2003－CSEC－23 (11)
2003／12／19

着脱可能暗号トークンを用いた携帯電話向けPKI S/Wアーキテクチャの提案

米田 健, 中川路 哲男[1]

携帯電話を利用したオンラインバンキング、オンラインショッピング等ユーザ認証が必要なオンラインサービスが普及してきた。一方、キャッシュカードやクレジットカードは、PKI機能を備えたICカードに置き換わりつつある。携帯電話とICカードが連携することで、ICカードサービス提供者のオンラインサービスを、容易に安全に携帯電話で利用することが可能となり、利用者の利便性が向上する。そこで、本稿では、ICカードやUSBトークン等暗号トークンを携帯電話で利用するために必要な携帯電話のS/Wアーキテクチャを提案する。PCのエミュレート環境で試作システムを開発することで、着脱可能暗号トークンを利用する携帯電話S/Wの実装フィージビリティを確認した。

PKI S/W Architecture for Mobile Phone Using Removal Encryption Token

Takeshi Yoneda, Tetsuo Nakakawaji[2]

Online services by mobile phone such as online banking and online shopping, which require user authentication, have become popular. On the other hand, cash cards and credit cards are now being replaced by smart cards which have strong user authentication function using PKI technology. If mobile phones can use the smart cards, mobile phone users can access online services easily and safely provided by smart card service providers. So in this paper, a PKI S/W architecture for mobile phone using removable encryption token such as smart cards and USB tokens is proposed. By developing a prototype system based on the architecture, the mobile phone S/W implementation feasibility is confirmed.

1. はじめに

ブロードバンド加入者は2003年5月に1000万人を超え、ネットワークの大容量化、通信コストの低価格化が進展したため、オンラインショッピングやオンラインバンキング等オンラインサービスが急速に普及している。また、インターネット対応携帯電話の契約数も2003年9月には6600万を超え、各種オンラインサービスが携帯電話対応を進めた結果、携帯電話を用いたオンラインサービスも急速に普及している。一方、ICカードの発行枚数は、2003年度6000万枚を越えることが予想されており、今後数年で、財布の中に通常入れているキャッシュカード、クレジットカードはPKI機能に対応したICカードになっていると予想される。

IC カードを外部から装着して利用できる携帯電話は現時点で国内には存在しないが[3]、今後ニーズが高まると予想される。なぜならば、携帯電話とICカードが連携することで、ICカードサービス提供者のオンラインサービスが容易に安全に携帯電話で利用できれば、利用者の利便性も向上するからである。ま

[1] 三菱電機株式会社 情報技術総合研究所
[2] Mitsubishi Electric Corporation, Information Technology R&D Center

[3]内部組込みタイプのICチップは第3世代携帯電話にて、UIM(User Identification Module)として利用されている。

た、ICカードサービス提供者にとっても、
・ICカードの利用箇所が専用端末から携帯電話に広がることでビジネスの拡大が見込める、
・通信事業者がオーナーであるUIMよりも、ICカードサービス提供者自らがオーナーであるICカードを利用する方が、責任範囲が明確であるという観点から、証明書・鍵の運用管理が容易になる、
といったメリットがある。
そこで、本稿では、ICカードやUSBトークン等暗号トークンを携帯電話で利用するために必要な携帯電話のS/Wアーキテクチャを提案する。提案するアーキテクチャをベースとしてPC上のエミュレータ環境で試作システムを開発し、着脱可能暗号トークンを利用する携帯電話S/Wの実装フィージビィリティを確認した。
本稿の構成を以下に示す。2章では、着脱可能暗号トークンを携帯電話と連携して利用するシナリオを提示する。3章ではシナリオを参考とした要件を記述する。4章では要件を満たす機能を示す。5章では暗号トークンに格納が必要となる情報を示す。6章にて試作システムの実装を記述し、7章にまとめを述べる。

2. シナリオ

暗号トークンを携帯電話で利用する典型的なシナリオとして、銀行のPKI機能対応ICキャッシュカードを携帯電話で利用するシナリオを紹介する（末尾図2.1参照）。

1) 利用者は携帯電話の電源ON後、待ち受け状態になっている携帯電話に対して、財布から取り出したA銀行のICキャッシュカードを挿入する。

2) ブラウザが自動的に起動され、A銀行のホームページが自動的に選択され、SSLクライアント認証が実施される。利用者はICキャッシュカードのパスワードに相当するPIN(Personal Indentification Number)を入力すると、ユーザ認証が完了し「ようこそ」画面が表示される。

3) 利用者は家賃の振込を行う。

4) 振込処理終了後利用者はICキャッシュカードを携帯電話から抜く。すると、「カードが抜かれました」と表示され、SSL通信は自動的に切断され、ブラウザも自動的に終了する。そして待ち受け画面が表示される。

3. 要件

2章に記述したシナリオを参考に、着脱可能暗号トークンを利用する携帯電話に対する要件を抽出する。以下では理解を容易にするために"暗号トークン"を"ICカード"と記述する。

1) 高いセキュリティ
ICカードの暗号機能を用いてユーザID/パスワード方式よりも強力な相互認証と暗号通信を実現する。また、ICカードを抜いた場合にICカードのPKI機能を用いて獲得したセキュリティコンテクスト[4]を破棄することで、ICカードが抜かれた状態で、ICカードの利用者に成りすますことを困難とする。

2) 容易な操作性
ICカードサービスの提供者が特定のホームページに利用者をアクセスさせたい場合がある。その場合、利用者にアプリケーションの選択、接続先の選択をさせることなく、ICカードを挿入するだけで、自動的にアプリケーションの起動、ホームページへの接続が実施されるようにする。

3) ICカード着脱時挙動のカスタマイズ
ICカード挿入時/抜き時の挙動に対しての要求が、利用者間、ICカードの提供者間で異なる場合がある。

[4] セッション鍵や信用するルートCA証明書等の認証・暗号の要となる携帯電話のRAM/フラッシュメモリに保持されているセキュリティ情報

そこで、ICカード挿入時のアプリケーション自動起動機能のON/OFF, 起動したアプリケーションからの自動ネットワーク接続機能のON/OFFを利用者やICカードサービス提供者が選択できるようにする必要がある。また、IC カード抜き時の通信自動切断ON/OFF、アプリケーションの自動終了ON/OFFを、利用者やIC カードサービス提供者が選択できるようにする。

4) 異なる種類のIC カードを携帯電話のS/W が同様に扱える。

異なる種類のIC カードが携帯電話に装着された場合でも、携帯電話のS/W からはそれらは同種のICカードと認識される必要がある。したがってICカードはISO 7816-4[1], ISO7816-8[2], PC/SC[3]等の標準に準拠している必要がある。

4. 機能

本章では、前章で述べた要件を実現する機能について記述する。

1) アプリケーション管理機能

容易な操作性を実現するためには、暗号トークンの着脱通知を受けて、暗号トークンを利用する適切なアプリケーションを起動・終了する機能が必要となる。本機能は図3.1のアプリケーション管理モジュールに該当する。

2) 暗号トークン着脱検知機能

暗号トークンの着脱を検知・通知する機能

利用可能な暗号トークンの増減をチェックすることで暗号トークンの着脱を検知する。検知された着脱イベントを上位のアプリケーション(ex. アプリケーション管理モジュール)に対して通知する。図3.1の暗号トークン着脱検知モジュールに該当する。

3) 暗号トークンインターフェース機能

証明書の保存、取得、検索機能および署名の生成といったPKI機能を標準的なAPIで提供する。本機能により異なる種別の暗号トークンを同一のPKI機能を提供する同種の暗号トークンとして抽象化することができる。図3.1の暗号トークンインタフェースモジュールに該当する。

4) 暗号トークン情報フォーマット機能

暗号トークンの種別に依存しないPKIオブジェクト種別(証明書、鍵等)、PKI オブジェクトの格納形式及び格納場所を提供する機能。本機能を用いることで暗号トークンインターフェース機能は、証明書の格納、取得機能を実現する。図3.1の暗号トークン情報フォーマットモジュールに該当する。

5) 複数暗号トークン管理機能

利用可能な暗号トークンのリストを保持し、各暗号トークンとのセッションの確立/解放および、セッション上でのコマンドの発行、レスポンスの受信機能を提供する。本機能を用いて暗号トークンインターフェースの機能が実装される。図3.1の暗号トークンリソース管理モジュールが該当する。

6) 暗号通信機能

相互認証機能、暗号・復号機能、改ざんチェック機能を有する暗号通信機能。

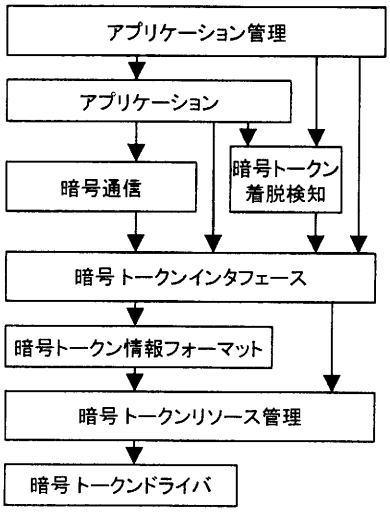

図 3.1 機能モジュール構成

4. 暗号トークンに格納する情報

暗号トークンに格納する情報は PKI 関連の情報と、その他の情報に分類できる。

1) PKI 関連情報

表 4.1 に PKI 関連の暗号トークン格納情報を示す。

表 4.1 PKI 関連の暗号トークン格納情報

格納情報	説明
信用するルート CA 証明書	IC カード提供者の指定する信用するルート CA 証明書。複数可能。
証明書のチェイン	IC カードユーザの証明書およびその証明書の発行した CA の証明書
秘密鍵	IC カードユーザの秘密鍵
公開鍵	IC カードユーザの公開鍵

2) その他の情報

PKI 関連以外の格納情報を表 4.2 に示す。

表 4.2 その他の暗号トークン格納情報

格納情報	説明
起動 AP 情報	起動する AP 特定情報 (Application ID 等)
暗号トークン挿入時 AP 起動フラグ	暗号トークン挿入時の起動有無を示す
通信接続先	起動された AP の接続先情報 (ex. URL)
通信可能接続先リスト	許容される接続先リスト。AP は本リストに記載された接続先のみにアクセスできる。アクセス制御は AP が実施することを想定。
暗号トークン抜き時 AP 終了フラグ	暗号トークン抜き時の AP 終了の有無を示す。

5. 試作システムの実装

試作システムの実装では、機能の実現に利用する標準の選択、標準に規定されていない事項の規定を実施した。

1) 機能の実現に利用する標準

試作システムの実装において、2 章で示した機能の中で利用可能な標準があるものは標準を採用することとした。

表 5.1 機能実現に利用する標準

機能	利用する標準および理由
暗号トークンインターフェース機能	PKCS#11 [4] 規定の API。OS の種別に依存することなく幅広く利用されているため。
暗号トークン情報フォーマット機能	PKCS#15 [5] を利用する。他に本領域の有力な標準なし。WAP WIM にて採用実績あり。
複数暗号トークン管理機能	PC/SC Resource Manager 規定の API。本領域の API を定めた有力な標準は他にはなし。

2) 試作システムの H/W 構成

H/W 構成を図 4.1 に示す。携帯電話が PKI 機能を持った UIM と、外部から着脱できる IC カードの 2 つの暗号トークンをサポートすることを想定し、その構成を PC にてエミュレートした。

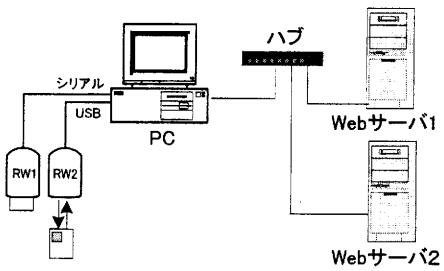

図 5.1 H/W 構成

表 5.1 H/W 構成要素

構成要素	携帯電話利用ケースでの相当物
PC	携帯電話

RW1 の IC カード (カード抜差し無)	UIM (通常抜かれない)
RW2 の IC カード (カード抜差し有)	動的に着脱される暗号トークン
Web サーバ 1	UIM の PKI 機能で SSL クライアント認証を実施する Web サーバ
Web サーバ 2	動的に着脱される暗号トークン挿入 (IC カードは抜差しされない) 時に自動的に接続される Web サーバ

RW1--- GemPlus GemPC410

RW2--- GemPlus GemPC430

IC カード---GemPlus GPK16000

3) 試作システムの S/W 構成

提案するアーキテクチャの基づく試作システムの S/W 構成を図 5.2 に示す。OS には RedHatLinux9.0 を用いた[5]。各モジュールの実装を表 5.2 に示す。

表 5.2 S/W 構成要素

モジュール	実装
アプリケーション	サンプルアプリケーションプロセス
アプリケーション管理	同上
暗号トークン着脱検知	暗号トークン着脱検知スレッド
暗号通信	OpenSSL 0.96b ライブラリ
PKCS#11	OpenSC 0.7 ライブラリ
PKCS#15	OpenSC 0.7 ライブラリ
暗号トークンリソース管理	PC/SC Lite IC カードドライバアクセスライブラリ
	PC/SC Lite IC カード状態管理プロセス (デーモン)
暗号トークンドライバ	IC カード RW ドライバ (ifd-gempc-0.8.0)

暗号トークンを利用するアプリケーションとして SSL クライアント認証を利用するブラウザ相当のサンプルアプリケーションをプロセスとして実装した。アプリケーション管理機能は、アプリケーションが一つに限定されていることよりサンプルアプリケーションプロセスに実装した。表 4.1 に示した PKI 関連情報は PKCS#15 の仕様に従って格納する。表 4.2 に示した情報については、PKCS#15 に規定された Data Object として格納し、PKCS#11 の DataObject 取得 API で取得することとした。

[5] 携帯電話の OS は Embedded Linux 等マルチプロセス機能をもつ OS を想定した。

4) 動作シーケンス

試作システムにおける IC カード着脱時の動作シーケンスを末尾図 5.3 に記述する。試作システムにおいて、アプリケーション管理とアプリケーションリケーションは単一のプロセスで実装しているが、一般的な動作シーケンスを示すために、それぞれ独立したモジュールとして記述した。

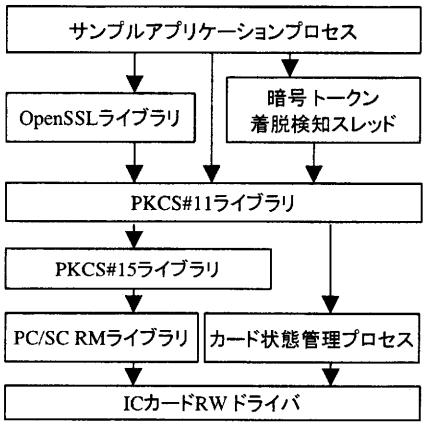

図 5.2 S/W 構成

6. まとめ

試作システム実装の結果、提案する S/W アーキテクチャに基づいて PKCS#11, PKCS#15, PC/SC のリソースマネージャを利用し着脱可能暗号トークンを利用した携帯電話 S/W を構築できることが確認できた。ただし、暗号トークン着脱時挙動情報に関しては該当する規定が存在しないので新規に定義し標準化することが必要である。今後は、携帯電話の実機に移植し、性能評価を実施予定である。

参考文献

[1] ISO/IEC 7816-4 Information technology -Identification cards -Integrated circuit(s) cards with contacts- Part4: Interinductry commands for interchange

[2] ISO/IEC 7816-8Information technology -Identification cards -Integrated circuit(s) cards with contacts- Part8 Security related interindustry command

[3] PC/SC, "Interoperability Specification for ICCs and Personal Computer Systems Part 8: Recommendations for ICC Security and Privacy Devices," The PC/SC Workgroup, December 1997

[4] RSA Laboratories, "PKCS #11: Cryptographic Token Interface Standard," version 2.01, December 1997

[5] RSA Laboratories, "PKCS #15: Cryptographic Token Information Format

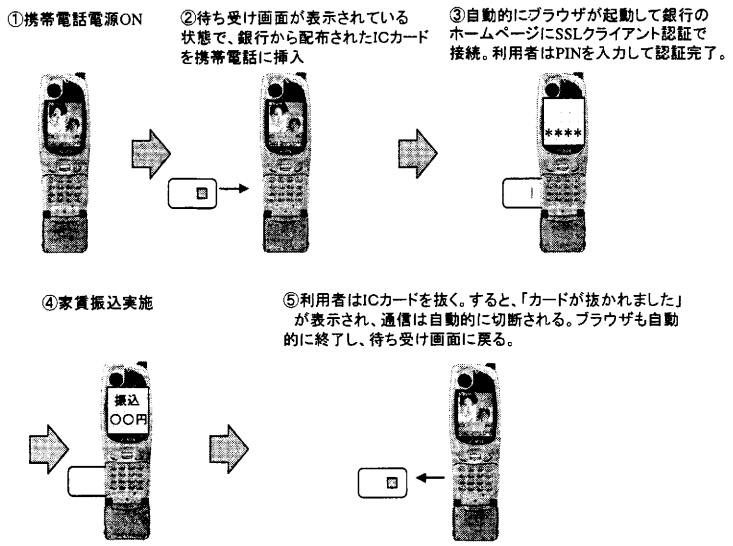

図2.1 ICカードの携帯電話連携シナリオ

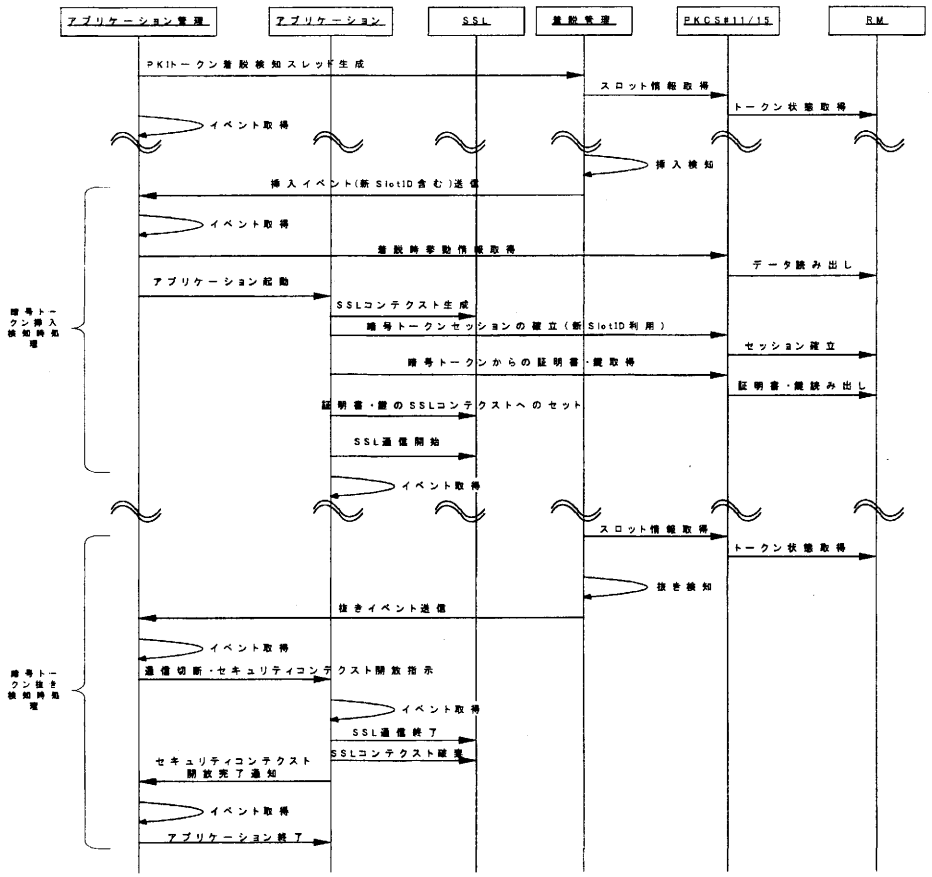

図5.3 動作シーケンス