平成２１年度民間基盤技術研究促進制度応募研究開発課題

「汎用用途でも利用可能な Web 専用電子証明書用 IC カード」

［1］研究開発課題の内容

1－1　研究開発課題の背景

Web サービスの認証において、ID・パスワード認証ではセキュリティが充分でない場合が多く、電子証明書認証でも IC カードを利用しなければ、ID・パスワード認証よりもセキュリティが下がる場合がある。Web サービスの認証を便利する自動ログインソフトウェアが流行しているが､マスターパスワード 1 つですべてのパスワードを管理している場合が多く、便利だがセキュリティの問題が残る。
自動ログインソフトウェアのような便利さと、IC カードによるセキュリティの高さを合わせもつ製品の開発が望まれる。
既存の IC カードでも複数の電子証明書をインポートすることは可能であるが、一度 PIN を入力すると全部の証明書が有効になる問題がある。例えばネットバンクの残高照会用の電子証明書と決済用の電子証明書の２つが 1 枚のカードに入った例を考えます。既存の IC カードでは、残高照会のために PIN を入力すると決済用の電子証明書も同時に有効になり､コンピュータウィルスが勝手に決済用の電子証明書で決済を行ってしまうかもしれないのです。このため電子証明書ごとに PIN を持たせる機能を本提案の IC カードは持っています。

1－2　研究開発課題の内容

(株)＊＊＊＊＊の汎用用途の接触型 IC カード(容量 32Kbyte)のカード OS を改良した IC カード myuCard 32K を開発。myuCard 32K で動作する 2 種の IC カードミドルウェア PassCertBook と myuToken を開発する。

ア IC カード OS 改良

軽い OS に必要最小限の機能を追加することで、容量の小さい安価な IC カードを利用可能とする。原価低減や販売価格低減に貢献する。汎用的で高機能な OS で容量の大きい IC カードでは、ミドルウェアの入れ替によって必要以上の機能となるため、IC カードの販売価格を抑えることができない。OS に追加される機能は、中国人剰余定理を使った RSA 512/1024/2048bit。その実行権のつけ方を簡素にすることで OS への追加コードを小さくする。

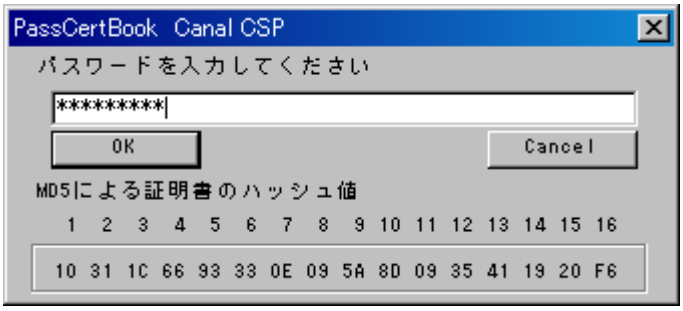
イ Web 専用 IC カードミドルウェアの開発 (PassCertBook)

Internet Explorer で電子証明書認証する場合、RSA が利用可能な CSP(Crypto Service Provider)ソフトウェアが必要。Microsoft の Microsoft Base Smart Card CSP では、電子証明書ごとに PIN を設定することができないため、独自 CSP を開発する。Microsoft Base Smart Card CSP の最新バージョンである「Windows Smart Card Minidriver Specification」Ver6.02 では、複数の PIN を設定できるように改良されたが、サポートされる OS が Windows Vista SP1 以降である。また 1 枚の IC カードに設定できる最大 PIN 数は 8 で､すでに 3 個が割り当て済みであるため本提案の目標

である電子証明書10枚分に必要な10PINにたらず､独自CSPの開発が必要である。

FireFox などのブラウザで電子証明書認証する場合、PKCS#11 のソフトウェアが必要。電子証明書ごとに PIN を設定できるよう標準の PKCS#11 とは多少、異なる実装をする。

電子証明書ごとに PIN を設定できても、PIN を覚えるのは一苦労である。そこで電子証明書の MD5 によるハッシュ値を PIN 入力画面で表示できる機能を追加する。



独自 CSP の PIN 入力画面

この MD5 のハッシュ値を利用して PIN を覚えやすくする。
たとえば、ベースとなる PIN に MD5 の 1 バイト目の 2 文字を追加する。
上記の例では、ベースとなる PIN を"PASSWD"とした場合、"PASSWD10"になる。証明書のハッシュ値だけに頼る PIN 記憶方法だけでなく、その他の工夫をすることで、覚えやすく安全性の高い PIN 管理が可能となる。

ウ　汎用用途 IC カードミドルウェアの開発(myuToken)

汎用用途で利用するため業界標準の MS-CAPI、PKCS#11 のソフトウェアを開発。すでに開発されている myuCard 8K 版のソースを流用。RSA 2048bit の機能追加や容量拡大の機能追加を行う。

<table>
<tr><td colspan="2">MS-CAPI 対応のアプリケーション
Microsoft Office や S/MIME、VPN など</td><td>Thunder Bird(S/MIME メーラ) etc
PKCS#11 対応のアプリケーション</td></tr>
<tr><td>iCanal myuToken
Crypto Provider</td><td>Microsoft Base
Smart Card CSP</td><td>PKCS#11 DLL</td></tr>
<tr><td colspan="3">Windows Smart Card Minidriver Specification Ver5.07 の myuCard 32K 用の DLL</td></tr>
<tr><td colspan="3">Microsoft WinSCard API</td></tr>
<tr><td colspan="3">日立 IC カードリーダ付属 PC/SC ドライバ</td></tr>
</table>

図 1-2　開発ソフトウェアの説明

Windows Smart Card Minidriver Specification の DLL には、Microsoft の動作検証ソフトウェアが存在し、エラーコードまで厳格にチェックすることが可能。