PKI暗号ライブラリにおけるICカードの利用（1）

2L－4

－概要－

辻　宏郷、榊原 裕之、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

PKI（Public Key Infrastructure）は、公開鍵暗号技術を用いて電子署名や暗号化を実現するための基盤技術である。我々は、PKI に必要となる各種機能を実装した PKI 暗号ライブラリを開発してきた[1]。今回、公開鍵・公開鍵証明証の管理及び暗号処理デバイスとして、IC カードを使用するための拡張を行った。本稿では、拡張の目的、ライブラリの開発方針、開発モジュールの構成について報告する。

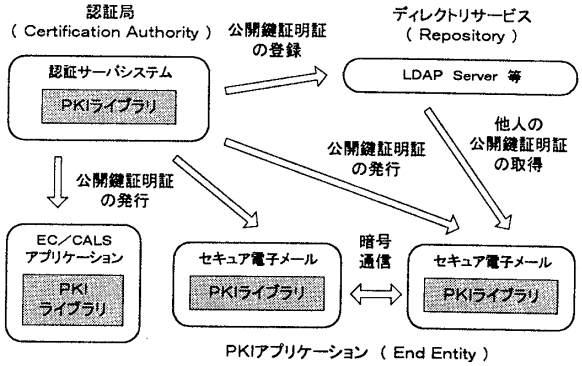

図1　PKIの構成要素とPKI暗号ライブラリ

2. PKI暗号ライブラリMCrypto

PKI は、公開鍵とその所有者の結び付きを証明する公開鍵証明証（public key certificate）を発行する CA（Certification Authority）、公開鍵証明証を配布するリポジトリ、公開鍵証明証を利用するアプリケーションである EE（End Entity）から構成されている（図1）。PKI 技術に基づく情報セキュリティシステムを開発するためには、公開鍵暗号や共通鍵暗号等の暗号アルゴリズムの実装に加えて、公開鍵や公開鍵証明証の管理機能、署名・暗号化メッセージ形式の作成機能等が必要である。MCrypto は、これらの機能を実装した PKI 暗号ライブラリであり、以下に示す特長を持っている。

(1) PKI に必要となる全機能を、基本暗号処理、鍵管理、電子署名、暗号化・鍵交換、ASN.1 符号化、証明証管理、証明証検証の各機能に分割して実装。

(2) 暗号処理、公開鍵証明証やメッセージの形式は、国際標準規格や業界標準規格に準拠。

(3) 各機能は、暗号アルゴリズムから独立した API と実際に暗号処理を行う CSP との二階層構成となっており、CSP の交換によって、暗号アルゴリズムの種類や強度、公開鍵や公開鍵証明証の格納デバイス、公開鍵証明証の検証方法等の変更や拡張が可能。

3. 鍵管理・暗号処理デバイスとしてのICカード

今回、PKI 暗号ライブラリ MCrypto における公開鍵や公開鍵証明証の格納デバイスとして、IC カードを追加した。IC カードは、既存の格納デバイスであるファイルシステムやポータブル FD 等と比較して、以下に示す利点がある。

(1) 第三者による鍵の盗用防止
使用しない時にICカードをリーダライタから抜いておくことで、鍵を他人に盗用されることを防止可能。

(2) 異なる場所・PC における鍵や証明証の共用
会社と自宅、本社と支社等の異なる計算機の間で、IC カードを持ち運ぶだけで、鍵や証明証を共用することが可能である。

(3) 鍵漏洩防止（カード内部における暗号処理）
鍵を用いた暗号化や復号は IC カード内部で実行される。鍵データを一旦 PC に読み出すことが不要となるので、鍵の漏洩を防止可能である。

(4) 複製の困難性
IC カードは複製が困難なので、許可なく鍵を複製することを防止した方針の下での運用が可能となる。

Application of ICC to Cryptographic Library for Public Key Infrastructure (1) – Overview –
Hirosato TSUJI, Hiroyuki SAKAKIBARA, Kazumi SAITO, Hidenori OHTA
Information Technology R&D Center, Mitsubishi Electric Corporation

4. PKI暗号ライブラリのICカード対応

4. 1 開発方針

(1) PKCS #11 API の採用

MCrypto では、公開鍵や公開鍵証明証の格納場所毎に「拡張モジュール」を用意することによって、格納場所の変更を実現している。今回の開発では、IC カード格納用拡張モジュールを作成する代わりに、IC カードのドライバ・ソフトウェアの上に、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 PKCS #11[6]の API 仕様に準拠したライブラリを作成した。そして、PKCS #11 仕様準拠のデバイスを格納場所とする拡張モジュールを開発した(**図2**)。PKCS #11 API を採用した狙いは、以下の通りである。

- ○ PKCS #11 に準拠する各種デバイス(異なる IC カードや鍵管理装置[5])に対応可能とする。
- ○ IC カード中の公開鍵や公開鍵証明証を、MCrypto を用いて開発したアプリケーションだけでなく、WWW ブラウザから利用可能とする[4]。

(2) 性能解析支援機能の実装

IC カード内部の暗号処理や PC・リーダライタ間の通信速度は低速であるため、IC カードを利用する PKI アプリケーションは、性能チューニングが不可欠である。アプリケーション開発過程における性能ボトルネック解析を支援するために、速度性能の統計情報を取得する機能を組み込むこととした。

4. 2 開発モジュールの構成

(1) IC カード版 PKCS #11 ライブラリ

PKCS #11 のセッション管理、鍵管理(公開鍵ペアの生成とバックアップ)、公開鍵証明証の管理、IC カード中の鍵を用いた暗号化と復号、任意形式データの管理の各機能を提供する。API は、PKCS #11 の Version 2.01 に準拠している。

(2) IC カード・フォーマッタ

IC カードに対して、PKCS #11 ライブラリで使用するためのフォーマットを行うユーティリティ[2]。

(3) PKCS #11 Extension for KeyStore ライブラリ

MCrypto において鍵管理機能を提供する API (KeyStore ライブラリ)用の拡張モジュール。PKCS #11 準拠のデバイスを用いて鍵管理を実現する[3]。

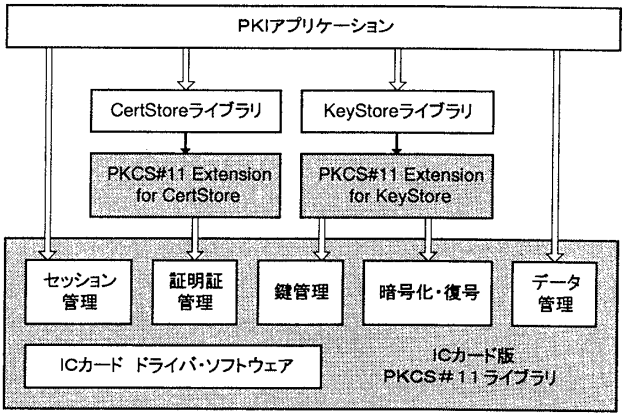

図2 ICカード対応PKI暗号ライブラリの構成

(4) PKCS #11 Extension for CertStore ライブラリ

MCrypto において証明証管理機能を提供する API (CertStore ライブラリ)用の拡張モジュール。PKCS #11 準拠のデバイスを用いて証明証を管理する。

5. おわりに

PKI 暗号ライブラリを拡張し、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。今後は、システム開発に適用すると共に、改良を進めていく。

参考文献

[1] H.Tsuji, K.Saito, H.Sakakibara, T.Yoneda, "Cryptographic Library Architecture for Secure Application Development", 電子情報通信学会研究報告 ISEC97-47, 1997.

[2] 榊原・辻・齋藤・太田, "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－", 情報処理学会第 58 回全国大会 2L-05, 1999.

[3] 齋藤・榊原・太田・辻, "PKI 暗号ライブラリにおける IC カードの利用(3)－鍵管理－", 情報処理学会第 58 回全国大会 2L-06, 1999.

[4] 太田・辻・榊原・齋藤, "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－", 情報処理学会第 58 回全国大会 2L-07, 1999.

[5] 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.

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