




TIES — Technologies for Information Environment Security

Sandy Shaw
University of Edinburgh



Aim

- ◆ To implement a pilot Public Key Infrastructure for authentication of H&FE users to services in the JISC Information Environment

Objectives

- ◆ Demonstrate proof of concept for an authentication service for the licensed resources of the JISC IE
- ◆ Identify practical issues of certificate handling by users and institutions
- ◆ Consider the wider use of digital certificate technology across the H&FE sector

Partners

- ◆ Lead partner
 - ◆ University of Edinburgh
 - ◆ EDINA
 - ◆ Computing Services
- ◆ Associate partners
 - ◆ University of Paisley
 - ◆ Stevenson College
 - ◆ Newark and Sherwood College
 - ◆ Institute of Physics Publishing

Scope

- ◆ Services in the JISC Information Environment ...
- ◆ ... accessed by standard browsers

- ◆ But, looking forward:
 - ◆ Local institutional services
 - ◆ Grid services
 - ◆ VLE resources

Assets

- ◆ Commercial
 - ◆ Market value of IE resources
- ◆ Institutions
 - ◆ Reputation
- ◆ Academic PKI
 - ◆ Services other than JISC IE

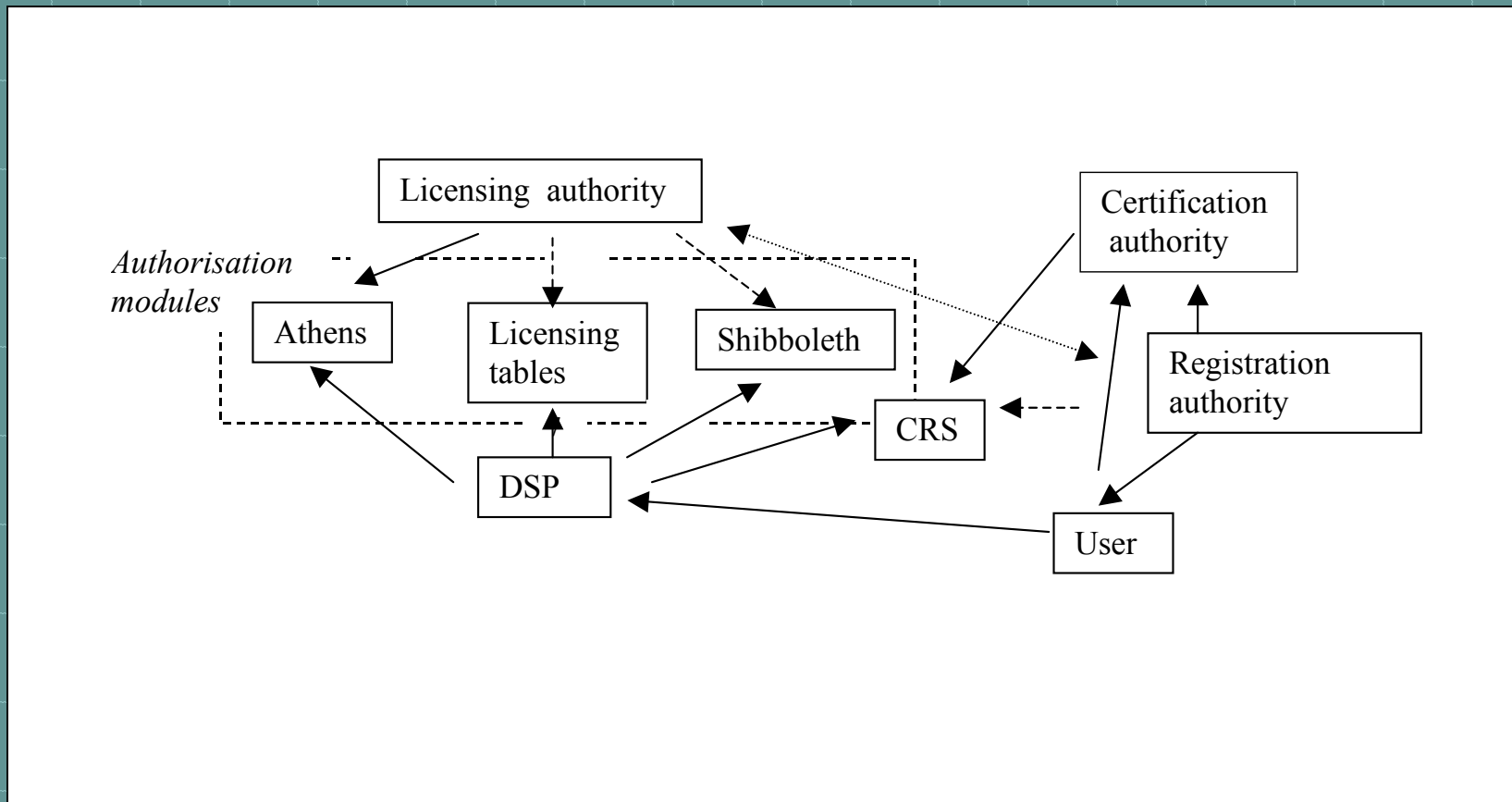
First pass on risk assessment

- ◆ JISC IE services
 - ◆ Low, for today's services
- ◆ Academic PKI
 - ◆ Moderate
- ◆ Future PKI applications
 - ◆ Potentially high
 - ◆ Importance of authorisation

Practical considerations

- ◆ Tenable procedures for institutions
- ◆ Tenable procedures for users
 - ◆ Users forget passwords
 - ◆ Users make mistakes
 - ◆ Manual export/import of certificates is non-trivial

TIES model



TIES components

- ◆ Certificate server
- ◆ Registration server
- ◆ DSP certificate verifier
- ◆ DSP authorisation package
 - ◆ Athens migration
 - ◆ Shibboleth
 - ◆ Licensing authority tables
- ◆ Institutional data model
- ◆ Technology watch
- ◆ Draft specification

Certificate distribution

- ◆ Methods:
 - ◆ CMC
 - ◆ CMP
 - ◆ Central key management
- ◆ Data formats
 - ◆ PKCS#7
 - ◆ PKCS#10
 - ◆ PKCS#12

Key usage

- ◆ Single key pair
- ◆ ... supporting digital signature
- ◆ ... but not non-repudiation

- ◆ Excludes data encipherment (secure email)

Policy

- ◆ Two-tier policies for institutions?
 - ◆ Basic level assurance for JISC IE
 - ◆ Higher level for additional services
- ◆ Academic PKI server policies
 - ◆ CA servers / RA servers / Certificate verifiers
- ◆ Authorisation policies?
- ◆ Important that all policies are congruent

Contacts

- ◆ Peter Burnhill <p.burnhill@ed.ac.uk>
- ◆ Sandy Shaw <s.shaw@ed.ac.uk>
- ◆ Christine Rees <c.rees@ed.ac.uk>

- ◆ Project: <http://edina.ac.uk/projects/ties>