



# **TIES II — Feasibility study for a JISC national certificate issuing service**

Middleware studies meeting

11 March 2004

# Aim

- ⇒ To consider the deployment of digital certificates to a significantly expanded e-Science community, and make recommendations to JISC

# Technical options

- ⇒ Community operated open source CA
- ⇒ Community operated insourced CA
- ⇒ Fully outsourced CA

# JISC IE Background

- ⇒ TIES I study recommended model of single national CA with institutional RAs
- ⇒ TIES I envisaged full rollout of certificates for JISC IE services as well as e-Science
- ⇒ But Shibboleth now adopted as preferred solution for IE
- ⇒ Remaining role for digital certificates?

# e-Science background

- ⇒ All e-Science resources currently require users to present identity certificates
- ⇒ One CA per country
- ⇒ One flavour: medium assurance certification
- ⇒ Unpopular with users and RAs
- ⇒ RAL CA issues certificates at ~£220 a pop
- ⇒ RAL CA will not scale above ~1000 certificates
- ⇒ Due to expand rapidly (~20,000 in 5 years)
- ⇒ How to afford? How to scale? How to make acceptable?  
How to handle non-institutional users?

# Approach

- ⇒ Two levels of assurance: basic and medium
- ⇒ CA based on commercially provided software
- ⇒ Single trust anchor

# Specification

- ⇒ Three types of certificate:
  - Two flavours of identity certificates for users:
    - Medium assurance for high-value and non-UK resources
    - Basic assurance for the rest (including students), UK-only
  - Certification for SSL-enabled servers engaged in cross-institutional secure communication
    - e.g., for Shibboleth servers
- ⇒ Uses: identity assurance (users and servers), signed email
- ⇒ Choice of insourced/outsourced solution

# Next steps

- ⇒ Briefing note for discussion
- ⇒ Confirm requirements (balance constraints and ambitions)
- ⇒ Firm up specification (numbers of RAs, certificates, policy, key usage, CRL regime)
- ⇒ Talk to suppliers

# Contacts

- ⇒ Sandy Shaw, EDINA
- ⇒ Fiona Culloch, EDINA
- ⇒ David Chadwick, University of Salford
  
- ⇒ <http://edina.ac.uk/projects/ties2/>
- ⇒ TIES I report:  
[http://edina.ac.uk/projects/ties/ties\\_23-9.pdf](http://edina.ac.uk/projects/ties/ties_23-9.pdf)