

## **Expert Report (TCS Testing Phase 1)**

David Groep (Nikhef)

Probably the most significant improvement experienced in the very fast validation time, combined with the fact that DigiCert Validation has access to and is willing to use a wider range of reliable data sources to identify organisations. This agility was especially noticeable for code signing and extended-validation certificates. For eScience Personal certs, we have been able to make the transition to the 3rd generation TCS almost completely transparent: naming will stay the same, and in most cases users will not have to take any action. For this to work, subscribers have to register the very same organization name with DigiCert validation that they used in the previous Confusa system: here the wider range of acceptable organization names that DigiCert allows really helps.

The DigiCert also makes machine-to-machine authentication certificates available for the first time in TCS. These “Grid Robot” type certs look superficially similar to personal certs, but can be issued (via CertCentral) for use in web portals and science gateways and there enable several additional permitted uses of e-Infrastructures. This should make Robot certificates more widely available across Europe.

The fact that the DigiCert API now becomes available to subscribers presents a significant benefit – at least for those who have some programming skills. Bulk operations, including requesting, approving, and installing certificates on server clusters can now be fully scripted. The potential downside is that the API is extremely rich and ‘powerful’, and subscribers should take extra care to make sure the tools and credentials for API use do not fall in the wrong hands. Both API and portal are powerful and they are a real blessing for those subscribers knowledgeable about PKI and having programming skills. Others should be careful and regularly review issued certs and active API credentials in the CertCentral portal.

In summary, the experience has been very positive. The challenge before us will be how to present all these capabilities to the Subscribers and how to manage the transition process: the with more powerful tools available to them, all will need to exercise some restraint in using them to ensure that the use is compatible with the policies and intended practices of the new service.