PKI の構成とその構成における秘密鍵の受け渡し手法に関する提案

HAYASHI yu-ichi
Core and Information Technology Center

1 はじめに

ネットワーク上での個人の認証，通信の暗号化などを行う場合それぞれの通信に対して個別の方法を利用することは非常に煩雑であり，かつそれらを通信や認証ごとに管理運用することは非常に困難である．PKI(Public Key Infrastructure)を利用することによりそれらの手間を軽減させ，多種多様な目的に公開鍵基盤を利用した通信，認証を行うことができる．

2 PKI を構成する機関の仕組み

PKI を構築する際必要となる機関は CA・RA・リポジトリからなる．これらの機関を組み合わせて PKI を構築し，エンドエンティティ(ユーザ)はリポジトリから取得した公開鍵証明書を利用し，暗号化電子メール（S/MIME），IP セキュリティ(IPSec)，Web 利用における通信の暗号化（SSL）に利用することができる．

以下各機関の働き，仕組み，構成について述べる

2．1 認証局（Certification Authority，CA）

ユーザ A から申請のあった公開鍵とユーザ A の情報に対し，CA のポリシーに適合しているかチェックを行い，それをクリアしていれば申請のあった公開鍵に対して証明書を発行する．CA は公的証明機関として信頼されていることが前提であり，CA により発行された証明書は CA の署名があるため通信途中で改ざんされればそれがわかり，またユーザ A の情報も証明書に含まれているため，改ざんの検出はすぐに行うことができる．また上記で記述したポリシーに関しては CA が自ら決定するものであり，CA ごとにポリシーは異なる．また発行したユーザ A の公開鍵が失効した場合には CA は CRL を発行し，それをリポジトリに格納することによって各ユーザはユーザ A の証明書の失効を知ることができる．また CA 間で相互認証を行うことにより他 CA が発行した証明書に関しても信頼できるようになる．上記からも察することができるように CA は非常に高いセキュリティで守られなければならない．なんらかの理由で CA の秘密鍵が流出したり，CA 本体が乗っ取られたりした場合はその CA により署名された公開鍵証明書はすべて失効する．

今回 OpenSSL[1]を利用することによりローカル CA を構築した．また CA を構築する際 CACAnet 福岡[2]により発行されている文章を参考にした．これにより発行される証明書のフォーマットは次のようになっている．

標準フィールド	バージョン
	シリアル番号
	証明アルゴリズム
	発行者名
	有効期限
	サブジェクト
	公開鍵情報
拡張フィールド	
署名フィールド	

表：CA により発行される X.509 証明書

2．2 登録局(Registration Authority，RA)

RA はユーザからの登録申請を CA に伝えるエンドエンティティと CA の中間に位置する機関である．ここではユーザの公開鍵への CA の署名への適合性や，リポジトリへの登録の許可などを行います．前項で記述した CA は基本的に証明書の発行・失効リストの発行とリポジトリへの登録という作業は RA からの依頼があった場合は自動で行い，人の手は一切介入しない構成になっています．RA は管理者がユーザへの証明書発行に関する判断と許可を与えるという位置づけになっています．

今回は RA では ApacheSSL による Web サーバが稼働しており，ここでユーザとの間はサーバ認証を用いた SSL の通信を行い，CA との間は SSH を用いたトンネルで通信を保護しています．

2．3 リポジトリ

リポジトリは CA により発行された公開鍵証明書をあらゆるユーザが参照できるようにそれらが格納・公開される場所である．それにより CA により発行されたユーザの証明書はここに格納され任意のユーザがこれらの証明書と CA の証明書を取得することができる．また証明書失効リストもリポジトリに格納されるため，各ユーザの証明書を利用する場合には参照し利用することができる．

今回は OpenLDAP[3]を用いてリポジトリを構成した．

またリポジトリを構築する際にも CACAnet 福岡により発行されている文書を参考にした．

2．4 エンドエンティティ

エンドエンティティとはここではユーザという扱いで考えることにする．主に公開鍵に証明を求め，それらを利用する立場にあるものである．

3 PKI の運用構成図[4]

PKI を運用する際，構成図のように各機関を配置し全体を構成するが，公開鍵と対になる秘密鍵を生成できないユーザに対して，どのように秘密鍵を受け渡すかという問題がある．この秘密鍵を CA で生成した場合ユーザに対して安全にこれらを届けることは非常に困難である．現在では生成した秘密鍵をフロッピーなどの媒体によりエンドエンティティへの配布を行っているが，エンティティの数が増えれば増えるほど配布が困難になるためにここではより汎用的な配布方法を提案する必要がある．

4 秘密鍵の安全で，効果的な配布方法

秘密鍵を配布する上で守らなければならない点は

- 秘密鍵を配布するユーザ本人であるかどうかの特定
- 配布経路上でその秘密鍵が改ざん，盗聴されてはいけない

と言う点である．

上記の 2 点を満たした上で考えられる配布方法をここで提案する.

4. 1　　連想フレーズによるユーザの特定

秘密鍵・公開鍵の生成と公開鍵への署名を求める要求を RA に行う場合ユーザはある質問を記述し，また別の方法で RA に対してそれに対する回答を伝達する. 別の方法とは配達証明で行ったり，電話で行ったりし，申請の経路とは違う方法で行う．これにようり秘密鍵の受け渡しの際に CA はユーザに対し質問をメールで行い，その回答を CA の公開鍵をもちいて CA に送り返しそれが一致すれば CA はその鍵をユーザに対して自らの秘密鍵でユーザの秘密鍵を暗号化し，ユーザはそれらを CA の公開鍵で開封する.

4. 2　　登録局の細分化による秘密鍵の受け渡し

現在のモデルでは CA は１つ, RA も１つとし構成を保っている. CA はほかの CA と相互認証することにより範囲を広げることができる．ここで RA を細分化し，ローカル環境ごとに RA を設置し，それらが CA から各ユーザの秘密鍵を受け取りユーザへの配布を行うという方法をとる．このモデルの場合 RA は CA から認証されており，安全であるという過程のもので行い，細分化された RA からユーザまでの距離（物理的距離も含め）がきわめて近いために配布を行う際非常に高い機密性を保つことができる．またなんらかのトラブルによりあるユーザの秘密鍵が配布時に漏洩した場合 CA はどの RA がユーザに配布を行ったかを特定することができ，すべての RA の機能を停止しなくとも，その RA により配布されたユーザを失効させることにより，情報漏洩における証明書の安全性の低下をくいとめることができる. 以下例を示す. ある大学に CA があり，RA は各研究室ごとに配置されそれらは CA から信頼されているという位置づけにある．各研究室のユーザは CA への秘密鍵と公開鍵の発行と証明を申請する際ローカルな RA に対し申請を行う．研究室単位ではユーザもそれほど多くないはずであるから RA 管理者は秘密鍵の配布を記憶メディアやセキュアな通信路を介して簡単にユーザに渡すことが可能になる. またこの構成で数個の研究室を束ねる学部ごとの RA を設置し，その管理者が学内 CA に申請を行うことでより信頼性のある証明書を作成することができる[5].

5　　おわりに

上記の提案した方法により安全に秘密鍵の受け渡しが行われても，エンドエンティティの秘密鍵の管理に問題があっては全く意味がない．各ユーザは十分に注意し，安全に秘密鍵を保管するようつとめるべきである.

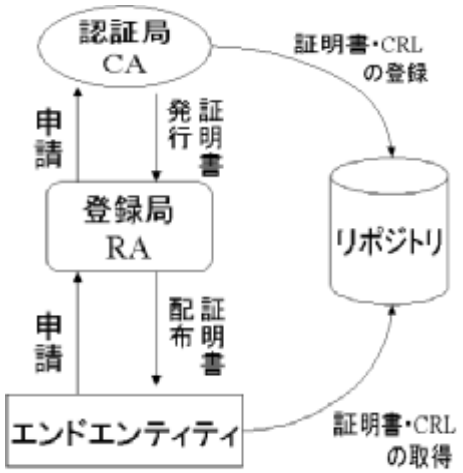
参考文献

[1] OpenSSL: http://www.openssl.org/

[2] CACAnet 福岡: http://www.cacanet.org/

[3] OpenLDAP: http://www.openldap.org/

[4] ローカル PKI の運用構成図



[5] 分散 RA による秘密鍵の配布