暗号ライブラリと認証局パッケージの開発

4T－4

若山公威*　奥野琢人*　岩田彰*　村瀬晋二**　鈴木春洋**
*名古屋工業大学　電気情報工学科
**（株）シーティーアイ　SI事業部

1. はじめに

近年、電子証明書を用いたセキュリティシステムのニーズが高まっている。このようなシステムを開発する場合、暗号関数に加え電子証明書を扱う関数を一から実装する必要がある。この実装のためには、開発者がX.509やPKCS[3]などの業界標準に精通することに加え、ベンダーごとの独自の拡張についても考慮しなければいけない場合があるため、開発に手間がかかる。既存のライブラリを用いることも可能だが、現状の商用ライブラリはライセンス料が高く、開発者と利用者に負担となる。フリーのパッケージでは、Eric Young、Tim Hudsonらによって開発されたSSLeay[1]が有名であるが、同パッケージは開発が終了しており不十分な点が残っている。SSLeayの後継の1つとしてOpenSSL[2]があり、熱心に開発が行われているが、SSLeay同様にドキュメントが少なく利用しづらい点がある。また、日本国内ではこのようなパッケージは皆無である。

我々は、一般に公開し広く使用してもらうことを目的として暗号ライブラリと認証局パッケージの開発を行った。

2. 暗号ライブラリ AiCrypto

本ライブラリは表1の暗号関数、ハッシュ関数をサポートしている。RSAは、最大2048bitまで使用可能である（コンパイル時に変更可能）。DESは64bit（56bit）、Triple-DESは192bit（168bit）、RC2では1024bitの鍵長をもっており、証明書等を扱うならば十分な機能を持っている。

実際、セキュリティ関連システムを開発する場合、暗号関数のみではなく、その周辺技術のライブラリも必要となる。

表1　サポート暗号・ハッシュ一覧

公開鍵暗号	RSA
共通鍵暗号	DES（ECB, CBC, CFB）
	3DES（ECB, CBC）
	RC2（ECB, CBC）
ハッシュ関数	MD2, MD5, SHA1, HMAC

表2　サポートファイル形式

証明書	X.509(DER,Base64) PKCS#7(DER)
CRL	X.509(DER,Base64) PKCS#7(DER)
証明書+秘密鍵+CRL	PKCS#12(DER)
証明書要求	PKCS#10 (DER,Base64)

本ライブラリのサポートするファイル形式を表2に示す。現状の一般に広く使用されているWWWブラウザやS/MIMEメーラに対応したツールやシステムを作るには、RSA Data Security社が提唱しているPKCS（Public-Key Cryptography Standards）、CCITTのX.509に対応させる必要がある。本ライブラリは、このPKCSとX.509に対応しているため、実用的なシステムを容易に開発できる。

PKCSやX.509では、各種フォーマットはASN.1という抽象構文により表現されており、DER（Distinguished Encoding Rules）によりエンコードされている。さらにBase64でテキスト形式に変換されている場合もある。本ライブラリではASN.1解釈、DER変換、Base64変換に関する関数も用意してある。

本ライブラリはソースを公開しており、一般的なUNIXならばどのOSでもコンパイルして使用することが可能である。現在、下記プラットフォームでの動作を確認している。

Solaris2.5.1（Sparc），Solaris2.6（x86），
IRIX5.3, BSD/OS 3.0, Linux（RedHat5.2）

3. 認証局パッケージ AiCA

AiCryptoを用いて、電子証明書を発行する認証

Implementation of Cryptographic Library and Certification Authority Package
Kimitake WAKAYAMA*, Takuto OKUNO*, Akira IWATA*, Shinji MURASE**, Shun-yo SUZUKI**
*Nagoya Institute of Technology
**CTI Co., Ltd.

局パッケージ AiCA を開発した。本パッケージを用いることにより、自己署名のローカル CA（Certification Authority）を容易に運用することが可能となる。

AiCA の大きな特徴としては、PKCS#12 形式ファイルを標準でサポートしている点が挙げられる。PKCS#12 形式は、証明書チェイン上の複数の証明書、CRL、秘密鍵をすべて保持できるファイル形式である。この形式は、一般に広く使用されている WWW ブラウザや S/MIME メーラで採用されているので、本認証局パッケージで作成した証明書を実際のアプリケーションに容易にインポートして使用することができる。

また、PKCS#12 をサポートすることにより、RA（登録局）を容易に運用することができる。RA がユーザに代わり鍵ペア作成をし、CA に対して証明書申請を行うことにより、ユーザの手間を省くことが可能となる。さらに、秘密鍵紛失時のためにバックアップを RA で保管することも可能である。

その他、本認証局パッケージには以下のような特徴がある。

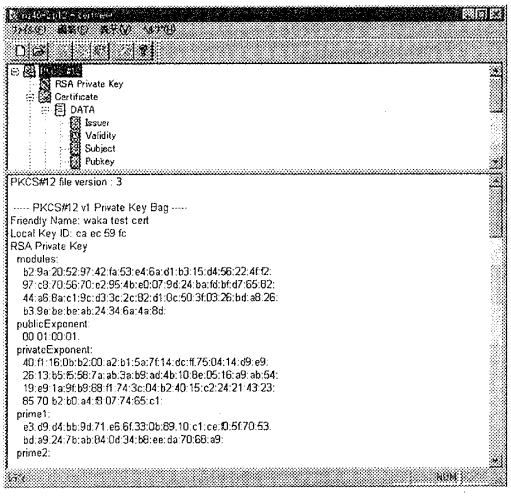
- 階層構造が可能。
- 証明書の廃棄をサポートし、CRL の発行が可能。
- シリアル番号を指定した証明書の発行が可能。
- シリアル番号や公開鍵をそのままにして有効期間だけを変更する証明書の更新が可能。
- Netscape 用の証明書拡張フィールドの設定が可能。

Netscape Communicator 4.6, Internet Explorer 5.0 付属の S/MIME メーラに、本認証局パッケージで作成した PKCS#12 ファイルをインポートして、暗号メール、電子署名付きメールのやりとりができることを確認した。

その他、本認証局パッケージには、証明書を管理・使用する上で便利な、以下のようなツールを含んでいる。

- 証明書変換ツール
  以下のような証明書、CRL、秘密鍵のファイル形式相互変換を行う。
  PKCS#12→証明書＋秘密鍵＋CRL
  証明書＋秘密鍵＋CRL→PKCS#12
  PKCS#7 証明書/CRL→X.509 証明書/CRL
  X.509 証明書/CRL→PKCS#7 証明書/CRL
- 証明書表示ツール
  証明書、CRL、証明書要求、PKCS#12、秘密鍵（SSLeay 互換）の各ファイルをテキスト表示する。Windows 98/NT 用の GUI 版も用意している（図 1）。
- 証明書検証ツール
  CA 証明書と CRL を用いてユーザ証明書の検証を行う。上位 CA の証明書も再帰的に検証する。
- ASN.1 形式解析ツール
  DER 形式のファイルを、ASN.1 文法解析して表示する。X.509 や PKCS#7 証明書, PKCS#12 ファイルの中身の表示も可能である。

図 1　証明書表示ツール



4 おわりに

本論文では、我々が開発した暗号ライブラリ AiCrypto と、このライブラリを用いて開発した認証局パッケージ AiCA の紹介をした。

AiCrypto, AiCA は、日本国内での学術目的のための使用に限って利用を許可しており、以下の URL から取得できる。

http://mars.elcom.nitech.ac.jp/

今後、更なる機能強化とメンテナンスを行っていきたいと考えている。多くの方に本ライブラリ、認証局パッケージを用いて様々なセキュリティ関連システムを開発していいただき、セキュリティ技術分野で貢献できれば幸いである。

参考文献

[1] http://www.ssleay.org/ssleay/
[2] http://www.openssl.org/
[3] http://www.rsa.com/rsalabs/pubs/PKCS/