# Mobile端末PKI実証実験用証明書運用管理規定（暫定）

東京大学情報基盤センター

2008年8月21日

## 1　はじめに

### 1.1　概要

本文書は、東京大学情報基盤センターPKIプロジェクト（以下、PKIプロジェクトとよぶ）が、KDDI研究所との共同研究 (2006年度〜) において推進するMobile端末PKI実証実験において運営するCAについての証明書ポリシーと運用規定についての文書である。

本実証実験はPKI実証実験プロジェクトのひとつとして運用されているUTCAの下位CAとして構成する。UTCAの運用管理規定はRFC3647CPまたはEducauseのモデルキャンパスCPのLOA medium–highに対応する運用技術と運用経験を蓄積することを目的とするもののそれらに準拠して制定されてはいないので、本文書も正式な運用ポリシーを定めるものではない。しかし、CAの運用について一定の技術水準を満たすものであることを示すことが実験参加者にとっての利益になることから、この文書を定めるものである。したがって、たとえばPKI-liteのような低い要求水準は当然クリアしていること、大規模証明書管理に向いていることが実証されていないシステムを採用していないこと、運用に関係する人間が十分な研修を受けていることを本文書作成の前提条件として主張するものである。

本実験の終了は2009年3月の予定である。それ以後については規定しない。

### 1.2　文書名と文書識別

本文書名はPKIプロジェクト作成の「Mobile端末PKI実証実験用証明書運用管理規定（暫定）」である。OIDは、本実験終了までは取得しない。

### 1.3　本PKI関係者

#### 1.3.1　CA

本PKIのCAは、IAとRAのみによって構成される。運用主体はPKIプロジェクトである。

#### 1.3.2　RA

本CAは、PKIプロジェクト内にRAをおく。

#### 1.3.3　利用者

利用者は、東京大学またはKDDI研究所の構成員であり、かつ実験に参加しているものである。実験は東京大学情報基盤センターとKDDI研究所の共同研究「大学電子認証基盤におけるプライバシー保護技術の研究（以下、共同研究という）」(2006–2008年度) のもとで行なう。実験参加者は共同研究参加者とする。

### 1.4 証明書の用途

証明書は、クライアント認証と通信路におけるデータの暗号化に利用することができる。

### 1.5 ポリシー管理

#### 1.5.1 管理組織

この CP の保守管理は PKI プロジェクトがが行う。

#### 1.5.2 連絡先

連絡先は以下のとおりである。

東京大学情報基盤センター PKI プロジェクト（事務窓口 佐藤周行）

#### 1.5.3 CP 適合性の決定者

本 CP は、PKI プロジェクトで適合性を決定する。

#### 1.5.4 CP 承認手続き

この文書は PKI プロジェクトが承認する。

## 2 公表とリポジトリの責任

### 2.1 リポジトリ

リポジトリは`ldap.pki.itc.u-tokyo.ac.jp`である。文書の一部については`www.pki.itc.u-tokyo.ac.jp`に公開する。

### 2.2 証明書情報の公表

リポジトリでは、証明書の状態に関する情報を公開する。情報は最低 1 日 1 回更新する。

### 2.3 リポジトリへのアクセス管理

リポジトリは、東京大学のキャンパスにある端末からアクセスすることができる。

## 3 名前と認証

### 3.1 名前

証明書中の CN については、以下のとおりとする。東京大学側の参加者については東京大学で運用されている「共通 ID」に基づき、個人の一意性を保証された ID 体系に基づいて決定される。また、KDDI 研究所側の参加者については共通 ID を使わず、KDDI 研究所所属であることと個人の一意性を保証された ID 体系に基づいて決定される。

### 3.2 初期身元確認

初期身元確認は、共同研究の東京大学側の代表または KDDI 研究所側の代表が通常行なう方法で実施する。

### 3.3 キー再発行要求の際の認証

キーは再発行しない。

### 3.4 失効要求の際の認証

失効要求の際の認証は、共同研究の東京大学側の代表または KDDI 研究所側の代表が通常行なう方法で実施する。

## 4 証明書ライフサイクル管理

### 4.1 実験参加申請

申請は、実験参加者が文書によって行う。
そこには申請者の自署または押印が要求される。

### 4.2 証明書申請処理

RA は、実験参加申請文書を受け取った後、すみやかに処理を行い、承認または拒否の判断をする。この処理と承認には、共同研究の東京大学側の代表または KDDI 研究所側の代表が関与する。RA は鍵の代理生成を行ない、その後に利用者は証明書発行申請を行なう。

### 4.3 証明書発行

CA は、証明書発行申請を受け、証明書を発行する。
証明書発行は、RA を通して申請者に通知される。

### 4.4 証明書受領

申請者は、RA に出頭し、本人確認を受けた上で証明書つきの mobile 端末の借り出しを行なう。

### 4.5 キーペアと証明書の利用

規定しない。

### 4.6 証明書更新

証明書は更新しない。

### 4.7 証明書再発行

証明書は再発行しない。

### 4.8　証明書変更

証明書は変更しない。

### 4.9　証明書失効

証明書は、利用者が RA に文書で申請することで失効することができる。文書での申請に先立ち、本人確認を行ったうえで、RA は失効手続を開始することがある。

### 4.10　証明書情報公表

リポジトリにおいて、失効情報を CRL で公表する。OCSP は運用しない。

### 4.11　証明書破棄

証明書は実験中破棄しない。

### 4.12　キー預託と復帰

キー預託および関連する事業は行わない。キーのバックアップはとらない。

## 5　施設、管理、および運用

### 5.1　物理的管理

IA および、RA の機器は、施錠した部屋・区画に管理される。この部屋は地階にはない。この鍵を持つものは IA および RA の操作を禁止される。

### 5.2　手続管理

IA および RA を操作するものは以下のとおりである。

- システム管理者
- CA 管理者
- CA 監査者

これらの要員はすべて PKI プロジェクト内で任命され、CA 運用責任者の命令で操作を行う。
IA および RA の操作のすべてにおいて 2-person 規則が適用される。

### 5.3　要員管理

要員の研修を含む士気の維持と技術の保証については、PKI プロジェクトが努力する。

### 5.4　監査ログ採取

本プロジェクトの終了を含む任意の時点で監査ログを採取して検査を行うことがある。

### 5.5 記録

記録については、PKI プロジェクトが有意な情報を残すように最大限の努力を払う。

### 5.6 キー変更

キー変更は行わない。

### 5.7 侵入・事故および復帰

ソフトウェア、システム的なシステム攻撃の防御については PKI プロジェクトが最大限の努力を払う。事故からの復帰については別途定める。

### 5.8 CA の終了

CA は、実験が終了した時点で終了する。終了の手続は別途定める。

## 6 技術的セキュリティ管理

CA についての技術的なセキュリティ管理については、別途定める。なお、実験中の CA は、セキュリティを技術的に担保するためのソフトウェアシステムを構築した上で運用されている。
以下、利用者のキーペア生成とインストールのみについて規定する。

#### キーペア生成とインストール

RA は、貸し出す mobile 端末上で別に定める方法でキーペアを代理生成する。この方法は私有鍵の管理を適切にする方法であることが保証される。mobile 端末は FIPS140 レベル II 相当以上のセキュリティレベルをもつものとする。

#### 鍵のサイズ

利用者のキーは RSA1024 ビットである。

## 7 証明書、失効リスト、OCSP の各プロファイル

### 7.1 証明書プロファイル

証明書プロファイルは、以下のとおりとする。

| | |
|---|---|
| バージョン | V3 |
| シリアル番号 | |
| 署名アルゴリズム | sha1withRSAEncryption |
| 発行者 | CN=Certification Authority for Mobiles, O=The University of Tokyo, C=JP |
| 有効期間の開始 | UTCTime |
| 有効期間の終了 | UTCTime |
| サブジェクト | CN=< 共通 ID>, O=The University of Tokyo, C=JP |
| 公開キー | RSA (1024 Bits) |
| キー使用法 | Digital Signature, Key Encipherment |
| 拡張キー使用法 | クライアント認証 (1.3.6.1.5.5.7.3.2) |
| CRL 配布ポイント | [1] Directory Address:CN=CRL1, CN=Internal Certification Authority, O=The University of Tokyo, C=jp<br>[2] URL=http://ldap.pki.itc.u-tokyo.ac.jp/repository/InternalCertificationAuthority.crl<br>URL=ldap://ldap.pki.itc.u-tokyo.ac.jp/cn=Internal%20Certification%20Authority,o=The%20University%20of%20Tokyo,c=jp?certificateRevocationList?base?objectClass=cRLDistributionPoint |
| 機関キー識別子 | KeyID=20 バイト |
| サブジェクトキー識別子 | 20 バイト |
| 基本制限 | ”Subject Type=End Entity, Path Length Constraint=None” |

### 7.2 失効リストプロファイル

失効リストプロファイルは次のとおりとする。

| | |
|---|---|
| バージョン | V2 |
| 発行者 | CN=Certification Authority for Mobiles, O=The University of Tokyo, C=JP |
| 有効開始日 | UTCTime |
| 次回の更新予定 | UTCTime |
| 署名アルゴリズム | sha1withRSAEncryption |
| CRL 番号 | |
| 機関キー識別子 | KeyID=20 バイト |

### 7.3 OCSP プロファイル

OCSP は運用しない。

## 8 監査

外部監査は実施しない。PKI プロジェクト内部での監査を適宜実施する。

## 9 その他、学内規則を含む法令への対応

今後調整する。