

## UK E-SCIENCE CERTIFICATION AUTHORITY

Dr Jens G Jensen, Dr David Boyd  
CLRC e-Science Centre and UK Grid Support Centre

**Key words to describe the work:** PKI, authentication, certification authority, security, Grid

**Key Objectives:** The objective is to present the new Certification Authority to the UK e-Science community. Since Certification is the most fundamental part of any Public Key Infrastructure, it is important that we present this work to the community. For example, any member of any UK e-Science project will have to get a certificate from us to be able to work with the Grid.

**Motivation for the work (problems addressed):** The CA will issue digital certificates to members of e-Science projects allowing them to use Grid resources both inside the UK and in international collaborations.

A key element of working in a Grid environment is security, both for individuals and resources. The Certification Authority (CA) exists to provide participants in the programme with a trustable digital identify with which they can then access resources in a secure way.

The CA holds the most fundamental role in any Public Key Infrastructure (PKI). Its role is to issue (create and sign) certificates, make the valid certificates publicly accessible, revoke certificates when necessary and regularly issue revocation lists. The CA must also keep records of all its transactions.

The CA issues personal certificates to users; the purpose of the personal certificates is to allow users to identify themselves to remote entities. A personal certificate can also be used for digital signatures.

The CA also issues host (server) and service certificates. Each computer (resource) connected to the Grid must be able to identify itself. Similarly, in a web services framework, each service must be able to identify itself. The CA will provide such certificates as well.

Since the programme started in 2001, we have been issuing digital certificates in an informal way relying on personal checks by CA staff to confirm the identity of applicants. We are now ready to move the operation of the CA onto a more formal basis as defined in our Certificate Policy and Practice Statement (CPS), a document which all CAs are required to publish. Our intention is that the UK e-Science CA will be accepted both inside and outside the UK as operating a trustable authentication

procedure and thus its certificates will be widely accepted as proof of identity.

In particular, the procedure requires the appointment of Registration Authorities (RAs) at each location where a project has members who will need certificates issued. The RA's role in the PKI is to verify the identify of the users who request certificates. Thus, the trust in the CA and the certificates issued by the CA rests not only on the operational procedures of the CA but also on the trustworthiness of the RAs. To this end, the CA specifies rules for setting up RAs, and for operating an RA, and it is very important that we describe these rules to the projects and the e-Science centres, since the projects and centres will be involved in setting up RAs in order to ensure that their members can be verified when they request a certificate. Users will normally be required to go to a local RA bringing proof of identity so that the RA can approve their requests.

As usual, setting up a PKI is a trade-off between convenience and security. Make things too secure and people will find it difficult to follow the rules, or try to circumvent the security. Making things less secure makes life easier for the users but makes the identity less trusted. Resource administrators are less likely to allow people with less trusted identities to use their resources. Our aim is to build a "sufficiently secure" certification: it is not so secure that it is too difficult for users to obtain a certificate, but it is sufficiently secure that we are trusted by the Grid resource administrators and our international collaborators.

The process is made easier and more convenient for both the end users and the RAs by the fact that we

provide easy-to-use web interfaces to the CA. Users enter their personal details in a web form and the browser generates keys and submits the request. Once satisfied about the user's identity, the RA approves the request by going to the same web site, where approving or rejecting a certificate request is as simple as a few clicks with the mouse. Not only does this make life simpler for the RA, it also saves a lot of time. It is thus easier for local institutions to set up a new RA when the RA staff do not have to spend too much time or effort on RA procedures. The final step is for the CA to sign the user's certificate request using the CA's private key to create a valid certificate.

As a part of this security process, we need to explain the authentication process to the users and how authentication fits inside the PKI. We also need to explain the procedures to the users so that the transition to the new CA will be as painless as possible. The e-Science All-Hands meeting is an ideal opportunity for doing this and for answering questions from the people who will actually be involved in the process.