IAとアーキテクチャ

西村　健
PKIプロジェクト
情報基盤センター
東京大学

東京大学情報基盤センター PKIプロジェクトについて

- 目標：東京大学にPKIを普及させる
  - PKIがID管理の中核となることを目指す
  - 約40,000人の大学構成員
  - 全学レベルから研究室レベルまで多岐にわたるサーバ

従来の認証局

- いわゆる集約型
  - 1つのIA（Issuing Authority, 発行局）と1つのRA（Registration Authority, 登録局）
  - 資源を集約することによって作業の効率化統一的な管理

認証局構築における問題点

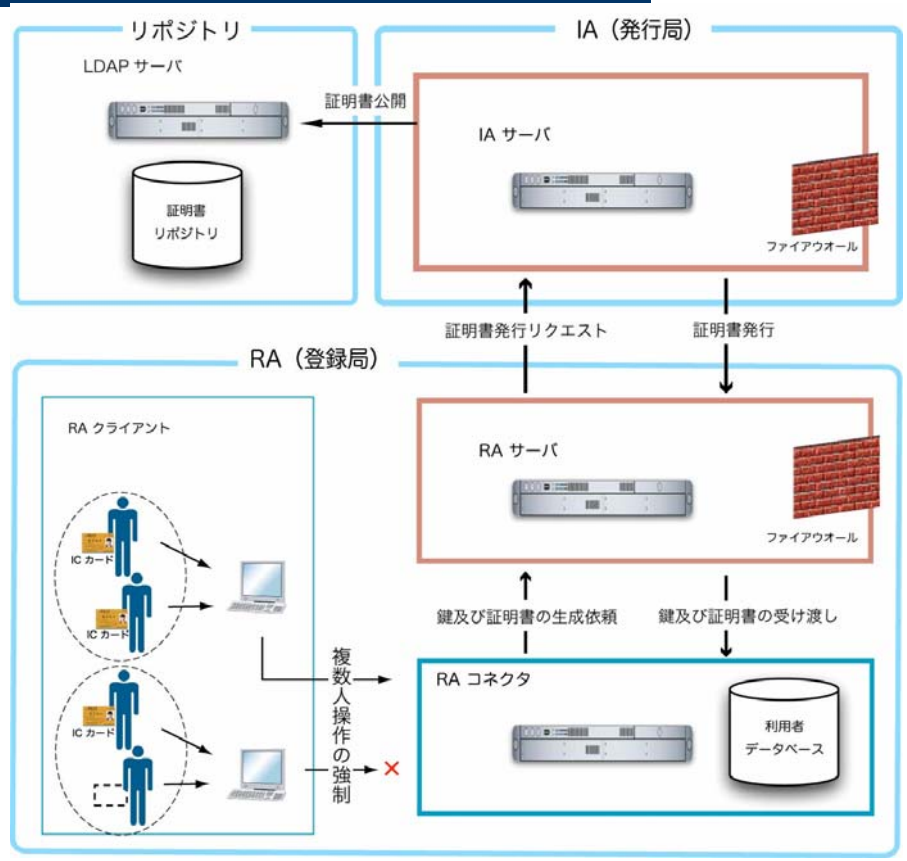
- 分散型
  - 学部や研究科等の部局の独立性を最大限尊重しなければならない
    - 人事情報が分散化
    - 既存のワークフローと整合性をとるため
- 信頼性
  - 認証局はPKIの信頼の根幹である
  - 安全な操作のためのシステムによる強制

実装：UT-CA

- 認証局UT-CAを設計、プロトタイプを実装
  - 分散型登録局
  - 操作者の相互牽制
- 実証実験を通して改善を図る

模式図

- IAサーバ
- LDAPサーバ
- RAサーバ
- RAコネクタ
- **RAクライアント**



各サーバの役割

- IAサーバ
  - 証明書の発行
- RAサーバ
  - 情報の集約、発行依頼
- RAコネクタ
  - RAサーバとRAクライアントの仲介
- LDAPサーバ
  - 証明書情報、失効情報の公開（インターネットとの接点）
- DBサーバ
  - 登録情報の保管
- RAクライアント
  - RA操作者が登録情報を入力・承認するための端末

前提条件

- Identity
  - 東京大学構成員の大部分には、**共通ID**と呼ばれるランダムな数字列がすでに各人に割り当てられており、これを利用する
  - 部局間異動の可能性も考慮し、証明書に記載する情報は最小限にとどめる
    - S/MIMEのためのメールアドレスなど
- 鍵格納デバイス
  - **ICカード**
    - 既にICカード化された職員証・学生証が配付されているので、これを利用することを想定

登録局の分散化

- 各部局に、登録局の支部（**部局RA**と呼ぶ）を置き、部局に所属する教職員・学生に対する証明書の発行・失効業務を行なう
- 部局RAにRAクライアントを設置し、部局所属の担当者が操作する

複数人操作の強制

- 部局RAの担当者として**審査者**および**承認者**を任命する
- それぞれ専用のICカードで認証し、2人の操作があって初めて証明書の発行が行なわれる
- 審査者…申請の入力　等々
- 承認者…入力された情報の確認

既存の事務組織上に展開

- 教職員・学生に相対している総務／庶務係および教務係に部局RAの担当を依頼する
- この部分（利用者の本人性・実在性確認）のコストを圧縮できる

ダウンロードクライアント

- 鍵はRAサーバで代理生成する
  - セキュリティ上のウィークポイント
- 鍵をICカードに格納するのは申請者自身
  - 鍵が不正に複製されないことを確認できる
  - 部局RAの負担減 を目論んだが…
- RA操作者が操作する端末(RAクライアント)とは別に申請者が操作する端末を用意する
  - RAクライアントと同じく部局RAに設置される

マスタレコード

- RAクライアントからの部局外の人員に対する証明書発行を拒否することは共通IDを用いた単純なアクセス制御では困難
- 所属部局を併記した共通IDのリストを別途管理する　＝**マスタレコード**

- 発行申請時の共通IDのタイプミスも検出できる
- 将来的には人事システムとの連携などの効率化が必要

試験運用で明らかになった問題点

試験運用として数部局でUT-CAの運用を行なっている

- IA運用側
  - マスタレコードの管理
    - より上位の機関による承認が必要
- 部局RA側
  - 通常業務に加えて過大な負担　→以後の発表にて
- 利用者側
  - 鍵受け渡し方法の検討
  - 利用者マニュアルの充実

利用者の負担：鍵受け渡し方法

- 現在、鍵はRAサーバで代理生成している
- 専用端末で空のICカードへの鍵書き込み操作を利用者本人にやってもらう
  - 不正防止の観点から
  - 場所の問題　時間の問題

- 別案1：部局RA担当者が鍵書き込みまで行なう
- 別案2：利用者本人の日常使用する端末でダウンロード・書き込みを行なう

まとめと今後の課題

- 東京大学内において全学展開を目指す認証局を構築している
  - 登録局の分散化
  - 複数人操作の強制
- 明らかになってきた問題点を解決し、実運用に耐えうる認証局にする
- 大学における認証局のあり方を提案する