Middleware Requirements for Credential Validation

The wish list for the authentication functionality from EGI

Peter Solagna, EGI.eu – peter.solagna@egi.eu
David Groep, Nikhef and BiG Grid, the Dutch NGI,EGI

e-infrastructure

Why the wishlist?

- Recurring issues
  - Trust anchor releases repeatedly run into ‘trouble’ in deployment
    - Inconsistencies in the distribution itself (1.39/1.41)
    - Increasing number of trust anchors
    - Supposedly-standard features not supported in M/W
  - Middleware behaviour ‘suddenly’ changes
    - Use of namespaces Relying Party Defined Namespaces Constrains (RPDNC) format in VOMS/Admin implemented in 2009 appeared in production in 2011. It is a useful change, but it needs to be well-advertised
  - Operational issues
    - CRL downloading *and checking* is not reliable
      - in recent EGI ops VO incident, revocation did not take effect at some sites even after 18 hours
- For the future
  - try to prevent spreading of Network Security Service library use in m/w
    since this is dangerous for scalability and stability
  - re-confirm adherence to Community Best Practices and standards

Wish List: functionality

- Support throughout all middleware for the SHA-2 family of hash algorithms for X.509 certificates
  - Starting from Jan-2012 SHA-2 based certs may start to appear
- All proxy certs should have RSA key size >=1024
  - RSA512 can be cracked within the life time of the proxy
- Support for OCSP allowing for *both* use in
  - AIA in the EE certificates itself
  - For site-configured trusted responders
- Support any number of CAs
- Failures should be graceful
  - incorrect or expired data for a single trust anchor should not affect the other trust anchors in the set

Wish List: compliance

- Honour meaning and scope on extensions
  - an attribute that says emailProtection is to protect email, not for signing documents, etc.
- Accept RFC3820 proxies *(Proxy Certificate Profile)*
  - and do the proper thing for *proxyPathLen* constraints
  - beware of NSS again!
- Allow CRL files to be updated on a file system
  - be prepared to re-read such files and implement new CRL contents at any time
- Allow middleware to make authorization decisions based on the certificate policy OID extension.

Wish List: don't break it!

- Continue to support drop-in (directory based) trust anchor distributions
  - No monolithic databases please, no NSS on disk
- Announce semantic changes to EGI/NGI&IGTF
  - E.g. moving to namespaces may need preparation for RPs
  - Document, and tell which component does what
- The signing_policy format is not sufficiently expressive/ well-defined, even for the current use cases.
  - Could EMI contribute to the drafting of a new standard for an RPDNC language?
    - based on the GFD.189 analysis
  - Participate in OGF's CAOPS-WG

Thanks!