	R 9.1.0.3 複数のIC カードに対し統一した操作性が確保されている方が良い。(機能要件・オプション)				
	9.2 端末の機能、性能				
	R 9.2.0.1 PINを入力可能な方が良い。(機能要件・オプション)				
	R 9.2.0.2 IC カードにアプリケーションが搭載されているかを表示できる機能を持つ方が良い。(機能要件・オプション)				
	R 9.2.0.4 アプリケーションの選択が容易に出来る方が良い。(機能要件・オプション)				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	9.3 端末におけるセキュリティ				
	R 9.3.0.2 PIN 入力時の盗視、盗聴が困難な構造である方が良い。(機能要件・オプション)				
	9.4 非接触IC カード対応端末の要件				
10 サーバシステムの要件					
	10.1 サーバシステムの基本要件				
	R 10.1.0.1 システムはIC カード種別にできるだけ依存しないほうが望ましい。(機能要件・オプション)				
	R 10.1.0.2 カード発行者とサービス提供者を区別して構築できなければならない。(機能要件・必須)				
	10.2 サーバシステムの基本機能				
	R 10.2.0.1 登録認定機関サーバ、カード発行者サーバ、サービス提供者サーバ、端末はそれぞれインターネットなどのネットワークで接続されている方が良い。(機能要件・オプション)				
	R 10.2.0.2 オンラインでアプリを追加、削除出来る機能を有する方が良い。(機能要件・オプション)				
	10.3 サーバシステムのセキュリティ				
	R 10.3.0.1 端末とサーバシステムの間のセキュア通信をした方がよい。(機能要件・必須)				
	R 10.3.0.2 登録認定機関とカード発行者又はサービス提供者間のやり取りは安全な手段を取らなければならない。(運用要件・必須)				
	R 10.3.0.3 サーバシステム内部の利用者のプライバシー情報が漏洩しない為の対策が打たれていなければならない(機能要件・必須)				
	R 10.3.0.4 外部ネットワークからのアタックやハッキングに防御するための対策がなされていなければならない。(機能要件・必須)				