

実証環境構築の進捗状況 ～ 公開鍵証明書との 連携について ～

2008年11月10日
シングルサインオン実証実験中間報告会

東京大学情報基盤センター
PKIプロジェクト
西村 健 ・ 佐藤 周行

構築環境

- IDプロバイダ (IdP)
- LDAPサーバ
- パスワード登録サーバ



公開鍵証明書との連携 (1/2)

- 既存の個人証明書(UT-CA証明書)と連携する
 - 証明書はICカードの形で提供されているが、常にICカードを利用できる環境にあるとは限らない
 - 文献サービスのような用途には証明書による強固な認証は不要



証明書を持つ者がオンラインで自由にパスワードを登録することができるLDAP認証を提供する

公開鍵証明書との連携 (2/2)

効果

- 複数の認証手段から選択することで、安全性と利便性のバランスを取ることができる
 - 同じエンティティに対して追加的な認証手段を提供する
- 証明書による間接的な認証を行うことによって、PKIの影響範囲を拡大することができる
- PKIの認証によってシンプルな実装が可能

実演

現状

- プロトタイプは構築済
- 属性管理システムを実装中
 - 管理者による管理／本人による管理
 - 証明書による認証／パスワードによる認証
- LDAPサーバ部分を独立して大学構成員の認証手段として提供することを模索
 - Ex. 学外からのVPN接続の認証