Grid Security:Status and Issues

19 Apr 2002

HEPiX/HEPNT, Catania

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

Overview

- Security requirements
- Security Technology in (some) Grid projects
  - Globus
  - DataGrid (EDG)
  - PPDG
  - DataTAG/iVGDL/HICB
- Web Services Security
- (Some) Security Issues
  - Authentication
  - Authorisation
  - Grid Deployment

What is Security?

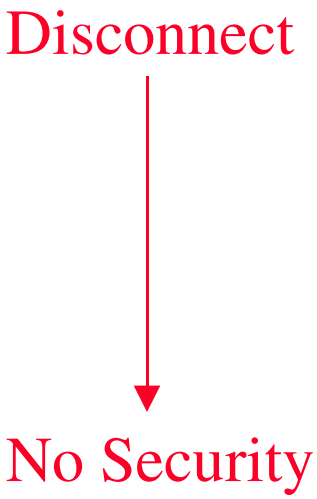
- *Authentication, Authorisation, Accounting, Auditing, Confidentiality, Integrity, Non-repudiation, Delegation, Firewalls, Intrusion Detection, Legal, Physical,…*
  (the list goes on!)
- Also requirements for Security implementations
  - *Reliability, Ease of use, Manageability, etc.*

Security Requirements

The usual tension: *functionality vs. security*

- But with some special features for Grid
  - Scale of users and resources

- **Site Security Officer**
  - Protect the site from hostile attack
- **Resource/Site System Manager**
  - Complete control of the local resources
- **Virtual Organisation**
  - Allocate resources to members, groups, roles
- **User**
  - Easy and transparent access to resources
    e.g. single sign-on



Grid Security Technology

Globus

Grid Security Infrastructure (GSI) today

- PKI (X.509 certificates)
- Users, hosts and services are authenticated (both directions)
- Single sign-on
  - Delegation via Proxy credential (limited lifetime)
- Authorisation via "Grid Mapfile"
  - Maps certificate DN to local user (Unix, Kerberos)
  - Authorisation via local security mechanisms
- *Next 4 Slides shown by Bill Allcock (ANL) in Paris DataGrid meeting (8 Mar 02)*

Ongoing/Future GSI Work

- Protection against compromised resources
  - Restricted delegation, smartcards
- Standardization
  - Current certificates are not compliant with standards in front of GGF/IETF so will need to change.
- Scalability in numbers of users & resources
  - Credential management
  - Online credential repositories (“MyProxy”)
  - Account management
- Authorization
  - Policy languages
  - Community authorization

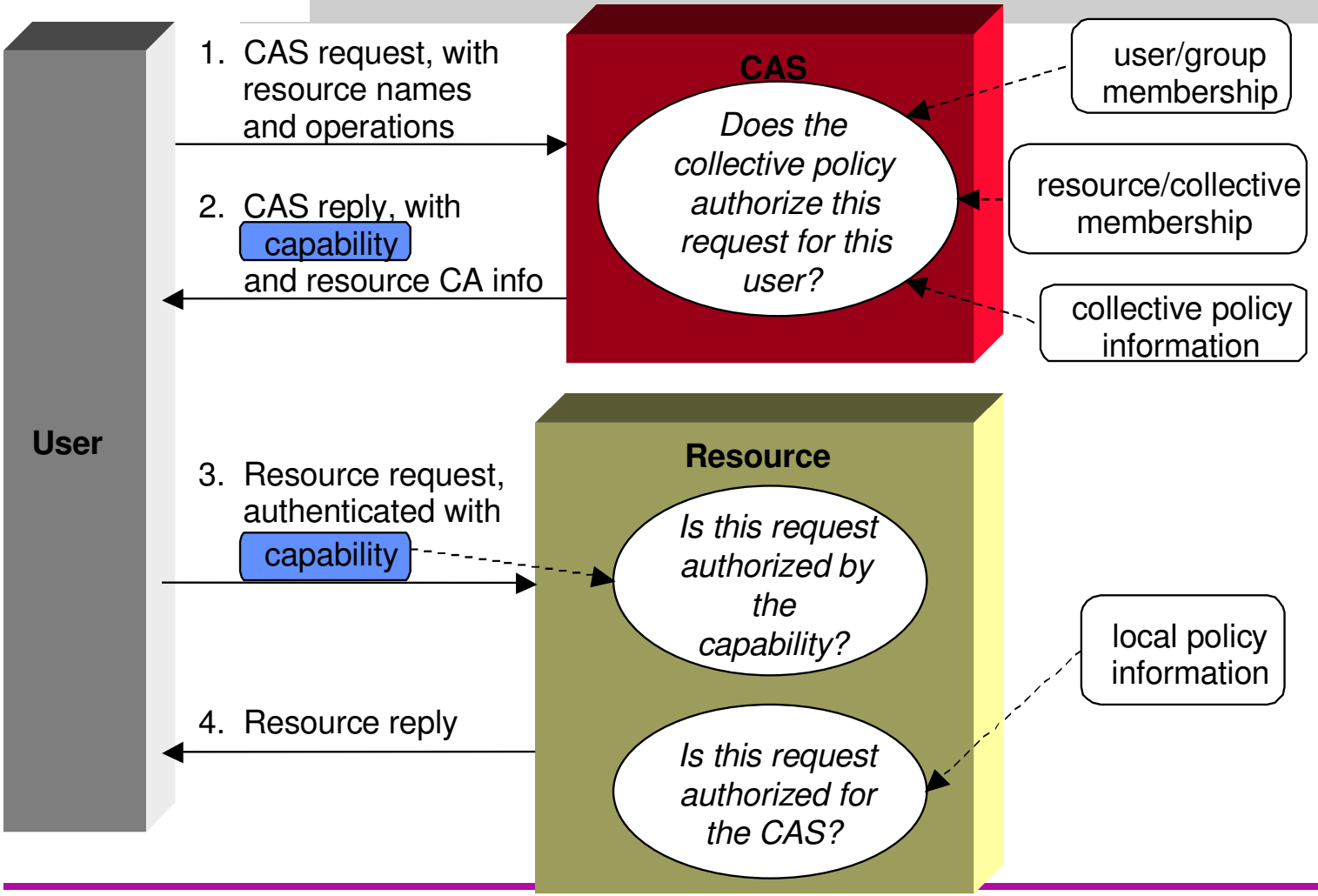
Security Standardization

- Based on existing standards:
  - SSL/TLS, X.509 & CA, GSS-API
- Standards Documents in Progress
  - draft-ggf-gss-extensions-04.txt
    - Being considered by GGF GSI working group. Not yet submitted to IETF.
    - Credential import/export, delegation at any time in either direction, restricted delegation, better mapping of GSS to TLS (SSL)
  - draft-ietf-pkix-proxy-01.txt
    - Being considered by IETF PKIX working group / GGF GSI working group
    - Defines proxy certificate format, including restricted rights and delegation tracing
  - draft-ietf-tls-delegation-01.txt
    - Being considered by IETF TLS working group / GGF GSI working group
    - Defines how to remotely delegate an X.509 Proxy Certificate using extensions to the TLS (SSL) protocol

Community Authorization Service

- Question: How does a large community grant its users access to a large set of resources?
  - Should minimize burden on both the users and resource providers
- Community Authorization Service (CAS)
  - Community negotiates access to resources
  - Resource outsources fine-grain authorization to CAS
  - Resource only knows about "CAS user" credential
    - CAS handles user registration, group membership…
  - User who wants access to resource asks CAS for a capability credential
    - Restricted proxy of the "CAS user" cred., checked by resource

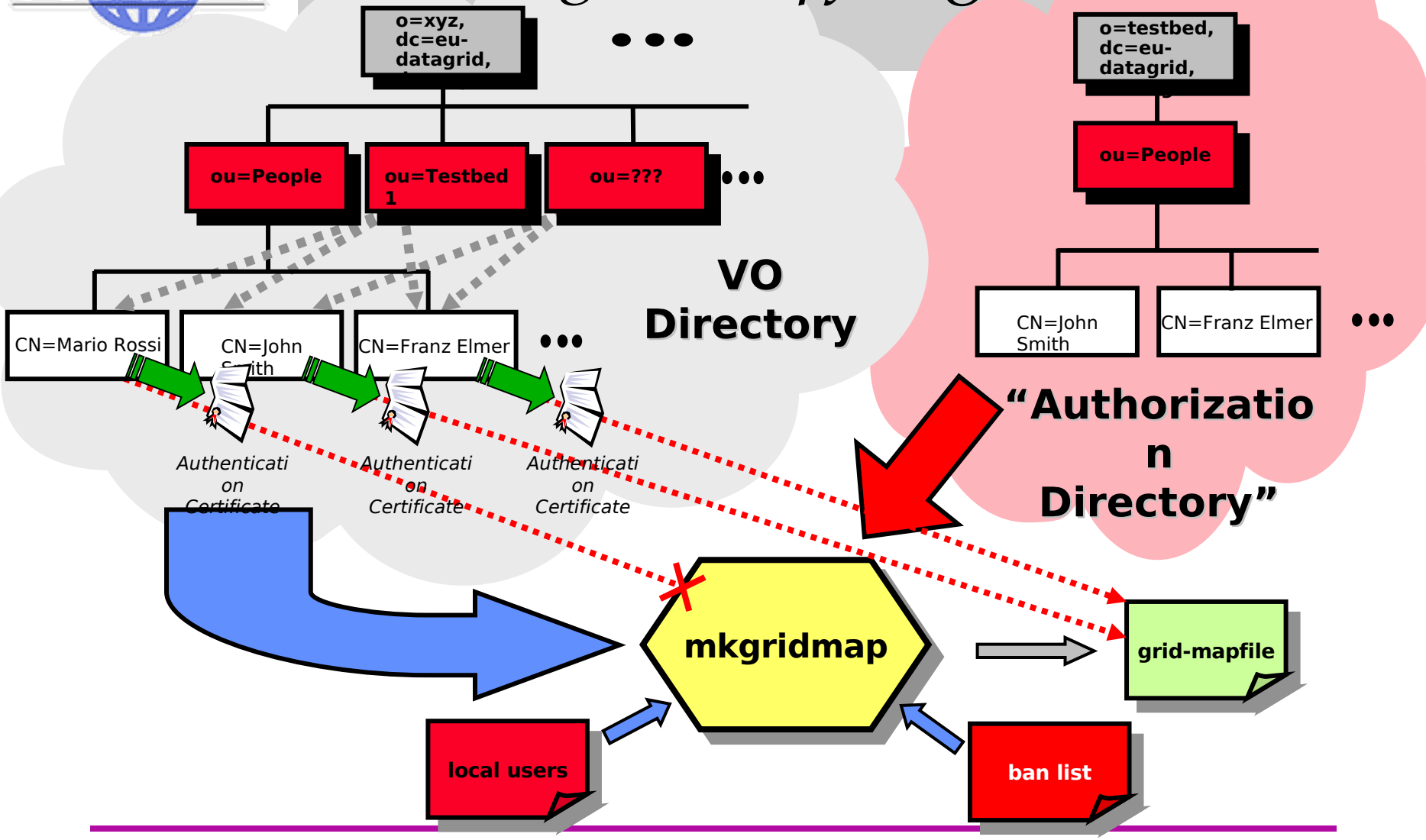
Community Authorization Service



DataGrid - Authentication

- 11 DataGrid (EDG) National Certificate Authorities
  - includes Registration Authorities – check identity
- CNRS (France) acts as "catch-all" CA
- Matrix of "Trust" (work ongoing) – much work!
  - WP6 CA Mgrs check each other against list of minimum requirements
- Started work on cross-Authentication between Grid projects
  - USA and CrossGrid

EDG Authorisation
grid-mapfile generation



DataGrid Authorisation

Future plans

- Improve existing VO LDAP system
  - Better VO Directory management
  - Support of replicas of VO Directories
  - Users belonging to more than one VO can choose
  - Support for users' attributes in the VO Directories
    - e.g. the AUP signing information (with expiration date...)
- Evaluation of Globus CAS (see before) and PERMIS
  - n.b. CAS alpha – only for GridFTP
  - *http://www.permis.org* (EU funded project)
  - Policy-based (XML) Role-based Access control
    - Standards based
    - PMI using Attribute certificates

PPDG

- Using Globus GSI
- US DOE Science Grid CA now in operation
  - Working on "trust" of EDG CA's
    - Download files to include EDG CA details
  - PPDG work in this area likely to be accepted by GriPhyN and iVDGL (April meeting)
- Authorisation
  - DataGrid VO LDAP system/tools
  - Globus CAS
- "Grid Site AAA" project (new proposal) - extension to PPDG
  http://www.ppdg.net/docs/PPDG-AAA-Proposal.pdf
  - Examine/evaluate the impact of GSI on local site security
  - An important contribution – not yet tackled by DataGrid

DataTAG/iVDGL/HICB

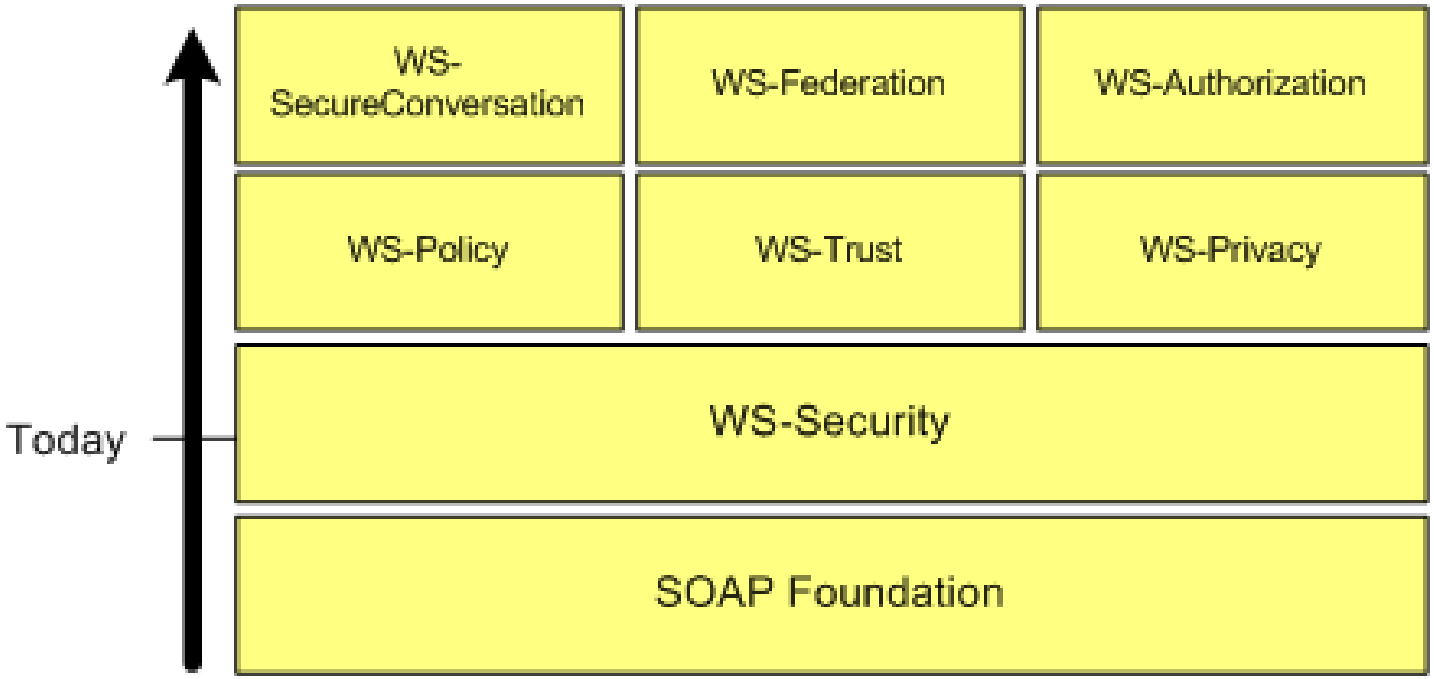
- HICB = "HENP Intergrid Collaboration Board"
- Transatlantic Testbed(s)
  - Interoperability essential for HEP applications!
- Cross project Authentication
  - US DOE SciGrid CA already "trusted" by EDG
  - US projects working on "trust" of EDG CA's
- Cross project Authorisation
  - DataTAG WP4 has resources to work in this area

Web Services Security

- Open Grid Services Architecture (OGSA)
  - Globus V3
  - GGF *http://www.gridforum.org/ogsi-wg/*
  - Based on web services, SOAP, WSDL, …(IBM and Globus)
- Announcement on 11th April 2002
  - IBM, Microsoft and VeriSign Announce New Security Specification to Advance Web Services
  - *http://www.microsoft.com/presspass /press/2002/Apr02/04-11WSSecurityPR.asp*
  - *http://msdn.microsoft.com/ws-security/*
  - *WS-Security supports, integrates and unifies several popular security models, mechanisms and technologies, allowing a variety of systems to interoperate in a platform- and language-neutral manner in a Web services context.*

WS-Security

- WS-Security – basis for the other security specs (to come later)



Grid Security Issues

Authentication issues

- Don't mix Authentication and Authorisation
  - But authentication often includes *some* implicit authorisation
- How to define list of "trusted" CA's?
  - CP/CPS important
  - Audit of CA procedures – 3rd party?
  - GGF GridCP working group important here
- Scaling problems
  - How many CA's can we cope with?
  - Or should the experiments issue Authentication certs?
  - Or use Kerberos at the site and generate certs online
- *Authorisation* is where the real identity checks need to be made
  - We should avoid heavy-weight Authentication
  - Is MS .NET passport good enough?

Authorisation issues

- We need more functionality
  - "Dynamic policy-based Access control"
  - Users with more than one allowed role
  - Move away from Unix uid based security? (and grid mapfile?)
  - Applicable to all Grid services (and callable from)
    - Maybe different levels for different services
- Users may belong to multiple VO's
  - Authorisation may need to be based on "joins"
- The development of new technology will take **many years**!
- Global vs Local authorisation mechanisms
  - need to negotiate policy – Global/VO/Local

SlashGrid (WP6 - McNab)

- **Framework for creating "Grid-aware" filesystems**
  - different types of filesystem provided by dynamically loaded plugins
  - Uses CMU Coda kernel module
  - Source, binaries and API notes: *http://www.gridpp.ac.uk/slashgrid/*
- certfs.so plugin provides local storage governed by Access Control Lists based on DN's.
- Since most ACL's would have just one entry, this is equivalent to **file ownership by DN rather than UID**.
- Also, a GridFTP plugin could provide secure replacement for NFS.

Issues – Grid Deployment

- Legal, political, site security policies, etc.
  - The user does not (need) to know where the jobs will run
    - Cannot sign registration forms everywhere
  - Acceptable Use policies
    - What is needed for User Registration?
  - We have a solution for EDG Testbed
    - But not yet for full production
  - What is acceptable to Site Security Officers?
    - PPDG "Grid Site AAA" project working on this
  - An extremely important area – could kill the Grid!

Issues – Deployment (2)

- VO's need to manage their members and sites/resource providers negotiate with VO's
  - Only system which will scale
    - Sites cannot manage large number of Grid users
  - Not just a technical problem!
  - Must develop procedures to allow this to happen
  - VO/experiments not used to managing resources
  - Will Computer Centres give up full control?

My personal view

- Today
  - Computer centres register users (lots of rules and checks) but then allow them to do almost anything!
- In the GRID future
  - Computer centres will register VO's
    - VO's manage their users
  - "Trust" established between VO's and Sites
  - The applications will be tightly controlled
    - Using e.g. Community restricted delegation and signed apps
  - The actual user does not matter (but must have audit trail)
- *Control the "What" and not the "Who"*