

キャンパス PKI 調達仕様ガイドライン

初版 (ver1.0)

国立情報学研究所
学術情報ネットワーク運営・連携本部
認証作業部会

2007 年 6 月 6 日

目次

1. はじめに	1
1.1 目的.....	1
1.2 概要.....	1
2. 先行大学 2 大学調達仕様書比較結果	2
2.1 前提条件	2
2.1.1 認証局階層構造	2
2.1.2 アウトソース範囲	2
2.1.3 発行対象者と証明書利用用途	3
2.2 認証局システム要件	3
2.3 登録局システム要件、登録用端末(アプリケーション)要件	4
2.4 証明書格納媒体要件	4
2.5 アウトソース要件	5
2.6 保守要件	6
2.6.1 保守体制等	6
2.6.2 保守作業.....	6
2.6.3 提出物	6
2.7 教育、支援体制要件.....	6
3. 調達仕様ガイドライン	7
3.1 認証局システム要件	7
3.2 登録局システム要件	9
3.2.1 RA サーバアプリケーション要件	9
3.2.2 登録アプリケーション要件.....	10
3.3 認証基盤リポジトリ	11
Web サーバ要件	11
3.3.1.....	11
3.3.2 LDAP サーバ要件	11
3.3.3 OCSP レスポンダ要件	12
3.4 アウトソース及びインソースでのファシリティ、その他の要件	12
3.4.1 IA/RA サーバの運用をアウトソースする場合	12
3.4.2 IA サーバの運用をアウトソースする場合	13
3.4.3 IC カード発行業務をアウトソースする場合 * (オプション)	14
3.5 IC カードに関する要件 * (オプション)	15
3.6 CP/CPS 及び運用手順書の提供	16
3.7 保守要件	16
3.8 費用.....	17
4. 用語集	18

1. はじめに

1.1 目的

大学共同利用機関法人 情報・システム研究機構 国立情報学研究所（以下、「本研究所」という）では、大学間のサービスをセキュアに連携するための全国共同電子認証基盤（以下、「UPKI」という）構築事業を推進している。

UPKI は、これに参加する大学を結ぶトラストドメインを形成し、相互認証を行う共通認証基盤である。本キャンパス PKI 調達仕様ガイドライン（以下、「本ガイドライン」という）は、「UPKI 相互運用フレームワークの要件定義仕様書」を参考にし、各大学に設置が予定されるプライベート認証局の構築に関する調達のためのガイドラインを示し、相互運用性を確保することを目的としている。

なお、将来的に GPKI 等他の認証基盤と相互接続を行う場合、証明書の用途を電子署名とする等、認証局ポリシーを見直す必要がある。

1.2 概要

本ガイドラインは、先行してプライベート認証局を構築した両大学（A 大学、B 大学）の調達仕様書を参考とし、相互運用性の確保のための要件をまとめたものである。2 章は、先行 2 大学の調達仕様書の比較を実施している。3 章は、2 章の結果及び「UPKI 相互運用フレームワークの要件定義仕様書」を参考に調達仕様ガイドラインを記述している。

本ガイドラインは、以下の条件の際に適用されるよう記述している。

- 発行局 (IA サーバ) の運用及び IC カード発行業務を外部に委託する場合
- 発行局 (IA サーバ) 及び登録局 (RA サーバ) の運用及び IC カード発行業務を外部に委託する場合

2. 先行大学 2 大学調達仕様書比較結果

本章では、認証局システム及び IC カード、認証業務の一部をアウトソースで調達する場合について重要なポイントを示し、そのポイント毎に先行大学の調達仕様書の規定内容について比較した結果を記述する。シングルサインオンや VPN 装置といった製品や、認証局以外のソフトウェア及びハードウェアの調達に関する比較は行わない。

本章で行う比較については、各大学の調達仕様書の優劣を比較しているのではない。

以下に相互運用性を確立した認証局システムを調達する上で重要なポイントを示す。

- (1) 前提条件
- (2) 認証局システム要件
- (3) 登録局システム要件、登録用端末(登録アプリケーション)要件
- (4) 証明書格納媒体要件
- (5) アウトソース要件
- (6) 保守要件
- (7) 教育、支援体制要件

2.1 前提条件

2.1.1 認証局階層構造

A 大学は、セルフサイン証明書を持つ認証局であり、階層構造を持たない。B 大学は、ルート認証局、中間認証局(発行認証局)からなる階層構造を持つ。

相互認証先と相互認証証明書の取り交わしを行うことによって相互認証する場合、階層構造を持つことによって、認証パス構築等で処理に負担がかかることが予想される。相互認証方式は現段階では未決定であるが、ポリシー上階層構造を持たせる必要性が低ければ、セルフサインの証明書を持つ認証局を前提にした方が良い。

2.1.2 アウトソース範囲

現在、A 大学は IA サーバ及び RA サーバの運用、IC カード発行業務をアウトソースしており、一方で B 大学は IA サーバの運用のみアウトソースしている。このように、両大学ではアウトソース範囲が異なっている(B 大学は、本格運用の際には、IC カード発行業務もアウトソースする予定)。キャンパス PKI CP/CPS ガイドラインにおいては、アウトソースの範囲は両大学と同様に以下の 2 パターンを前提としている。従って、本ガイドラインにおいてもアウトソース範囲は IC カード発行業務に加え、以下を前提としている。

- 発行局(IA サーバ)の運用を外部に委託する場合
- 発行局(IA サーバ)及び登録局(RA サーバ)の運用を外部に委託する場合

委託先に期待するホスティングサービスの内容、稼働実績、サービスレベル等については調達仕様書に明記することが必要である。

なお、ICカード発行業務は、IAサーバを運用する認証設備室と同等の環境(ファシリティ、リソース)で実施されることが望ましいため、これを満たすことができる委託先にアウトソースすることが期待される。

2.1.3 発行対象者と証明書利用用途

両大学とも、発行対象者は人(教職員、学生、その他大学が認めた者)としている。共通の証明書の利用用途は、以下の通りである。

- Webポータルや無線LAN、VPN、SSOにおけるクライアント認証の用途
- スマートカードログオン(Windows、MacOS、Linux)の用途

B大学は、ドメインコントローラ等の機器にも証明書を発行している。認証の用途であるため、機器への証明書の発行を行うことも必要なことであり、人及び機器への発行手順がそれぞれ確立されていれば、この違いが相互運用性に影響を与えるものではないと考える。

また、両大学共にS/MIMEや電子署名の用途での利用を検討しているが、B大学は、S/MIME及び電子署名の用途の証明書を発行する認証局を委託先認証ベンダーのパブリック認証サービスを利用し、別途、構築・運用している。

2.2 認証局システム要件

両大学が共通に規定している(あるいは同等と判断できる)要件は以下の通りである。両大学ともに認証局システムは、アウトソースされることが前提である。

- 公開鍵証明書プロファイルは、X.509v3に準拠すること
- 失効リストのプロファイルは、X.509v2に準拠すること
- CAの公開鍵の鍵アルゴリズムと鍵長はRSA2048bitであり、署名アルゴリズムは、SHA-1withRSAEncryptionであること
- 利用者の公開鍵の鍵アルゴリズムと鍵長はRSA1024bitであり、署名アルゴリズムは、SHA-1withRSAEncryptionであること
- 認証局の鍵管理を行うハードウェアはFIPS140-1レベル3相当の認定を受けていること
- アウトソース先の認証局システムと接続する学内登録システムはSSL等で接続先の認証を行い、通信路の盗聴を防止すること
- 電子証明書のプロファイルのカスタマイズを容易にできること
- 発行した証明書を自動的にリポジトリに登録できること

また、B大学は以下の特徴を有する。

- ルート認証局を構築できること(階層構造を持たせているため)

- 機器用証明書の発行リクエストを PKCS#10 形式で受付け、PKCS#7 形式によって発行できること(機器に対して証明書を発行しているため。利用者用証明書は PKCS#12 形式で発行することが要件)
- CRL を OCSP で公開する機能を有していること(OCSP を採用しているため)

2.3 登録局システム要件、登録用端末(登録アプリケーション)要件

両大学が共通に規定している(あるいは同等と判断できる)要件は以下の通りである。

- RA サーバは、IAサーバのフロントエンドとして証明書発行、失効に関する登録、指示を行う機能を備えること
- 登録用端末(登録アプリケーション)の操作職員を、ICカードを用いたPKIによる認証を行えること、サーバクライアント間通信がSSLであること
- 証明書の発行、失効に関する利用者情報を既存のデータベースと連携し、CSV形式で登録でき、確認の上、一括発行及び一括失効できること
- 証明書発行後、ICカードに格納するパターンと利用者がWebブラウザを利用してPKCS#12ファイルをダウンロードするパターンの両方をサポートしていること

A 大学は以下の特徴を有する。

- 登録用端末(登録アプリケーション)のIPアドレスを制限する機能を備えること
- 個人情報を手入力することにより、新規登録者をシステムに反映できること
- ICカードの券面情報等を送信または送付用ファイルとして出力できること(ICカード発行業務をアウトソースしているため)

B 大学は以下の特徴を有する。

- 登録用端末(登録アプリケーション)はMS-Windows2000またはXPで動作し、登録アプリケーションはInternet Explorer v6で動作できること
- 個別発行及び個別失効できること
- 属性をキーに利用者を検索できること
- 写真データを参照し、本人確認できるインタフェースを装備すること

2.4 証明書格納媒体要件

両大学共に証明書格納媒体はICカードとしており、身分証明書としての役割を持っている。両大学が共通に規定している(あるいは同等と判断できる)要件は以下の通りである。

- 耐タンパ性を備えること
- 接触及び非接触のインタフェースを1枚のICカード上で実現できること
- 秘密鍵暗号処理機能を有し、PKI認証に利用する機能を備えること
- 複数のアプリケーションを搭載できること
- ICカードPINの桁数及び試行回数を設定できること(ヒアリング結果より)
- Windows上でICカードを利用した時点で、自動でカード内の証明書がWindows証明書ストアに登録される機能を備えること、また、ICカードを外した時点で登録された証明書が解除される機能を備えること(ヒアリング結果より)

また、ICカードリーダ及びPKI用のドライバに関し、共通に規定している要件は以下の通りである。

- Windows2000、WindowsXP SP2 以降で利用できること
- USB タイプのカードリーダを提供すること
- Microsoft Crypto API(CSP)及び PKCS#11 に準拠したインタフェースを提供できること

IC カードプリンタに関する共通要件は以下の通りである。

- 写真データを取り込み、カラー印刷できること
- IC カードの両面を印字できること
- 外字を含んだ日本語文字列を印字できること(ヒアリング結果より)

IC カードプリンタについては、B 大学では学内に設置され、A 大学では IC カード発行業務をアウトソースしている関係上、学内には設置されていない。証明書の変更等、少量発行を早期に実施しなければならない場合を考えると、学内のセキュリティレベルの高い施設において IC カードプリンタを設置・運用することも検討する価値があるものと考えられる。

A 大学はマトリクス認証を PKI による認証と併用できるシステム(サービス)が存在するため、IC カードの裏面にマトリクスを印字することを規定している。

B 大学は磁気ストライプを IC カード上に搭載している。

2.5 アウトソース要件

両大学が共通に規定している(あるいは同等と判断できる)要件は以下の通りである。

- 認証局システムの設計及び設置場所への搬入・据付、配線、設定等を請負者で実施し、動作確認を行うこと
- 認証局システムの発行業務は請負者が実施すること
- 請負者は、認証局システムに精通しており、パブリック認証局と同等の認証局運用実績があること
- 認証局システムのネットワーク構成図、サービスレベルに関する技術資料等を提供すること
- 学内の設備から認証局システムにアクセスする際はインターネットを利用するが、認証及び盗聴防止の機能を実現すること

A 大学はプライベート認証局を調達しており、そのアウトソース範囲は IA サーバ、RA サーバの運用及び IC カード発行業務である。CP/CPSを準備する上で必要な情報は請負者が提出することになっているが、作成は A 大学が実施している。

B 大学はプライベート認証局及びパブリック認証局(S/MIME、電子署名用途)の両方を調達し、それらCP/CPSは請負者側で作成することを規定している。アウトソース範囲は、IA サーバの運用である。また、バックアップサイトを 500km 以上離れている別サイトに設けることを要件としている。

2.6 保守要件

両大学が共通に調達仕様書内で規定している要件はないが、以下の A 大学及び B 大学の要件は一般的なものであると考えられる。

2.6.1 保守体制等

- 保守対応日は平日、すなわち土・日、祝祭日、年末年始(12月29日～1月3日)以外とし、保守時間帯は9時から17時とすること
- 保守受付窓口においては認証設備に関するソフトウェア及びハードウェアの故障等においても一元的に受付けること
- 連絡体制、保守体制、担当者を記載した資料を提出すること
- 電話・FAX・電子メールによる3つの方法の全てによる保守受付窓口を用意すること
- 障害対応、問い合わせ対応に関する一次受付は大学職員が行うため、請負者はその後の一次受付対応を行うこと

2.6.2 保守作業

- 運用に必要なハードウェア、ソフトウェアに保守継続上の問題点が見つかった場合、大学と協議の上、速やかに対応をとること
- 登録局システムへの派遣が必要とされた後、請負者が1営業日以内に現地に到着できる体制であること(RAサーバをインソースした場合の現地対応)
- 通常の使用で発生した故障の修理については発生都度対応し、また定期的保守点検については大学が指定する時期に年1回以上実施すること
- 認証局システムが障害等の理由で停止する場合は、速やかに大学に報告し、大学システム担当者の了承を得た上で復旧に努めるものとする
- 認証局システムにJPCERT勧告によるセキュリティ上の欠陥が発見された場合、速やかに大学と協議の上、対処すること
- システム更新時に不具合が起きないことを検証するための検証環境を請負者側で用意すること
- 設置場所で保守作業が行えること

2.6.3 提出物

- ハードウェア、ソフトウェア、インストール、保守・運用に関するマニュアルドキュメントを提出すること
- システムの運用管理に必要なマニュアルは日本語で提供すること

2.7 教育、支援体制要件

両大学が共通に調達仕様書内で規定している要件はないが、以下の B 大学の要件は一般的なものであると考えられる(B 大学は RA サーバの運用をインソースで実施しているため、改めて支援体制を明記したものである)。

- 平日の9時から17時に対応する支援窓口を用意すること
- 支援窓口においては、認証設備に関するソフトウェア及びハードウェアの故障等においても一元的に受付けること
- 導入時に大学システム担当者に適切な教育、研修を実施すること
- 電話・FAX・電子メールのいずれにおいても対応する支援窓口を用意すること

3. 調達仕様ガイドライン

本章は IA サーバや RA サーバの運用及び IC カード発行業務をアウトソースする場合 (RA サーバのアウトソースは必須ではない) について「UPKI 相互運用フレームワークの要件定義仕様書」を考慮し、調達仕様書のガイドラインを示すものである。

本章は認証システム及び IC カードに関して必要()、ある方が望ましい()と思われる要件を示す。各大学の要件に応じて追加すべき内容及び相互認証を行う上で将来的に調整が必要な内容が含まれることに留意すること。

例において*()の記載があるものは、注意書きを意味する。また、相互認証についての記述は、参考として記載しており、将来的に見直しが必要である。

3.1 認証局システム要件

認証局は登録局からの指示により証明書の発行及び失効を行い、また、失効リストを発行する。

アウトソース先の認証局システムの要件を以下に示す。

(1) 認証局基本機能及び証明書発行機能

- 認証局の秘密鍵は FIPS140-2 レベル 3 相当の認定を受けた HSM 上で管理できること
- 認証局の信頼モデルとして階層構造に対応すること
- 予め信頼された登録局からの発行申請を受け付け、証明書を発行できること
- 信頼する認証局との間で相互認証(相互認証証明書の発行)を行うことができること
- 主体者の証明書プロファイルは SSL、スマートカードログオン、無線 LAN、VPN 等の用途に耐えうるプロファイルを選択できること
- 証明書プロファイルは柔軟に追加・変更できること
- 登録局と発行局との間の通信は PKIX-CMP 又は HTTPS であること
- 公開鍵アルゴリズムは RSA とし、メッセージダイジェスト関数は SHA-1 を使用すること。SHA-1 アルゴリズムが危殆化した場合でも、代替のアルゴリズムで運用維持ができること
- 次のエクステンションをサポートしていること
 - Authority Key Identifier
 - Subject Key Identifier
 - Key Usage
 - Extended Key Usage
 - Certificate Policies
 - Policy Mapping
 - Subject Alternative Name
 - Issuer Alternative Name
 - Subject Directory Attributes
 - Basic Constraints

- Name Constraints
 - Policy Constraints
 - CRL Distribution Points
 - AuthorityInfoAccess
 - 主体者には同じ CN で複数の証明書が発行できること* (変更や留年等で新しい証明書の発行が必要となる場合があり、その新しい証明書が発行されるまでの重複期間に同じ CN の証明書が発行されることになるため)
 - 電子政府推奨アルゴリズムに含まれる RSA 以外の公開鍵暗号アルゴリズムのうち楕円暗号を含む 1 つ以上のアルゴリズムをサポートしていること
- (2) 証明書失効機能
- 予め信頼された登録局からの失効申請を受け付け証明書を失効できること
 - 利用者用証明書の失効情報は CRL として公開できること
 - 認証局の証明書及び相互認証証明書は ARL として公開できること
 - 利用者用証明書を発行する認証局の ARL/CRL の発行間隔は 24 時間とし、nextUpdate は 48 時間などと設定できること
 - 認証局の秘密鍵危殆化等の処置として、全ての証明書の一括失効登録が出来ること
- (3) 操作者認証管理機能
- IA サーバを操作する権限のあるリソースを予め登録することにより、認証機能を実現することが出来ること
- (4) パブリッシュ機能
- 発行した証明書の中から予め設定された証明書を LDAP サーバ等にパブリッシュすることができること
 - 設定された間隔あるいは契機に失効情報 (ARL、CRL) を LDAP サーバ、Web サーバ等、指定されたリポジトリにパブリッシュできること
- (5) ログ収集機能
- 認証局を操作した全てのログについて操作日時、アクセス元端末特定情報、操作者、リクエスト先、イベント内容、リクエスト結果が分かる記録を取得できること
 - ログの検索が可能であること
 - ログの改ざん検知が可能であること
- (6) バックアップ機能
- 認証局をリカバリする上で必要なデータをサードパーティ製品等を用いてバックアップし、リカバリさせることが出来ること

3.2 登録局システム要件

3.2.1 RA サーバアプリケーション要件

RA サーバは IA サーバのフロントエンドとして、大学内に設置される登録用端末(登録アプリケーション)からのリクエストを受付け、IA サーバに指示するためのサーバである。一般的には利用者の鍵ペア生成、PKCS#12 の生成等の機能も持つ。

RA サーバの要件を以下に示す。

- (1) 登録局基本機能
 - 予め登録された登録用端末(登録アプリケーション)の権限に応じてリクエスト先である認証局を識別できること
 - 利用者に代わって鍵ペアの生成を行え、PKCS#12 形式で提供できること
 - CSV ファイルによる一括発行、一括失効機能を提供できること
 - 審査者や承認者等の権限を識別でき、操作者を認証できること

- (2) ログ収集機能
 - 登録局を操作した全てのログについて操作日時、アクセス元端末特定情報、操作者、操作時刻、リクエスト先、イベント内容、リクエスト結果が分かる記録を取得できること
 - 操作者を認証し、ログの検索、参照を可能とすること
 - ログの改ざん検知が可能であること

- (3) 個人情報連携機能
 - 利用者の情報を予め信頼しているデータベース等と照合するか CSV 形式で入出力し、その存在性、同一性の確認ができること

- (4) メールによるサーバ証明書配付、通知機能
 - 指定された申請者のメールアドレスに対し、証明書の取得方法、あるいは証明書ファイルを送付できること*(主に機器に対して証明書を発行した場合で機器の管理者に対して配付する方法として)
 - 指定されたメールアドレスに証明書の有効期限終了及び証明書発行に関する案内メールを送付できること

- (5) PKCS#12、パスフレーズの安全な消去
 - 認証局が主体者に代わって鍵ペアを生成するフローの場合、生成した PKCS#12 及びパスフレーズを復元できないように消去できること

3.2.2 登録用端末(登録アプリケーション)要件

登録用端末(登録アプリケーション)は、RA サーバに対し利用者用証明書の発行及び失効のリクエストを登録・指示し、発行された証明書、あるいは PKCS#12 データを出力するためのものである。

登録用端末(登録アプリケーション)の要件を以下に示す。

(1) ログイン、ログアウト機能

- 登録用端末(登録アプリケーション)を操作するにあたり、ログイン画面において IC カード等を利用して操作者の認証、権限の確認を行い、ログイン、ログアウトする機能を備えること

(2) 登録、審査機能

- 発行及び失効の処理を行うにあたり、申請データの入力、あるいは CSV ファイルを読み込む機能を備えること

発行登録、審査機能

- 発行の審査処理を行うにあたり、事前に登録されたオペレータのみが実行できること
- 発行申請データの登録を個別入力、あるいは CSV ファイルを読み込んで行えること
- CSV フォーマットの構文エラーやデータベース連携に関する問題等が発生した場合、エラー情報を出力すること
- 利用者用証明書の発行登録に関しては、IC カード発行、あるいは PKCS#12 ダウンロードの選択ができること
- 機器用証明書は、CSR の登録を行えること
- 利用者が同時期に複数の証明書を持っている場合は全ての証明書を画面に出力出来ること
- 同じ CSR で複数回の発行リクエストがあった場合、警告等できること
- 証明書を発行していないステータス*(登録直後等)であれば発行申請データの破棄(取り消し)が出来ること。*(例えば、取り消しされたデータは月 1 回のバッチ処理等、後から、消去出来ること)

失効登録

- 失効申請データの登録を個別入力、あるいは CSV ファイルを読み込んで行えること
- 失効登録は既に発行済みの有効な証明書であるデータのみを対象とできること
- CSV の構文エラー等が発生した場合、エラー情報を出力すること
- 機器用証明書の失効登録を行う場合、CN や OU*(存在する場合)、証明書シリアルナンバ等の情報で検索し、失効登録が出来ること

(3) 承認(発行指示)機能

- 登録を行ったオペレータとは異なるオペレータが承認(発行指示)を行えること
- 二重の発行処理が行われないようコントロールする機能を備えること

(4) 発行出力機能

- 事前に指定したフォルダに PKCS#12 及び PKCS#12 の PIN の出力機能を備えること
 - 事前に登録されたオペレータのみが出力を行えること
 - IC カード発行をアウトソースした場合出力した利用者の鍵及び証明書データを同じ利用者の IC カードに関係づけることが可能であること
 - 出力した PKCS#12 及びパスフレーズを復元できないように消去できること
- (5) ログ収集、参照機能
- 登録アプリケーションは操作ログを収集する機能を備えること
 - 収集する記録は操作日時、アクセス元端末特定情報、操作者、操作時刻、リクエスト先、イベント内容、リクエスト結果であること
 - 事前に登録されたオペレータのみが検索、参照できること
 - ログの改ざん検知が可能であること

3.3 認証基盤リポジトリ

認証基盤リポジトリは主に失効情報を提供している Web サーバ、LDAP サーバ、OCSP レスポンダである。一般的に認証局は、これらサーバを1つあるいは複数組み合わせで失効情報を提供する。リポジトリサービスを 24 時間 365 日提供できることを目指した場合、冗長化等を考慮すること。

リポジトリサーバである 3 種類のサーバについての要件を以下に示す。

3.3.1 Web サーバ要件

- HTTP / HTTPS: HTTP インタフェースを装備していること
- CGI スクリプトや JAVA サブレットを利用し、Web 画面に連動したスクリプト処理を行えること
- 負荷分散が可能であること
- 可用性確保のため二重化運用が可能であること

3.3.2 LDAP サーバ要件

- LDAP v3 対応であること
- ITU-T 勧告 X.500、X.520 及び X.521 で定められている全てのオブジェクトクラスと属性をサポートしていること
- LDAP Referral (リフェラル) v3 に対応していること
- 標準的な認証方式 (LDAP over SSLv3 / TLSv1.0: SSLv3 / TLSv1.0 / SASL 認証 (DIGEST-MD5/EXTERNAL/KERBEROS) 等) に対応していること
- 各認証局システムから発行された X.509v3 電子証明書を格納する為のスキーマを標準装備していること
- ユーザパスワードを暗号化できること
- X.500 アクセス制御規格 X.501 に完全準拠していること
- LDIF に対応していること
- 障害監視機能を備えること

- オンラインでディレクトリデータの全体/差分バックアップ処理が可能であること
- LDAP は二重化運用が可能であること
- シングルサーバで 規模のエントリ格納が可能であること* (利用者の規模等、発行枚数に応じて必要なエントリ格納数を指定し、調達要件とすること)
- LDAP サーバ製品は、Active Directory との連携が可能な複数の製品をサポートできること* (Windows スマートカードログオンを行う場合)
- DISP(Directory Information Shadowing Protocol)、チェイニング/マルチキャスト等の一般的なサーバ連携プロトコルに対応していること

3.3.3 OCSP レスポンダ要件

- RFC2560 に準拠していること
- 認証局への OCSP レスポンダ自身の証明書の発行要求と発行された証明書の受け入れ、もしくは自己署名証明書の生成が可能であること
- 利用者からの証明書検証要求を受け付けられること
- 認証局が発行した失効情報の検証が可能であること
- 利用者に証明書検証結果を返答出来ること
- 証明書検証結果の返答に OCSP レスポンダ自身の電子証明書の添付が可能であること
- HTTP、HTTPS をサポートしていること

3.4 アウトソース及びインソースでのファシリティ、その他の要件

本ガイドラインにおいては、認証業務の一部をアウトソースすることを前提に記述している。従って、アウトソースする業務の範囲によって、アウトソース先及びインソースにおけるファシリティ要件は異なる。

ファシリティについての要件を以下に示す。

3.4.1 IA/RA サーバの運用をアウトソースする場合

(1) アウトソース先のファシリティ要件

- 認証設備を収容する建築構造物は停電、地震、火災、水害及びその他の災害の被害を容易に受けまいよう防止策を講じていること
- 発行局認証設備室は隔壁による独立した区画であること
- 認証設備室への入退室については以下の管理が実施されていること
 - 2人による生体認証装置の識別、認証操作による入室
 - 入室操作に要する時間、試行回数の制限
 - 不正な操作による開扉があった場合の通報
 - 入室の際、入室者数と同人数の退室を確認
 - 遠隔監視カメラによる継続的な監視の実施及びその記録
- 認証局の電源設備は運用に十分な電源容量を確保した無停電電源装置であること
- 認証設備室の空気調和機には防水堤と漏水検知器を設置すること
- 建物は耐火構造であること。認証設備は建物の防火区画内に設置し、自動火災報知機や消火設備を備えること

(2) 構築、運用要件

- 請負者は、認証局におけるネットワーク等の基盤及び認証局システムを一元的に設計、構築すること
- 試験期間、試行運用期間を設けること
- 準拠性監査は定期的に、あるいは大学が指定した際の実施し、その報告を行うこと
- 問い合わせに対応するためのサポート体制を確立し、受付窓口を設置すること
- 定期的に認証局システムの重要なデータのバックアップを取得すること
- LDAP 等のリポジトリは十分な可用性を確保すること
- * (管理上必要な情報がある場合、どの程度の頻度で、どのような内容が必要か条件を示す。例えば、「発行及び失効、障害、保守作業に関する報告書を月次で提出すること」等)
- * (希望に合わせて受付窓口に関する条件を示す。例えば、「受付窓口は、平日営業日 9 時から 17 時とし、電話・FAX・電子メールでの対応を行うこと」等)

(3) 委託先要件

- 請負者は ISO/IEC27001:2005(UKAS)または JIS Q 27001:2006(JIPDEC)の認証を取得しているかプライバシーマークを取得していること
- 請負者は電子署名及び認定認証業務に関する法律における認定認証業務の構築、あるいは運用の実績があること

(4) 大学内のファシリティ要件 * (参考情報)

登録用端末(登録アプリケーション)を設置する部屋は以下の要件を満たすよう設置されることが望ましい。

- 登録用端末(登録アプリケーション)を設置する部屋は間仕切り、あるいは隔壁により区切られ、施錠管理できること
- 入室権限のある者のみが入室できること。入室権限のない者が入室する場合は入室権限のある者が立ち会うこと
- 申請書等の機密情報を管理するための施錠可能な書庫もしくは金庫が設置されていること
- 自動火災報知機や消火設備を設置していること

3.4.2 IA サーバの運用をアウトソースする場合

(1) アウトソース先のファシリティ要件

3.4.1(1)の要件と同様とする。

(2) 構築、運用要件

3.4.1(2)の要件と同様とする。

(3) 委託先要件

3.4.1(3)の要件と同様とする。

(4) 大学内のファシリティ要件

登録局設備室(RA サーバを設置する部屋)の要件は、以下を満たすこと。

- 登録局設備室を収容する建築構造物は停電、地震、火災及び水害その他の災害の被害を容易に受けまい防止策を講じていること
- 登録局設備室は間仕切り、または隔壁による独立した区画であること
- 登録局設備室への入退室については以下の管理が実施されていること
 - 2人によるICカード等の識別、認証操作による入室
 - 入室操作に要する時間、試行回数の制限
 - 不正な操作による開扉があった場合の通報
 - 入室の際、入室者数と同人数の退室を確認
 - 遠隔監視カメラによる継続的な監視の実施及びその記録
- 認証局の電源設備は運用に十分な電源容量を確保した無停電電源装置であること
- 認証設備室の空気調和機には防水堤と漏水検知器を設置すること
- 建物は耐火構造であること。認証設備は、建物の防火区画内に設置し、自動火災報知機や消火設備を備えること

登録用端末(登録アプリケーション)を設置する部屋の要件は、3.4.1(2)と同様とする。

3.4.3 ICカード発行業務をアウトソースする場合*(オプション)

(1) ファシリティ要件

- ICカード発行を行う室(ICカード発行室)を収容する建築構造物は停電、地震、火災、水害及びその他の災害の被害を容易に受けまい防止策を講じていること
- ICカード発行室は隔壁による独立した区画であること
- ICカード発行室への入退室については以下の管理が実施されていること
 - 2人による生体認証装置の識別、認証操作による入室
 - 入室操作に要する時間、試行回数の制限
 - 不正な操作による開扉があった場合の通報
 - 入室の際、入室者数と同人数の退室を確認
 - 遠隔監視カメラによる継続的な監視の実施及びその記録
- ICカード発行室の電源設備は、運用に十分な電源容量を確保した無停電電源装置であること
- ICカード発行室を収容する建物は耐火構造であり、認証設備は建物の防火区画内に設置し、自動火災報知機や消火設備を備えること

(2) 構築、運用要件

- 試験期間、試行運用期間を設けること
- 準拠性監査は定期的に、あるいは大学が指定した際に実施し、その報告を行うこと
- 問い合わせに対応するためのサポート体制を確立し、受付窓口を設置すること
- ICカード書き込み後、入手したPKCS#12及びPKCS#12のPINを直ちに削除すること

- 監査ログを取得し、指定した期間まで管理できること
- ICカードの管理は厳重に行うこと
- ICカードの在庫管理を行うこと
- ICカード及びPIN通知書は大学が指定する場所に安全に配送されること
- * (管理上必要な情報がある場合、どの程度の頻度で、どのような内容が必要か条件を示す。例えば「発行枚数、発行不良件数、在庫管理情報に関する報告書を月次で提出すること」等)
- * (希望に合わせて受付窓口に関する条件を示す。例えば「受付窓口は、平日営業日9時から17時とし、電話・FAX・電子メールでの対応を行うこと」等)

3.5 ICカードに関する要件* (オプション)

UPKI 相互運用フレームワークの要件定義仕様書において証明書格納媒体としてはICカードを推奨しており、本調達仕様においてもICカードを推奨する。

また、ICカードプリンタは大学内で少量のICカードを発行する場合に必要となる。ICカードを発行する部屋については、RAサーバを設置する部屋と同等の要件がかかるものと考えられる。大学内でICカードの発行を行わない場合には調達は不要である。

ICカード、ICカードプリンタ等に関する要件を以下に示す。

(1) ICカード要件

- 接触(ISO7816)のインタフェースを持つこと
- 暗号方式は公開鍵暗号方式及び共通鍵暗号方式をサポートすること
- 書き換え可能記憶容量は、複数の証明書を格納した上で更に十分な容量を持たせていること
- 通信方式、通信プロトコル、ICカードに搭載する暗号方式、カードOS及びカードアプリケーションの外部インタフェースはオープンな仕様に基づくものであること
- ICカード内のデータフォーマットの著作権は大学側にあること
- 契約時にICカードの詳細技術仕様を公開すること
- 非接触(ISO14443)のインタフェースを持つこと
- 複数のアプリケーションを搭載でき、アプリケーションの追加や削除が行えること。アプリケーション例は以下の通り
 - PCセキュリティ
 - 認証・決済系アプリケーション
 - キャッシュレスサービス
 - 金融系アプリケーション
 - 入退室コントロール等

(2) ICカードリーダー、ドライバ要件

- Windows2000、WindowsXPで利用できること。将来的にWindowsVistaをサポートすること* (大学の環境に応じ条件を示す)
- Microsoft Crypto API(CSP)及びPKCS#11に準拠したインタフェースを提供できること* (大学の環境に応じ条件を示す)
- MacOSXで利用できること* (大学の環境に応じ条件を示す)

- USB タイプ(または、PC カードタイプ)のカードリーダーを提供すること*(大学の環境に応じ条件を示す)
 - IC カードドライバはダウンロードサービスが存在すること
- (3) IC カードプリンタ要件
- 写真データを取り込んでカラー印刷できること
 - IC カードの両面を印字できること
 - 外字を含んだ日本語文字列を印字できること

3.6 CP/CPS 及び運用手順書の提供

CP/CPS 及び下位の運用手順書、マニュアル等必要な規定文書を提供することを条件として示す。

- 「キャンパス PKI CP/CPS ガイドライン」に基づき、CP/CPS を提供すること
- 下位運用手順書(審査登録業務)、登録用端末(登録アプリケーション)のシステム管理手順書を提供すること

3.7 保守要件

保守体制及び保守作業の要件を以下に示す。

- (1) 保守体制等
- *(各大学の希望に合わせて保守対応に関する条件を示す。例えば「保守対応日は、平日、すなわち土・日、祝祭日、年末年始(12月29日~1月3日)以外とし、保守時間帯は9時から17時とする。電話・FAX・電子メールによる3つの方法の全てによる保守受付窓口を用意すること。」等)
 - 保守受付窓口においては認証設備に関するソフトウェア及びハードウェアの故障においても一元的に受付けること
 - 連絡体制、保守体制、担当者を記載した資料を提出すること
 - 障害対応、問い合わせに関する一次受付は、大学職員が行うので請負者はその後の一次受付対応を行うこと
- (2) 保守作業
- 運用に必要なハードウェア、ソフトウェアに保守継続上の問題点が見つかった場合、大学と協議の上、速やかに対応すること
 - 通常の使用で発生した故障の修理については発生都度対応し、また定期的保守点検については大学が指定する時期に年1回以上実施すること
 - 認証局システムが障害等の理由で停止する場合は、速やかに大学に報告し、大学システム担当者の了承を得た上で、復旧に努めるものとする
 - 認証局システムに JPCERT 勧告によるセキュリティ上の欠陥が発見された場合、速やかに大学と協議の上、速やかに対応すること

- システム更新時に不具合が起きないことを検証するための検証環境を請負者側で用意すること
- 設置場所で保守作業が行えること

3.8 費用

- 定期的な外部監査を予定している場合には、CP/CPS の準拠性監査の監査項目及び概算の監査費用を含む年間の運用費用を提示することを要件として示すこと

4. 用語集

RFC2828¹に基づき、本ガイドライン中で用いた用語の定義を行う(引用したものは とする)。RFC2828 に定義がないものは、本ガイドライン独自で定義している。

あ行

- アクセスコントロール (Access Control)

権限のないアクセスに対するシステムリソースの保護。システム資源を使用するプロセスは、セキュリティポリシーによってコントロールされ、権限を持った主体 (ユーザ、プログラム、プロセス、または他のシステム) によってのみセキュリティポリシーに基づいて許可される。

「資源に対する権限のない使用を防止すること。権限のない方法による資源の使用を防止することも含む。」

- アルゴリズム (Algorithm)

問題を解決するためのステップごとの命令または計算手順の有限個のセットで、特にコンピュータに実装されるもの。

- 一時停止 (Suspension)

証明書を一時的に無効な状態にすること。

か行

- 下位認証局 (Subordinate CA)

公開鍵証明書が、別の (上位) CA によって発行されている CA。

- 鍵ペア (Key Pair)

公開鍵暗号技術に使われる数学的に関連する一対の鍵 (公開鍵と私有鍵) であり、私有鍵を公開鍵の知識から引き出すことが計算量的に非現実的なやり方で生成される。

¹ <http://www.ipa.go.jp/security/rfc/RFC2828-03AJA.html#access%20control>

鍵ペアの所有者は、データの暗号化、デジタル署名の正確性検証、保護されたチェックサムの計算もしくは鍵共有アルゴリズムにおける鍵の生成にその鍵を使えるように、他のシステム主体に公開鍵を開示する。それに対応するプライベート鍵は、データの復号、デジタル署名の生成、保護されたチェックサムの正確性検証もしくは鍵共有アルゴリズムにおける鍵の生成のためにそれを使う所有者によって秘密に保たれる。

- 鍵長 (Key Length)

鍵ペアのデータ長のこと。一般に鍵が長ければ長いほど解読がされにくいとされる。

- 鍵の預託 (Key Escrow)

特定の環境下において、暗号技術的な鍵が復元でき、使えるように、その鍵もしくはその部分についての知識を、ひとつ、あるいは、複数の「寄託エージェント(escrow agent)」と呼ばれる第三者のカストディに蓄積するための鍵回復テクニック。鍵寄託は、典型的には、知識分割テクニックとして実施される。例えば、Escrowed Encryption Standard は、デバイス固有の分割鍵の 2 つのコンポーネントを分離された寄託エージェントに委託する。そのエージェントは、そのコンポーネントを、その特定のデバイスによって暗号化された遠隔通信の電子的な監視を行うことが法的に認可された者にのみ提供する。このコンポーネントは、デバイス固有の鍵を再構築するために使われ、これは、通信を復号するために必要とされるセッション鍵を取得するために使われる。

- 活性化情報 (Activation Data)

鍵以外のデータ値で、暗号化モジュール等に格納されている秘密鍵にアクセスするためのもの。具体的には、PIN コード、パスフレーズ等を指す。

- 危殆化 (Compromise)

セキュリティ侵害のひとつ。ここで、システム資源が、不正(無権限)アクセスに対して露出されるか、あるいは、潜在的に露出される。

本ガイドラインでは、秘密鍵や関連秘密情報等が盗難や漏洩、第三者による解読等によって、秘密性を失ったか、あるいはその可能性があること。

- 公開鍵 (Public Key)

公開鍵暗号技術について使われる暗号技術的な鍵のペアのうち、公衆に開示可能なコンポーネントの方。

「(公開鍵暗号システムにおいて)ユーザの鍵ペアのうち、公知の鍵。」

さ行

- 自己署名証明書 (self-signed certificate)

その公開鍵が証明書内にあり、そのプライベート鍵が証明書に署名するのに使われる公開鍵証明書が、署名者の同一の鍵ペアのコンポーネントであるもの。

自己署名 X.509 公開鍵証明書において、発行者の DN は、サブジェクトの DN と等しい。

- 失効 (Revoke, certificate revocation)

CA によって発行され、有効であったデジタル証明書が無効になったことを CA が宣言したときに発生するイベント。通常、失効日と共に宣言される。

X.509 では、証明書を記載した CRL を発行することにより、潜在的な証明書ユーザに失効が通知される。失効と CRL のリストは、証明書の期限が切れる前のみ必要である。

- 失効リスト (Certificate Revocation List = CRL)

予定された有効期限を迎える前に、発行者によって失効されたデジタル証明書を列挙するデータ構造体。

「有効とみなされなくなった証明書のセットを示す、証明書の発行者による署名付きのリスト。CRL に掲載された後で証明書の有効期限が切れると、次回の CRL にはその証明書は掲載されない。CRL は、失効された公開鍵証明書または属性証明書を識別するために使用され、認証局またはユーザに発行された証明書の失効を表す。また、CRL という用語は、CRL、ARL、ACRL 等を含むさまざまな種類の失効リストに適用される一般的な用語としても用いられる。」

- 信頼者 (Relying Party)

デジタル証明書によって提供された情報の正当性 (他の主体の公開鍵の値など) に依存するシステム主体。

「確信をもって、他の主体の公開鍵を知る必要がある主体。」

システム主体は、人間、組織、あるいは人間またはシステムによって制御されているデバイスまたはプロセスである。

た行

- 登録局 (Registration Authority = RA)

(CA からは分離された) オプションとしての PKI 主体であり、これは、デジタル証明書にも、CRL にも署名しないが、証明書や CRL を発行し、他の証明書管理機能を行うために CA によって必要とされる情報 (特に、サブジェクトの身元) の部分または全体の記録もしくは正確性検証について責任を負う。

しばしば、CA は、その CA が証明書に署名しているすべてのエンドユーザのために、すべての証明書管理機能を行う可能性がある。また、大規模な、あるいは、地理的に分散したコミュニティにおけるように、CA の 2 番目の役割の重責を降ろして、それらをアシスタントに代理させる一方で、CA は、主要な機能(証明書や CRL に署名すること)を維持することが必要不可欠、もしくは、渴望される可能性もある。CA によって RA に代理されるタスクは、個人の認証、名前の割り当て、トークン配布、失効報告、鍵生成およびアーカイブ化を含む可能性がある。RA は、CA からは分離された、副次的な機能を割り当てられたオプションとしての PKI コンポーネントである。RA に割り当てられた義務は、場合に応じて様々であるが、下記の事項を含む可能性がある。

サブジェクトの身元を検証すること。すなわち、個人認証機能を行うこと。

サブジェクトに名前を割り当てること。

「サブジェクトが 証明書について要求された属性をもつ資格があること」を検証すること。

「サブジェクトが 証明書について要求された公開鍵に対応するプライベート鍵を所持すること」を検証すること。

鍵ペア生成、トークンの配布および失効報告の取り扱いのような登録以外の機能を行うこと。(このような役割は、CA と RA の両方から分離された PKI 要素に割り当てられる可能性がある。)

PKIX における用法： オプションとしての PKI コンポーネントであり、CA とは別のもの。RA が行う機能は、場合に応じて様々であるが、身元認証および名前の割り当て、鍵生成、および、鍵ペア、トークン配布および失効報告のアーカイブ化を含む可能性がある。

- 電子証明書(Public-key Certificate)

システム主体の身元を公開鍵の値に結合し、追加的なデータ項目にも結合する可能性があるデジタル証明書。公開鍵の所有を証明するデジタル的に署名されたデータ構造体。

公開鍵証明書上のデジタル署名は、偽装不能である。それゆえ、その証明書は、ディレクトリに収めることによって、(ディレクトリが証明書のデータインテグリティを保護する必要なく)公開できる。

「ユーザの公開鍵は、何らかの他の情報とともに、それを発行した認証機関のプライベート鍵で署名することによって偽装不能なものとして与えられる。」

- 電子署名(Digital Signature)

データのあらゆる受信者が、その署名をデータの発信元およびインテグリティを検証するために使えるようなやり方で、暗号アルゴリズムによって算出され、データオブジェクトに追加される値。

「データユニットの受信者がデータユニットの源泉とインテグリティを証明できるようにし、(例：受信者による)偽装から防護する、データユニットに追加されたデータ、もしくは、データユニットの暗号技術的な変換。」

典型的にはそのデータオブジェクトは、ハッシュ関数に対する最初の入力であり、次に、そのハッシュ結果は、署名者のプライベート鍵を使って、暗号技術的に変換される。最終結果としての値は、そのデータオブジェクトのデジタル署名と呼ばれる。その署名の値は、保護されたチェックサムである。なぜなら、暗号技術的ハッシュの属性は、「データオブジェクトが変更された場合、そのデジタル署名は、もはや一致しないこと」を確保するからである。デジタル署名は、偽造不能である。なぜなら、想定される署名者のプライベート鍵を知らずして、署名を正しく作成することや、変更することについて、確信を持つことはできないからである。

デジタル署名スキームには、ハッシュ結果を変形するために、公開鍵暗号アルゴリズムを使うものがある。それゆえ、アリスがボブに送るためにメッセージに署名する必要があるとき、彼女は、そのハッシュ結果を暗号化するために彼女のプライベート鍵を使うことができる。ボブは、メッセージとデジタル署名の両方を受け取る。ボブは、アリスの公開鍵をその署名を復号するために使うことができ、次に、平文の結果を彼が自信でメッセージをハッシュ化して求めたハッシュ結果と比較する。値が等しい場合、ボブは、そのメッセージを受け入れる。なぜなら、それはアリスからのものであり、変更されずに到着したと確信を持てるからである。その値が等しくない場合、ボブは、そのメッセージを棄却する。なぜなら、そのメッセージも、その署名も経路において変えられているからである。

他のデジタル署名スキームは、そのハッシュ結果をデータ暗号化するためには直接使うことができないアルゴリズムで変換する。このようなスキームは、そのハッシュから署名値を作成し、その署名値を検証するやり方を提供するが、署名値からハッシュ結果を復元するやり方は提供しない。国によっては、このようなスキームは、輸出可能性を高め、利用における他の法的制約を避ける可能性がある。

な行

- 認証局 (Certification Authority = CA)

デジタル証明書 (特に X.509 証明書) を発行し、証明書内のデータ項目間の結びつきを保証する主体。

「1人以上のユーザに信用され、証明書を作成および割り当てる機関。認証局がユーザの鍵を作成することもある。」

証明書ユーザは、証明書によって提供された情報の正当性に依存する。このため、CA は、証明書ユーザが信頼する第三者でなければならず、通常、政府、企業、またはその他の組織によって認められた権限をともなう公的な地位を持つ。CA は、証明書のライフサイクルを管理する責任を持ち、証明書の種類および適用する CPS に応じて、その証明書に対応する鍵ペアのライフサイクルを管理する責任を持つことがある。

- 認証局運用規程 (CPS: Certification Practice Statement)

「認証局が証明書の発行のために採用する運用規定」

CPS は公開されたセキュリティポリシーで、特定の CA から発行された証明書が特定のアプリケーションで十分に信頼できるかどうかを証明書ユーザが判断するときに役立つ。CPS は、

- (a) CA によるシステムの詳細と証明書管理業務で採用している既定の定義、
- (b) CA と証明書を発行された主体との間の契約の一部、
- (c) CA に適用される法令または規制、
- (d) 複数のドキュメントを含むこれらの種類の組み合わせ である。

通常、CPS は証明書ポリシーよりも詳細で手続き的な目的を持つ。CPS が特定の CA または CA コミュニティに適用されるのに対し、証明書ポリシーは CA 間また CA コミュニティ間に適用される。1 つの CPS を持つ CA が複数の証明書ポリシーをサポートすることがある。これは、異なる適用目的として、または異なるユーザコミュニティによって使用される。それぞれ異なる CPS を持つ複数の CA が、同じ証明書ポリシーをサポートすることがある。

は行

● ハッシュ関数

(通常、可変長であり、非常に大きい可能性があるメッセージもしくはファイルのような)データオブジェクトに基づいて値を計算するアルゴリズム。これによって、データオブジェクトをより小さなデータオブジェクト(「ハッシュ結果(hash result)」通常は固定長)に対応づける。

「広範囲(非常に広範囲である可能性がある)ドメインからの値を、より狭い範囲に対応づける(数学的)関数。「良い」ハッシュ関数は、その関数をドメイン中の(大きな)値に適用した結果が、全域にわたって一様な分散(かつ、乱雑に見えるもの)となるものである。」

セキュリティアプリケーションに必要とされる種類のハッシュ関数は、「暗号技術的ハッシュ関数(cryptographic hash function)」と呼ばれる。このためのアルゴリズムについて、(ブルートフォースよりも効果的な攻撃は無いので)下記の条件は計算量的に現実的でない。

- (a) データオブジェクトが事前に定めたハッシュ結果になる(「一方向」性)。あるいは、
- (b) 2 つのデータオブジェクトが同一のハッシュ結果になる(「衝突困難」性)。
- (c)暗号技術的ハッシュは、ハッシュ関数の定義に記述されている意味において「良い」といえる。入力データオブジェクトに対するいかなる変更も、高い確率で、異なるハッシュ結果をもたらすので、暗号技術的ハッシュ(cryptographic hash)の結果がデータオブジェクトについての良いチェックサムを作り出すようになる。

● 秘密鍵(Private Key)

公開鍵暗号技術について使われる暗号技術的鍵のペアの秘密コンポーネント。

「(公開鍵暗号システムにおいて)ユーザの鍵ペアのうち、そのユーザのみが知っている鍵。」

- 秘密鍵管理モジュール (Hardware Security Module)

暗号鍵の生成、保管、利用等において、セキュリティを確保する目的で主に認証局で使用されるハードウェアのこと。

- プロファイル (Profile)

証明書、失効リスト (CRL) 等の設定情報のこと。

- 本人性確認 (Identification & Authentication)

システム主体によって / システム主体について、主張された身元を検証するプロセス。認証過程は、2つのステップから成る。

1. 識別ステップ:

識別子をセキュリティシステムに渡す。

(認証された同一性はアクセス制御サービスなどの他のセキュリティサービスのベースとなるので、識別子は慎重に割り当てなければならない。)

2. 検証ステップ:

主体と識別子間のバインディングを確認する認証情報を提供または生成する。

ま行

ら行

- リポジトリ (Repository)

デジタル証明書や、(CRL、CPS および証明書ポリシーを含む) 関連情報を蓄積し、証明書ユーザに配布するためのシステム。

「証明書や証明書に関する他の情報を蓄積・取得するための信用に値するシステム。」

証明書は、リポジトリ中に置くことによって、必要とする可能性がある者宛に発行される。このリポジトリは、通常、公衆がアクセス可能なオンラインサーバである。例えば、Federal PKI において、期待されるリポジトリは、LDAP を使うディレクトリであるが、DAP を使う X.500 ディレクトリ、もしくは、HTTP サーバ、もしくは、匿名によるログインを許容する FTP サーバである可能性もある。

- 利用者 (Certificate User)

大学により利用者用証明書の使用を認められたその大学に所属する個人。

- ルート認証局 (Root Certification Authority)

エンド主体によって直接、信用されている CA であり、root CA の公開鍵の値の入手は、回線外の手順によることを含む。

階層型 PKI (Hierarchical PKI) における用法:

認証階層(certification hierarchy)において、最高レベルの(最も信頼される)CA。すなわち、すべての証明書ユーザが信用の基礎とする公開鍵をもつ機関。

階層型 PKI において、root は、2 番目に高位なレベルである CA のひとつもしくは複数宛に公開鍵証明書を発行する。これらの各 CA は、3 番目に高位なレベルの CA 等宛により多くの証明書を発行できる。階層型 PKI の運用を開始するために、ルートの初期公開鍵は、すべての証明書ユーザ宛に PKI の認証関係に依存しないやり方でセキュアに配布される。ルートの公開鍵は、単純に数値として配布される可能性があるが、典型的には、root がサブジェクトである自己署名証明書中において配布される。ルートの証明書は、認証階層(certification hierarchy)において高位の者がいないので自己署名される。それゆえ、ルートの証明書は、すべての認証パスにおいて最初の証明書となる。

- ログ(Log)

コンピュータの利用状況や、通信の記録を取ること。また、その記録。操作やデータの送受信が行われた日時と、行われた操作の内容や送受信されたデータの中身等が記録される。

A - G

- ARL (Authority Revocation List)

CA 宛に発行されたが、予定されていた失効日以前に発行者によって無効化されたデジタル証明書を列挙するデータ構造。

「証明書発行者によって、もはや有効ではないとみなされる機関に対して発行された公開鍵証明書のリストを含む失効リスト。」

- CA (Certification Authority)

= 認証局

- CN (Common Name)

(以下の文字列を示す。

(a) ディレクトリオブジェクト("commonName" 属性)の X.500 DN の一部である可能性があり、

(b) 何らかの制限付きスコープ内でオブジェクトが一般的に知られるために使用されている

名前(多義の可能性があり)で、

それが対応する国または文化での命名規則に従う。

- CRL (Certificate Revocation List)

= 失効リスト

- DN (Distinguished Name)

X.500 DIT (Directory Information Tree) において、オブジェクトを一意に表現する識別子。

DN は、DIT のベースから命名されたオブジェクトに至るパスを識別する一式の属性値である。X.509 公開鍵証明書もしくは CRL は、その発行者を識別する DN を含み、X.509 属性証明書は、そのサブジェクトを識別する DN もしくは他の形態の名前を含む。

- FIPS 140-1 (Federal Information Processing Standard)

コンピュータ および通信システム中の秘密区分とされていない情報を防護するために使われる暗号技術的モジュールが適合すべきセキュリティ要件についての米国政府標準。

この標準は、広範な潜在的アプリケーションや環境を扱うために、4 つの段階的なレベル ("Level 1" から to "Level 4" まで) の要件を規定する。この要件は、基本設計と文書化、モジュールインターフェイス、認可割れた役割とサービス、物理的セキュリティ、ソフトウェア・セキュリティ、オペレーティングシステムセキュリティ、鍵管理、暗号アルゴリズム、電磁的インタフェースと電磁的互換性 (EMI/EMC)、および自己検査に対応する。NIST とカナダの CSE (Communication Security Establishment) は、共同でモジュールを認定する。

- FIPS 140-2 (Federal Information Processing Standard)

セキュリティレベル 4 段階の位置付けは FIPS 140-1 とほぼ変わらない。FIPS 140-2 ではセキュリティ要件の 2 項目について見直しが行われている。セキュリティ要件 11 項目の内、ソフトウェア・セキュリティと暗号アルゴリズムがなくなり、代わりに以下が加えられた。

- ・設計保障
- ・コンフィグレーション管理, 配布と運用, 開発, ガイダンス文書, 機能テストの規定。
- ・その他の攻撃の軽減
- ・現時点でセキュリティ要件が明確になっていない攻撃の軽減。

- FQDN (Fully Qualified Domain Name)

ドメイン名に、サブドメイン名およびホスト名を付加したものをいう。ドメイン・ネーム・システムにおいて 1 個の IP アドレスと対応関係をもつ。

H - N

- HSM (Hardware Security Module)

= 秘密鍵管理モジュール

- IA (Issuing Authority)

= 認証局

- IC カード(IC Card、Smart Card)

コンピュータの CPU、メモリおよび入出力インターフェイスの機能を行うひとつ、もしくは複数の集積回路のチップを含むクレジットカードの大きさのデバイス。

しばしば、この用語は、若干厳密に、銀行や商人によって発行されたプラスチックのクレジットカードの類の形態と外観に適合するカードの意味で使われる。また、この用語は、広く、クレジットカードよりも大きなカード(特に、PC カードのように、より厚いカード)を含むように使われることもある。

「スマートトークン」は、スマートカードの規定に準拠するデバイスである。ただし、このトークンが、犬の首札やドアの鍵の形態のような何らかの他の形態にパッケージ化されて、標準的なクレジットカードの形態をもたない場合を除く。

- IETF(Internet Engineering Task Force)

インターネット技術の開発に貢献する人々によって自己組織化されたグループ。これ自体は ISOC の一部ではないが、インターネット標準を開発することに携わっている主たる主体である。(IETF は)WG(ワーキンググループ)から成り、これらは、(セキュリティエリアのように)エリアとしてまとめられており、各々は、ひとり、もしくは、複数名のエリアディレクター(Area Director)によって調整されている。IAB および IESG への指名は、ボランティアとして常連の IETF 会合参加者の中から無作為に選択された委員会によって行われる。

- LDAP(Lightweight Directory Access Protocol)

X.500 ディレクトリ(もしくは、他のディレクトリ サーバ)の基本的用途を DAP (Directory Access Protocol) 全部の資源要件を招くこと無く(訳注: 軽便に)サポートするクライアント/サーバ プロトコル。

シンプルな管理と、シンプルな読み書きの双方向的ディレクトリサービスを提供するブラウザアプリケーションのために設計された。クライアントのディレクトリ サーバに対する認証として、シンプル認証とストロング認証の両方をサポートする。

O - U

- OCSP(Online Certificate Status Protocol)

クライアントによって、サーバからデジタル証明書に関する有効性の状態と他の情報を入手するために使われるインターネットプロトコルのひとつ。

(高額の商取引を扱うアプリケーションのような)アプリケーションにおいて、CRL によるより適時な証明書失効状態の入手、あるいは、他の状態情報の入手が不可欠である可能性がある。OCSP は、定期的な CRL に照らしてチェックすることの代わり、もしくは、追加的なものとして、デジタル証明書の現在の状態を判定するために使われる可能性がある。OCSP クライアントは、OCSP サーバ宛に状態リクエストを発行し、サーバがレスポンスを提供するまで当該証明書の受領を保留する。

- PIN(Personal Identification Number)

個人識別番号。

- OID(Object Identifier)

一連の整数(ASN.1 標準で規定されているように整形・割り当てされる)で書かれた、あるものについての公式な地球規模で固有な名称であり、概要仕様中のものをプロトコルにおけるセキュリティサービスの交渉時に参照するために使われる。

「オブジェクトと関連づけられた (すべての他のこのような値から区別可能な) 値。」

OID によって命名されたオブジェクトは、オブジェクト識別子の木の葉である。(これは、X.509 ディレクトリ情報の木と似ているが別のものである。)各 arc (すなわち、各木の枝)には、非負の整数のラベルが付けられる。OID は、木のルート(根)から名前がついたオブジェクトに至るパス上の一連の整数である。

OID の木は、ルート直下に 3 つの arc をもつ。

{0} ITU-T 用

{1} ISO 用

{2} 両者の共同利用

下記 ITU-T には、4 つの arc があり、ここで、{0 0} は、ITU-T 勧告 (recommendation) 用である。下記 {0 0} には、26 の arc があり、一連の勧告のための arc は、A から Z までのアルファベットで始まり、これらのもとに各勧告のための arc がある。それゆえ、ITU-T 勧告 X.509 についての OID は、{0 0 24 509} である。下記 ISO には、4 つの arc があり、ここで、{1 0} は、ISO 標準用であり、これらのもとに各 arcs は、各 ISO 標準用である。それゆえ、ISO/IEC 9594-8(the ISO number for X.509)用の OID は、{1 0 9594 8} である。

次のものは、追加的例示である。

ANSI は、branch {joint-iso-ccitt(2) country(16) US(840) organization(1)} 下に組織体名を登録する。NIST CSOR は、branch {joint-iso-ccitt(2) country(16) us(840) gov(101) csor(3) pki(4)} 下に PKI オブジェクトを記録する。米国国防総省は、INFOSEC オブジェクトを branch {joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1)} の下に登録する。PKIX プライベート拡張のための OID は、{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) 1 1} というように、当該 PKIX 名前空間についての arc の下の arc の中に定義される。

- PKI(Public Key Infrastructure)

公開鍵暗号技術のアプリケーションについてのユーザのコミュニティのために、何らかの証明書管理、アーカイブ管理、鍵管理およびトークン管理機能を行う認証局(および、オプションとして登録局および他の支援的なサーバやエージェント)のシステム。

PKIX における用法:

一式のハードウェア、ソフトウェア、人間、ポリシー、および手順であり、公開鍵暗号技術に基づくデジタル証明書を作成・管理・蓄積・配布・失効するために必要とされる。

PKI の核となる機能は、次のとおり。

- (a) ユーザを登録し、その公開鍵証明書を発行する。
- (b) 要求されたとき、証明書を失効する。
- (c) 後日、証明書の十分性を検証する。

必要とされるデータをアーカイブする。データの守秘性のための鍵ペアは、CA もしくは RA によって生成(および、おそらく寄託)される可能性があるが、PKI クライアントに自身のデジタル署名鍵ペアを生成することを要求することは、暗号技術的システムのシステムインテグリティを維持管理するのに有用である。なぜなら、このようにすれば、当該クライアントのみが、常に自身が使うプライベート鍵を所持するからである。また、PKI のコンポーネントが運用する際に準拠するセキュリティポリシーである CPS を承認し、調整するために、機関が設立される可能性がある。

数多くの他のサーバやエージェントがコア PKI をサポートし、PKI クライアントがそれらからサービスを得る可能性がある。このようなサービスの全体像は、まだ完全には理解されておらず、進化しつつあるが、サポートする役割は、アーカイブエージェント、認定された配布エージェント、確認(confirm)エージェント、デジタル公証人、ディレトリ、鍵寄託エージェント、鍵生成エージェント、発行者やサブジェクトが PKI において一意の識別子をもつことを確保する命名エージェント、リポジトリ、チケット交付エージェントおよびタイムスタンプエージェントを含む可能性がある。

- PKIX(Public Key Infrastructure X.509)

IETF において、X.509 形式にもとづいた PKI 技術の標準化を行っているワーキンググループ。

- RA(Registration Authority)

= 登録局

- RFC(Request for comment)

インターネット標準文書と、IESG (Internet Engineering Steering Group)、IAB (Internet Architecture Board) およびインターネットコミュニティ全般の他の発行物についての公式なチャンネルである一連のアーカイブするシリーズの文書のひとつ。

この用語は、"Internet Standard" の同義語ではない。

- RSA

1977 年に Ron Rivest、Adi Shamir および Leonard Adleman によって発明された公開鍵暗号技術についてのアルゴリズム。

RSA は、2 つの大きな素数から得られる整数の剰余演算を使う。RSA 解読の困難性は、ほぼ同じ大きさの 2 つの大きな素数から得られる整数の素因数分解の困難性と等価であると信じられている。

RSA 鍵ペアを作成するために、2 つの大きな素数 p と q を無作為に選択し、剰余演算 $n = pq$ を計算する。 n 未満であり、かつ、 $(p-1)(q-1)$ の素数である公開する指数 e を無作為に選択する。 $ed-1$ が $(p-1)(q-1)$ を割り切れるように公開しない他の d を選択する。この公開鍵は、数 (n,e) の組であり、そのプライベート鍵は、組 (n,d) である。

プライベート鍵 (n,d) をその公開鍵 (n,e) から算出することは、困難であると想定されている。しかし、 n が p と q に素因数分解可能である場合、そのプライベート有鍵 d は、容易に算出できる。それゆえ、RSA のセキュリティは、「2 つの大きな素数から成る数を素因数分解することは、計算量的に困難である」という想定に依存する。(当然ながら、 p と q は、プライベート鍵の一部として扱われるか、あるいは、 n を算出した後、破壊される。)

ボブ宛に送られるメッセージ m を暗号化するために、アリスは、 $m^{*e} \pmod n = c$ を計算するためにボブの公開鍵 (n,e) を使う。彼女は、 c をボブ宛に送る。ボブは、 $c^{*d} \pmod n = m$ を計算する。ボブのみが d を知っているのので、ボブのみが m を戻すために $c^{*d} \pmod n = m$ を計算できる。

ボブ宛に送るメッセージ m のデータ発信元認証を提供するために、アリスは、 $m^{*d} \pmod n = s$ を計算する。ここで、 (d,n) は、アリスのプライベート鍵である。彼女は、 m と s をボブ宛に送る。アリスだけが送ることができたメッセージを復元するために、ボブは、 $s^{*e} \pmod n = m$ を計算する。ここで (e,n) は、アリスの公開鍵である。

データ発信元認証に加えてデータインテグリティを確保することは、追加的な計算ステップを要求し、ここで、アリスとボブは、暗号技術的ハッシュ関数 h を(デジタル署名について説明したように)使う。アリスは、ハッシュ値 $h(m) = v$ を計算し、次に v を彼女のプライベート鍵で s を得るために暗号化する。彼女は、 m と s を送る。ボブは、 m' と s' を受信し、これらのいずれもが、アリスが送信した m と s から変更されている可能性がある。これをテストするのに、彼は、 v' を得るために s' をアリスの公開鍵で復号する。彼は、次に、 $h(m') = v'$ を計算する。 v' が v と等しい場合、ボブは、 m' はアリスが送った m と同一のものであると確信できる。

- SHA-1 (Secure Hash Algorithm 1)

SHA-1 (Secure Hash Algorithm) という、 $2^{*}64$ ビット未満の長さのいかなる入力について、160 ビットの出力 (ハッシュ結果) を作り出す暗号技術的ハッシュ関数を規定する米国政府標準。

- SHA-256

FIPS 180-2 SECURE HASH STANDARD として SHA-1 と共に、規定されたハッシュ関数群の中の 256 ビットのハッシュ値を出力する MD 型ハッシュ関数である。

- SSL (Secure Socket Layer)

(もともと Netscape Communications 社によって開発された) インターネットプロトコル。これは、クライアント (しばしば、Web ブラウザ) とサーバの間のトラフィックにデータ守秘性サービスおよびデータ インテグリティサービスを提供し、オプションとしてクライアントとサーバ間におけるピア主体認証を提供できるようにするためのコネクション指向の「エンド to エンド」暗号化を使う。

SSL は、HTTP の下、かつ、信頼できる TCP (トランスポートプロトコル) の上の層である。SSL は、カプセル化するアプリケーションとは独立しており、いかなる上位層プロトコルも、SSL 上に透過的にのせることができる。しかし、多くのインターネットアプリケーションは、IPsec によってより良く提供される可能性がある。

SSL は、2 つの層をもつ。

(a) SSL の下位側の層である SSL レコード プロトコルは、トランスポートプロトコルの上に位置し、上位層のプロトコルをカプセル化する。このようなカプセル化されたプロトコルのひとつが SSL ハンドシェイク プロトコルである。

(b) SSL の上位側の層は、サーバ認証用に (サーバの身元をクライアントに対して検証する) 公開鍵暗号技術を提供し、オプションとしてのクライアント認証用に (クライアントの身元をサーバに対して検証する) 公開鍵暗号技術を提供し、さらに、そのアプリケーションプロトコルがデータを転送 / 受信する前に、それらが (データの守秘性保護のために使う) 共通鍵暗号化アルゴリズムおよび秘密のセッション鍵を交渉できるようにする。鍵付ハッシュは、カプセル化されたデータにデータインテグリティサービスを提供する。

- S/MIME

Secure/Multipurpose Internet Mail Extensions。インターネットメールメッセージについて、暗号化とデジタル署名を提供するインターネットプロトコルのひとつ。

- TLS (Transport Layer Security)

TLS バージョン 1.0 は、SSL バージョン 3.0 に基づいた、同様のインターネットプロトコルである。

TLS プロトコルは、誤称である。それは、これは、トランスポート層 (OSI 第 4 層) 上で動作するからである。

V - X

- X.500

ITU-T 勧告。これは、X.500 ディレクトリを規定する ITU-T/ISO 共同の複数パート標準 (X.500 - X.525) の一部であり、OSI 主体、プロセス、アプリケーションおよびサービスに分散型のディレクトリ機能を提供するシステムの概念的な収集である。(ISO における同等のものは、IS 9594-1 および関連する標準 IS 9594-x である。)

X.500 ディレクトリは、木(ディレクトリ情報の木)として構築されており、情報は、ディレクトリ項目に保管される。各エントリは、オブジェクトについての情報の収集であり、各オブジェクトは、DN をもつ。ディレクトリのエントリは、各々種別と、ひとつもしくは複数の値をもつ属性から成る。例えば、PKI が証明書を配布するためにディレクトリを使う場合、エンドユーザの X.509 公開鍵証明書は、通常、ディレクトリ項目中の「証明書の対象である DN をもつ "userCertificate" 種類」の属性値として保管される。

- X.509

ITU-T 勧告。データ発信元認証サービスとピア主体認証サービスを提供しサポートするフレームワークを規定する。X.509 公開鍵証明書、X.509 属性証明書、X.509 CRL についてのフォーマットを含む。(ISO における同等物は、IS 9498-4。)

X.509 は、2 つのレベルの認証を記述している。パスワードに基づく「シンプル認証」と、公開鍵証明書に基づく「ストロング認証」。

- X.509 v3

X.509 v1 か v2 か v3 によって規定されたフォーマットのひとつで表現された公開鍵証明書。(X.509 公開鍵証明書 についての v1 と v2 の指定は、X.509 CRL についての v1 と v2 の指定と、X.509 属性証明書についての v1 の指定によって、支離滅裂なものとされた。)

X.509 公開鍵証明書は、一連のデータ要素を含み、そのシーケンスに基づいて計算されるデジタル署名をもつ。この署名に加えて、3 つのバージョンすべてが、下記の 1 から 7 までの要素を含む。v2 と v3 証明書のみが、8 と 9 も含む可能性があり、v3 のみが 10 を含む可能性がある。

以上