2L－7

PKI暗号ライブラリにおけるICカードの利用 (4)
－ブラウザとの連携－

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

1 はじめに

我々はPKI (Public Key Infrastructure)で必要になる各種機能を実装したPKI暗号ライブラリを開発しており[1]、ICカードのAPIにPKCS #11[2]を採用している。一般的なWWWブラウザの中には暗号ライブラリとのインタフェースにPKCS #11を使用し、ビルトインのライブラリだけではなくサードパーティ提供の暗号ライブラリを追加組み込み可能となっているものがある。今回我々は、PKI暗号ライブラリ用ICカードをWWWブラウザで共用するための開発を行なった。本稿では、ブラウザに組み込む際の問題点と結果について報告する。

2 開発方針

今回、PKI暗号ライブラリとICカードを共用するWWWブラウザは、すでに暗号機能を持っている。また、PKCS #11では、仕様で定義されているすべての機能を実装する必要はないとされており、暗号ライブラリで提供している機能を呼び出し側のアプリケーションに知らせるためのインタフェースが定義されている。したがって、ブラウザがビルトインのライブラリと外部のライブラリを、必要に応じて切り替えて使用する構造になっていれば、暗号機能すべてを開発する必要はなくなる。そこで我々は、開発中のライブラリのトレースを解析して、ICカード内の秘密情報を安全に取り扱うために必要な最小限の機能を調査し、実装することにした。

また、ビルトインのライブラリと同様に一般ユーザがPINを初期化できるようにするためには、ブラウザにPKCS #11で定義されていないフラグを返す必要がある[3]。しかしながら、他のアプリケーションとライブラリを共用するためには、非互換の機能は望ましいことではない。そこで、このような非互換の部分はコンパイル時のオプションなどで、容易に切り離せるようにしておいた。

3 PKCS #11の概要

PKCS #11は暗号トークンを用いた暗号ライブラリのAPIの業界標準である。暗号機能はトークンとの間にセッションを確立して使用する。セッションは、使用する機能や状況に応じて、R/O (Read-Only)とR/W (Read/Write)の2種類がある。また、利用者と管理者を示す、UserとSO (Security Officer)という2種類の役割があり、それぞれが、セッションにログインすると、User セッション、SO セッションとなる。またログインされていないセッションは Public セッションと呼ばれる。ログインの状態はすべてのセッションで共有される。つまり、あるセッションにログインすると、すべてのセッションがログインしている状態になる。

4 問題点と解決法

ここでは開発の際に直面した問題のうちいくつかを挙げ、解決案を示す。

4.1 一般的な問題点

PKCS #11ではUserのPINを初期化する場合、SOがログインして設定することになっている。また、SOがログインできるのはR/Wセッションのみである。ところが、ブラウザはライブラリをロードするとすぐに、R/O Public セッションをオープンしている。ここで、別のセッションをオープンし、SOがログインすると、すでにオープンされているR/OセッションにSOがログインすることになってしまい、規定に反すること

Application of ICC to Cryptographic Library for Public Key Infrastructure (4) – Working with WWW Browsers –
Hidenori OHTA, Hirosato TSUJI, Hiroyuki SAKAKIBARA, Kazumi SAITO
Information Technology R&D Center, Mitsubishi Electric Corporation

になる。この問題を解決するには、SO がログインしないようにするか、SO がログインする際に他のセッションをクローズする必要がある。すると次のような方法が考えられる。

- ブラウザが User に PIN を初期化させるようにするフラグを返す。
- IC カードに前もって PIN を設定しておく。
- 最大セッション数を 1 に設定する。

4.2 IC カード特有の問題点

ライブラリのトレースを解析した結果、ブラウザは、抜き差しなど、IC カードの状態を調べるための API を頻繁に呼び出していることがわかった(図 1)。ところが、我々のライブラリでは、処理の途中で IC カードがリーダ・ライタから取り出されたことを検出するために、API の単位で、IC カードのオープン、クローズを行なっている。そのため、IC カードとの間に通信が生じる。一度にかかる時間はたかだか数十～数百 msec であるが、頻繁に呼び出されると速度低下に対する影響が問題となる。改善案としては、例えば IC カードに格納されている情報のうち秘密情報以外は、読み出した情報をメモリ中にキャッシュすることによって、極力 IC カードへのアクセスを減らすといった方法が考えられる。

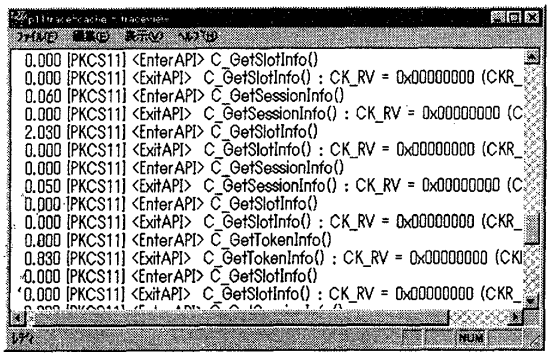

図1: ライブラリのトレース表示

5 ブラウザ対応 IC カードライブラリの実装

5.1 機能

解析結果に基づき、IC カードを使用した公開鍵暗号(RSA)の暗号化、復号化、署名、検証、鍵生成、そして、秘密鍵取り出しのための共通鍵暗号(DES-EDE3, RC2)を実装した。ブラウザに組み込むことによって(図 2)、以下の機能が使用可能となった。

- RSA 公開鍵対の生成及び証明書の申請・取得
- SSL におけるクライアント認証
- S/MIME における署名の生成及び暗号化メールの復号
- PKCS #12 フォーマットでの秘密鍵の取り出し・組み込み

5.2 問題の解決

前章で示した PIN の初期化に関する解決方法を試したところ、すべて正常に動作した。但し、他のアプリケーションとのライブラリの共用や速度性能などを考慮すると前もって PIN を設定しておく使用法が望ましいと考える。また、秘密情報以外のキャッシュを行なうと、モジュールの情報を表示するといった単純な操作において、300%近い速度の向上が見られた。また、ブラウザの起動、証明書の申請・取得、メールの署名、SSL のクライアント認証などの項目でも、速度が向上したことを確認した。

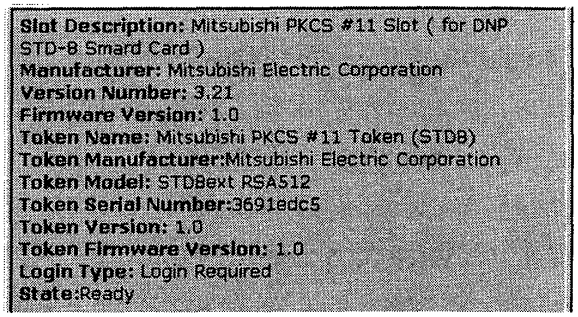

図2: 組み込み暗号ライブラリの情報

6 まとめ

PKI 暗号ライブラリ用 IC カードをブラウザに組み込み、ブラウザから利用可能にした。今後の課題として、さらなる速度の向上が挙げられる。

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] RSA Laboratories, "PKCS #11 Cryptographic Token Interface Standard," 1997

[3] Netscape Corporation, "Implementing PKCS #11 for the Netscape Security Library," http://developer.netscape.com/docs/manuals/security/pkcs/pkcs.htm, 1998