



Certificates for DataGrid Testbed0

David Kelsey
CLRC/RAL, UK
d.p.kelsey@rl.ac.uk



Agenda

- Day 1 – 4th December, 2000, CERN
 - Aims , agenda, intro, etc.
 - Roundtable status reports
 - Authentication vs Authorisation
 - Which CAs?
 - CA Policies
 - Naming



Agenda (2)

- Day 2 – 5th December, 2000, CERN
 - CA Hierarchy
 - Revocation
 - Scope of certificates
 - Other Grid projects
 - Other issues
 - Summary of decisions / proposals



Attendees

- Jean-Luc Archimbaud CNRS, France
- Roberto Cecchini INFN, Italy
- Jorge Gomes LIP, Portugal
- Denise Heagerty CERN
- Dave Kelsey RAL, UK
- Daniel Kouril Cesnet, Czech Rep.
- Andrew Sansum RAL, UK

Apologies from:

Francesco Prelz and Guiseppe LoBiondo INFN

Aims of meeting

- Implement CA(s) for Testbed0
 - But also plan for the future
- Keep it simple! (at least for now)
- Report to WP6 meeting – Milan 11 Dec
- Report to ATF?
- Proposal for authorisation?



Summary of roundtable status

- National CAs already in place and ready for Testbed0
 - Czech Republic
 - France
 - Italy
 - Portugal
 - UK
- CERN not yet ready
- Not sure about status of sites not present



Authentication vs Authorisation

- User requirement for easy access to resources while system managers need to control access
- Strong recommendation not to mix these
 - For non-HEP CAs we will not be able to request the addition of HEP-specific attributes
 - Industry trends
 - PMI (privilege management infrastructure)
 - X.509V3 extension fields should only carry authorisation information that is stable and constant over time
 - “Attribute Certificates” – PKIX IETF working group
 - Also CAS from Globus



Authentication vs Authorisation (2)

- Breaks Globus GSI model
 - Privacy – public certificate should include minimal information – user may have control over disclosure
 - Recommendation to start a task force on Authorisation
 - Users want easy access to resources
 - Initially – grid map-files
 - then LDAP?
 - Account creation – requires coordination?
-

Which CAs?

- Recommendations
 - Each country/site wishing to join Testbed0 must find a CA willing to issue certificates for them with published and accepted procedures
 - By Testbed0 cutoff date, decide list of initial CA's + a catch-all solution
 - phase out use of CA's not meeting the minimum standards within 6 months, e.g. existing Globus CA
 - Should be a small group with responsibility for “accepting” new CA's



Which CAs? (2)

- CAs should be aware that we will review after 6 months
 - At this point new recommendations may be made
- Short lived CAs may be a good choice for getting started
- Recommend a maximum lifetime for personal certificates of 1 year



CA Policies for Testbed0

- CPS (cert practice statement) for CAs
 - Try to agree minimum set for Testbed0 or a mechanism for agreement of procedures
 - Use beyond Testbed0 at decision of each site?
 - Private key must be offline?
 - Physical access to CA – controlled area
 - Off line CA/signing machine?
 - Security of private key – who? How many?
 - Minimum Key lengths?

CA Policies for Testbed0 (2)

- Minimum policy for RA's
 - Confirmation from trusted person at each site
 - Identity
 - Request was issued by that person
 - What does it assert?
 - Method of confirmation (RA to CA) must be specified
 - Telephone?, digitally signed mail
 - Must be a mechanism for revocation
 - Owning a certificate is not sufficient for creation of accounts



Naming

- To date, different choices have been made
- Longer term, do we want a hierarchical namespace? (o=hep?)
- Coordination with LDAP namespace?
- This needs further study
- How to map single certificate onto multiple accounts?

CA Hierarchy

- Root CA signs lower level CA certificate
 - proposed changes to globus toolkit would allow clients and servers to only trust the root CA
- Pros
 - Formalises the checking of CPS
 - Simpler / scaleable configuration for growing number of CAs (if mods made to globus)

CA Hierarchy (2)

- Cons
 - Have to trust the root CA
 - In conflict with generic use of certificates
 - Suggests a common scope
 - Would need dedicated DataGrid CAs
 - Heavy reliance (unacceptable?) on the private key of the root CA
 - Compromised or disappearing root CA would cause major problems
 - But could move the root CA
- Conclude – not a useful idea



Revocation

- Each CA must maintain a CRL
- each server/client must regularly copy this CRL from each CA and store it in the “trusted certificates” directory (cron job)
- Globus (SSL) checks this local copy
- We need an agreed policy for CA updating its own CRL (e.g. compromised private key)



Scope of certificates

- Each CA can decide the scope of the certificates it issues.
- One reason not to use a hierarchy of CA's
- Each site is free to choose which CA's it trusts

Other issues – Security

- Communication between sites for removing users from authorisation scheme – in addition to revocation of certificate
- Should this certificate group continue?
 - With more general mandate than just certificates?
- Gatekeeper proxy certs
 - Limited functionality
 - Globus-rcp needs full function cert (returning job output)
 - Job for general security task force



Summary of Recommendations

- Use existing CAs, not necessarily specific to DataGrid
- Aim to phase out use of Globus CA
- For those orgs with no CA by cut-off date
 - find someone else willing to issue certs
 - We need a catch-all
- We will provide client/server configuration advice
- Q: What is the cutoff date?
- Q: WP6 should advise on “catch-all” CA



Summary of Recommendations (2)

- CA Hierarchy – not useful
- Authorisation in certificate – no!
- Agree minimum standards for CPS
 - Topic for future meeting of this group
- DataGrid should create a Security task force
 - Beyond testbed0 and certificates
- Authorisation needs to be tackled
 - By whom? LDAP + Security + ...?