

# TIES

Technologies for Information Environment Security

[www.edina.ac.uk/projects/ties](http://www.edina.ac.uk/projects/ties)

## Will Ubiquitous Digital Certificates Benefit the Grid?

The TIES project (Technologies for Information Environment Security), supported under the JISC Authentication, Authorisation and Accounting (AAA) programme, is investigating the task of deploying digital (identity) certificates to all users in UK higher and further education.

TIES has considered the technical and administrative issues involved, both from the point of view of an institution and of a data service provider.

## Why Certificates?

X.509 digital certification is the prevalent technology for security in web-based and other IT applications. It enables users to identify themselves to remote services that supply licensed content (journals, maps, bibliographic data) and other sensitive resources, and provides a replacement for today's name/password schemes.

Crucially, the technology is already deployed in all mainstream desktop web browsers. Ideally, a user will move between different web sites without having to log in each time, with the browser automatically presenting the user's identity certificate to each target site.

## Is Widespread Deployment Feasible?

This was the central question for TIES, and the short answer is yes. There are two sides to the question: issuing certificates to institutional members, and integrating certificate-checking into data service providers' authentication mechanisms.

In both cases, solutions were readily implemented using mainly off-the-shelf, Open Source software. (Note, however, that an in-house approach is not necessarily the most cost-effective solution.)

Traditionally, certificates have been seen as costly to deploy, both in software costs and administrative overhead. TIES proposes to minimise these costs by building on each institution's existing procedures for user registration.

A database of staff and student records is supplied each night to the institution's Registration Authority (RA), which transmits changes to a central Certification Authority (CA).

The user logs-in to the CA using locally-provided credentials and downloads the certificate.

This approach is less stringent than that required by the UK e-Science CA, but is substantially cheaper and is about as secure as current arrangements upon which institutions implicitly rely for assignment of credentials to access local institutional services.

## Consequences for the Grid

Certificates are already successfully used to identify entities within the Grid.

However, given the level of assurance currently required for these certificates and the consequently high costs (around £220 per certificate) there is interest in lower-cost approaches. See also

<http://www.nesc.ac.uk/talks/140/2.pdf>

TIES has demonstrated that a roll-out of certificates across UK higher education is practical, though the total cost of ownership (TCO) of an in-house, Open Source solution, may actually exceed that of commercial outsourcing.

The question is whether TIES-level certificates (basic-level assurance) would be acceptable for authentication to Grid services (which currently require medium-level assurance).

Where the answer to this is 'no', one solution would be to enable institutions to use a two-tier approach, to give the choice of employing different levels of operational assurance for registration of different groups of user.

While the underlying registration mechanisms would be similar in both cases, staff requiring certificates with medium-level assurance would undergo additional checks for authentication of identity, and follow more secure procedures for certificate assignment.

Another solution may be to switch additional security checks from the identity certification stage (authentication) to the privilege assignment stage (authorisation).

The level of checking might vary according to the sensitivity of the Grid application.

This approach would be congruent with the eventual adoption of a formal privilege assignment framework, such as the X.509 Privilege Management model.

Contact the TIES project team at:

[EDINA@ed.ac.uk](mailto:EDINA@ed.ac.uk)

