The X.509 Certificates and Proxy infrastructure in HEP

... with a look at VOMS

… and another look at some DESY developments

Andreas Gellrich, Yves Kemp
LSDMA Spring 2013 Meeting
Hamburg, 11.3.2013

HELMHOLTZ ASSOCIATION

DESY

Some basics about X.509

- X.509 is *one* standard for a Public-Key-Infrastructure
- The “Grid Certificates” are *one* implementation of it
  - Others exist – e.g. Global Certificates
- X.509 Public-Key-Certificates are for authentication only
  - I will deal with authorization later in this talk

- Purpose of Grid X.509 PKI:
  - Provide all Grid users (and hosts (and services)) with a “strong” digital identity
  - Take into account country- and institutional organization of HEP/Science
  - Enable HEP workflows

The Grid X.509 infrastructure

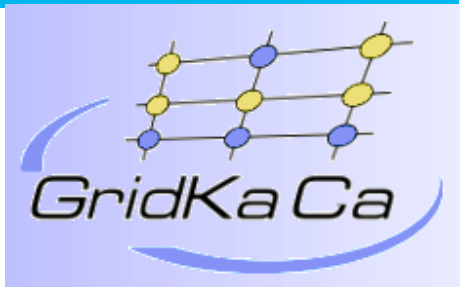
> The CA level

- Each country has (≥) **one CA** (Certification Authority)
- All Grid CA agree on the same policies – International Grid Trust Federation (IGTF)
- The ROOT certificate of the CA needs to be distributed (and some other information): Bundled e.g. by IGTF

> The RA level

- RA stands for Registration authority. Each CA has several RA in its country
- E.g. one RA in each institute
- The RA makes the correspondence “physical user” – “digital X.509 ID”
- GridKA CA: RA at: 17 institutes, 31 universities, and 8 Companies

Provide a “strong” digital identity: Policies



- The GridKa-CA Certificate Policy and Certification Practice Statement has 28 pages
  - E.g.: “The **Subject Name** in a certificate must be meaningful and must bear a reasonable association with the authenticated name or names of the subscriber. “
  - … description of security procedures, how keys are stored, ...
  - “Authorized RA's are verifying the **identity of a natural person** by Personal contact, comparing the information in the identity card with the information presented in the registration form and compares the photograph in the identity card with the real appearance of the person. “
- The issued certificates are quite strong – good link to identity of the person

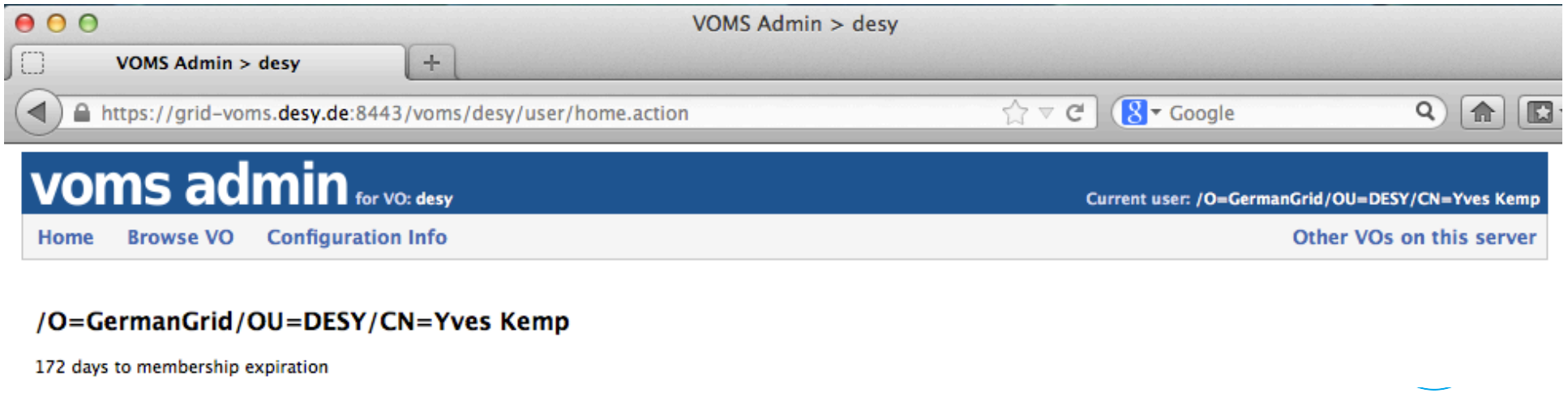
Some details on Grid certificates

- Example DN (Distinguished Name):
  - /C=DE/O=GermanGrid/OU=DESY/CN=Yves Kemp
- DN: Has the OU in its name – usually relates to RA
- Valid for one year – prolongation possible (technically new certificate)
  - “Global” certificates (e.g. DFN-PKI) usually valid for three years
- User can create “proxy certificates” – (usually) short-lived certificates signed by the original certificates
  - No password on private key – send with Grid jobs to serve as authentication (and eventually authorization with VOMS extension)
- Grid CA are their own ROOT-CA … and not contained in usual browser or mailer
  - No sub-CA structure possible with Grid CA
  - DFN Global certificates inherit “Deutsche Telekom ROOT CA 2”

DESY

VOMS: The Authorization part of X.509 in Grid

- X.509 defines Attribute Certificates (RFC 5755)
- Many different ways to create them. VOMS one standard used in Grid computing with Grid certificates
- HEP: *One* experiment is *one* collaboration is *one* VO
- Within an experiment/collaboration, sub-groups and roles are possible
  - E.g. /atlas/de , /cms/susy, … /hone/Role=swadmin
- The resource provider checks the identity contained within the certificate proxy and assigns system rights according to the authorization in the certificate proxy VOMS extension



… How does this look like

```
>voms-proxy-info  --all
subject   : /O=GermanGrid/OU=DESY/CN=Yves Kemp/CN=proxy
issuer    : /O=GermanGrid/OU=DESY/CN=Yves Kemp
identity  : /O=GermanGrid/OU=DESY/CN=Yves Kemp
type      : proxy
strength  : 1024 bits
path      : /afs/desy.de/user/k/kemp/k5-ca-proxy.pem
timeleft  : 11:59:53
=== VO cms extension information ===
VO        : cms
subject   : /O=GermanGrid/OU=DESY/CN=Yves Kemp
issuer    : /DC=ch/DC=cern/OU=computers/CN=voms.cern.ch
attribute : /cms/dcms/Role=NULL/Capability=NULL
attribute : /cms/Role=NULL/Capability=NULL
timeleft  : 11:59:53
uri       : voms.cern.ch:15002

>uberftp grid-cr5.desy.de "ls"
230 User cmsger081 logged in.
```

What can you do with a VOMS-Proxy?

- Submit jobs to the Grid – any site which supports the VO
- Using meta-scheduling systems (must support VO)
- Manage data with storage systems directly (must support VO)
- Using transfer systems and metadata catalogues (must support VO)

- … and some more

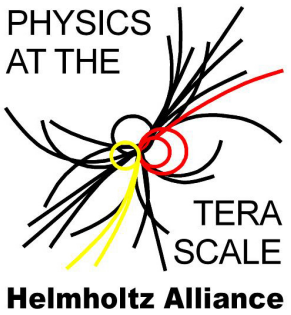
VOMS: What happens in the background?

- VO creation: Needs a VOMS server somewhere
- VO administration: Digital administration needs a real-world organizational backing

Now your VO is created:

- The resource provider(s) configure the VO and authorization rights on their resources
- The resource provider publishes the resources in the Grid information system

VOMS not the only possible authorization

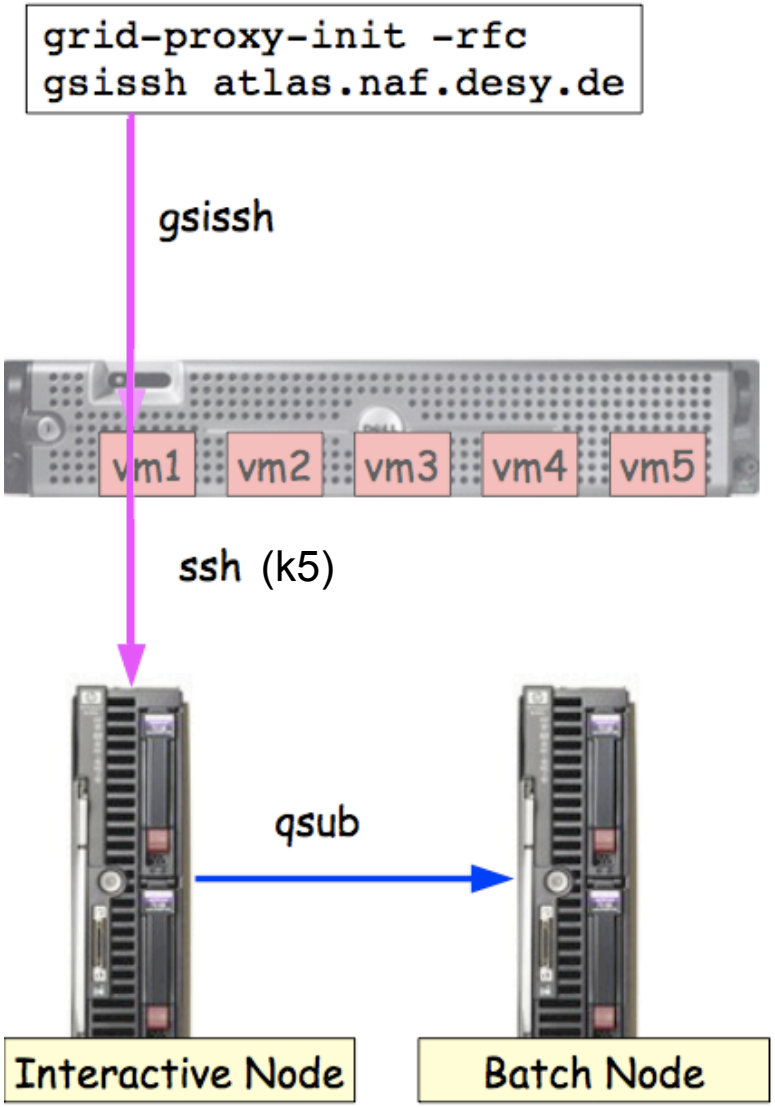


- E.g. NAF user registry at DESY
  - NAF: National Analysis Facility
- Steps:
  - Registration using web interface. Grid certificate in browser authenticates
  - Users asks for membership in e.g. ATLAS NAF group
  - NAF ATLAS admin accepts requests
  - User account created in NAF registry, ATLAS group
- User is only authorized for NAF resources of his experiment

- … basically creating gridmapfiles

DESY

Certificate login for the NAF

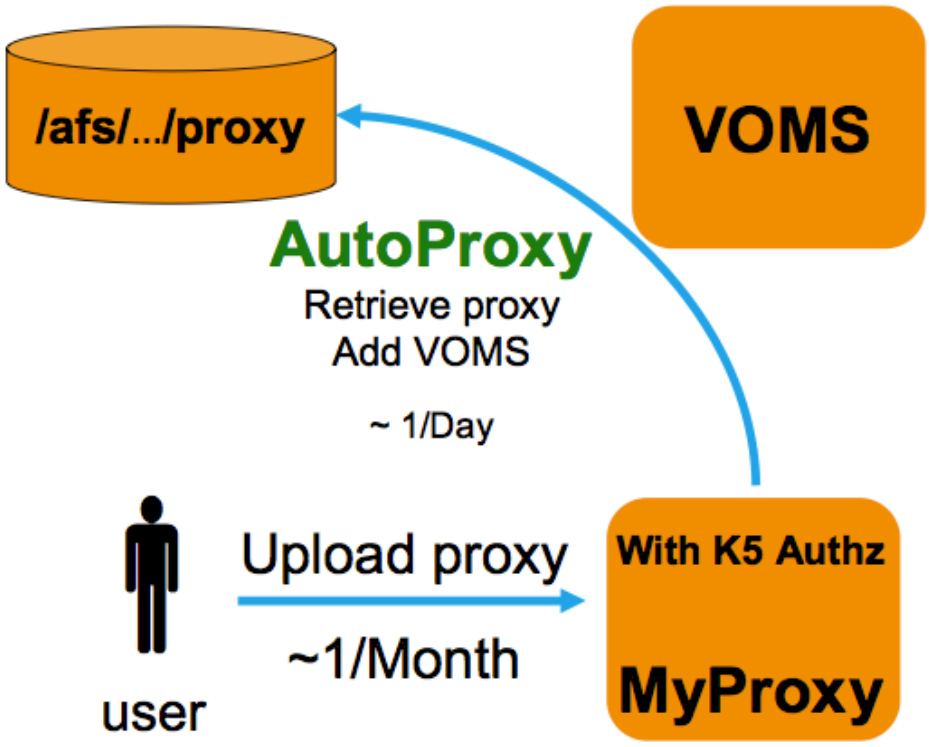


- Grid certificates can be used for interactive login via ssh
- GSI-OpenSSH adds support for GSI (Globus Security Infrastructure)
- Users can login using Grid Certificates or proxies
- In the NAF, users then get Kerberos and AFS token
  - Unfortunately, proxy cannot be used further
- Grid ➔ NAF transition using one authentication method

From the NAF to the Grid

- The other part of single-sign-on: NAF ➔ Grid
- Use case: A user is logged into the NAF, and wants to use the Grid
- NAF development: **AutoProxy**

- Once a month: A user creates a long-living proxy and stores it into a MyProxy-Server
- The NAF provides mechanisms that users with a valid K5 token can automatically request a valid short-living proxy from MyProxy
- The newly created short-living proxy is automatically put into AFS and can be used e.g. for job submission.



Two use-cases not (yet?) implemented in HEP workflows

- Grid certificates are only used for authentication
- They could also be used for digitally signing
  - E.g. appending a signature at the end of a data file to certify integrity and provenience
- They could also be used for encryption
  - E.g. storing encrypted files on a non-secure data store
- … these might be of interest for communities with higher privacy and data integrity needs

Summary

- Grid certificates on X.509 basis a well established standard of important use in HEP
- CA+RA infrastructure is there and in use
- Technology and tools are there and in use
- Authorization: VOMS used in HEP is only one implementation of X.509 Attribute Certificates

- Single-Sign-On using Grid X.509 works – worldwide!

DESY

Back slides – The “Marcus Hardt Checklist”

X.509 and the “Marcus Hardt checklist” _ 1

- Accessing data via
  - web portals ✓
  - the commandline ✓
- Giving access to guest scientists (potentially from outside europe)
  - To access measurement devices ✓ ✓
  - To store their dataTo ✓
  - run (grid, cloud based) computations on their data ✓ (cloud might need portal)
- In the worst case data may be
  - Created at Institute A ✓
  - by a user from Institute B ✓
  - Shared with users from additional institutes ✓
  - Archived at yet a different institute ✓
- All institutes will prefer to authenticate users against their existing user database ? (I might not fully understand the statement)

X.509 and the “Marcus Hardt checklist” _ 2

- How should we use the presented mechanism for combined data analysis and storage setup? ✓
- Is it possible to integrate existing (often Active Directory) userbases?
  - Yes – see NAF example
- Can jobs store output data on behalf of the user? ✓
- International Authentication (e.g.: Sharing data with colleagues from India) ✓
  - Would need adequate Authorization scheme
- mobile device support ? (Potentially yes – what are the exact requirements)
- Existing Interfaces / PAM Modules for User and Administrator, what protocol (i.e. RESTful, …) ✓ see X.509 description
- Is Authorisation included? … yes and no ☺
- OpenSource Licence? ✓
- Certified Security ✓
- Maintenance, organisational overhead (e.g.: Do I need to notify all IdPs when adding a new service?) : **No – use the Grid Information system for this**

DESY