Kalmarunion-NorduGRID CA

This project has since been folded into the TCS Personal/Grid Certificate Profile work in Terena

Purpose

The current CA operations for NorduGRID is a manual, highly person-dependent process which does not scale to more than a few GRID-users. The purpose of this project is to automate the identity proofing and CA issuance processes.

Goals/Deliverables

- Stand up an Online-CA for a sub-arc of the NorduGRID CA trust using a SAML-based federated login operated in the Kalmar Union cross-federation.
- Describe and deploy any new/changed RA-processes resulting from this change.
- Certify the Online-CA against the IGTF policy.

Timeline

Activities

What	When	RP	Due

Architecture

The basic idea is to spread the load of identity proofing by bootstrapping from any existing identity management already done today by home institutions around the Nordic countries while preserving the current organization of the NorduGRID CA. Today all GRID-certificates are issued by a single person working out of Denmark and while there may be economic benefits of sharing this resource between all NorduGRID members the identity proofing process used today scales poorly. By building on existing identity management processes it will be possible to increase the number of GRID users without increasing cost.

One way to delegate responsibility for identity proofing is to use a SAML identity federation to request authentication from any of the member organizations of that federation. Technically the SAML federation is a trust bridge using signed XML metadata documents to convey that a federation operator has vetted the identity management processes against a policy defined by the federation. In other words the members of the federation (which in our case would include the NorduGRID CA) can trust that identity proofing process is comparable across all members of the federation.

The Kalmar Union is a policy and technical infrastructure which supports the bridging of several identity federations who support comparable policies. The Kalmar Union enables the NorduGRID CA to technically remain part of the Danish e-infrastructure while offering its services to all Nordic countries.

There are several ways to realize an Online CA service. The easiest is to build a web-based service where a user is able to produce and revoke certificates. Such a service can easily be used together with a SAML identity consumer (aka "service provider" or "SP"). From the point of view of the CA service each session will have associated attributes provided by the users SAML identity provider such as a name, an affiliation and an email address. These attributes can of course be used as input to the certificate profiling.

There are already any number of these web-based CAs that can produce (eg) a pkcs#12 token or (if given a CSR) produce a simple certificate or certificate chain. Hence this project will in all likelihood not be forced to develop any actual software.