1F-6

生体識別技術の PKI への適用と評価

太田 英憲、河内 清人、辻 宏郷
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。PKI では署名を行なったり復号化を行なうための秘密鍵(Private Key)を安全に管理することが重要である。秘密鍵はハードディスクなどに暗号化されて保存されたり、IC カードなどのハードウェアトークンに格納されていることが多い。これらの秘密鍵を使用するためには、使用者が本人であるという確認を取る必要があり、従来は、一般的にパスワードや PIN と呼ばれる秘密情報を入力することによって確認が行なわれてきた。

また、近年、本人認証の手段として、生体識別技術を用いる認証機構に関する注目が集まっている[1]。生体識別技術をパスワードの代わりに用いることで、秘密鍵を格納している鍵管理デバイスと使用者の間で、容易かつ確実に本人認証が行なわれたり、パスワードと併用することで、より安全に本人認証を行なうことができる。

我々は、PC 用の指紋照合装置を用いて、PKI システムへの適用を目的とした認証ライブラリを開発した[2]。今回我々は、この認証ライブラリをセキュアメッセージングアプリケーション CryptoSign と組み合わせることによって、パスワードなしで IC カードを用いて、暗号化メッセージの復号化や署名メッセージの作成が行なえるように検討している。

2 指紋認証ライブラリ

2.1 構成

指紋認証ライブラリは図 1 のような構成となっている。

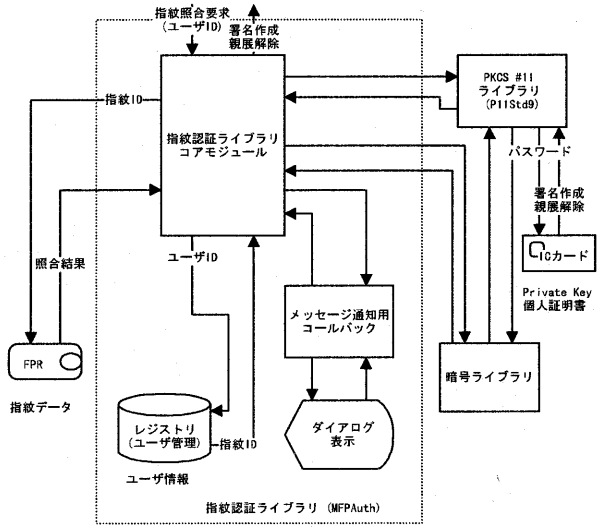

図 1 指紋認証ライブラリ構成

本ライブラリで使用する指紋照合装置は、複数の指紋データを保存することができるため、本ライブラリでは、任意のデータからなるユーザ ID で指紋データを識別して、複数人からライブラリを使用できるようにしている。指紋照合装置が識別する ID(指紋 ID)とユーザ ID の対応を取るためにはレジストリを使用する。また、IC カードに与えるためのパスワードは、指紋照合装置内に保存している指紋データから生成している。

2.2 使用手順

本ライブラリにおいて、指紋を用いて IC カードへのアクセスを行なうためのパスワード登録及び認証の手順は次のようになる。

登録時:

1. 指紋認証ライブラリに対して、ユーザ ID を指定して、登録要求

Applying and Evaluating Biometrics Technology to Public Key Infrastructure
Hidenori OHTA, Kiyoto KAWAUCHI, Hirosato TSUJI
Information Technology R&D Center, Mitsubishi Electric Corporation

2. レジストリの情報より、ユーザ ID に対応する指紋 ID 設定
3. 指紋 ID を指定して、指紋登録
4. 指紋照合用データより、パスワード生成
5. IC カード用パスワード変更

認証時:

1. 指紋認証ライブラリに対して、ユーザ ID を指定して、照合要求
2. レジストリの情報より、ユーザ ID に対応する指紋 ID 検索
3. 指紋 ID を指定して、指紋照合
4. 指紋照合用データより、パスワード計算
5. IC カードにパスワードを与えてログインすることで、署名生成・親展解除

3 CryptoSign への適用

CryptoSign は、S/MIME[3]に準拠したフォーマットを使用して署名メッセージや暗号化メッセージを作成するためのアプリケーションであり、PKCS #11[4]準拠の IC カードに対応している。

通常、CryptoSign では、Private Key を使用する演算、すなわち、IC カードを使用するタイミングで、使用者に対して、パスワードの入力を要求する。

今回、指紋認証ライブラリを CryptoSign に適用するために、CryptoSign がパスワードの入力を要求する代わりに、指紋認証ライブラリに対して照合要求するように変更を加えた。(図 2)

このような変更を加えた結果、パスワード入力を要求するダイアログが表示されるのではなく、指紋認証ライブラリから呼ばれるコールバックルーチンによって、指を指紋照合装置に置くように要求するダイアログが表示されるようになった。

4 まとめ

指紋認証ライブラリを CryptoSign と組み合わせることによって、パスワードを必要とせずに、暗号化メッセージの復号化や署名メッセージの作成を行なえるようになった。CryptoSign に対して加えた変更はわずかなものであり、指紋認証ライブラリの有用性が確認できた。

本指紋認証ライブラリは、登録した指紋データを元にパスワードを生成するため、指紋を登録してから IC カードのパスワードを設定する必要がある。一方、既存のアプリケーションに適用する際に、パスワードを変更したくないという要求もあり、今後の課題として、任意のパスワードを設定する方法の考案などが挙げられる。

参考文献

[1] 菅知之: “バイオメトリクス認証の動向”, 第 29 回 ECOM セミナー, 1999

[2] 太田・辻・齋藤・坂上: “生体識別技術の PKI への適用”, 2000 年暗号と情報セキュリティ・シンポジウム, SCIS2000-D03, 2000

[3] S.Dusse, et.al.: “S/MIME Version 2 Message Specification”, RFC2311, 1998

[4] RSA Laboratories: “PKCS #11 Cryptographic Token Interface Standard”, 1997

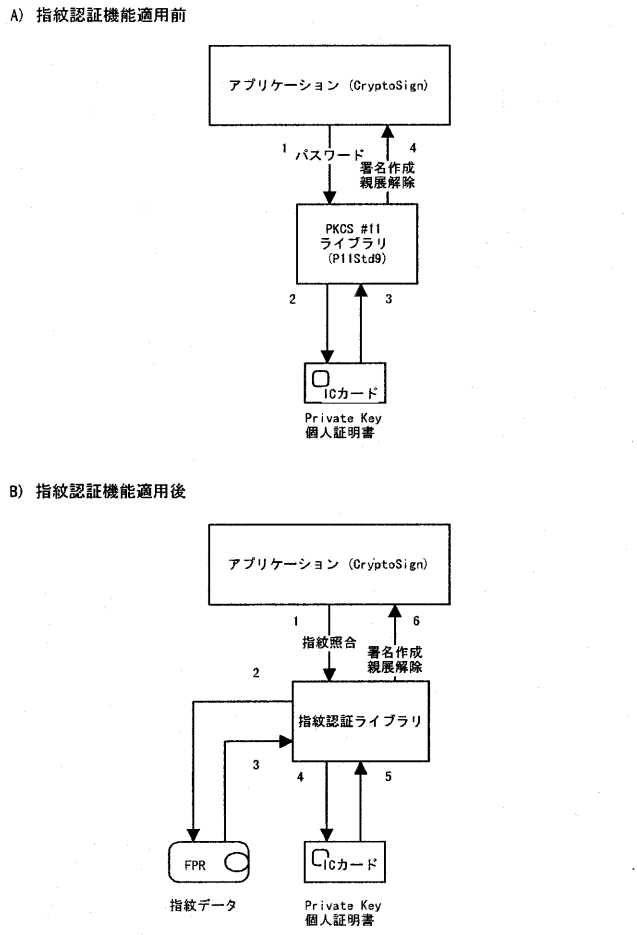

図 2 指紋認証ライブラリ適用