Contribution ID: **42** Type: **Poster**

Using hardware tokens to improve grid security

Describe the scientific/technical community and the scientific/technical activity using (planning to use) the EGEE infrastructure. A high-level description is needed (neither a detailed specialist report nor a list of references).

Hardware tokens offer the opportunity to store a grid certificate in a tamper-free environment. Grid security can be improved by using these hardware tokens to allow for 2-factor authentication. At Nikhef we have started using Aladdin eTokens to store and generated X.509 grid certificates and SSH public/private key pairs, on the Linux, Windows and Mac OS X platforms. We have also written a package to generate grid proxies directly from the token on all of these platforms.

Report on the experience (or the proposed activity). It would be very important to mention key services which are essential for the success of your activity on the EGEE infrastructure.

At Nikhef we have started using Aladdin eTokens to store and generated X.509 grid certificates and SSH public/private key pairs, on the Linux, Windows and Mac OS X platforms. We have also written a package to generate grid proxies directly from the token on all of these platforms.
Certificate Authorities in the UK and in the Czech republic are also in the process of using hardware tokens for grid authentication.

Describe the added value of the Grid for the scientific/technical activity you (plan to) do on the Grid. This should include the scale of the activity and of the potential user community and the relevance for other scientific or business applications

Hardware tokens offer the opportunity to store a grid certificate in a tamper-free environment. Grid security can be improved by using these hardware tokens to allow for 2-factor authentication. By 2-factor authentication we mean that authentication is based on 2 things, e.g. what you know (a password) and what you possess (a hardware token). Hardware tokens offer a secure and tamper-free environment on which a grid certificate can be stored or, better yet, generated. The private key of such a certificate can never be copied off the token, making it an ideal place to store security-sensitive information. These tokens can be used for storing personal grid certificates, SSH public/private key pairs but also robot certificates for use by Grid Portal sites.

Primary author: KEIJSER, Jan Just (NIKHEF)

Presenter: KEIJSER, Jan Just (NIKHEF)

Track Classification: Demo and Poster session