

Usability of the UK e-Science Certification Authority

1. AUTHORS

Jens G Jensen <j.jensen@rl.ac.uk>, Matthew Viljoen <m.j.viljoen@rl.ac.uk>, CCLRC.

2. ABSTRACT

The e-Science Certification Authority (CA) is a crucial component in the activities of the e-Science community. As one of the largest Grid CAs in the world, we have gained considerable experience with technical and operational issues. However, there are usability issues, some of which are inherent in a Public Key Infrastructure (PKI), others due to the level of assurance the CA must provide to be internationally accepted, others again for various technical reasons.

The purpose of this paper is to discuss the most important usability issues, the steps we have taken to alleviate them, as well as the steps we plan to take in the future.

3. DISCUSSION

The primary purpose of the Certification Authority (CA) is to deliver a production service, namely the issuing of X509 certificates with a certain level of assurance. To maintain this level of assurance a clearly defined procedure is necessary where the authenticity of users is verified by means of intermediate bodies known as Regional Authorities (RAs). Both users and RAs must follow this procedure closely, both in terms of meeting each other and dealing with identification documents, as well as interacting with the CA software via the web interface. Usability therefore becomes a major consideration in maintaining a PKI.

In this paper we investigate factors that affect usability of the CA. Such factors can be grouped into technical, policy-related, and PKI-specific, and some of them may be specific to Grids. As an example of technical factors, we consider how the upgrade this year addresses the most serious problems that have been encountered, namely robustness, scalability as well as the previous lack of browser support.

Apart from the traditional means of interacting with the CA software via the web interface, we also consider methods such as Java Applets and bash scripts. Scripts dramatically improve usability for some communities, and applets can facilitate the process of managing certificates and keys for communities who are new to PKIs.

Indeed, for many users new to certificates, the challenge of understanding PKI acts as a barrier and is the source of some problems that users encounter while using the CA. It has sometimes proved to be difficult to ascertain whether usability issues stem from this or from genuine problems concerning the CA and users' interaction with it. To this end we shall discuss surveys of specific user communities. Such surveys will additionally help us to assess concerns that were not addressed by the upgrade.

Aside from the current CA, we shall look at new technologies that can potentially increase security without affecting usability, for example, OCSP (Online Certificate Status Protocol). We shall consider factors influencing interoperability and coexistence between such solutions.

Finally we will explore usability implications to the CA of recent changes to UK law, in particular Data Protection Act (1998) and Freedom of Information Act (2000).