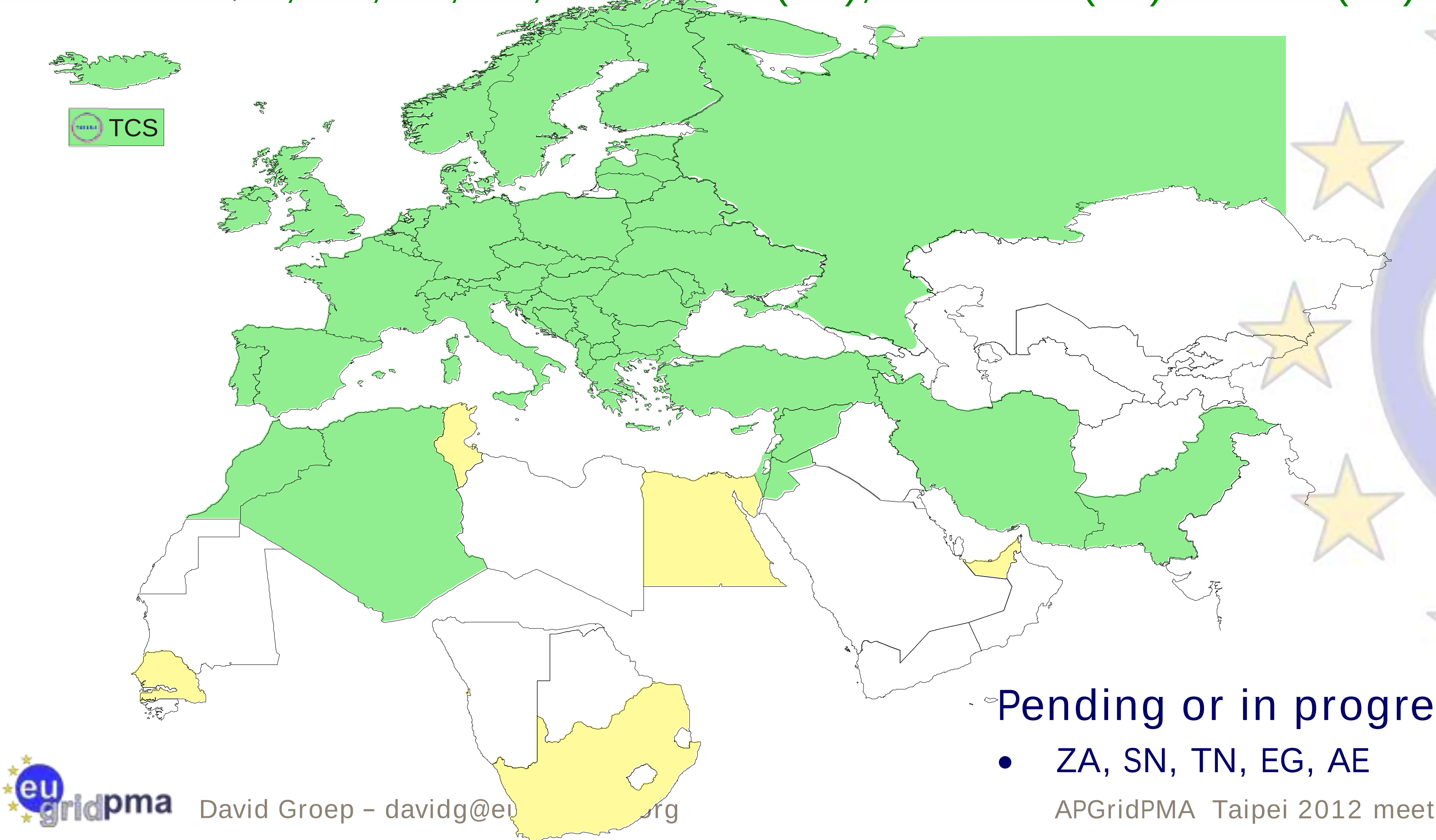
EUGridPMA

Status Review … and proposals

February 28, 2012
Taipei, TW

Geographical coverage of the EUGridPMA

- 25 of 27 EU member states (all except LU, MT)
- + AM, CH, DZ, HR, IL, IR, IS, JO, MA, MD, ME, MK, NO, PK, RO, RS, RU, SY, TR, UA, CERN (int), DoEGrids(US)* + TCS (EU)



Pending or in progress

- ZA, SN, TN, EG, AE

Current Topics in the EUGridPMA

- New TACAR policy (simpler!) approved
- Scaling issues for host certificates and automation
- PKP Guidelines clarification ongoing
- more 'EGI-friendly' pre-release schedule

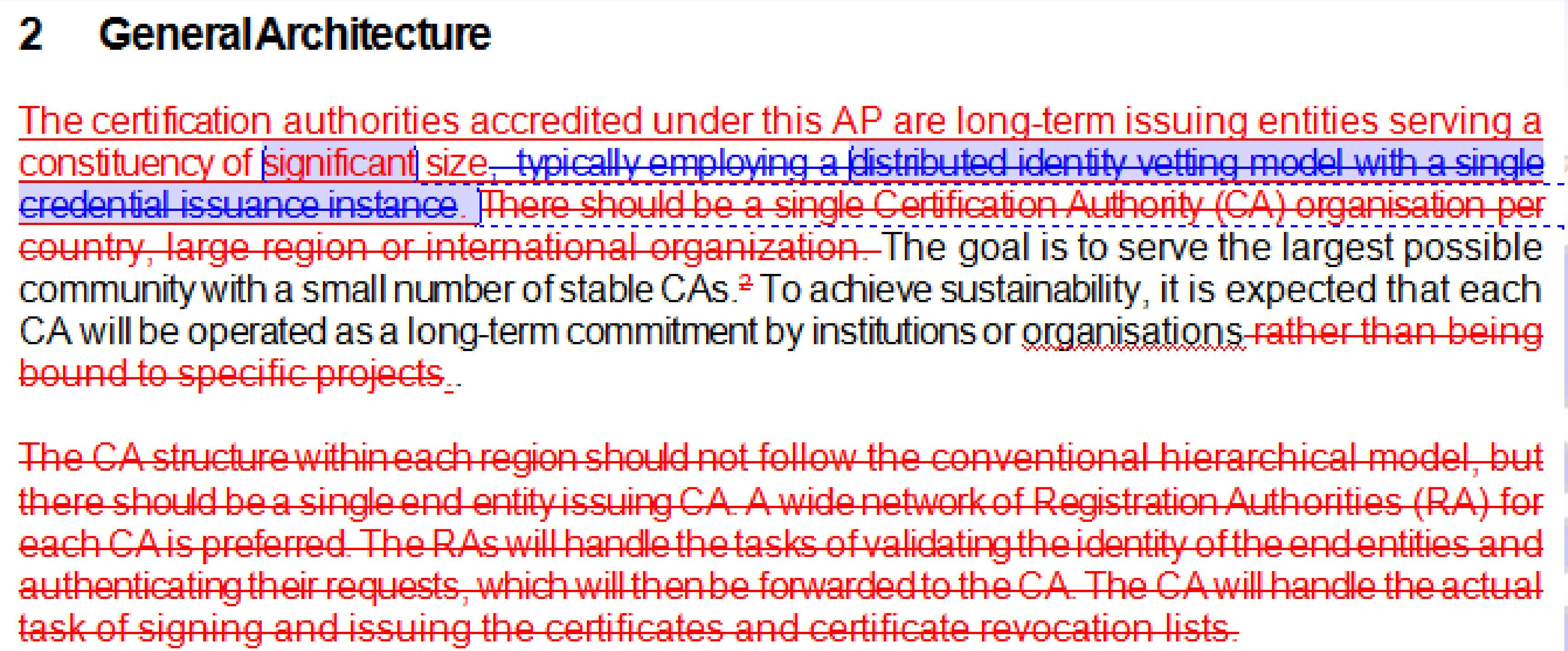
- Updates to the Classic AP (v4.4)
- Coordinated action by EGI.eu towards middleware providers for our AuthN needs

  and the SHA-2 and RFC-proxy issue
- Authorization Operations Guideline proposal

Updates to Classic AP

- Aim: make Classic AP a technical requirements document like the others (SLCS, MICS)
- Proposed changes should be minimal:
  - (re)move reference to one CA per country/region
    for EUGridPMA, this moved to Accreditation Guidelines
  - upgrade minimal EE key length to 2048 RSA-bits
  - upgrade key length for *new* CAs to 4096 RSA-bits
  - cleanup renewal for HSM-supported keys based thereon

(re)move the constituency scope part



2 General Architecture

The certification authorities accredited under this AP are long-term issuing entities serving a constituency of significant size~~, typically employing a distributed identity vetting model with a single credential issuance instance.~~ ~~There should be a single Certification Authority (CA) organisation per country, large region or international organization.~~ The goal is to serve the largest possible community with a small number of stable CAs.[2] To achieve sustainability, it is expected that each CA will be operated as a long-term commitment by institutions or organisations ~~rather than being bound to specific projects~~..

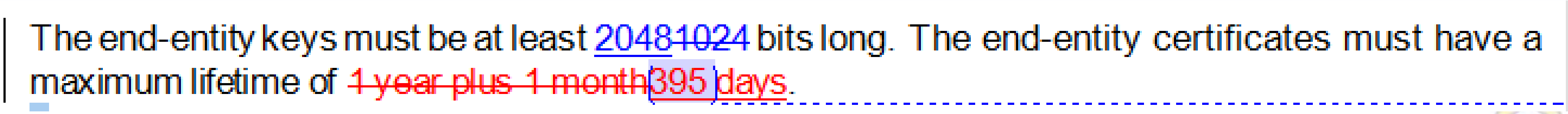
~~The CA structure within each region should not follow the conventional hierarchical model, but there should be a single end entity issuing CA. A wide network of Registration Authorities (RA) for each CA is preferred. The RAs will handle the tasks of validating the identity of the end entities and authenticating their requests, which will then be forwarded to the CA. The CA will handle the actual task of signing and issuing the certificates and certificate revocation lists.~~

NEW DRAFT

The certification authorities accredited under this AP are long-term issuing entities serving a constituency of significant size. The goal is to serve the largest possible community with a small number of stable CAs. To achieve sustainability, it is expected that each CA will be operated as a long-term commitment by institutions or organisations.

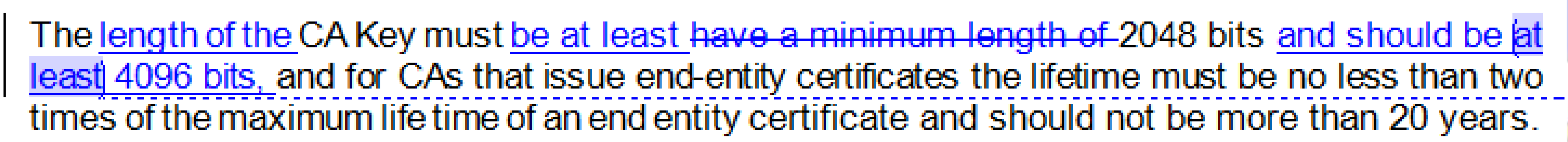
Key lengths

- For EECs increase to 2048 bits



The end-entity keys must be at least 2048~~1024~~ bits long. The end-entity certificates must have a maximum lifetime of ~~1 year plus 1 month~~395 days.

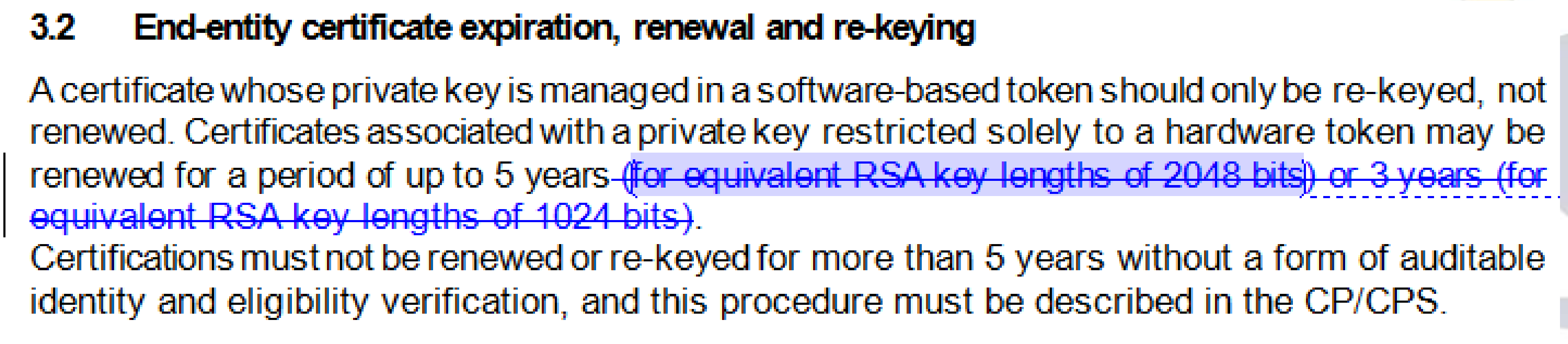
- and to 395 or 400 days
  - 397 is needed to allow for 31-day months in a leap year
- and for CAs to preferably 4096 for new CAs



The length of the CA Key must be at least ~~have a minimum length of~~ 2048 bits and should be at least 4096 bits, and for CAs that issue end-entity certificates the lifetime must be no less than two times of the maximum life time of an end entity certificate and should not be more than 20 years.

HSM backed key pairs - cleanup

- Remove reference to key length
  as it is now superfluous: all keys are 2048+



3.2 End-entity certificate expiration, renewal and re-keying

A certificate whose private key is managed in a software-based token should only be re-keyed, not renewed. Certificates associated with a private key restricted solely to a hardware token may be renewed for a period of up to 5 years ~~(for equivalent RSA key lengths of 2048 bits) or 3 years (for equivalent RSA key lengths of 1024 bits)~~.
Certifications must not be renewed or re-keyed for more than 5 years without a form of auditable identity and eligibility verification, and this procedure must be described in the CP/CPS.

THE IGTF WISH LIST AND EGI

Credential Validation Middleware Requests

compiling the wish list for authN functionality for EGI

David Groep, Nikhef and BiG Grid, the Dutch NGI, for EGI.eu global task O-E-15

This work is supported by EGI-InSPIRE (RI-251323) under NA2

Why, and Why Now?

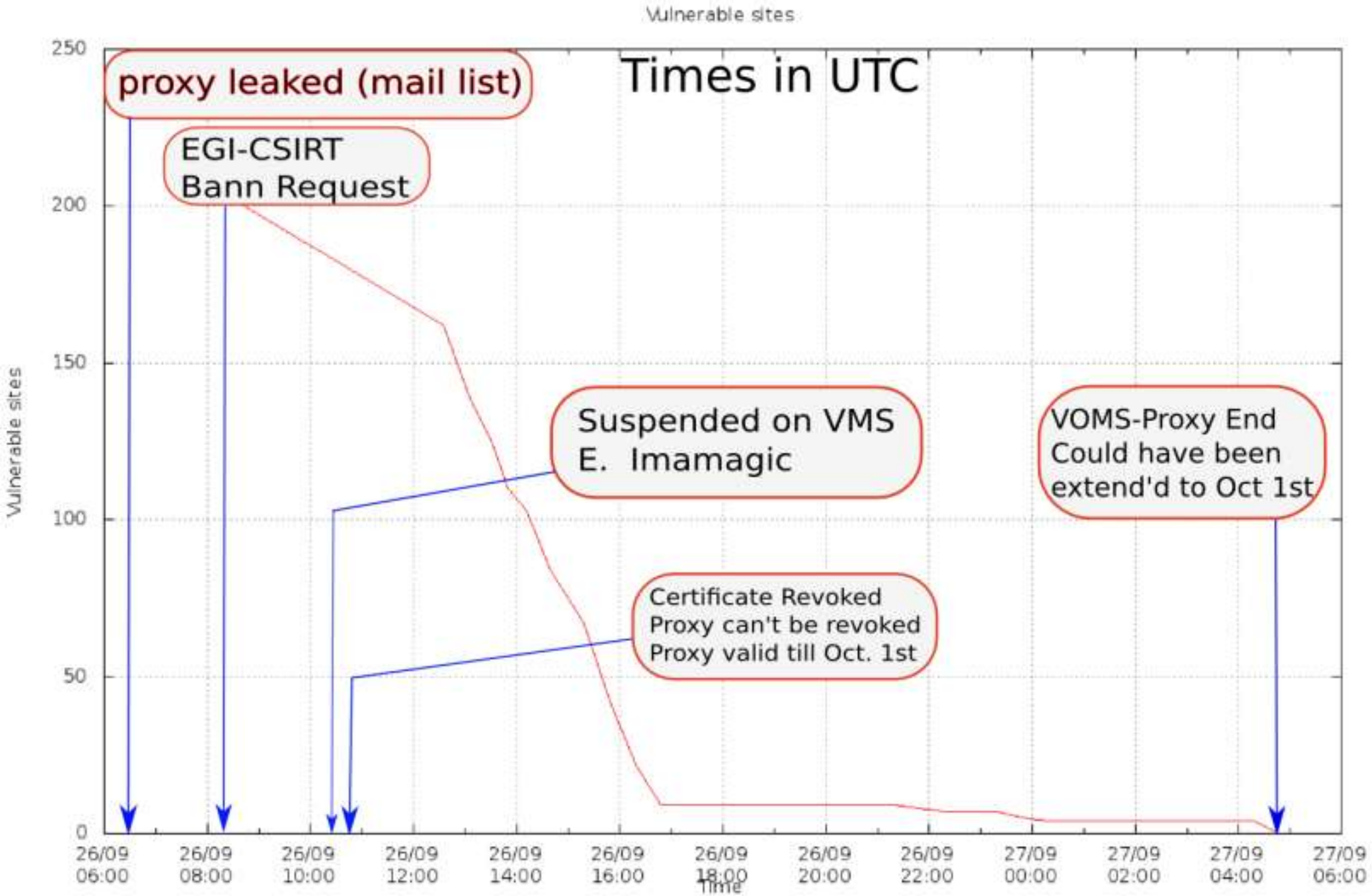
- Trust anchor releases repeatedly run into ‘trouble’ in deployment
  - – inconsistencies in the distribution itself (1.39/1.41)
  - – increasing number of trust anchors
  - – supposedly-standard features not supported in M/W
- Middleware behaviour ‘suddenly’ changes
  - – use of namespaces RPDNC format in VOMS/Admin implemented in 2009 appeared in production in 2011
    http://indico.cern.ch/getFile.py/access?contribId=16&resId=9&materialId=slides&confId=73381
  - – changes are useful, but not always sufficiently-well advertised

More reasons why

- Operational issues
  - CRL downloading *and checking* is not reliable
  - lots of superfluous downloads
  - in recent EGI ops VO incident, revocation did not take effect at some sites even after 18 hours
- Future hazards
  - try to prevent spreading of NSS library use in m/w since this is dangerous for scalability and stability
  - re-confirm adherence to CBP’s and standards

Effect of revocation ...

graphic: Sven Gabriel,Nikhef, for EGI.eu under contract O-E-16



proxy leaked (mail list)

Times in UTC

EGI-CSIRT
Bann Request

Suspended on VMS
E. Imamagic

VOMS-Proxy End
Could have been
extend'd to Oct 1st

Certificate Revoked
Proxy can't be revoked
Proxy valid till Oct. 1st

My Wish List: functionality

- Support for OCSP allowing for ***both*** use of
  - AIA in the EE certificates itself, and
  - for site-configured trusted responders
- Support throughout all middleware for SHA-2
  - starting January 2012, SHA-2 based certs may start to appear 'in the wild' without further warning…
- Support any number of CAs
- accept RFC3820 proxies everywhere

- *and a bit more… and stay away from Mozilla nss*

Where does the wish list go?

- via EGI TCB to the middleware providers with which EGI has an MoU
  - EMI – harmonize the stack, and define functional unity in any Common Authentication Library
  - IGE – is consistent, but needs OCSP support; and beware of NSS in moving to Fedora
- track progress using EGI mechanisms

EGI RT progress

- Trackers created for relevant technical issues
  - 3074 Unit Test for CRL refresh
  - 3075 Common Authentication Library (EMI) to configure the accepted proxy
  - 3076 Support for OCSP (EMI + IGE)
  - 3077 Argus to support OID extensions *but now Argus wants an explicit list of OIDs to convert each one into an XACML policy* ☹
  - 3078 SHA-2 family support*
  - 3079 Default key size for proxies >=1024
  - 3080 RPDNC constraints support
  - 3081 drop-in trust anchor distribution support

On #3078 “SHA-2 support”

- all modern middleware libraries supports it
  - but *not* all modern M/W still handles legacy GT2 proxies
  - in the case of jGlobus2, it’s even mutually exclusive
- and some M/W still stuck without RFC proxies
- moving to SHA-2 *now* would cause trouble

Current state of affairs and ideas

- There are various pieces of middleware and experiment-ware that need to be made ready for SHA-2 or RFC proxy support
  - SHA-2: dCache, BeStMan (RFC proxies already supported by these)
  - RFC: Argus, CREAM, WMS, DIRAC, … → SHA-2 should work, not tested…
- For EMI products the current time line is the EMI-2 release in April/May
  - OSG ?
- It may be many weeks before the affected products can be endorsed by UMD for generic deployment on EGI sites → run into the summer holidays
  - EMI-2 is a major release with many changes
- During the whole time the LHC run will be ongoing and nobody will be keen on significant upgrades → rather target December
- Nobody wants to upgrade right before the Xmas period, so we end up in early 2013, right after the winter conferences…
- We would have a year to get the 3 CAs fixed
  - Affected users could also use their CERN CA certificates instead
  - Affected services would not have an obvious alternative

Time line proposal by IGTF

… finally, with EGI, things started moving, and SHA-1 is on the brink of falling, so we should keep the pressure on…

- RAT (extended with more experts please!) does risk assessment of staying with SHA-1 for the next year, in light of current cryptanalytic evelopments and the deployment issues identified
- if SHA-1 is broken, the RAT makes an immediate assessment based on the integrity of the subscriber certs, and will act regardless of RP deployment consequences
- we will NOT rpt. NOT recommend CAs to move to SHA-2 for production use until the risk assessment completes - noting that this provision ends in January 2013

Time line proposal for SHA-2

But also …

- individual CAs MAY start issuing SHA-2 based certs on their own accord anyway (e.g. for testing, or to satisfy other needs)
- the date by which SHA-2 production certs may be issued will be NO LATER than January 2013 (and it is likely we will RECOMMEND CAs to move then, since it will take another 395 days to get rid of SHA-1 in a reasonable way)
- additional digest algorithms, in particular the successor to SHA-2 which is chosen this year, may ALSO be used in production certs in January 2013, but will NOT be introduced before SHA-2 is recommended for general use

… and conclude this time line at the IGTF All Hands meeting

On emailAddress

At the same time ...

- the emailAddress/EMail/E attribute is text-encoded differently in various middlewares
  (no standard exists), and jGlobus2 does not support all variants
  we really do need to get rid of emailAddress

- CAs still using emailAddress in their OWN name
  - IHEP
  - APAC
  - IUCC

- And others should stop using emailAddress in EEC
  - e.g. selected EECs from UKeScience

AUTHZ OPERATIONS GUIDELINES

- EUGridPMA in its January 2012 meeting produced version 1.0 of the AASP Operations Guidelines. See… http://www.eugridpma.org/guidelines/aaops/

- try this out with
  - a willing AA operator: Steve Traylen at CERN for wLCG
  - TAGPMA correctly concluded our own Distribution is an source of assertions as well – so would be good to assess the Distribution system against the guidelines ☺

    I'll do that – seems a good idea for both the Distribution setup and for the Guidelines …

- Discuss and try to agree during the All-Hands?

Agenda

- 25rd EUGridPMA and IGTF All Hands meeting
  Karlsruhe, May 7-9, 2012

- OGF34, CAOPS and FEDSEC
  Oxford, UK, March 12-15, 2012
- TERENA Networking Conference
  Reykjavik, May 21-25, 2012

- 26rd EUGridPMA meeting
  Tentatively 10-12 September 2012