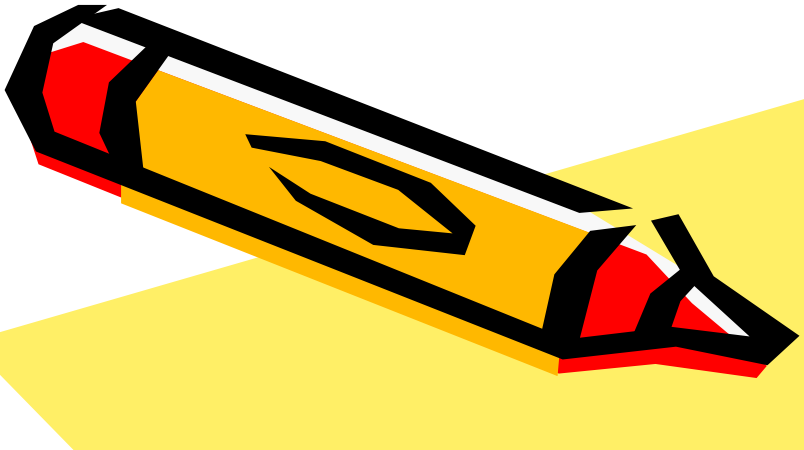
2008年7月23日

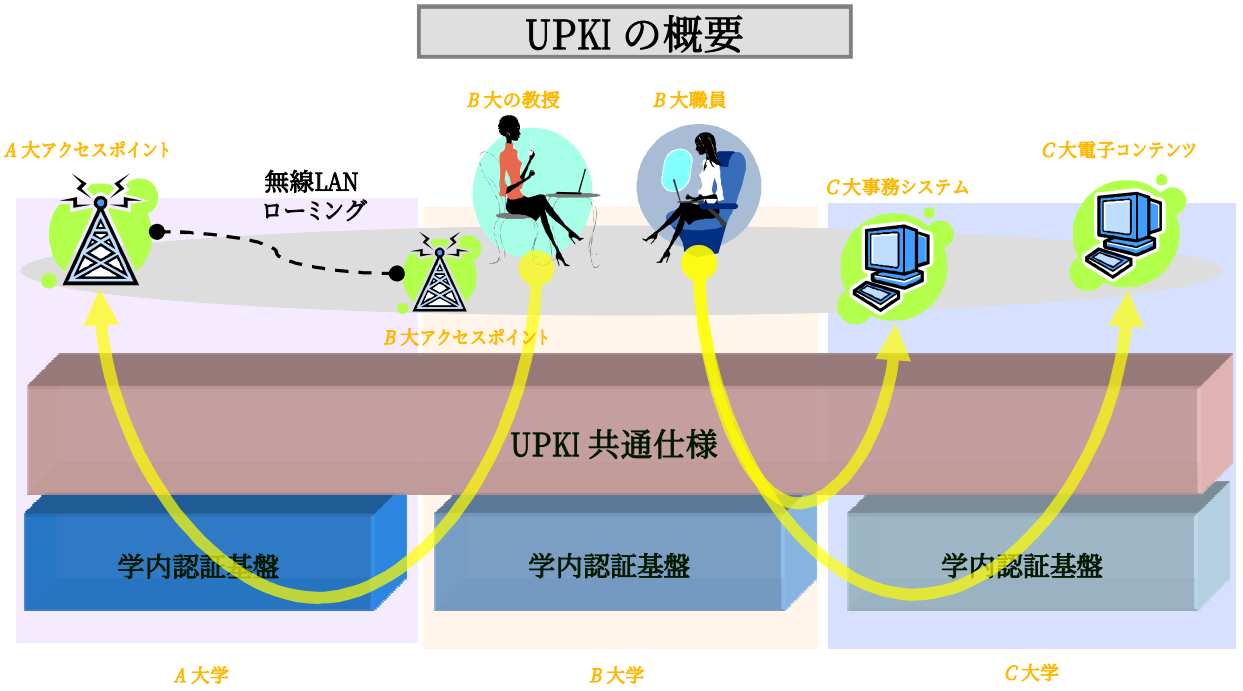


シングルサインオン実証実験の実施について

国立情報学研究所
学術情報ネットワーク運営・連携本部
認証作業部会

大学間連携のための
全国共同電子認証基盤（UPKI）とは

- 最先端学術情報基盤(Cyber Science Infrastructure)実現のため，大学等が保有する，教育・研究用計算機，電子コンテンツ，ネットワークおよび事務システムなどの学術情報資源を安心・安全かつ有効に活用するための電子認証基盤
- PKI（公開鍵認証基盤）を活用



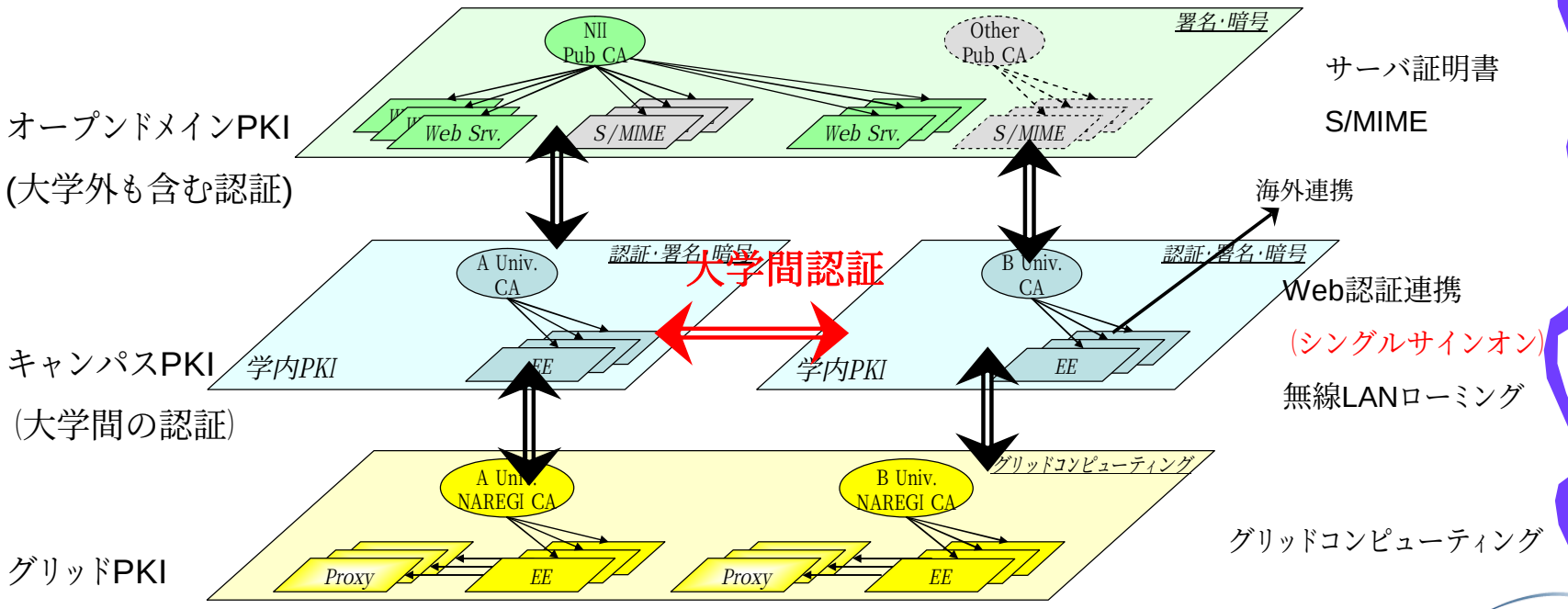
UPKI構築の全体スケジュール

	2006年	2007年	2008年	2009年以降
UPKI イニシアティブ	発足 ・仕様(案)の提示・導入事例の公開、仕様(案)への意見・要望 ・情報の共有・意見交換			
オープン認証	大学のサーバ証明、S/MIME			
UPKI 共通仕様	学内認証局 調達仕様ガイドライン 学内認証局のCP/CPSｶﾞｲﾄﾞﾗｲﾝ			
アプリケーション開発・相互運用	アプリケーションの調査、構築、実装	無線LANローミング	シングルサインオン	
認証局ソフトウェア	認証局ソフトウェアパッケージの開発	認証局ソフトウェアパッケージの配布、導入支援		

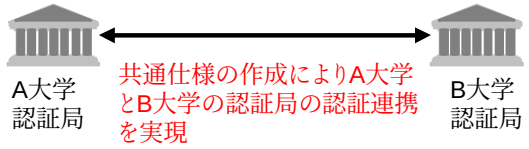
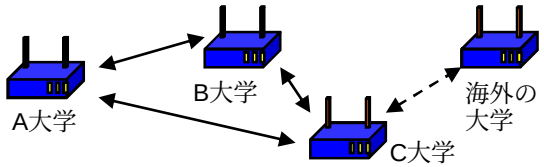
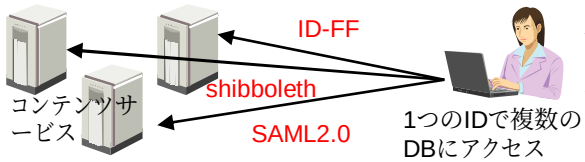
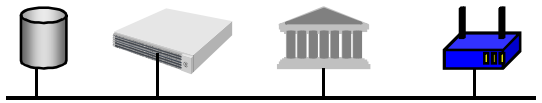
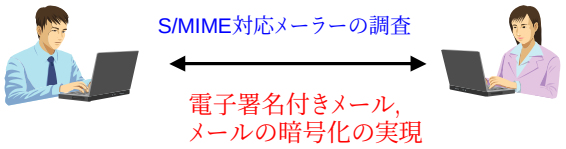
・各大学の認証基盤導入
・各大学との相互接続
・アプリケーションサービス連携
・社会産学連携の本格的運用

UPKIの基本アーキテクチャ

- 3階層のPKI (Public Key Infrastructure)による役割分担と連携

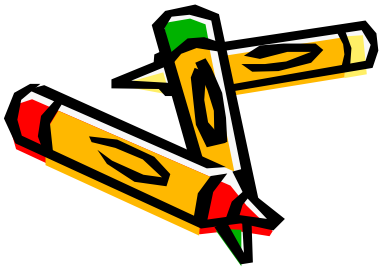


これまで実現したUPKIの成果

項番	事項	内容
1	「UPKI共通仕様」の作成と配布	 「UPKI共通仕様」の利用により大学等の ・学内認証局の構築 ・CP/CPS等の規程の整備 が容易に実現可能に
2	オープンドメイン認証局の構築とサーバ証明書の発行	 オープンドメイン認証局の構築により，全世界に通用するサーバ証明書を発行し，大学のWebサーバの実在性証明と通信の暗号化を実現
3	大学間無線LANローミングの実現	 eduroamによる大学間無線LANローミングを実現。海外のeduroam参加機関との連携も実現
4	コンテンツサービスのシングルサインオン実験	 各種データベースサーバへのシングルサインオンを実現するため，shibboleth，SAML2.0等の仕様を調査し，UPKIにふさわしい方式を検討
5	NAREGI-CAを利用した認証局ソフトウェアパッケージの開発	 オープンソースの認証局ソフトウェアあるNAREGI-CAを用いて，認証局を簡単に構築し，無線LAN認証を容易に実現できるソフトウェアを開発 これにより，大学の認証局構築を促進する
6	S/MIME証明書の試験利用	 S/MIME証明書を，認証関係者間で試験利用するとともに，対応メーラーの調査，WebメールでのS/MIME利用の調査研究を実施

UPKIとUPKI認証連携基盤

- 3層モデルのうち、キャンパスPKI層の学内認証と大学間認証を、シングルサインオンの技術で実現　→　*UPKI認証連携基盤*
- UPKI認証連携基盤は、「オープンドメインPKI層」、「グリッドPKI層」の本人確認にも利用
- 技術的には、SAML2.0標準を利用して、大学間の認証フェデレーション（認証を信頼するコミュニティ）の構築を目指す
- 　　→　*実証実験の実施*

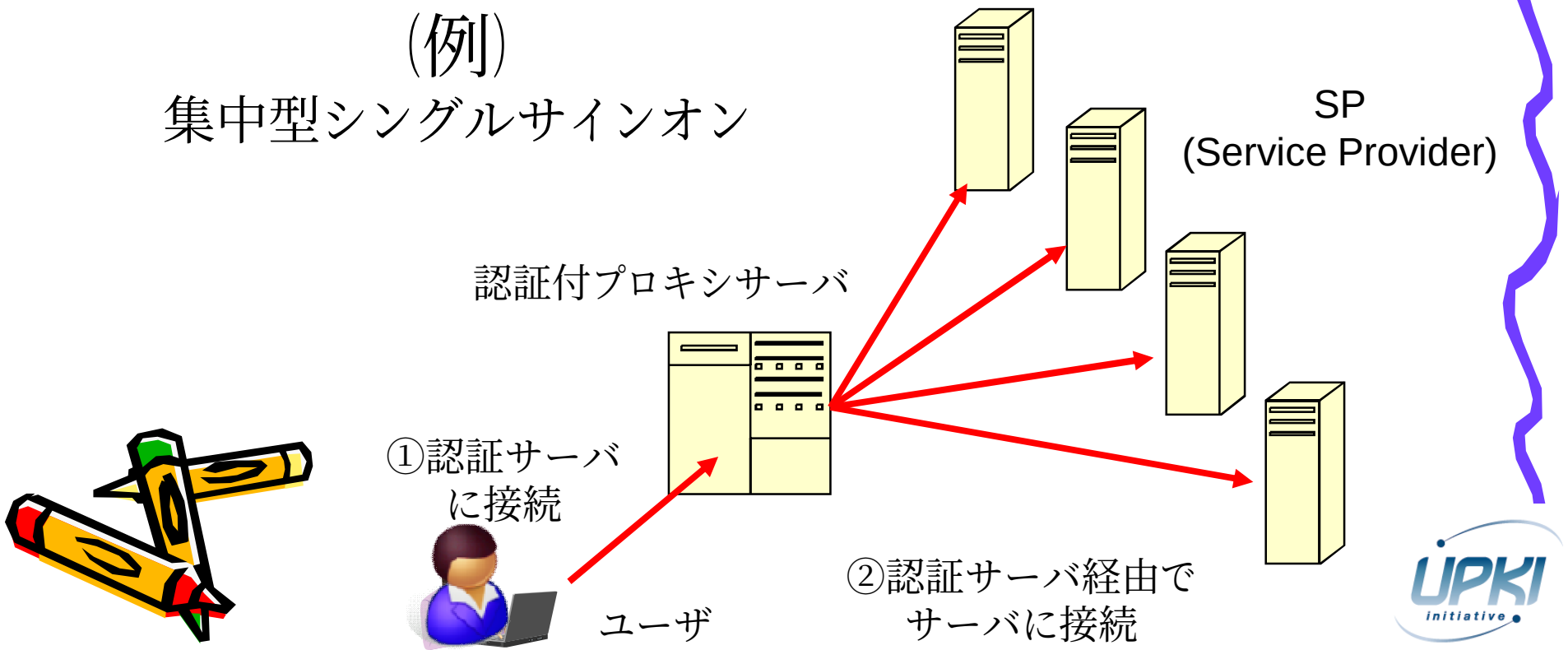


シングルサインオン(single sign on)

- 利用者が、1回のログイン手続きで、認証を必要とする複数のサービスを利用できるようにする仕組み
- 代わりにその1回のログイン手続きは十分セキュアにする

(注) 単にすべてのサービスで同じID/パスワードを使うのとは違う！

(例)
集中型シングルサインオン



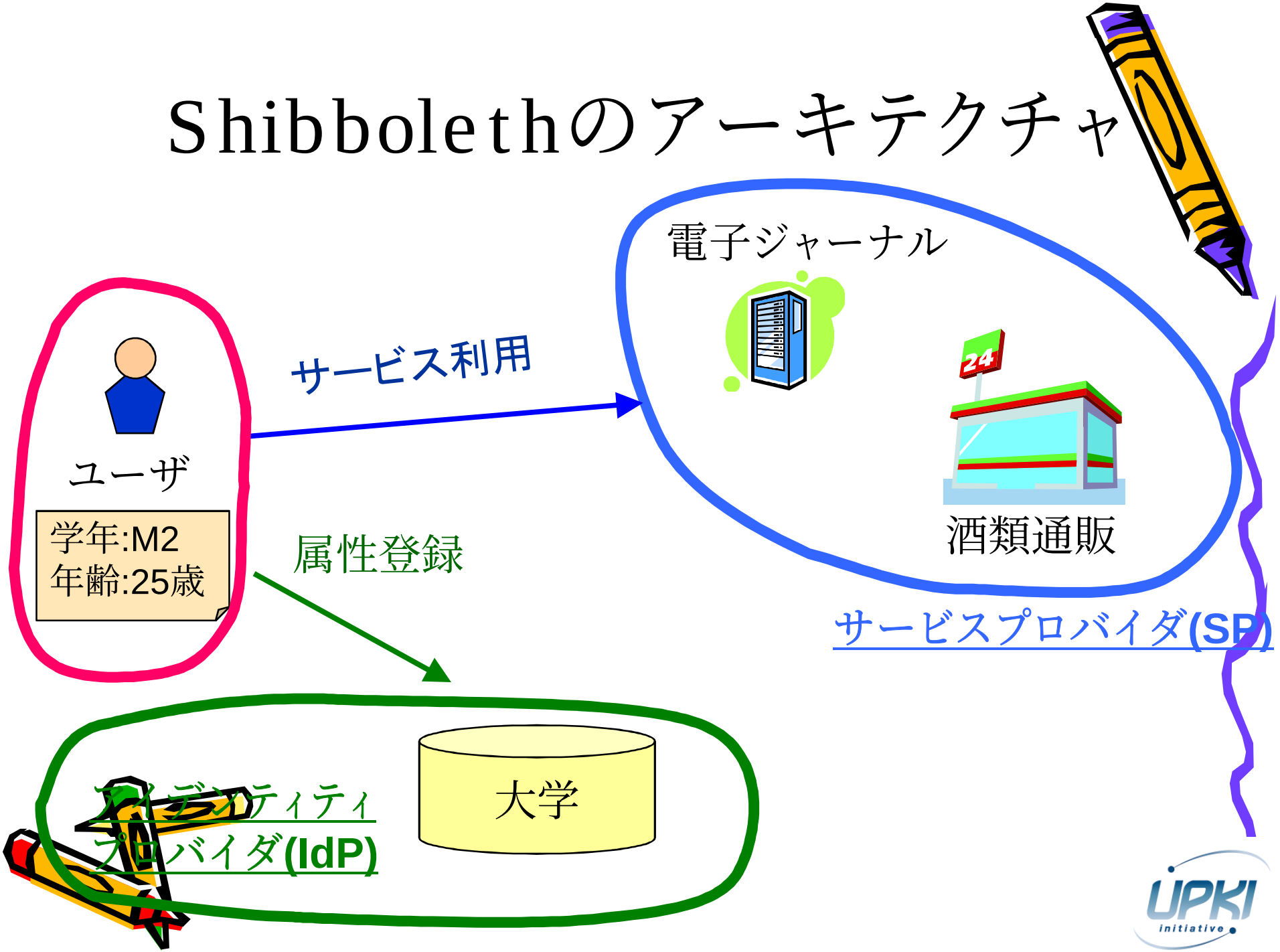
Shibboleth

Shibboleth

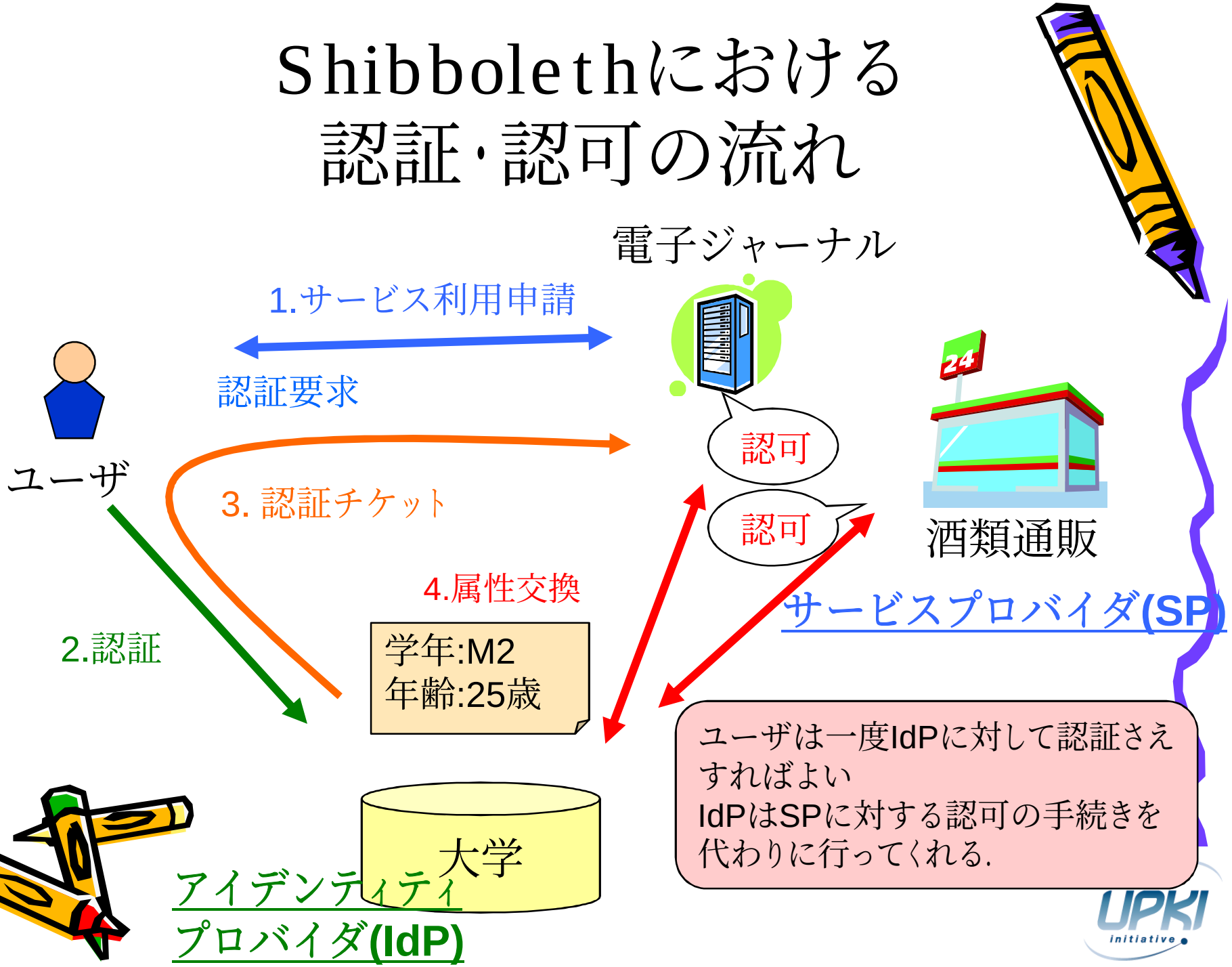
- Internet2/MACEプロジェクト
- SAMLをベースとした認証連携を実現するオープンソースの開発
  - SAML2.0準拠の実装であるShibboleth2.0が最新版(H20.3)
- 欧米の大学･図書館等で普及

[URL] http://shibboleth.internet2.edu/

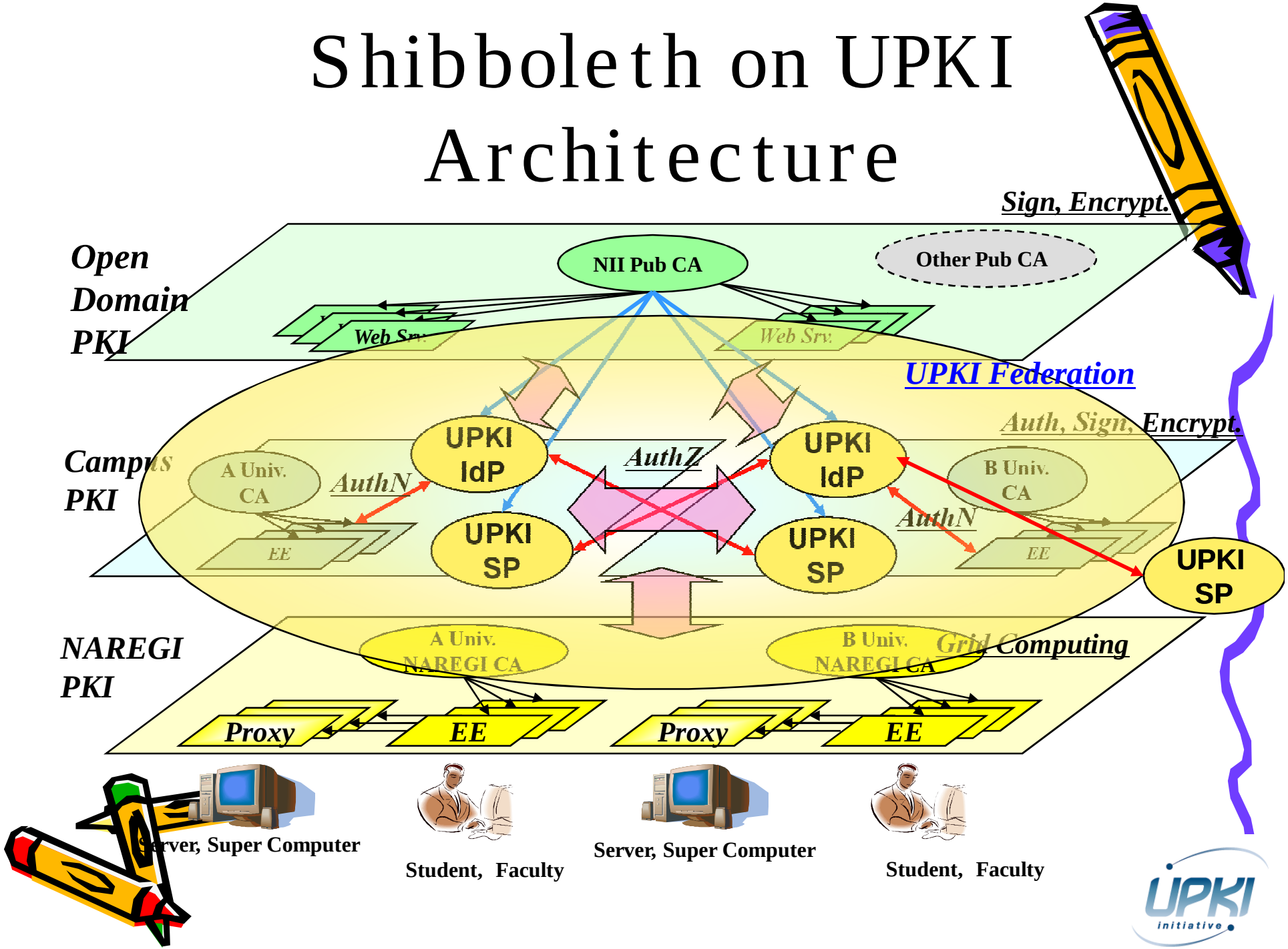
Shibbolethのアーキテクチャ



Shibbolethにおける認証･認可の流れ



Shibboleth on UPKI Architecture

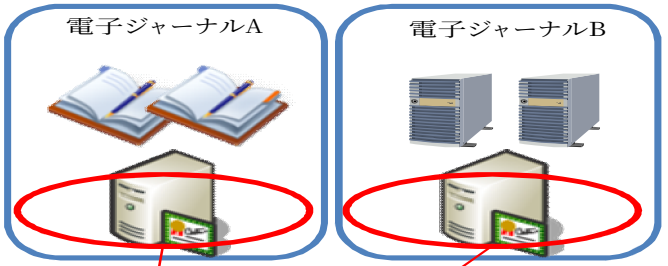


UPKI認証連携基盤の目標

現　状

○認証はサービス毎に必要

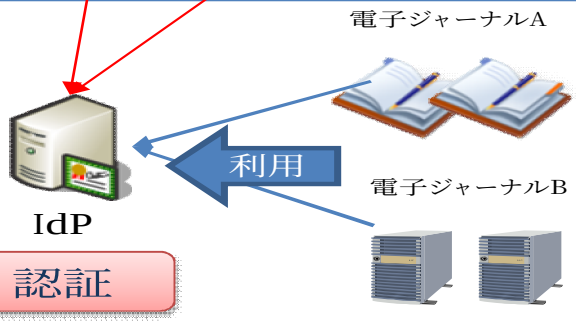
○各サービス分だけアカウントの管理が必要



実証実験

○サービス個別の認証について，サービスと認証を分離する

○認証管理の一元化を目指す



H21年度以降の目標

○学内の統合認証基盤として運用可能となる。

○多様な サービスへの対応
- ―サーバ証明書発行時の本人確認
- ―グリッド証明書発行時の本人確認
- ―無線LAN一時利用アカウントの発行