

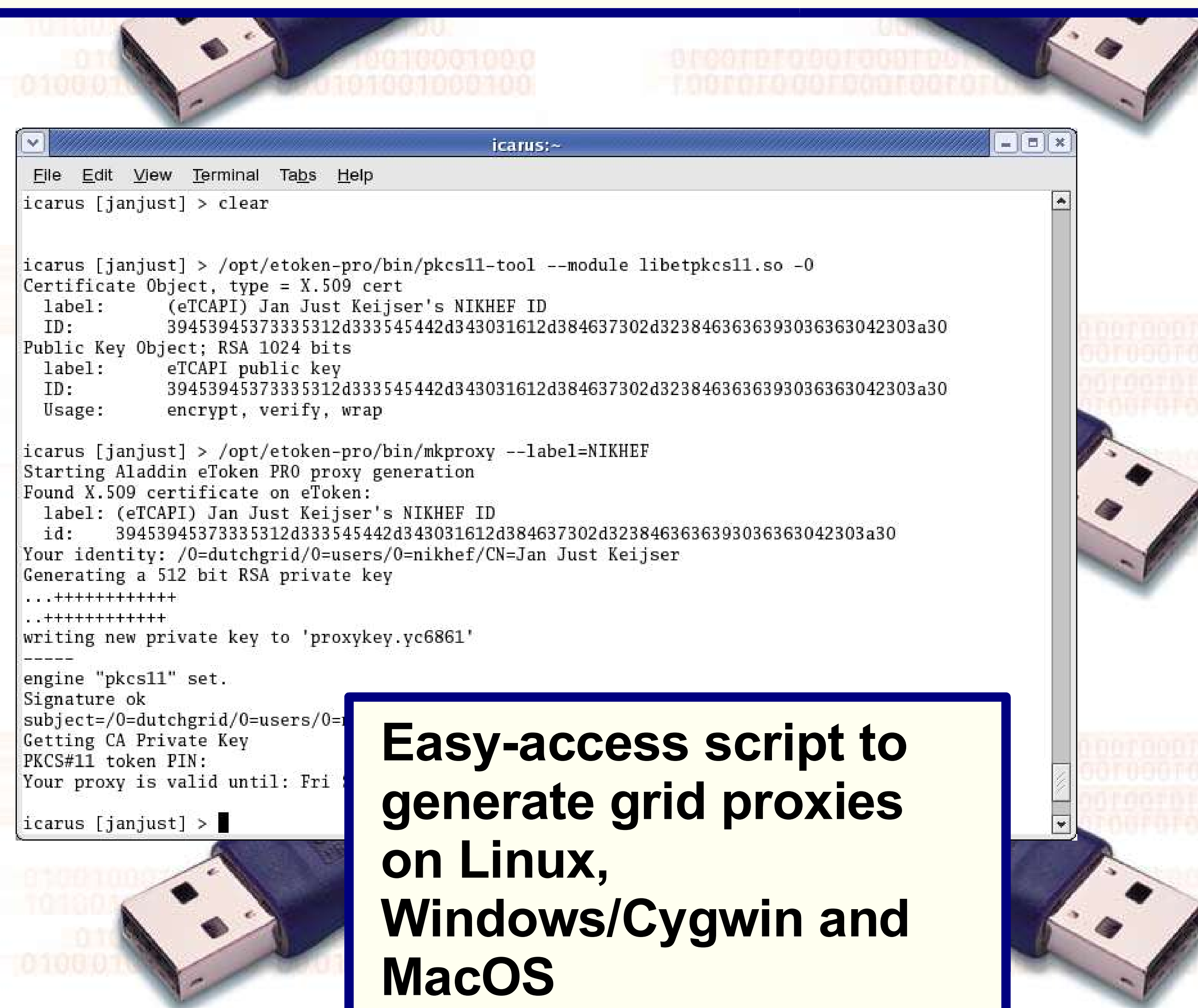
Using hardware tokens to improve grid security

Jan Just Keijser – Nikhef / Amsterdam

What are hardware tokens?

Hardware tokens are so-called smartcards with a USB form factor. At Nikhef we use Aladdin eToken PRO 32K tokens to store grid certificates. These tokens are supported on Linux, Windows and MacOS. They contain a miniature operating system, which can crypt and hash data. This allows us to generate an RSA key **on the token itself**.

Security can be improved by using these hardware tokens because it allows for two-factor authentication. Two-factor authentication means that authentication is based on two 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/X509 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.



Easy-access script to generate grid proxies on Linux, Windows/Cygwin and MacOS

What can hardware tokens be used for?

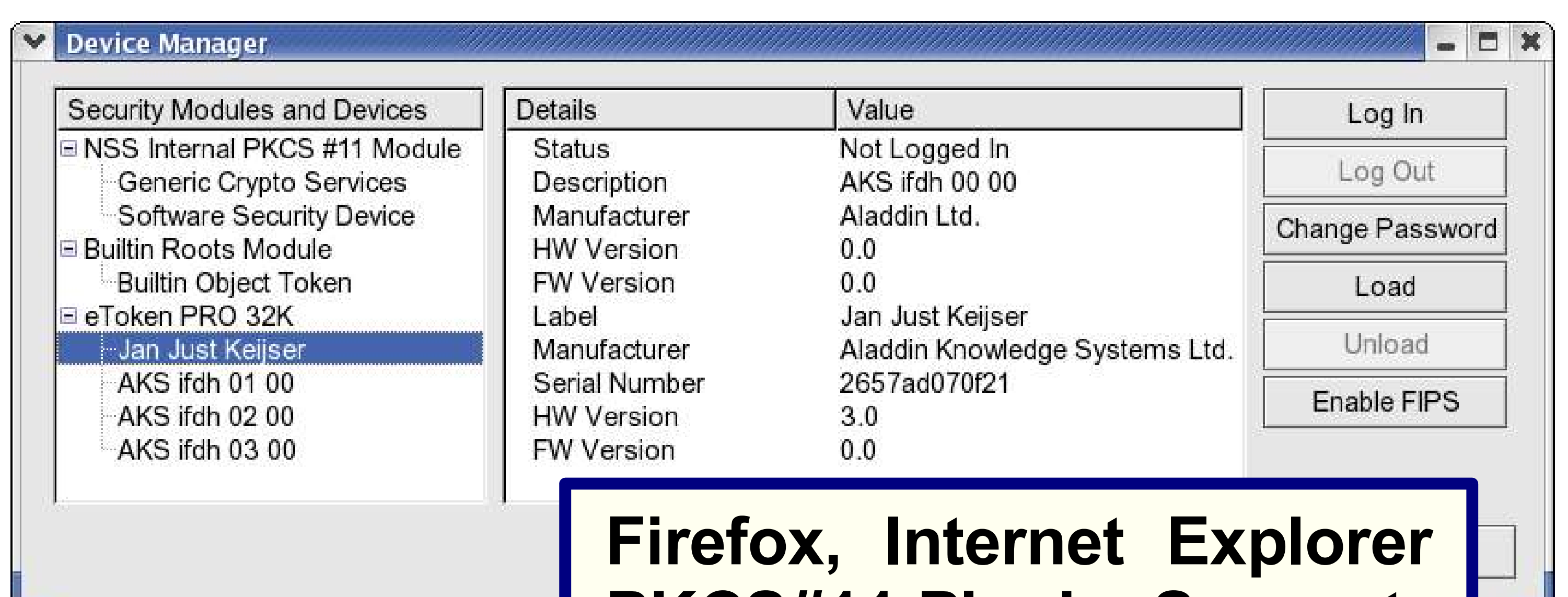
- Generate X509 grid certificates,
- Store X509 grid certificates,
- Store SSH public/private keypairs,
- Secure web access using a browser PKCS#11 plugin,
- Robot certificates for portals.

Developed and deployed at Nikhef

- mkproxy: a shell script with the same syntax as 'grid-proxy-init' to generate grid proxies from a certificate on the token. The same script is used for the Linux, Windows/Cygwin and MacOS platforms,
- An RPM for easy installation of all etoken drivers and tools on RHEL4, Fedora 5/6 and Suse 10,
- A Debian package for Debian Etch/Ubuntu.

Snags and Issues

- Our eTokens are based on Siemens CardOS 4.2B, which until recently was not supported by the OpenSC package,
- The latest version of OpenSC, 0.11.4, **does** support these tokens, but information stored on the tokens using OpenSC is not visible to the Aladdin RTE client software and vice versa,
- It is not possible (yet) to generate SSH keypairs on the token itself. These must be generated locally first,
- There is no FIPS-140 certification yet,
- The 'etoken-mkproxy' package does not support VOMS yet. A Beta of Voms-for-Windows which also supports token access is available at https://meta.cesnet.cz/mediawiki/index.php/VOMS_on_MS_Windows.



Firefox, Internet Explorer PKCS#11 Plugin Support

More Information

http://www.nikhef.nl/pub/projects/grid/gridwiki/index.php/Using_an_Aladdin_eToken_PRO_to_store_grid_certificates