オープンなPKI対応ICカードを扱うオープンソースソフトウェアの紹介

2008.7.3

有限会社ロボック伊藤大輔

ROBOC

ICカードと関連する規格はとてもたくさん

規格名／番号	内容
PCSC	接触型ICカードリーダ/ライタのインタフェース仕様
PKCS#15	データフォーマット仕様
ISO/IEC 24727	ICカードを利用するプログラムの、プログラミングインタフェース仕様
ISO/IEC 7816-4	交換のための構成，セキュリティ及びコマンド
ISO/IEC 7816-8 JIS X 6320-8	セキュリティ処理コマンド
ISO/IEC 7816-9 JIS X 6320-9	カード管理共通コマンド
ISO/IEC 7816-15 JIS X 6320-15	暗号情報アプリケーション
GSC-IS	NISTによるICカード相互互換ソリューション
Java Card	ICカードのプログラムをJavaで記述する仕様
Global Platform	ICカード関連のサービス、機器、インタフェース仕様をまとめた規格
その他、いろいろ	

ROBOC

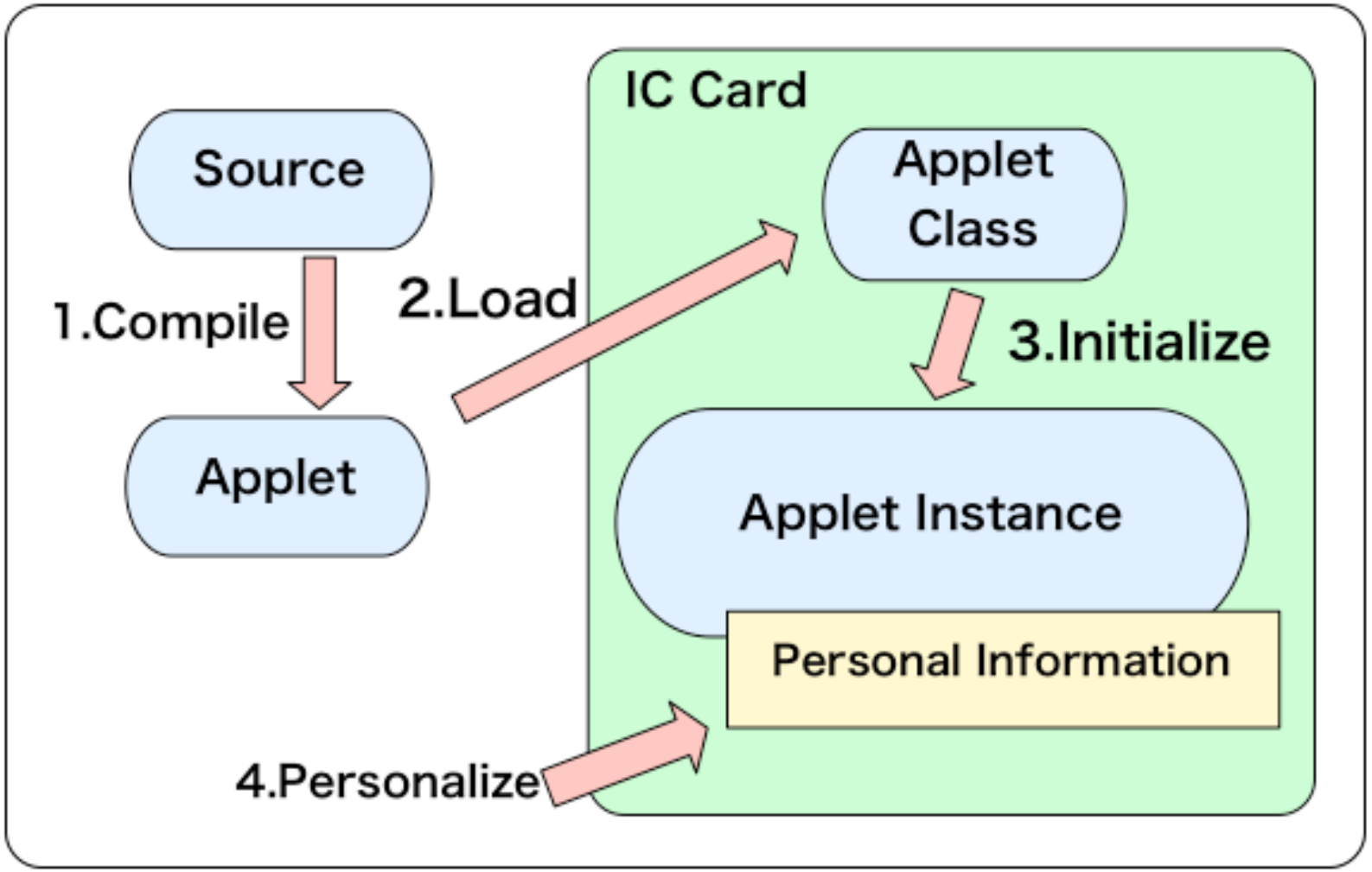
とにかく動かす

- 動かすことで、わかることもある
  - 仕様が公開されている
  - ドキュメントがたくさんある。ソースまである
- 出来ること
  - マルチプラットフォーム
    - Windows, Linux, Mac OSX
  - S/MIMEメール
  - SSLクライアント認証
  - ログイン（未検証）

ROBOC

ICカードを作る

やること


IC Card
Source
Applet
Class
1.Compile
2.Load
3.Initialize
Applet
Applet Instance
Personal Information
4.Personalize

ROBOC

ICカード(Javaカード)

NXP (PHILIPS) JCOP 31 V2.2/36K

JCOP-SmartCard as IBM implementation of the JavaCard 2.2.1 OS with 36kB EEPROM, With DES, RSA and ECC, Dual interface. IBM engineer sample card compatible which could be used to turn on IBM JCOP plugin for Eclipse. Product Details...

$15.00

Quantity: 1

Add to Cart

NXP (PHILIPS) JCOP 41 V2.2.1/72K

Min order 2 pcs

JCOP-SmartCard as IBM implementation of the JavaCard 2.2.1 OS with 72kB EEPROM, With DES, RSA, AES and ECC, Dual interface. IBM engineer sample card compatible which could be used to turn on IBM JCOP plugin fo Product Details...

$19.00

Quantity: 1

Add to Cart

送料40$

http://www.usasmartcard.com/

ROBOC

ICカードリーダ／ライタ

数千円くらい。持ち運ぶならドングル型の方が便利。

ROBOC

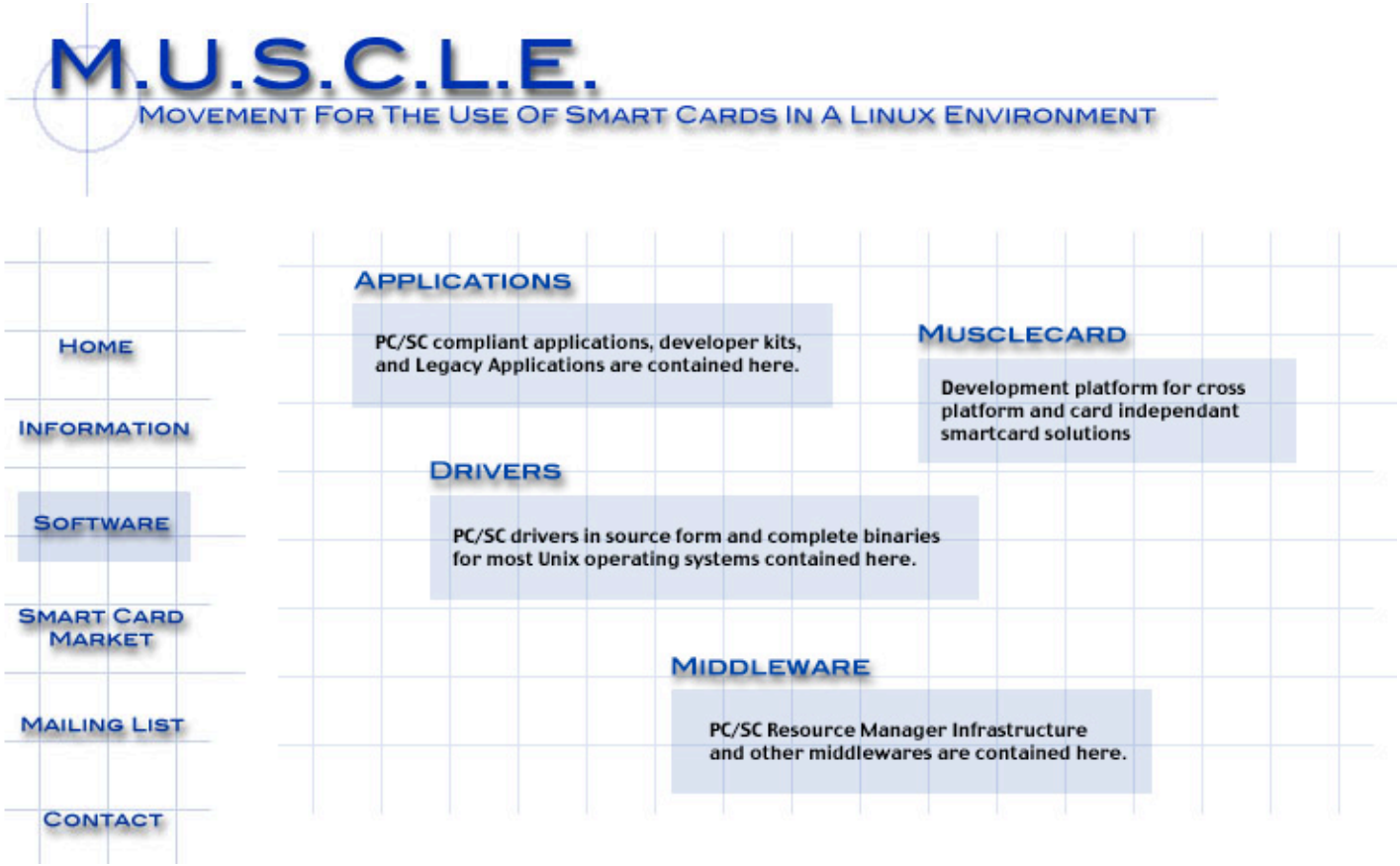
主要なソフトウエア

- OpenSC(linux,windows,macで動く）
  - http://www.opensc-project.org/
  - PKCS#11,PKCS#15対応ミドルウエア、ツール
- MUSCLEカードアプレット(javaソース)
  - http://www.linuxnet.com/
  - オープンソースのPKI対応JavaCardアプレット
- GPShell,GPLib(linux,windowsで動く。macでも動くらしいが未確認）
  - http://sourceforge.net/projects/globalplatform/
  - GlobalPlatform対応カードを操作するツール
- PCSC-lite(linux)
  - http://pcsclite.alioth.debign.org/
  - カードリーダを抽象化するAPI
- ID Ally(windows)オープンソースではない
  - http://www.identityalliance.com/identity_ally.ph
  - pkcs#11インタフェースの上にCrypto APIを提供

ROBOC

MUSCLE/とりあえず、何でもそろう

- http://www.linuxnet.com/



ROBOC

MCardApplet

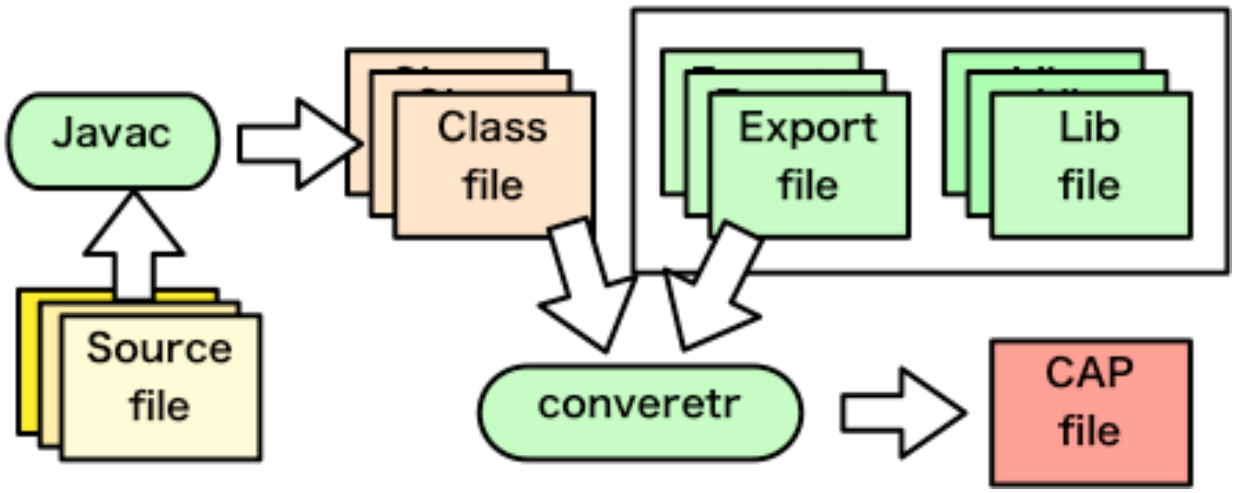
- MUSCLEカードエッジインタフェースを実装
  - これは、標準化団体が定めた仕様ではなく独自仕様。ただし全て公開されている。
- Java Card上で動くプログラム
- 5000ステップ
- Java言語（3つのクラス）
  - CardEdgeクラス
  - MemoryManagerクラス
  - ObjectManagerクラス
- http://www.linuxnet.com/musclecard/index.html

ROBOC

1.Compile
2.Load
3.Initialize
4.Personalize

JDK &JC

- JDK
  - http://java.sun.com/javase
  - Javaのソースコードをコンパイル
- JC
  - http://java.sun.com/javacard/
  - Appletを作るために必要なツールやクラスライブラリ



ROBOC

1.Compile
2.Load
3.Initialize
4.Personalize

GPShell

- Global Platform
  - The standard for smart card infrastructure
  - カード自体だけではなく、ICカードと関連する端末、アプリケーション、サービスなどの仕様
- GPShell
  - GlobalPlatform Card Specificationに準拠したカードに、細かい命令を送るためのプログラム

ROBOC

1.Compile
2.Load
3.Initialize
4.Personalize

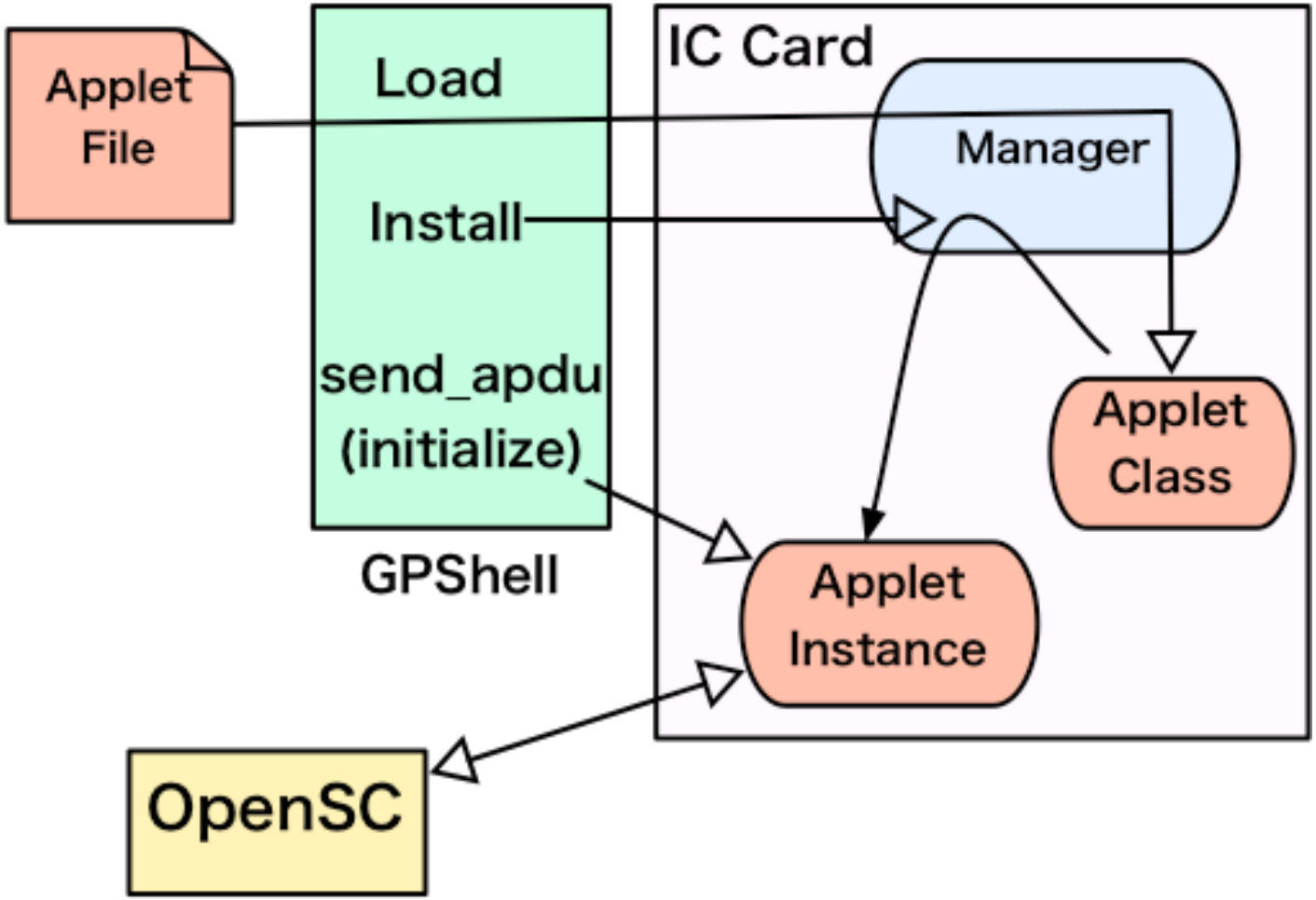
GPShellの機能

コマンド	機能
mode_201, mode_211	プロトコルのバージョンを設定
enable_trace	送受信しているAPDUをトレース
card_connect	カードに接続
open_sc	セキュアチャネルをオープン
select	アプレットを選択
load	アプレットをカードに送る
install_for_load	ロード済みのアプレットを、初期化する
install	ロードして、インストールする
get_status	カード内部のアプレットをリストする
send_apdu	APDUコマンドを直接カードと送受信する
その他	いろいろ

ROBOC

1.Compile
2.Load
3.Initialize
4.Personalize

GPShellがやること



ROBOC

1.Compile
2.Load
3.Initialize
4.Personalize

OpenSC

- OpenSCがやること
  - PINを設定
    - opensc-tool –s .... → APDUを直接発行
  - 私有鍵、公開鍵証明書をICカードにロード
    - pkcs15-init –E .... →カードを初期化（カードアプレットを初期化）
    - pkcs15-init –S <pcks#12> ... → pkcs#12ファイルをロード
  - PKCS#11 APIを提供

ROBOC

GPShellとOpenSC

- GPShellでアプレットを設定
  - アプレット自体のロード、インストール
  - PINの最低桁数や、何回間違えたらロックするのか？といったデータ
  - 生のカードをMUSCLEカードにする
- OpenSCでアプレットを利用
  - PINを設定
  - 証明書をロード
  - セキュリティ機能を利用(PKCS#11を提供)
  - MUSCLEカードを使う

ROBOC

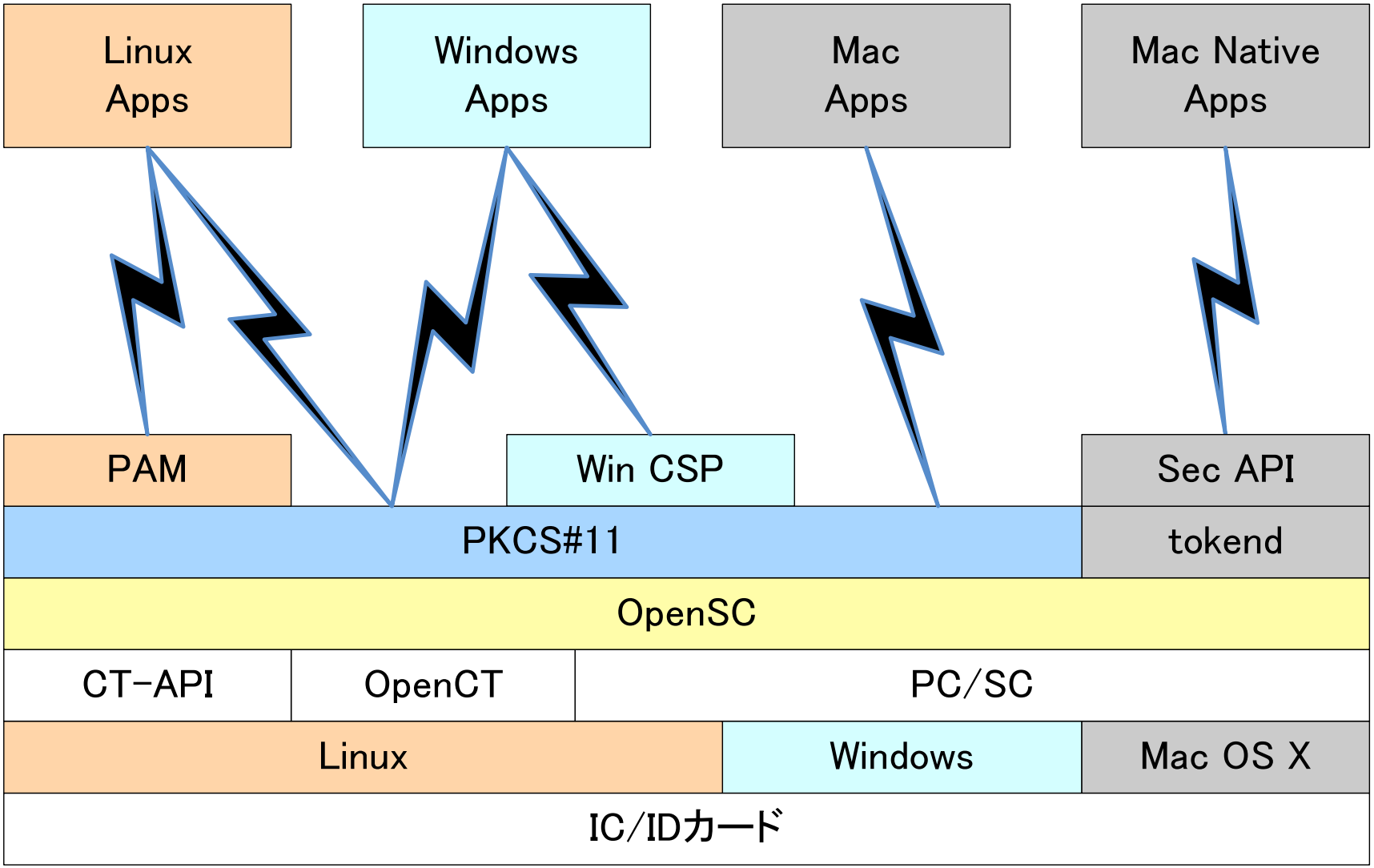
ICカードを使う

アプリケーション

- メーラ
  - S/MIME
- ウェブブラウザ
  - SSLクライアント認証
- ログイン
  - ログインWindow
- その他
  - デジタル署名など

ROBOC

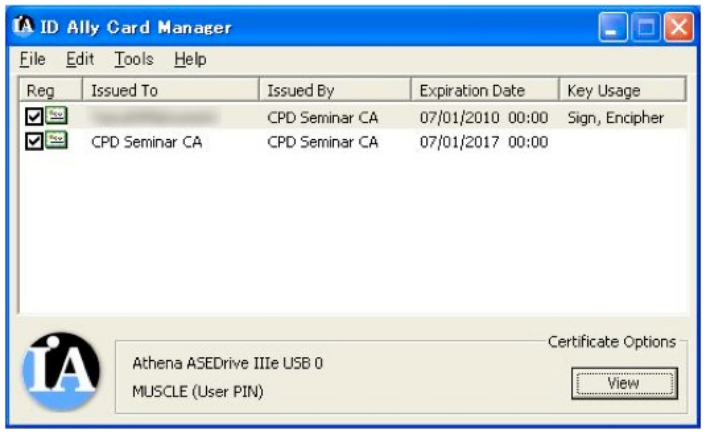
マルチプラットフォームで ICカードを利用する

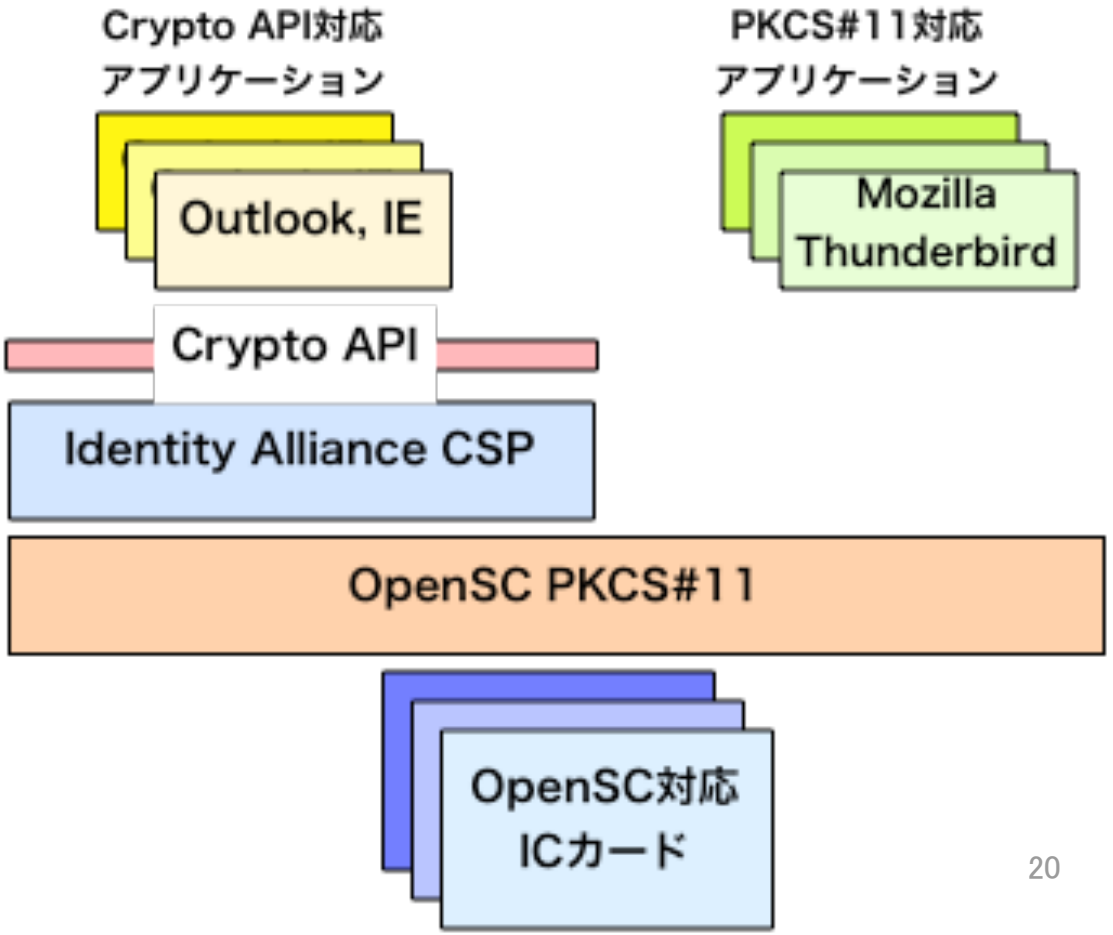


ROBOC

Windows:CryptoAPI& PKCS#11

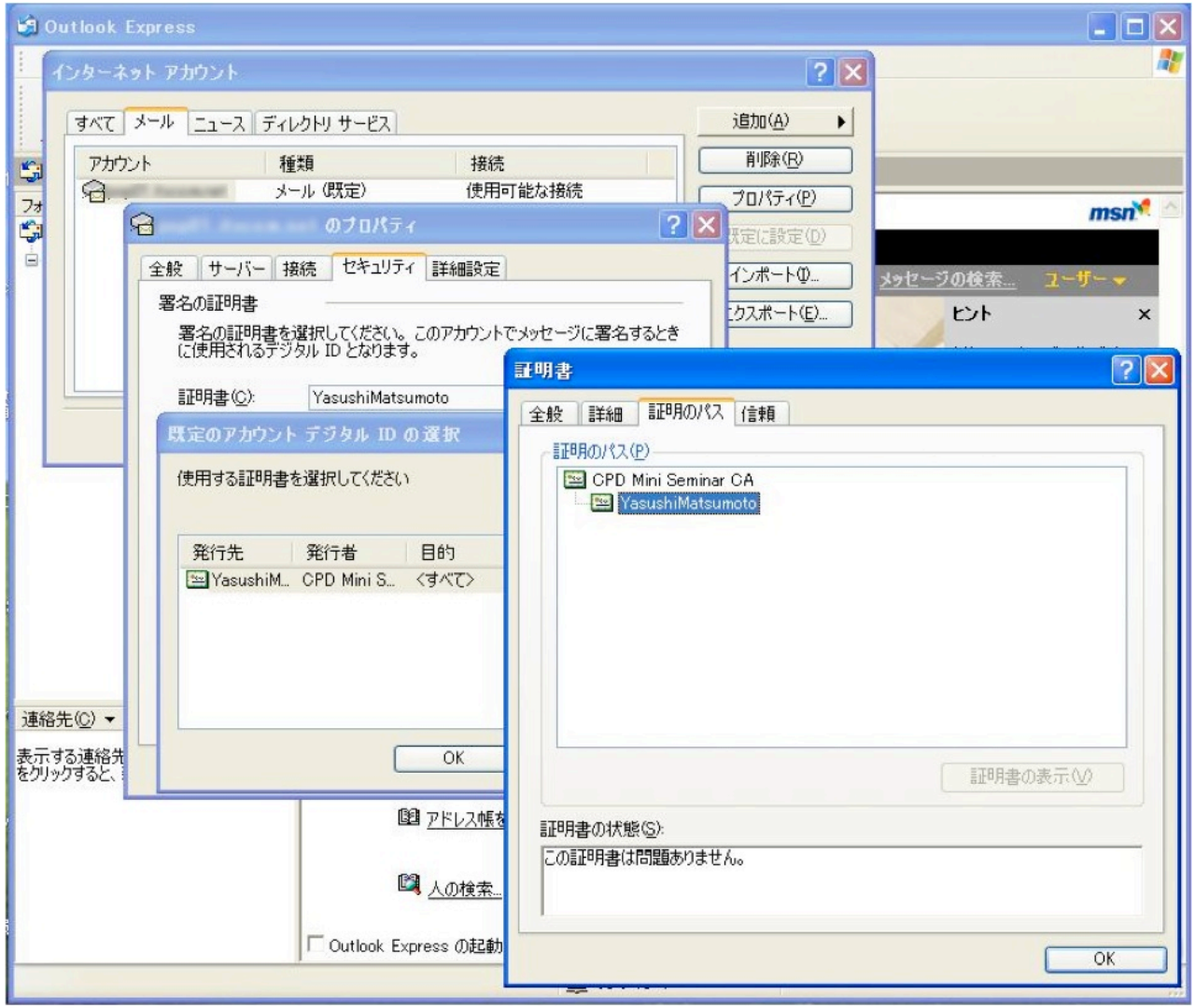
- ID Ally (CSP on PKCS#11)





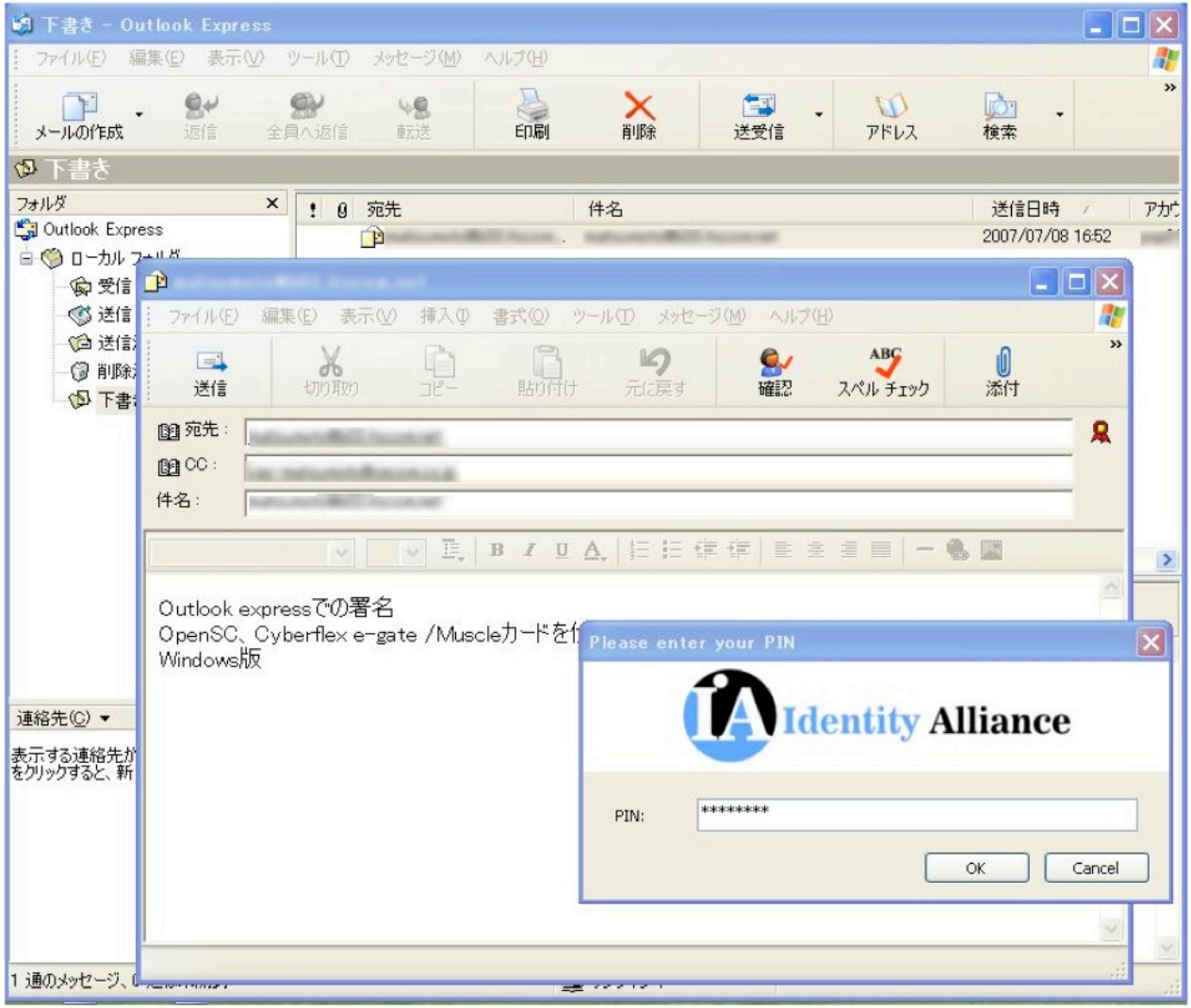
ROBOC

Windows Outlook Express(Crypto API)



ROBOC

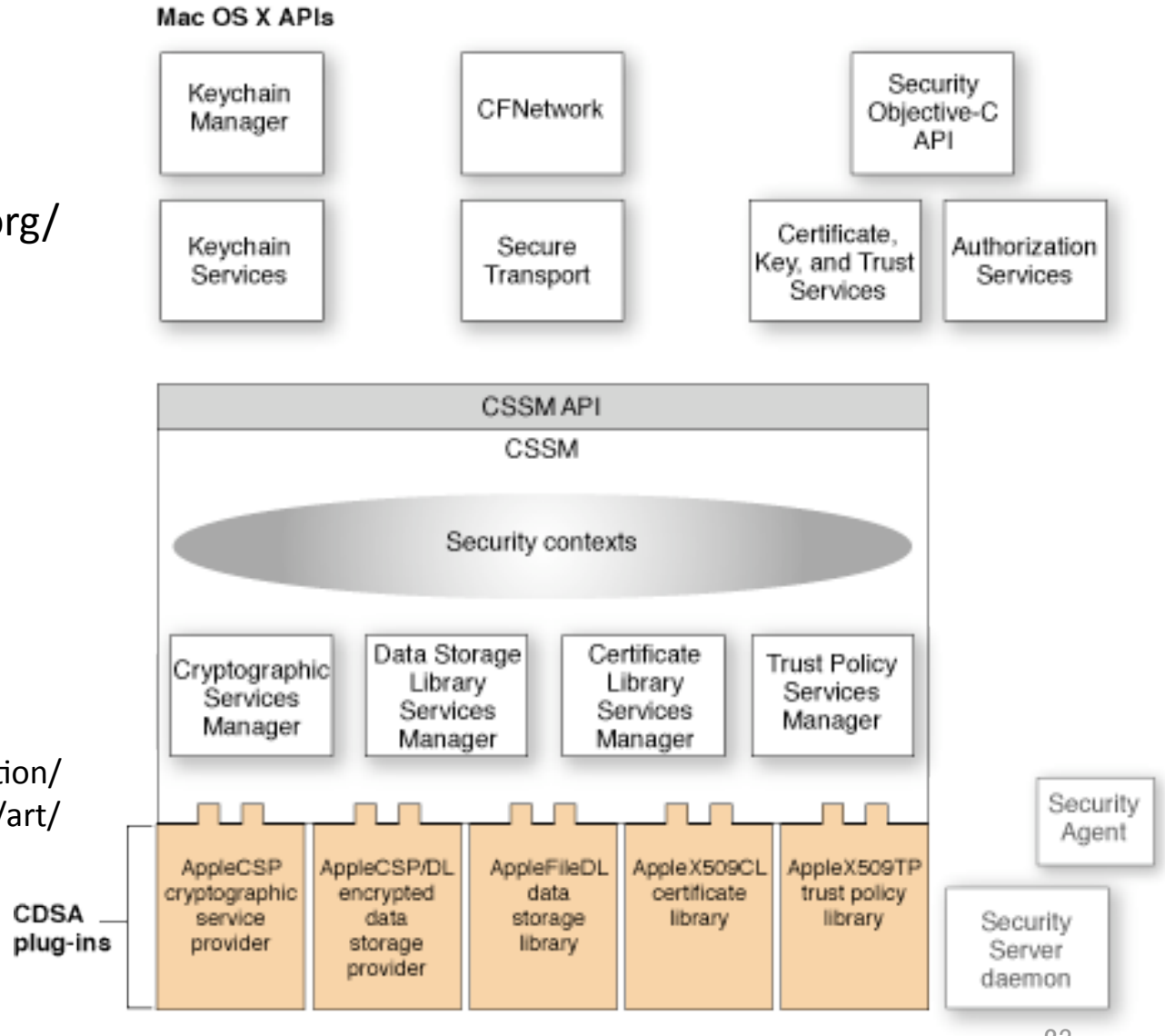
Windows Outlook Express(Crypt API)



ROBOC

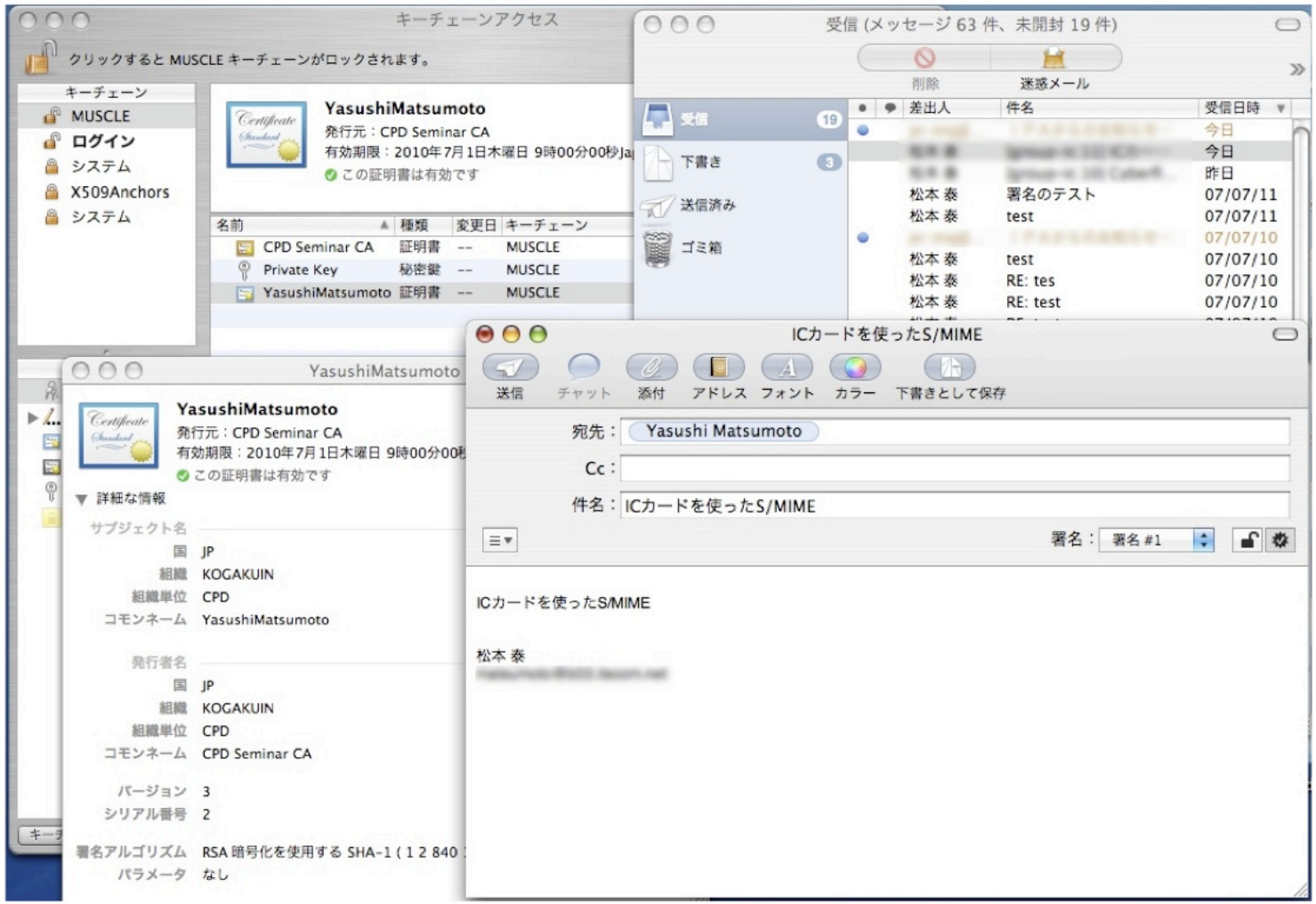
Mac OS X:CDSA & PKCS#11

- Common Data Security Architecture(CDSA)
  - http://www.opengroup.org/security/cdsa.htm



http://developer.apple.com/documentation/Security/Conceptual/Security_Overview/art/layered_arch_complete.gif

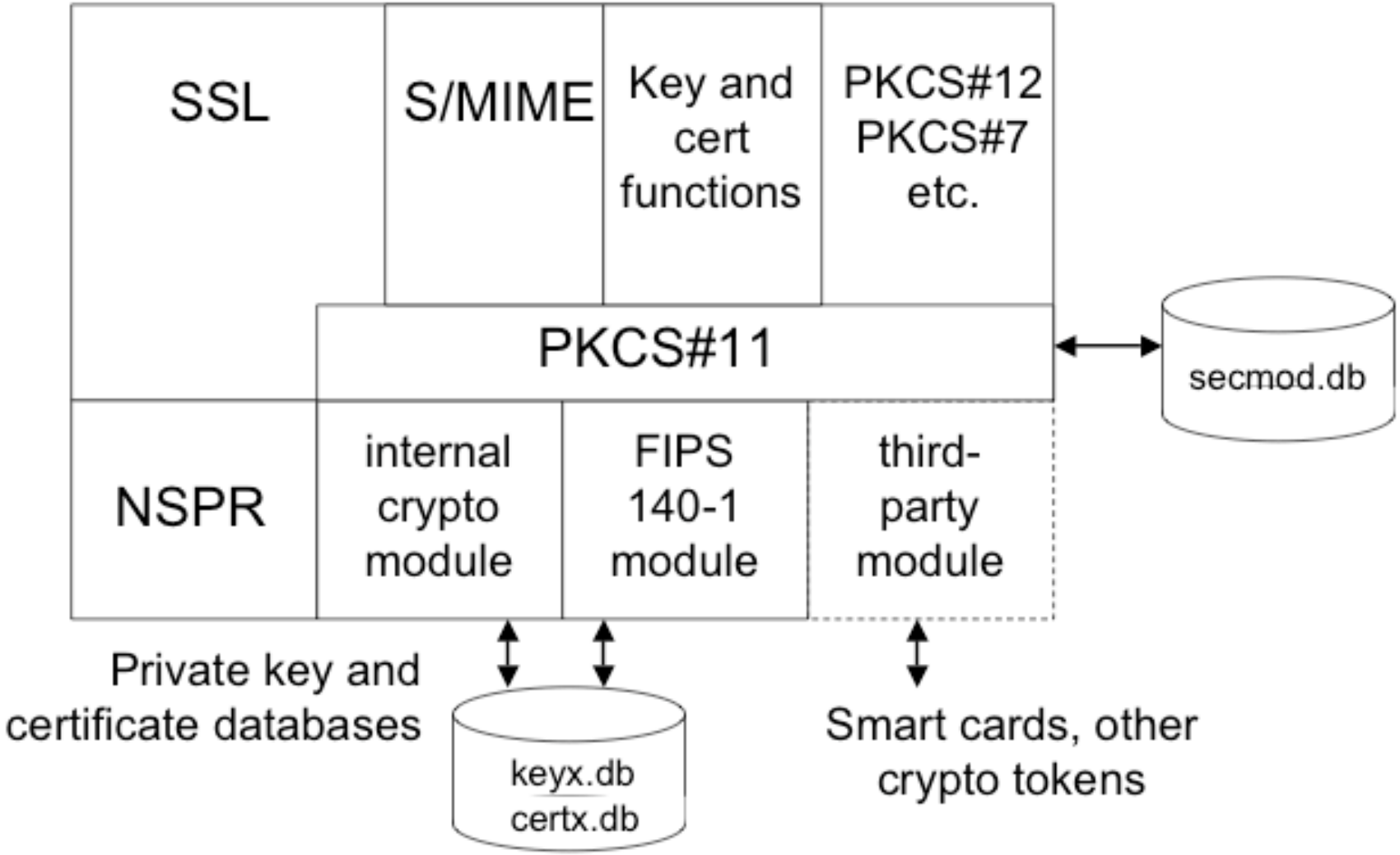
Mac OS X Mail



ROBOC

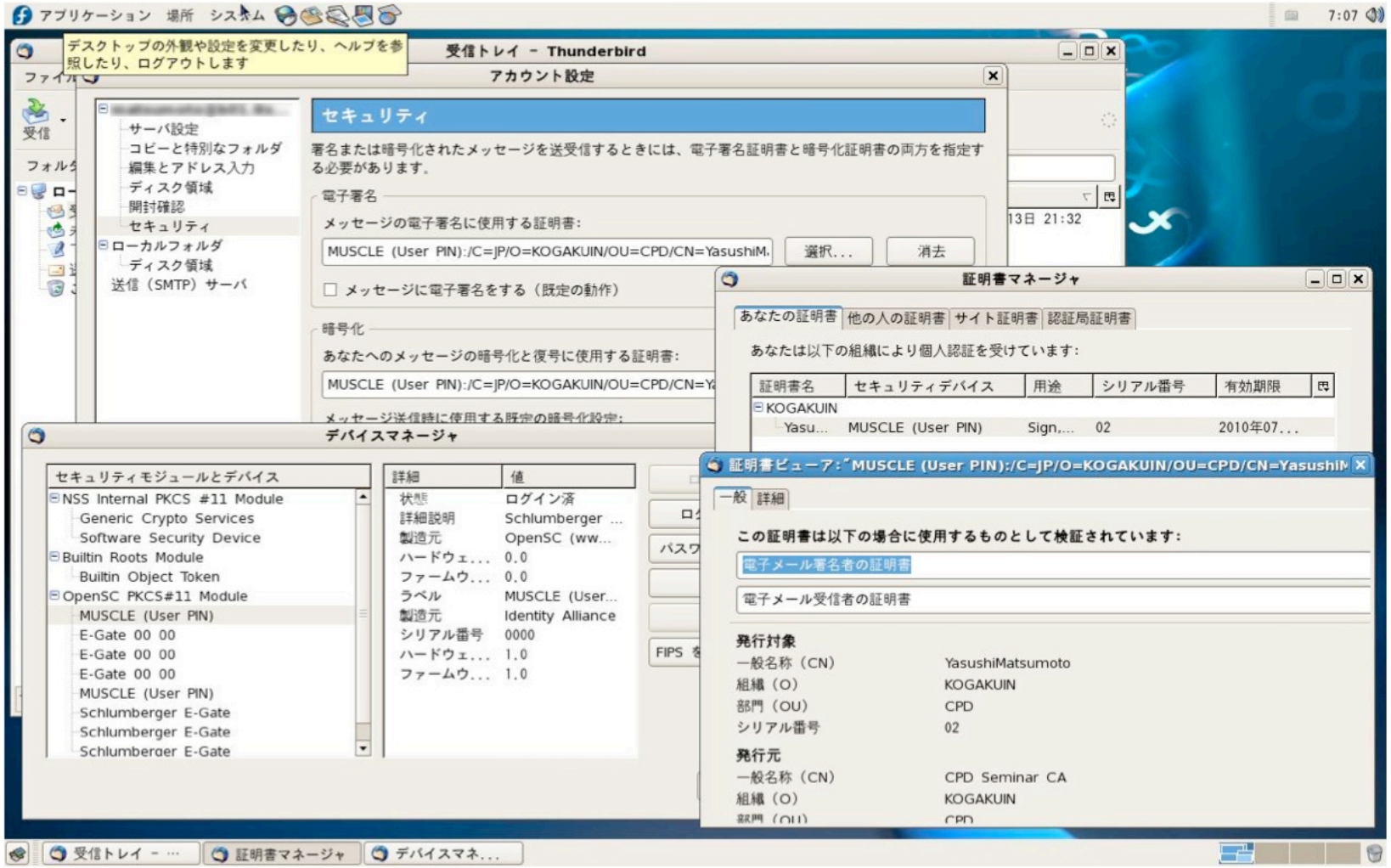
Linux: NSS & PKCS#11

Mozilla Network Security Services



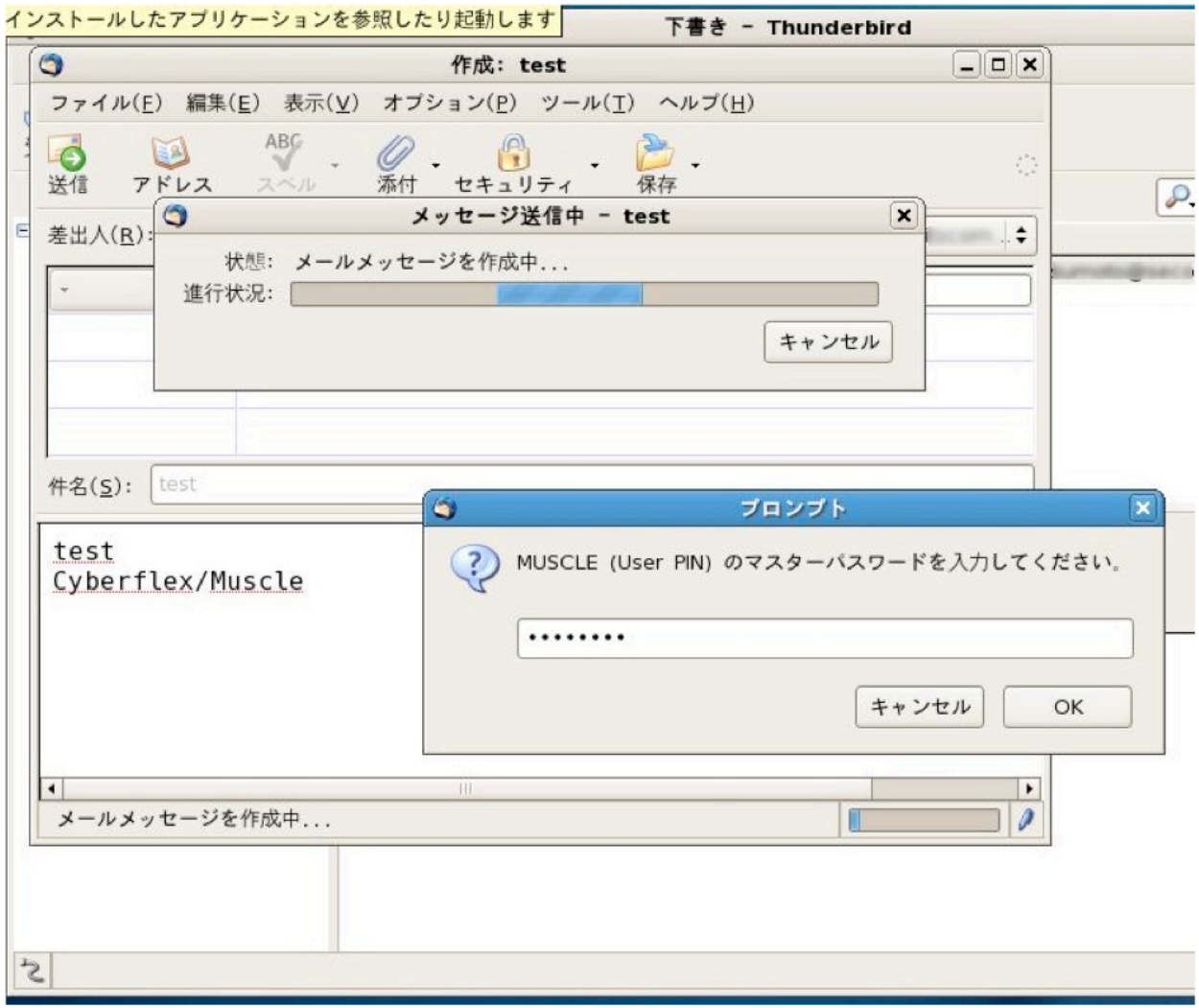
http://hecker.org/mozilla/mozilla-crypto-pki.pdf

Linux Mozilla Thunderbird



ROBOC

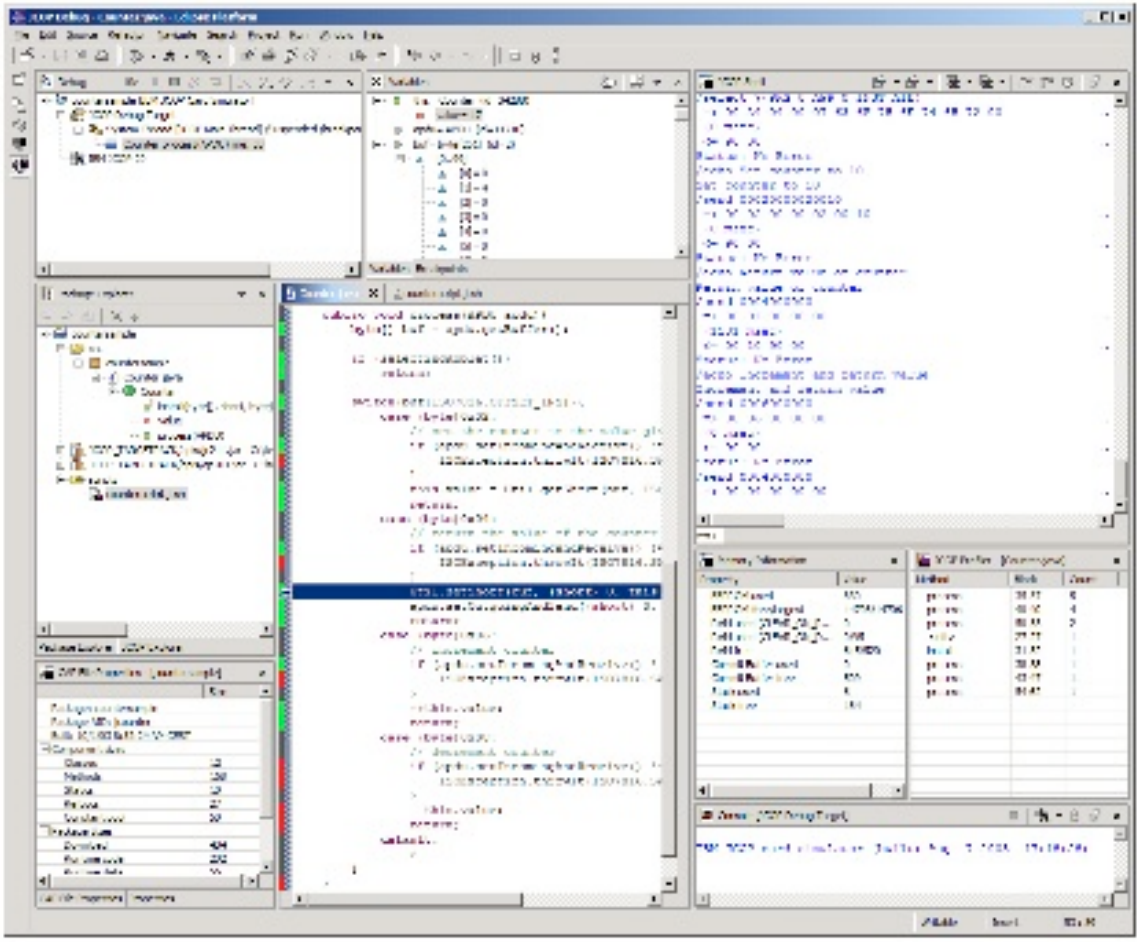
Linux Mozilla Thunderbird



ROBOC

開発ツール

- JCOPTool(eclipseplugin)
- JCOPエミュレータ
- デバッガ
- OpenPlatform(GlobalPlatform)用
- 以前はダウンロードできたが…



ROBOC

参考

- GlobalPlatform
  - http://www.globalplatform.org/
- OpenSC
  - http://www.opensc.org/
- Apple Developer Connection(Mac OS X Security Services)
  - http://developer.apple.com/documentation/Security/Conceptual/Security_Overview/Security_Services/chapter_4_section_1.html
- MUSCLE
  - http://www.linuxnet.com/
- mozilla(NSS)
  - http://www.mozilla.org/projects/security/pki/nss/
- Open group(CDSA)
  - http://www.opengroup.org/security/cdsa.htm

ROBOC