ドコモ電子認証サービス
FirstPass特集

移動機へのPKI実装技術

FirstPassサービスを提供するにあたり，FOMA移動機のF2102V, N2102VにSSLクライアント認証機能を実装し，従来機種に比べてサーバによる，より安全で簡易な端末認証機能を実現した．

高橋 和彦　榊原 裕之　濱津 誠
渡邉 信之　能川 千晶　野田 千恵

1. まえがき

SSL（Secure Sockets Layer）[1]は，インターネットにおいて普及しているセキュア通信プロトコルである．ドコモでは，すでにディジタル携帯電話方式（PDC：Personal Digital Cellular）の503iシリーズ，およびFOMA（Freedom Of Mobile multimedia Access）移動機においてエンド・ツー・エンドのサーバ認証機能を搭載し，暗号化通信とサーバ認証を実現している．しかし，従来のサーバ認証では移動機はサーバを認証することが可能である反面，サーバは移動機を認証できないという制約があった．そこで，FOMA移動機のF2102V，N2102V，およびUIMv2（User Identity Module version 2）（FOMAカード(緑)）（写真1）において，SSLクライアント認証（以下，クライアント認証）を実現するための機能開発を行い，“FirstPass”という名称で認証サービスを開始した．FirstPassは，移動体通信において，公開鍵暗号基盤（PKI：Public Key Infrastructure）に基づくクライアント認証を実装した，国内では初めての本

写真1　FirstPass対応端末（F2102V, N2102V, およびUIMv2）

格的な商用サービスである．FirstPassにおけるクライアント認証では，SSLハンドシェイクにおいて移動機がユーザ証明書と署名をサーバに提示することにより，FOMA契約ごとに割り当てられたIDの認証が可能となる．このように，サーバとクライアントの双方が相互に認証可能となるため，FirstPassを適応したサービスの拡大が期待される．

クライアント認証の実現にあたっては，ユーザ証明書をあらかじめ取得する機能，およびクライアント認証時にユーザ証明書と署名を提示する機能が必要となる．

本稿では，クライアント認証を実現するために必要となる移動機とUIM（User Identity Module）へのPKI機能の実装について解説する．

2. 移動機におけるPKI機能要件と課題

2.1 PKI機能要件

クライアント認証を行うためには，まずユーザ証明書を電子認証局であるドコモCA（Certification Authority）から取得する必要がある．その後，SSL通信時にサーバがクライアント認証を要求すると，移動機はサーバにユーザ証明書と署名を提示する．したがって，移動機には以下の機能が必要となる．

- ユーザ証明書の取得機能（鍵ペア生成・発行申請・ダウンロード）
- クライアント認証時のユーザ証明書提示と署名生成・提示機能

ユーザ証明書の取得機能に関しては，発行申請時に鍵ペアを生成する必要があり，特に秘密鍵は署名生成に利用されるため移動機側で安全に生成し保管する必要がある．また，利用者の移動機操作により，ドコモCAからユーザ証明書の発行申請とダウンロードを安全に実現しなければならない．

クライアント認証の署名生成においては，秘密鍵の漏洩を防ぎつつ署名を生成する機能が求められる．

2.2 従来機種での課題

PKI機能要件を満たすためには，鍵ペアと証明書の管理について検討が必要である．従来機種ではUIMv1（User Identity Module version 1）（FOMAカード（青））にPKI機能がなかったため，鍵ペアの生成・保管，および証明書の保管場所としては移動機内のメモリが考えられた．しかし，セキュリティの問題と機種を変更した場合の秘密鍵・証明書の引き継ぎができないという課題があったため，クライアント認証機能は実現されなかった．

3. FirstPass対応機種におけるPKI機能の実装

FirstPassに対応した移動機・UIMv2では2.1節における2つの要件を満たし課題を解決するために，鍵ペア・証明書の管理などのPKI機能をUIMに実装し，移動機から当該機能を利用することでSSLクライアント認証を実現した．特に，移動機とUIM間インタフェースとUIMのPKI機能については，実装可能な標準方式がなく，独自に開発を行った．

移動機では図1に示すように，UIM，証明書ダウンロードアプリケーション，iモードブラウザで，システムを構成する．UIMv2においては，鍵ペア生成機能と証明書格納機能，署名生成機能を実装している（3.1節）．証明書ダウンロードアプリケーションはドコモCAに接続し，UIMv2と連携してユーザ証明書の発行申請・UIMv2へのダウンロードの機能を有する（3.2節）．iモードブラウザはHTTP（HyperText Transfer Protocol）データを保護するためのSSLプロトコルスタックを装備し，クライアント認証時にUIMと連携してユーザ証明書と署名を送付する機能を持つ（3.3節）．以下に，各PKI機能の実装について解説する．

3.1 UIMv2のPKI機能について

SSLクライアント認証を行うために，UIMv2に実装するPKI機能には，主に次の3要素が必要である．

- 鍵ペア生成と秘密鍵の格納
- ユーザ証明書の格納

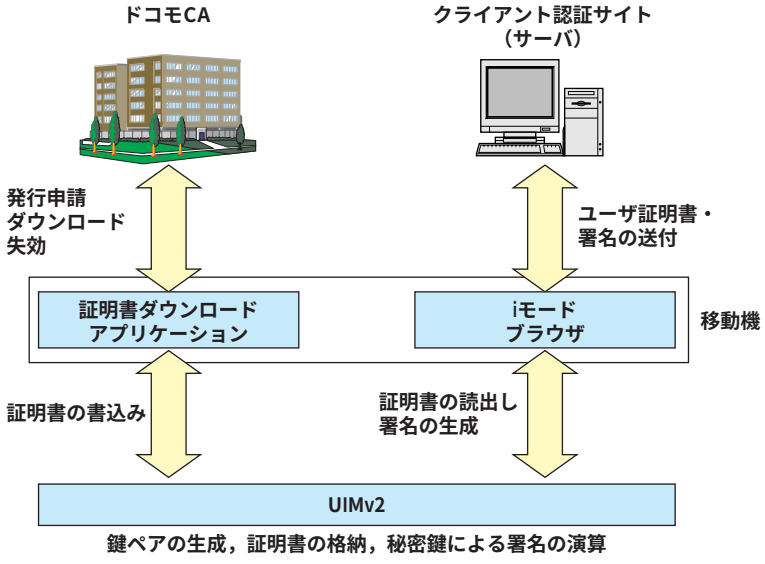

図1　システム構成

・署名生成機能（秘密鍵を使用した公開鍵暗号演算）

(1) 鍵ペア生成と秘密鍵の格納

ICカード内での鍵ペア生成は一般に数十秒単位の時間を要し，ドコモCAとの通信中に動的に鍵ペア生成を実施すると通信タイムアウトなどの問題が生じる．このため，UIMv2においては，UIM内での鍵ペア生成は行わず，UIMメーカからの出荷時にあらかじめ鍵ペアを格納するようにした．したがって，ドコモCAへの証明書発行申請時の鍵ペア生成は擬似的な鍵ペア生成であり，内部動作としてはあらかじめ格納しておいた鍵ペアを逐次使用する．あらかじめ格納可能な鍵ペアはUIM内のメモリの制約上，5対に制限した．

ICカードは耐タンパ性（Tamper Resistant）[*1]を有する情報格納媒体であり，秘密鍵については外部から読み出すことは不可能である．さらに秘密鍵を使用した演算を行う際には，PIN（Personal Identity Number）2コード入力を行うことを必須としたため，第三者に不正に使用されることがなくユーザ認証としてのセキュリティも確保される．

(2) ユーザ証明書の格納

UIMv2はユーザ証明書を格納する領域を有しており，このユーザ証明書の中の公開鍵に対応する秘密鍵に関連付けられている．ユーザ証明書はドコモCAにアクセスすることにより更新可能であるが，ドコモCA以外では更新することができないようにしており，第三者が勝手に不正な証明書を書き込むことができないようにセキュリティを保っている．

(3) 署名生成機能

FirstPassでは，公開鍵暗号方式として，インターネットで標準となっているRSA（Rivest Shamir Adelman）公開鍵暗号[2]を採用した．UIMに格納される鍵ペアの鍵長は1024bitsであり，UIMv2内でRSA公開鍵暗号演算の処理を行っている．

クライアント認証機能における主要諸元を表1に示す．

表1　SSLクライアント認証機能の主要諸元

対応プロトコル	SSL V3
公開鍵アルゴリズム	RSA（UIM）
鍵長	1024bits（UIM）
ハッシュアルゴリズム	SHA1, MD5

3.2 証明書ダウンロードアプリケーション

証明書ダウンロードアプリケーションは，ドコモCAに接続しユーザ証明書の発行申請・ダウンロード・失効に使用するアプリケーションである．本アプリケーションはHTTPブラウザの機能を有し，ドコモCAとの送受信データはHTTP上のHTML（HyperText Markup Language）コンテンツを基本としているため，コンテンツの作成や変更は容易に行うことができる．また，証明書ダウンロードを行えるようにHTMLの形式を一部拡張することで，ドコモCAとUIM間の命令・応答のプロトコル変換を行っている．ドコモCAとSSLセッションを確立することで，送受信データはSSLで保護されたHTTP上で送受信される．本アプリケーションは，iモードメニュー配下などにおいて「ユーザ証明書操作」メニューとして設置され，押下するとドコモCAに接続しFirstPassのメニューリストを表示する．

利用者は，発行申請を行ってからダウンロードを実施することにより，ユーザ証明書を取得する．

(1) 発行申請機能

図2は，ユーザ証明書の発行申請シーケンスを示している．“ユーザ証明書操作”を押下し証明書ダウンロードアプリケーションを起動すると，ドコモCAに接続しFirstPassのメニューリストが表示される．次に，“証明書発行”を押下するとサーバ認証後に証明書発行要求を送付し，ドコモCAからは鍵ペア生成命令・発行申請要求の生成命令が送信される（④）．移動機は鍵ペア生成命令をUIMへ転送し，UIM内部で鍵ペア（公開鍵／秘密鍵）が生成される（⑤）．次に，移動機はPKCS（Public Key Cryptography Standards）#10[3]形式の署名付きの発行申請要求を作成する．まず，UIMから読み出した公開鍵（⑥）を含む発行申請要求を生成する（⑦）．さらに，同要求のハッシュデータ（⑧）を生成しUIM内部での秘密鍵による演算を施した結果を得る（⑩）．最後に，両者をPKCS#10形式にフォーマット化して送付する（⑪）．なお，秘密鍵による演算においては，UIMでPIN2コードの照合が必要であるので，PIN2コード入力画面を表示し利用者に入力させる．

以上のように，生成された署名付きの発行申請要求をドコモCAに送信すると，受付完了通知とダウンロード可能時期が表示されるので，証明書ダウンロードアプリケーションを終了する．

(2) ダウンロード機能

図3は，発行申請の終了後のダウンロードシーケンスを示す．FirstPassのメニューリストにおいて“ダウンロード”を押下すると，ドコモCAからダウンロード対象のユーザ証明書の詳細が提示される．利用者が内容を確認したうえで実行ボタンを押下すると，ダウンロードが

＊1　耐タンパ性：装置の内部に格納されている秘密情報が正当な権利者以外に漏洩・改ざんされないことを意味する．

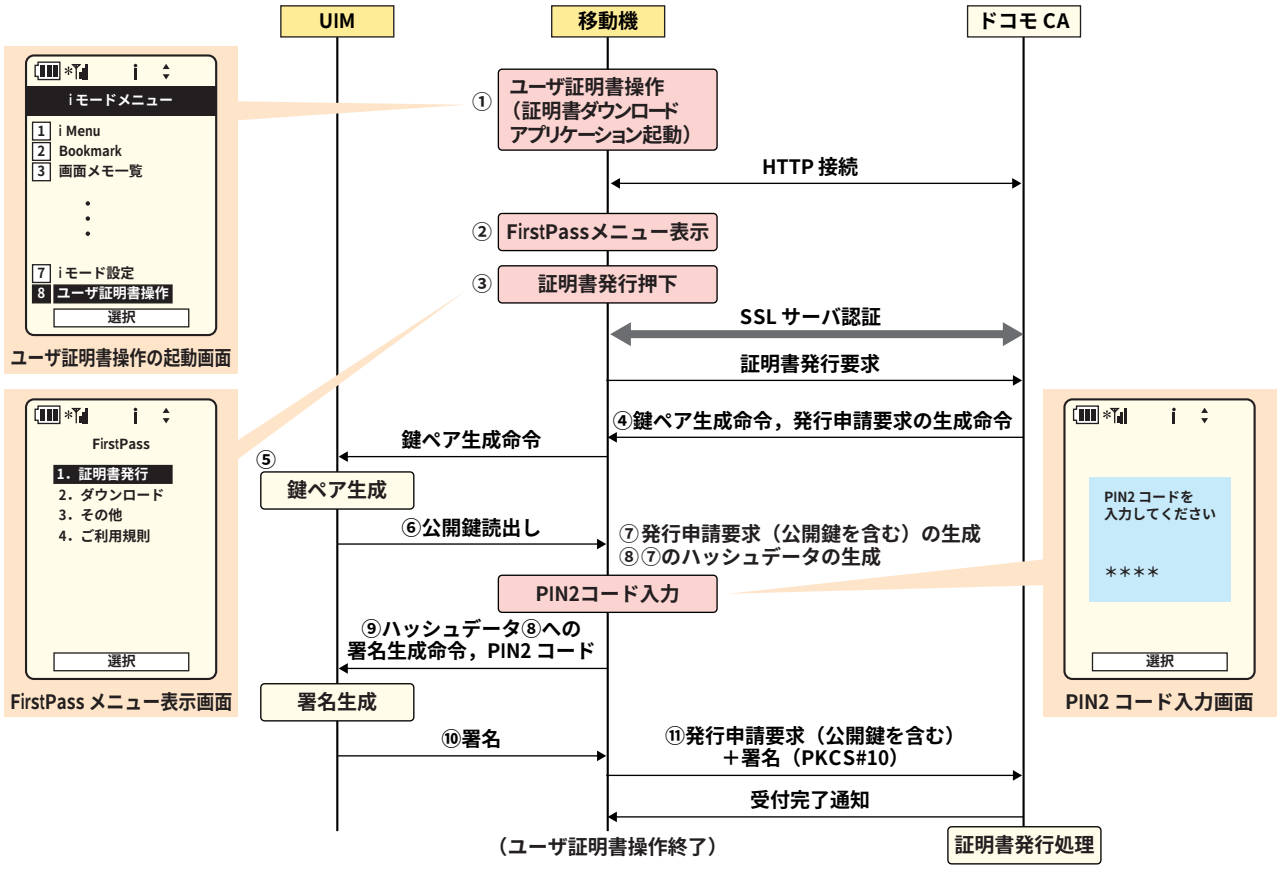

図2　証明書発行申請シーケンス

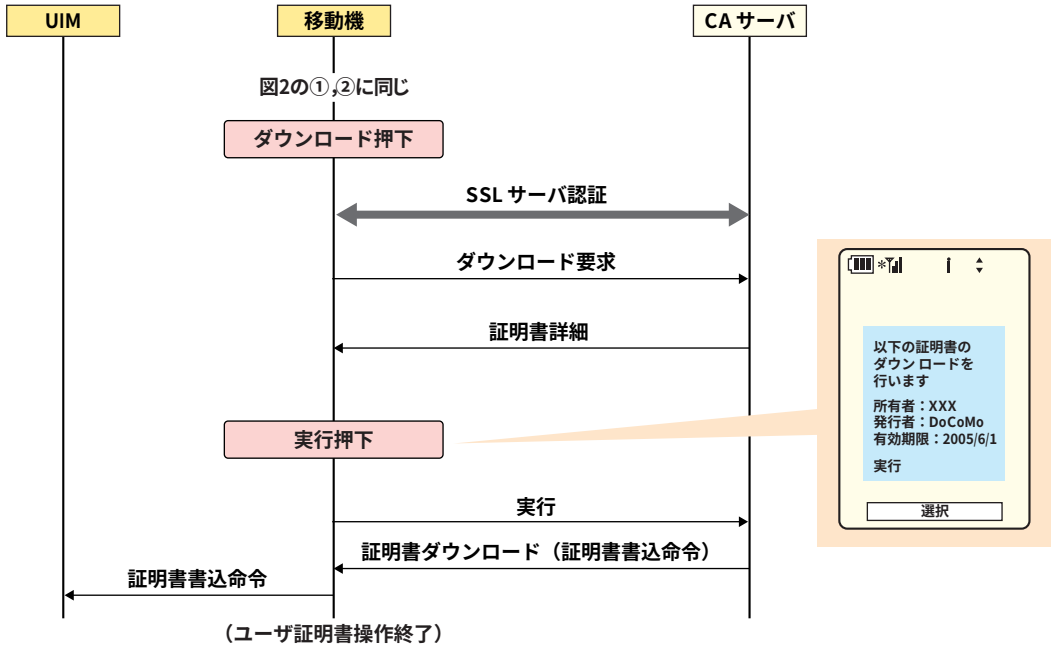

図3　証明書ダウンロードシーケンス

開始される．そして移動機はドコモCAから送信されるUIMへの証明書書込命令をUIMへ転送することにより，ユーザ証明書はUIMへダウンロードされる．

(3)　失効機能

FirstPassのメニューリストにおいて，“その他”に続いて“失効”を押下すると，ドコモCAとクライアント認証が実施される．その後，ドコモCAは現在使用してい

るユーザ証明書の詳細を提示し，利用者が“確認”を押下すると該当のユーザ証明書が失効される．このように，移動機操作で失効処理を行えるため，利用者の意思によって簡便かつ迅速にユーザ証明書の失効が可能である．

なお，失効時のクライアント認証処理は，後述のiモードブラウザでのクライアント認証と同様の処理となる．

3.3 iモードブラウザにおけるクライアント認証

iモードブラウザにおけるクライアント認証機能は，既存のサーバ認証機能の拡張機能として位置付けられる．図4に，クライアント認証時のハンドシェイクシーケンスを示す．移動機はiモードブラウザでサーバ（クライアント認証サイト）へ“ClientHello”を送信し，SSLハンドシェイクを開始する．サーバ認証のシーケンスとの違いは，ユーザ証明書と署名の提示をサーバが要求することである．サーバからのユーザ証明書の要求“CertificateRequest”(①）が送信されると，移動機からはユーザ証明書“ClientCertificate”(②）と署名情報である“CertificateVerify”(③）を送信する．サーバは，ユーザ証明書内の公開鍵を利用して“CertificateVerify”内の署名の正当性を検証する．これにより，ユーザ証明書の保持者の署名を検証したことになり，ユーザ証明書内のFOMA契約ごとに割り当てられたIDが認証可能となる（クライアント認証）．

なお，ユーザ証明書の送信の際は「ユーザ証明書を送信します」というメッセージおよび確認ボタン（OK/Cancel）を表示し，利用者に確認を促す．OKを選択するとユーザ証明書が送信される．

移動機は“CertificateVerify”の生成にあたり，“CertificateVerify”以前に送受信されたプロトコルデータなどをハッシュ化[*2]する．次に当ハッシュデータ[*3]をUIMに転送するとUIMでは秘密鍵における署名演算が行われる．移動機は，この結果を“CertificateVerify”としてサーバへ送信す

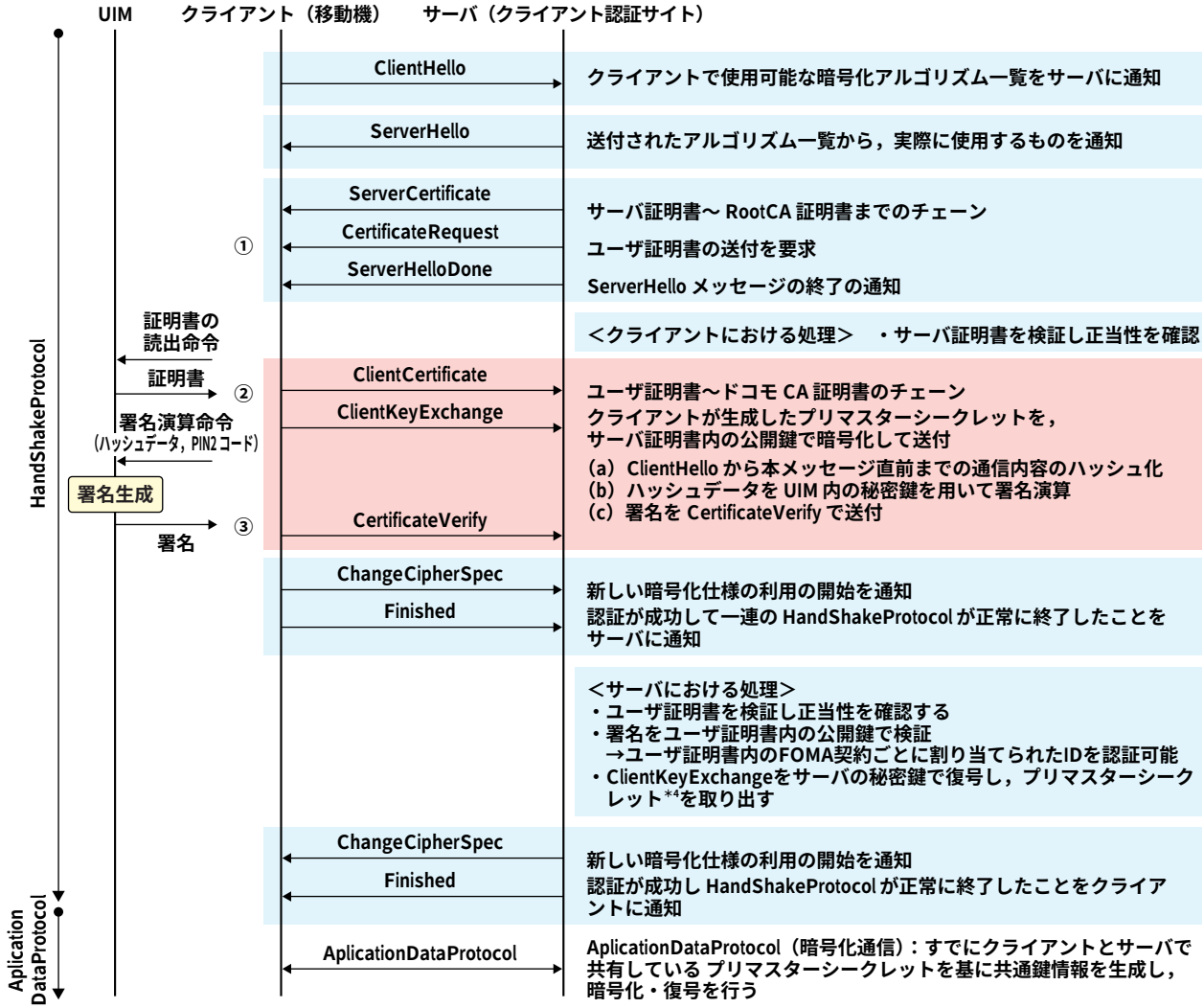

図4　SSLクライアント認証プロトコルシーケンス

る．なお，UIMで署名演算を実施するために利用者にPIN2コードを入力させる．

ハンドシェイク後はHTTPデータが暗号化され，サーバと安全なHTTP通信が可能となる．

4. あとがき

FirstPassサービスにおいて，移動機とUIMで安全なユーザ証明書のダウンロードとSSLクライアント認証を実現した．PKIベースのクライアント認証ソリューションを移動体通信に持ち込んだ点で画期的な進展であり，今後はUIMのユーザ証明書と署名機能を他のアプリケーションに適用し，より高度な認証サービスに発展させることが課題である．

＊2　ハッシュ化：元のデータをSHA1（Secure Hash Algorithm 1），MD5（Message Digest 5）などの一方向性のハッシュ関数で一定の長さのデータに圧縮すること．
＊3　ハッシュデータ：元のデータをハッシュ化した結果，得られるデータのこと．
＊4　プリマスターシークレット：SSL通信において各セキュリティパラメータの基になる情報のこと．

文　献

[1] A.O.Freier, P.Karlton and P.C.Kocher:“ The SSL Protocol Version 3.0 ”, draft-freier-ssl-version3-02.txt, Nov.1996.
[2] RSA Laboratories, PKCS#1 v2.0: RSA Cryptography Standard, Oct.1, 1998.
[3] B.Kaliski. RFC 2314: PKCS #10: Certification Request Syntax Version 1.5. Mar.1998.

用 語 一 覧

CA：Certification Authority
FOMA：Freedom Of Mobile multimedia Access
HTML：HyperText Markup Language
HTTP：HyperText Transfer Protocol
MD5：Message Digest 5
PDC：Personal Digital Cellular（ディジタル携帯電話方式）
PIN：Personal Identity Number
PKCS：Public Key Cryptography Standards
PKI：Public Key Infrastructure（公開鍵暗号基盤）
RSA：Rivest Shamir Adelman
SHA1：Secure Hash Algorithm 1
SSL：Secure Sockets Layer
UIM：User Identity Module
UIMv1：User Identity Module version 1
UIMv2：User Identity Module version 2