PKI暗号ライブラリにおけるICカードの利用(3)
－ 鍵管理 －

2L－6

齋藤 和美 、榊原 裕之 、太田 英憲 、辻 宏郷
三菱電機(株) 情報技術総合研究所

1. はじめに

今回、PKI 暗号ライブラリを拡張し、IC カードを利用可能とした[1]。本稿では、PKI 暗号ライブラリを構成するライブラリ群の一つであり、鍵管理機能を提供する KeyStore ライブラリに関して、ライブラリの構成や機能、IC カードを使用する際の鍵管理 API の要件及びライブラリへの適用について報告する。

2. KeyStore ライブラリ

KeyStore ライブラリは、PKI 暗号ライブラリにおいて、公開鍵に関する管理及び暗号処理を行う鍵管理機能を提供するライブラリである。

2. 1 KeyStore ライブラリの構成

KeyStore ライブラリは、一つの API モジュールと複数の拡張モジュール(Extension)から構成される(図 1)。拡張モジュールは、対応する鍵管理デバイスを用いて公開鍵の管理を行うモジュールである。利用者は、拡張モジュールを選択することによって、同一のインタフェースを通して、様々な鍵管理デバイスを用いた公開鍵処理を行うことが可能である。現在、ファイルシステム、ポータブル・フロッピー・ディスク、メモリ空間及び Microsoft CryptoAPI[3]の Key Database に対応する拡張モジュールを提供している。

2. 2 KeyStore ライブラリの機能

KeyStore ライブラリの機能を以下に示す。

- 公開鍵ペアの生成及び削除
- 公開鍵ペアの格納
- 公開鍵の検索
- 公開鍵を用いた暗号化及び復号

また、拡張モジュールによっては、格納されている公開鍵のアルゴリズムや鍵の構成要素を取得するための公開鍵パラメータ取得機能や、Private Key を用いたデータの暗号化時に利用者を確認するためのパスワード認証機能を提供している。

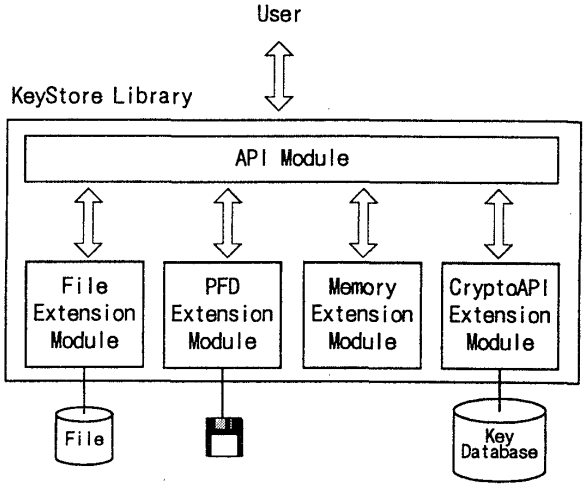

図1 KeyStore ライブラリの構成

3. IC カードを用いた鍵管理 API の要件

鍵管理デバイスとして IC カードを使用する際の鍵管理 API の要件を以下に述べる。

(1) 格納する鍵種類の選択

通常、IC カード内に格納可能なデータ容量には制限がある。このため、公開鍵について着目すると、公開鍵を IC カードに格納する際には、Private Key と Public Key のペアとして格納するか、Public Key は格納せず Private Key のみを格納するか選択可能であるべきである。例えば、公開鍵証明証と Private Key を IC カードに格納する場合は、Public Key の格納は不要である。

(2) 格納する鍵属性情報の指定

高いレベルの安全性が要求されるアプリケーションでは、Private Key に関する鍵情報を IC カードから取得及び削除する際には、そのレベルに応じた方法を取る必要がある。例えば、取得方法としては、取得不可、対称鍵を用いて暗号化することで取得可能、暗号化なしで取得可能とする方法が考えられる。ま

Application of ICC to Cryptographic Library for Public Key Infrastructure (3) – Key Management –
Kazumi SAITO, Hiroyuki SAKAKIBARA, Hidenori OHTA, Hirosato TSUJI
Information Technology R&D Center, Mitsubishi Electric Corporation

た、削除に関しては、削除不可、削除可能とする方法が考えられる。このような公開鍵に関する属性情報を、IC カードに格納する際に、公開鍵自身の情報に加えて指定できなければならない。

4. KeyStore ライブラリへの適用

KeyStore ライブラリにおける IC カードを用いた鍵管理は、既存の API モジュールを拡張すると共に、PKCS #11[4]拡張モジュールを新たに開発することによって実現した(図 2)。

4. 1 API モジュールの拡張

従来の KeyStore ライブラリでは、格納する公開鍵の種類や属性情報は、拡張モジュールごとに全て固定のため、拡張モジュール内部で保持されており、利用者が指定する必要はなかった。今回、格納する公開鍵の種類と属性情報設定機能を API モジュールに追加し、利用者が指定可能とした。

4. 2 PKCS #11 拡張モジュールの開発

PKCS #11 拡張モジュールは、PKCS #11 に準拠するデバイスを鍵管理デバイスとして動作させるための拡張モジュールである。PKCS #11 とは、暗号トークンを用いた暗号ライブラリの業界標準規格である。今回、我々は、PKCS #11 に準拠するライブラリを同時に開発し、IC カードへのアクセスを実現した。

(1) セッション管理方式

PKCS #11 に規定されているセッションの管理方式として、以下の二方式を利用者が選択可能とした。

(a) 利用者がセッション管理を行う方式

例えば、鍵管理と併用して、証明証管理や利用者独自のデータ管理のために IC カードを用いる場合、本方式が適切である。

(b) KeyStore ライブラリがセッション管理を行う方式

例えば、PKCS #11 準拠の鍵管理装置[2]を鍵管理デバイスとして用いる場合、本方式が適切である。

(2) 他社製 PKCS #11 準拠デバイスとの互換性

今回開発した IC カード対応版ライブラリ以外の、他の PKCS #11 準拠デバイスも使用可能とするために、PKCS #11 ライブラリへ渡す情報の設定方法に工夫を施した。以下に、具体的な設定方法を示す。

◆ 鍵の属性情報の設定方法

設定する値がデフォルト値と同一の場合はデフォルト値を用いる。これは、デフォルト値のみ使用可能な PKCS #11 準拠デバイスを考慮したものである。

◆ パラメータチェックの緩和

生成する鍵サイズやパスワードサイズ等のパラメータチェックを拡張モジュール内では実施せず、PKCS #11 ライブラリ内で実施する。KeyStore ライブラリでの制限を無くし、多様な PKCS #11 準拠デバイスを使用可能とする。

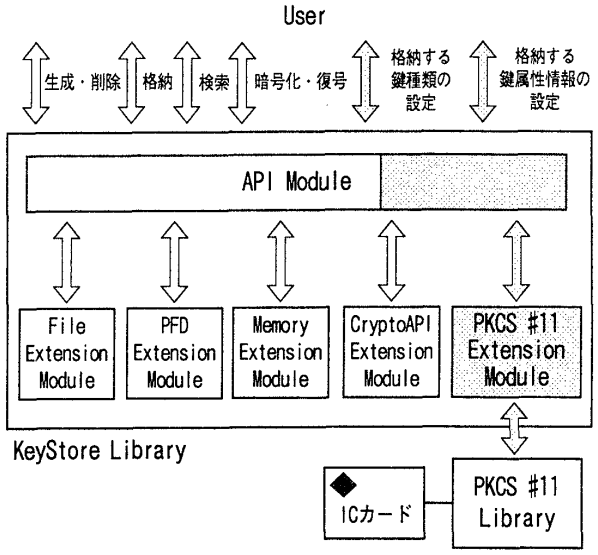

図 2 拡張 KeyStore ライブラリの構成

5. おわりに

本稿では、KeyStore ライブラリにおける IC カードを用いた鍵管理について述べた。今後は、拡張した KeyStore ライブラリに対し、他の PKCS #11 準拠デバイスを組み合わせた際の動作を検証していく。

参考文献

[1] 辻・榊原・齋藤・太田, "PKI 暗号ライブラリにおける IC カードの利用(1)－概要－", 情報処理学会第 58 回全国大会 2L-04, 1999.

[2] 竹原・中川路, "耐タンパー性を備えた暗号処理ボードの開発", 情報処理学会第 58 回全国大会 2L-08, 1999.

[3] Microsoft, "Microsoft CryptoAPI Version2.0 Application Programmer's Guide and Reference", 1997.

[4] RSA Laboratories, "PKCS #11:Cryptographic Token Interface Standard", Version 2.01, 1997.