2L－5

PKI暗号ライブラリにおけるICカードの利用(2)
－ 内部データ形式 －

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

1. はじめに

当社では、PKI 暗号ライブラリを拡張し、IC カード用 PKCS#11 ライブラリを開発することで、鍵管理・暗号処理デバイスとして、IC カードを使用可能とした[1]。本稿では、IC カードにおける、PKCS#11 ライブラリ用に設計したデータ形式の概要と考慮すべきセキュリティについて報告する。

2. IC カードについて

開発に利用した IC カードは ISO/IEC 7816[3]に対応しており、内部ファイル構造、セキュリティの設定方法もこれに準じた実装を行った。カードはタイプA、Bの2種類ある。表1に主な仕様を示す。

表1 IC カードの仕様

	タイプA	タイプB
暗号機能	Single-DES, RSA1024bit (private key のみ, 2秒以下で演算)	Single-DES, RSA512bit (1秒以下で演算)
容量	8Kbyte(ユーザ領域 6Kbyte)	8Kbyte(ユーザ領域 4Kbyte)
特徴		EF の削除が可能

3. IC カードのフォーマット

PKCS#11[2]用に設計したフォーマットの概要を説明する。カード内部は Master File(MF), Dedicated File(DF), Elementary File(EF, データ／PIN 用)と呼ばれるファイルで構成される（図1）。MF はルートのディレクトリ、DF はサブディレクトリ、EF は実データファイルに相当する。当 IC カードは DF を2階層まで創作可能である。

以下に各ファイルについて解説する。

3.1 EF

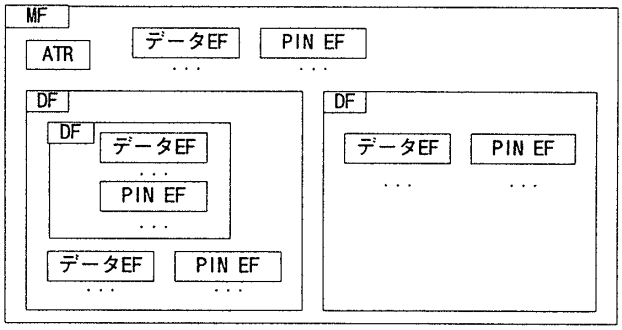
a. データ用 EF

PKCS#11 用に以下の情報ファイルを作成した。

① トークン情報 EF

PKCS#11 の C_GetTokenInfo で設定する情報であり、カードのモデル、製造番号等を格納する。

図1 ICカード内ファイル構成



② バージョン情報 EF

専用のフォーマッタのバージョン番号を格納する EF である。PKCS#11 ライブラリは、この情報を読むことでフォーマットのバージョンを識別し、ライブラリのバージョンとの整合性をチェックする。

③ オブジェクト EF

PKCS#11 における Data, Certificate, Key 属性のトークンオブジェクトを格納するファイルであり、C_CreateObject 関数等で動的に創作される。

④ オブジェクト個数情報 EF

③の各属性のオブジェクトに関して、格納個数の上限値を指定する EF である。各オブジェクトは、アクセスするために USER のログインを必要とする Private 属性、USER のログインは不要である Public 属性のどちらかを保持する。当ファイルは、③の各属性のオブジェクトごとに、Public/Private 属性を区別して、格納個数の上限値を指定可能である。アプリケーション毎に、必要とするオブジェクトの種類の比率が異なる場合があるので、当ファイルを最適化することで、IC カードのメモリを効率よく利用することができる。

b. PIN 用 EF

① SO PIN 用 EF

PKCS#11 では、トークンと USER PIN の初期化を行う Security Officer(SO)という管理者を規定し

Application of ICC to Cryptographic Library for Public Key Infrastructure (2) – Internal format –
Hiroyuki SAKAKIBARA, Hirosato TSUJI, Kazumi SAITO, Hidenori OHTA
Information Technology R&D Center, Mitsubishi Electric Corporation

ている。当EFはSO用のPINを格納する。

② USER PIN用EF

USER用のPINを格納する。当PINの初期化はSO権限で行い、変更はUSER権限で行えるように、EF創作時にアクセス制御用の属性を設定する。

3.3 DF

a. PKCS#11用DF

PKCS#11のオブジェクトを管理するためのDFをオブジェクトのPrivate/Public属性別に設けた。使用したICカードでは、DFの創作時に、DFへの書き込みのアクセス権を設定できるので、オブジェクトの属性ごとにDFを分けておいた方がセキュリティを保ち易い。実装では、Private属性オブジェクト用DFへの書込みは、USER PINの認証が成功した場合にのみ可能とした。Public属性オブジェクト用DF書き込みはアクセスフリーとした。

b.アプリケーション用DF

PKCS#11ライブラリを使用しないで、ICカードドライバを直接利用して情報を読み書きしたいというアプリケーションのために、MF直下に作業用DFを作成した。このDFへの書込みはアクセスフリーにする。このようなアプリケーションが複数存在する場合は、当DF下に、さらに、アプリケーションごとに専用のDFを作成し、その中でEFの管理を行う。ICカードの構造上、DFの階層は2段（MF-DF-DF）である。

4. オブジェクトのセキュリティ

4.1 実現方法

ICカード対応PKCS#11ライブラリにおいて、PKCS#11で規定されるオブジェクトへのアクセス制御の実現方法は2種類ある。

① PKCS#11ライブラリで論理的に実現する方法

ライブラリが、現在のログイン状況とアクセス対象のオブジェクトのPrivate/Public属性やオブジェクト固有の属性を内部で記憶しておくことで、オブジェクトへのアクセス制御を実現する。

例1：Private属性のPrivate Keyオブジェクトへのアクセスは、USERでログインしている状態でないと不可能である。例2：USERでログインしていても、構成要素の属性がCKA_SENSITIVE=TRUEであれば、その要素はそのままではICカードから取り出せない。

例3：CKA_DECRYPT=TRUEならば復号演算は可能である。

これらの様な、PKCS#11特有の木目細かなアクセス制御に関しては当方法を用いる。

② ICカードのOSの機能を利用して実現する方法

ICカードのOSの機能として、データ用EFを創作する時に、読み／書きのアクセス制御のためのPIN用EFを指定可能である。この機能を利用し、Private属性のオブジェクトを創作する時に、対応するデータ用EFにおいて、USER PIN用EFを読み書きのアクセス制御のためのEFとして指定する。この指定により、実際にUSER PIN用EFが認証されなければ、データ用EFへはOSレベルでアクセスが不可能となる。

本実装では、①と②を併用することによりアクセス制御を実現している。①のみの実装であると、ICカードのドライバで直接EFを参照される可能性がある。

4.2 フォーマット情報とセキュリティ

4．1の方法により、データ用EFへのアクセスは、PIN用EFの値が露呈しなければ不可能となる。しかし、PIN用EFに対してBrute Force Attackを可能とするような情報、例えば、ファイル番号、そのEFが存在するDFの名前／ID等は秘匿した方がセキュリティは向上する。従ってフォーマットに関する情報の守秘管理を考慮する必要がある。

5. おわりに

フォーマットの設計は、カードのセキュリティに関与するが、堅牢なセキュリティはパフォーマンスを低下させる場合もある。今後は、パフォーマンスとセキュリティを両立する設計方法の確立を課題としたい。

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] ISO/IEC 7816-4 Information technology-Identification cards-Integrated circuit(s)card with contacts- Part4 First edition 1995-09-01