Transparent access and coordination of eInfrastructures in the Nordics

Michael Gronager, PhD
NDGF Director

Open e-IRG Workshop
Uppsala, October 14-15th, 2009

NDGF
Nordic DataGrid Facility

Activity Outline

- Vision: A Nordic resource trading system
- Enabling
  - Initial problems outline
  - Locating enabling tools
- Next steps
  - New tools
  - New Policies

The Grid

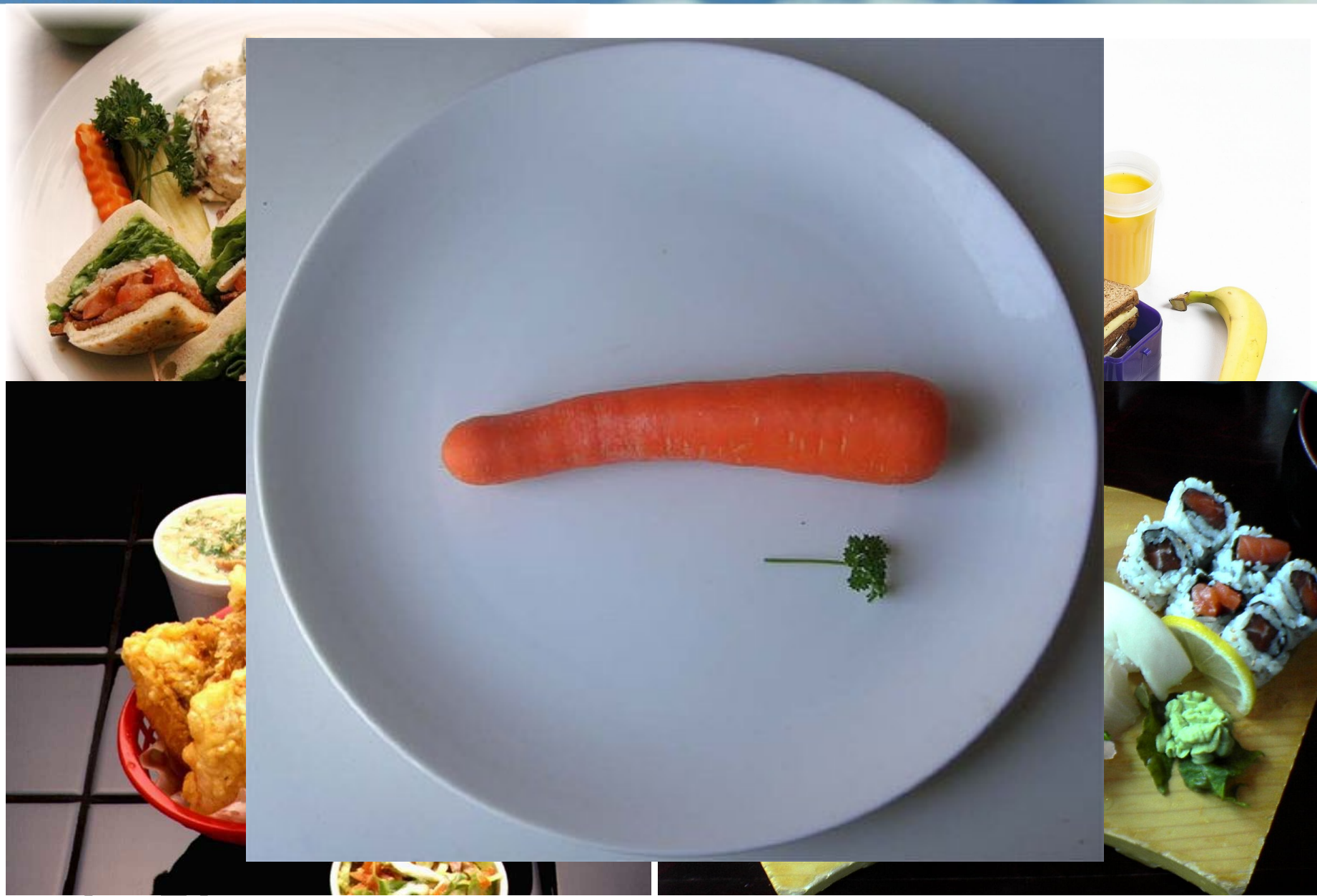
The Grid

NDGF
Nordic DataGrid Facility

Free Lunch!

NDGF
Nordic DataGrid Facility

This is Free Lunch...

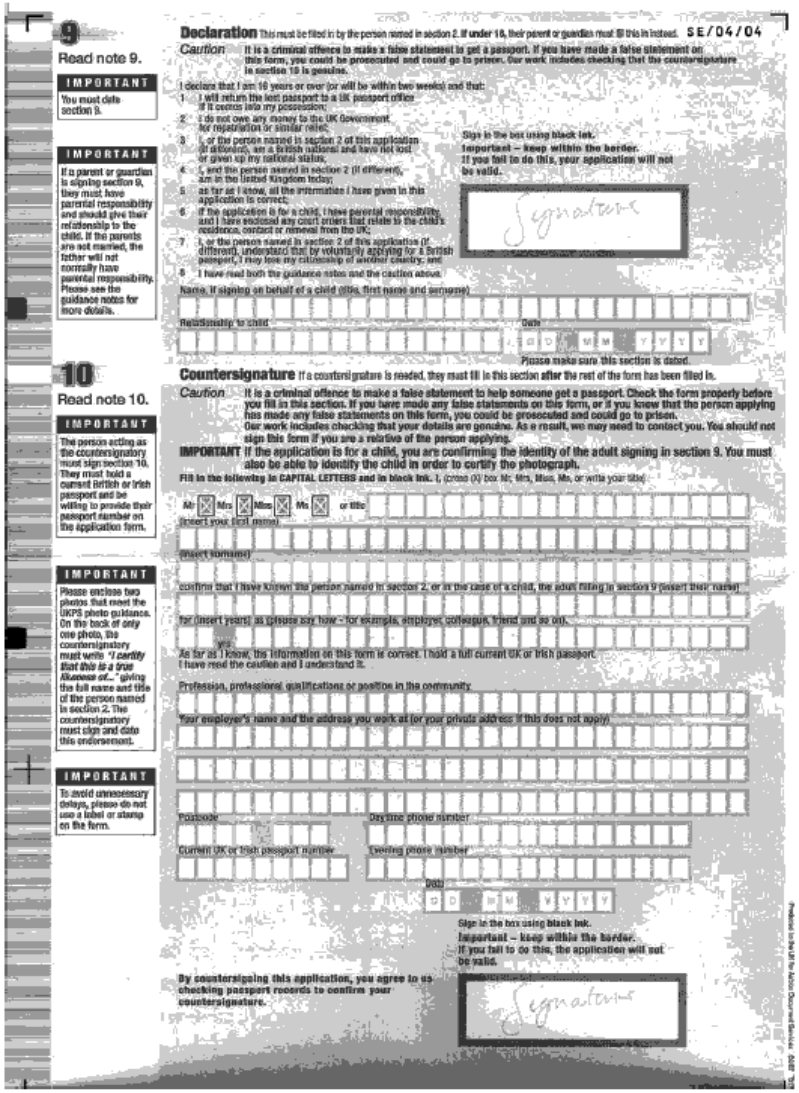


Problem I

- Free lunch is bad lunch
- Use of Grid services need to come with a "price"
- But first we need to know who used what ...

Digital Identities and Rights

are complicated to request...



9

Read note 9.

IMPORTANT
You must date section 9.

IMPORTANT
If a parent or guardian is signing section 9, they must have parental responsibility and should give their relationship to the child. If the parents are not married, the father will not normally have parental responsibility. Please see the guidance notes for more details.

10

Read note 10.

IMPORTANT
The person acting as the countersignatory must sign section 10. They must hold a current British or Irish passport and be willing to provide their passport number on the application form.

IMPORTANT
Please enclose two photos that meet the UKPS photo guidance. On the back of only one photo, the countersignatory must write "I certify that this is a true likeness of..." giving the full name and title of the person named in section 2. The countersignatory must sign and date this endorsement.

IMPORTANT
To avoid unnecessary delays, please do not use a label or stamp on the form.

Declaration This must be filled in by the person named in section 2. If under 16, their parent or guardian must fill this in instead. SE/04/04

Caution It is a criminal offence to make a false statement to get a passport. If you have made a false statement on this form, you could be prosecuted and could go to prison. Our work includes checking that the countersignature in section 10 is genuine.

I declare that I am 16 years or over (or will be within two weeks) and that:

1 I will return the lost passport to a UK passport office if it comes into my possession;
2 I do not owe any money to the UK Government for repatriation or similar relief;
3 I, or the person named in section 2 of this application (if different), am a British national and have not lost or given up my national status;
4 I, and the person named in section 2 (if different), am in the United Kingdom today;
5 as far as I know, all the information I have given in this application is correct;
6 if the application is for a child, I have parental responsibility and I have enclosed any court orders that relate to the child's residence, contact or removal from the UK;
7 I, or the person named in section 2 of this application (if different), understand that by voluntarily applying for a British passport, I may lose my citizenship of another country; and
8 I have read both the guidance notes and the caution above.

Sign in the box using black ink.
Important – keep within the border.
If you fail to do this, your application will not be valid.

Signature

Name, if signing on behalf of a child (title, first name and surname)

Relationship to child | Date D D M M Y Y Y Y

Please make sure this section is dated.

Countersignature If a countersignature is needed, they must fill in this section after the rest of the form has been filled in.

Caution It is a criminal offence to make a false statement to help someone get a passport. Check the form properly before you fill in this section. If you have made any false statements on this form, or if you know that the person applying has made any false statements on this form, you could be prosecuted and could go to prison. Our work includes checking that your details are genuine. As a result, we may need to contact you. You should not sign this form if you are a relative of the person applying.

IMPORTANT If the application is for a child, you are confirming the identity of the adult signing in section 9. You must also be able to identify the child in order to certify the photograph.

Fill in the following in CAPITAL LETTERS and in black ink. I, (cross (X) box Mr, Mrs, Miss, Ms, or write your title)

Mr ☒ Mrs ☒ Miss ☒ Ms ☒ or title

(insert your first name)

(insert surname)

confirm that I have known the person named in section 2, or in the case of a child, the adult filling in section 9 (insert their name)

for (insert years) as (please say how - for example, employer, colleague, friend and so on).

As far as I know, the information on this form is correct. I hold a full current UK or Irish passport. I have read the caution and I understand it.

Profession, professional qualifications or position in the community

Your employer's name and the address you work at (or your private address if this does not apply)

Postcode | Daytime phone number

Current UK or Irish passport number | Evening phone number

Date D D M M Y Y Y Y

Sign in the box using black ink.
Important – keep within the border.
If you fail to do this, the application will not be valid.

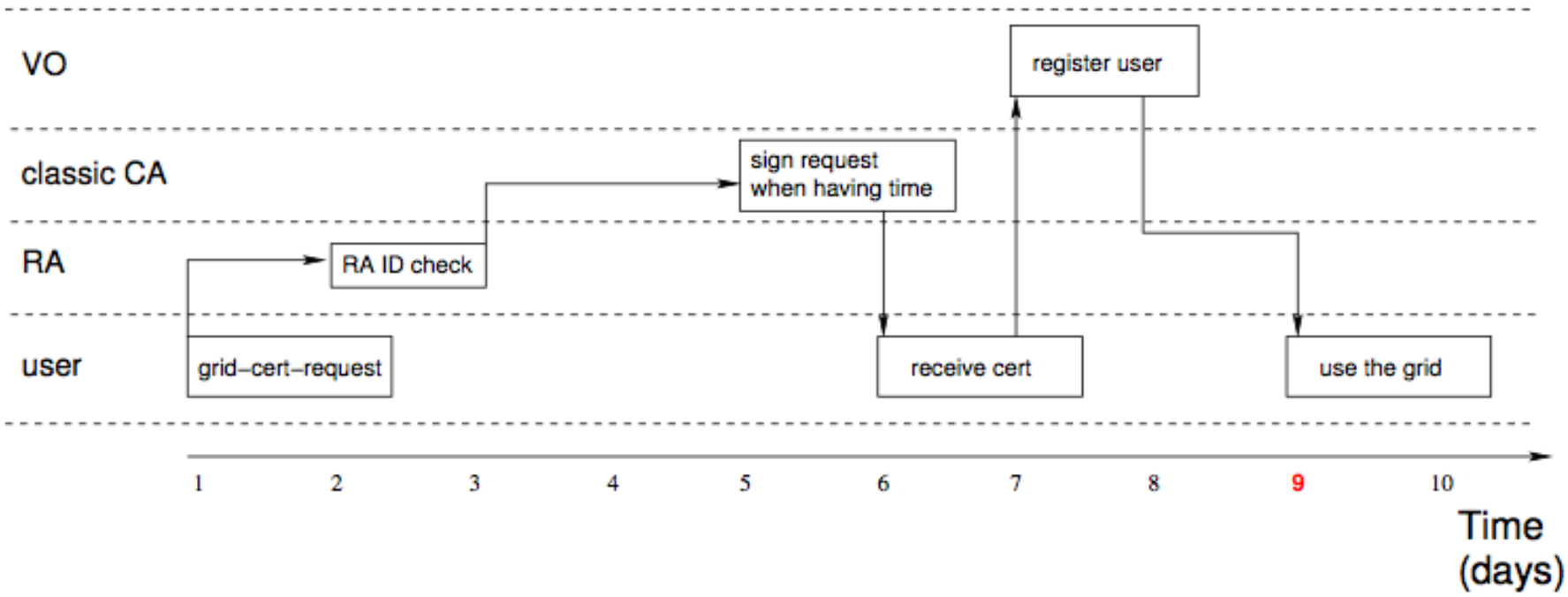
By countersigning this application, you agree to us checking passport records to confirm your countersignature.

Signature

and it takes too long...

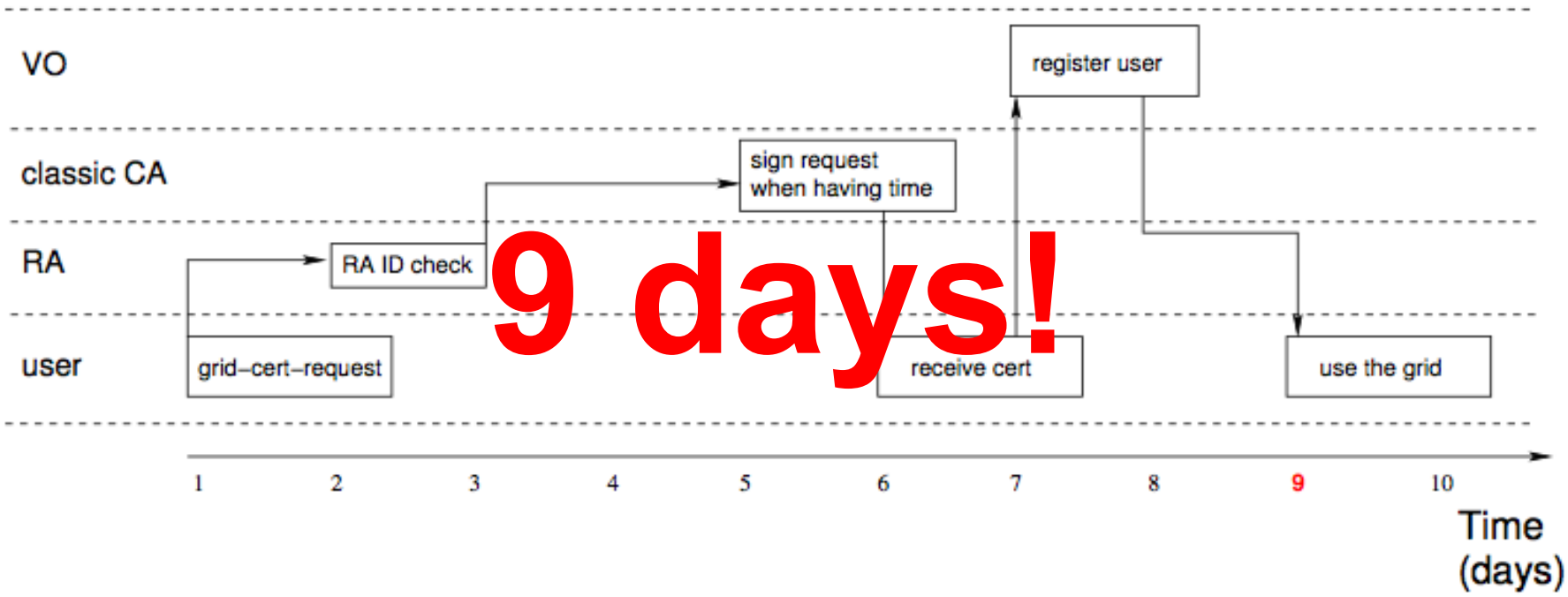
Problem II

- It is more complicated to Administer, Authenticate, and Authorize users than to login in to your home institution / cluster.



Problem II

- It is more complicated to Administer, Authenticate, and Authorize users than to login in to your home institution / cluster.

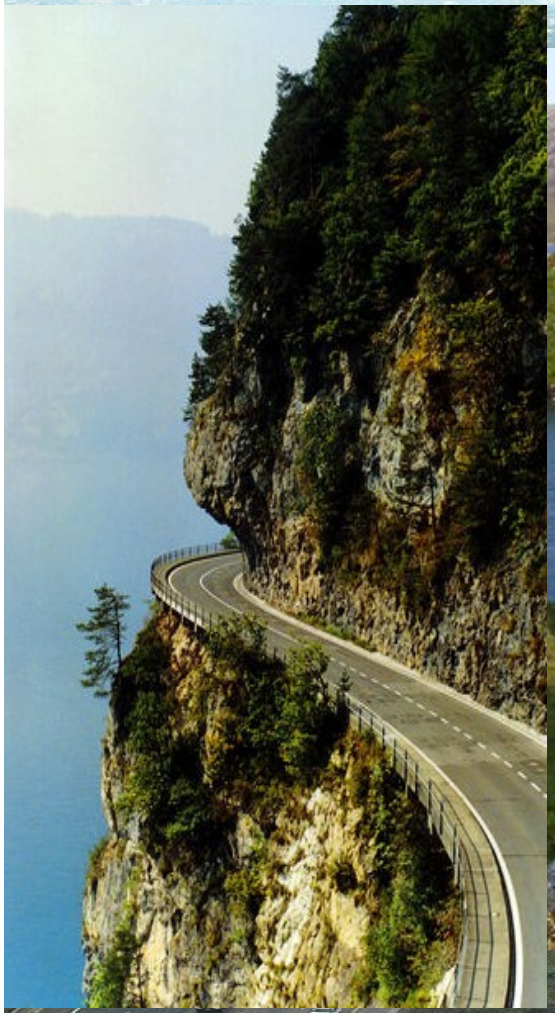


NDGF
Nordic DataGrid Facility

Access

NDGF
Nordic DataGrid Facility

Access patterns



Access patterns

Resources in different infrastructures:

- DEISA: ~10 sites, ~100k CPUs
  - shared machines, access is mainly through login (ssh)
- EGEE: ~300 sites, ~70k CPUs
  - mainly dedicated machines, about half of the access is through grid (based on GStat)
- NDGF / NorduGrid: ~70 sites, ~40k CPUs
  - shared machines, 10-15% of access is through grid, rest is local login accounts (ssh)
- (TeraGrid: Shared machines, 10% access through grid)

- Let's build infrastructure for all the users...

Problem III

- The perceived infrastructure depends today too much on the access pattern
  - SSH
  - Portal
  - Grid
  - Cloud
  - Indirect Services
- We need to solve **Problem I** and **II** independently of the users **access pattern**

Problems

- I – accounting
- II – easy user authentication and authorization
- III – enable it for all access patterns – transparent to the user.

Solutions

- Accounting:
  - SGAS and FSGrid
- Authentication:
  - IdP
  - The TERENA Grid CA Pilot Service:
    - A Personal Certificate Service (MICS) based on National Identity Federations
- Authorization (also as prioritization):
  - IdP, SAML2, and VOMS, SGAS
- All access pattern... GSISSH, PAM-modules

Solutions

- Accounting:
  - **SGAS** and **FSGrid**
- Authentication:
  - **IdP**
  - **The TERENA Grid CA Pilot Service**:
    - A Personal Certificate Service (MICS) based on National Identity Federations
- Authorization (also as prioritization):
  - **IdP**, **SAML2**, and **VOMS**, **SGAS**
- All access pattern... **GSISSH**, PAM-modules

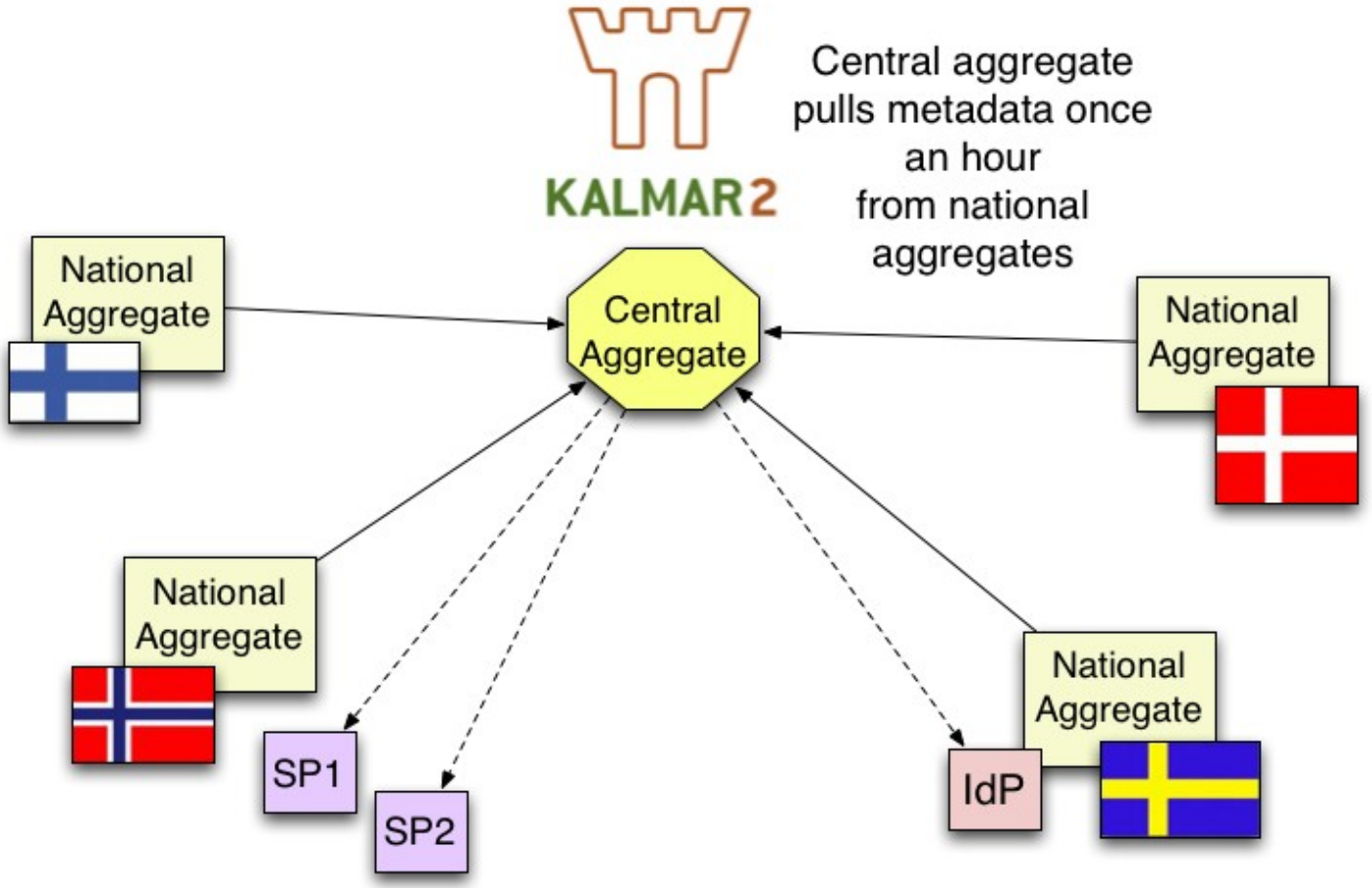
Identity Providers

- Users are already registered at their home institutions
- This identity vetting can be reused by services
  - (Shibboleth, SAML2...)
- In the Nordics we have national federations:
  - WAYF.DK in Denmark (and Iceland)
  - HAKA in Finland
  - FEIDE in Norway
  - SWAMI in Sweden

KALMAR2

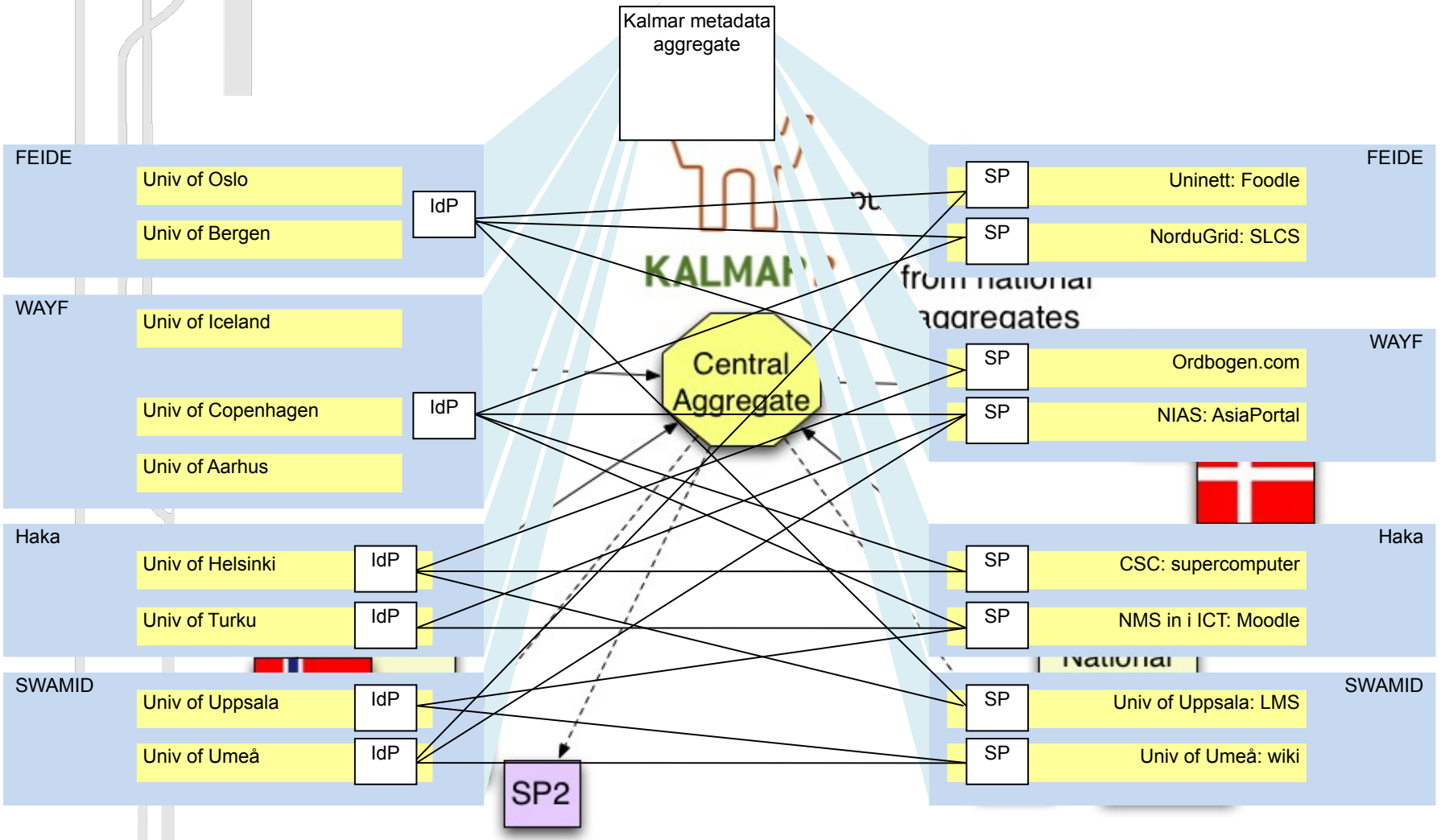
- And a Nordic confederation KALMAR2
- The IdPs provide access to campus and administrative resources and partly also to research resources

Meta-data aggregation



NDGF
Nordic DataGrid Facility

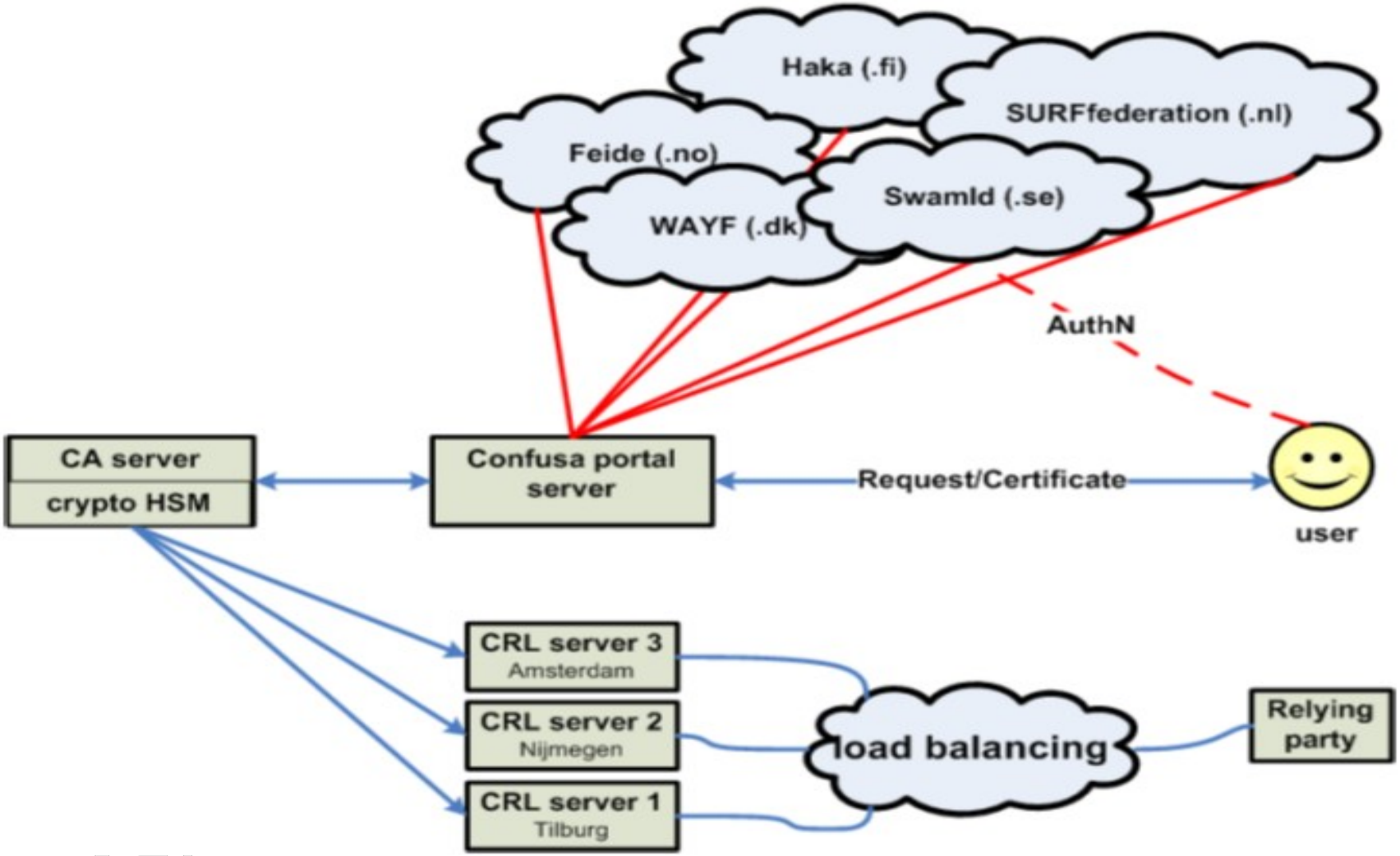
Meta-data aggregation



TERENA Grid CA Pilot Service

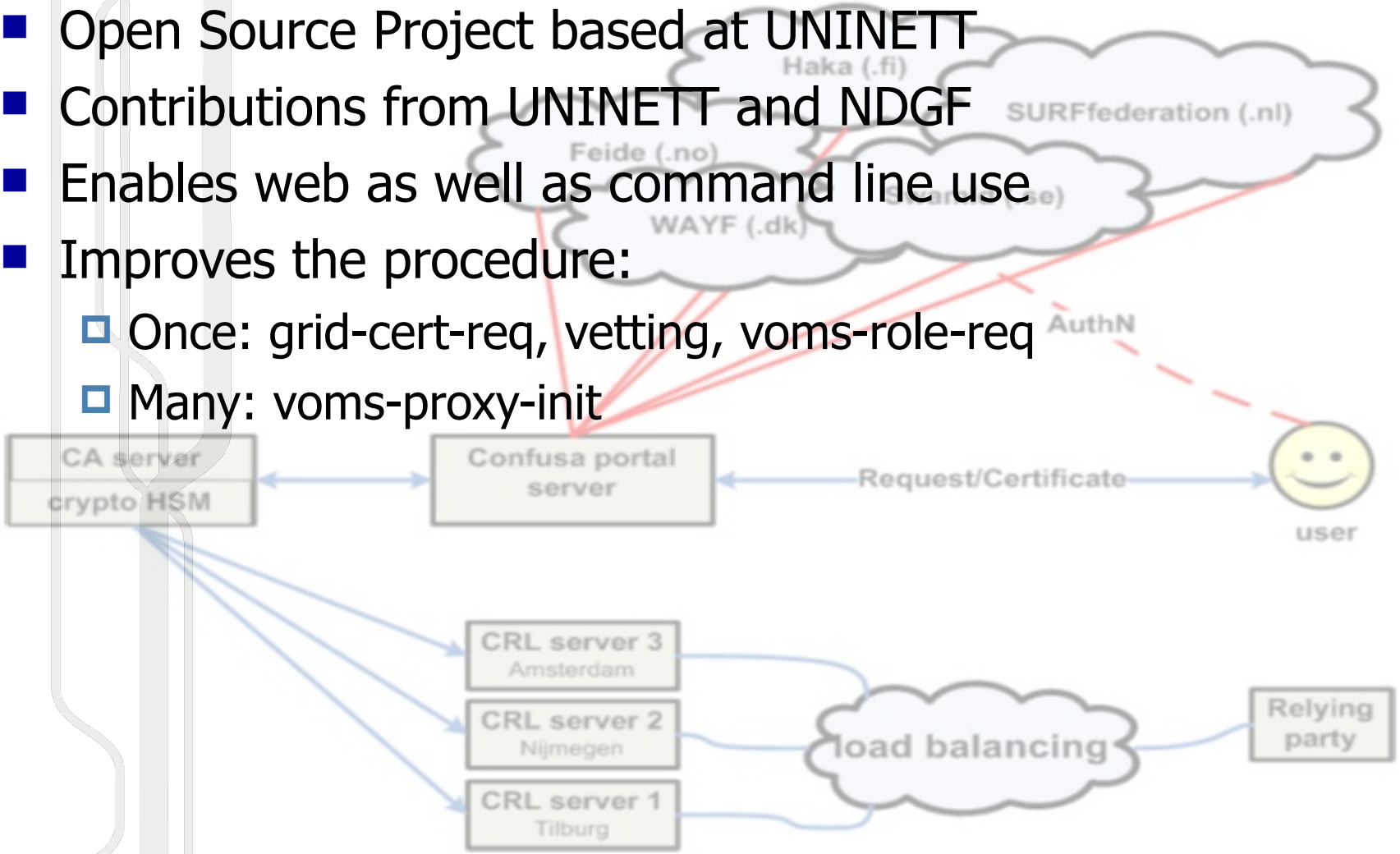
- Initiated by UNINETT in Norway and became the Nether-Nordic Short Lived Certificate Service
- Now TERENA is the organizational platform
- Ties Fed-Ids to Grid-Ids
- Enables creation of:
  - SLCs: Short Lived Certificates
  - MICs: Personal Certificates
- TERENA already provides a server certificate service
- Based on same root CA (COMODO) which means:
  - To become part of IGTF (can be used for Grid)
  - Part of Web of Trust
    - **End of Pop-Up-Windows when using Grid!**

Confusa


Haka (.fi)
SURFfederation (.nl)
Feide (.no)
SwamId (.se)
WAYF (.dk)
AuthN
CA server
crypto HSM
Confusa portal server
Request/Certificate
user
CRL server 3
Amsterdam
CRL server 2
Nijmegen
CRL server 1
Tilburg
load balancing
Relying party

Confusa

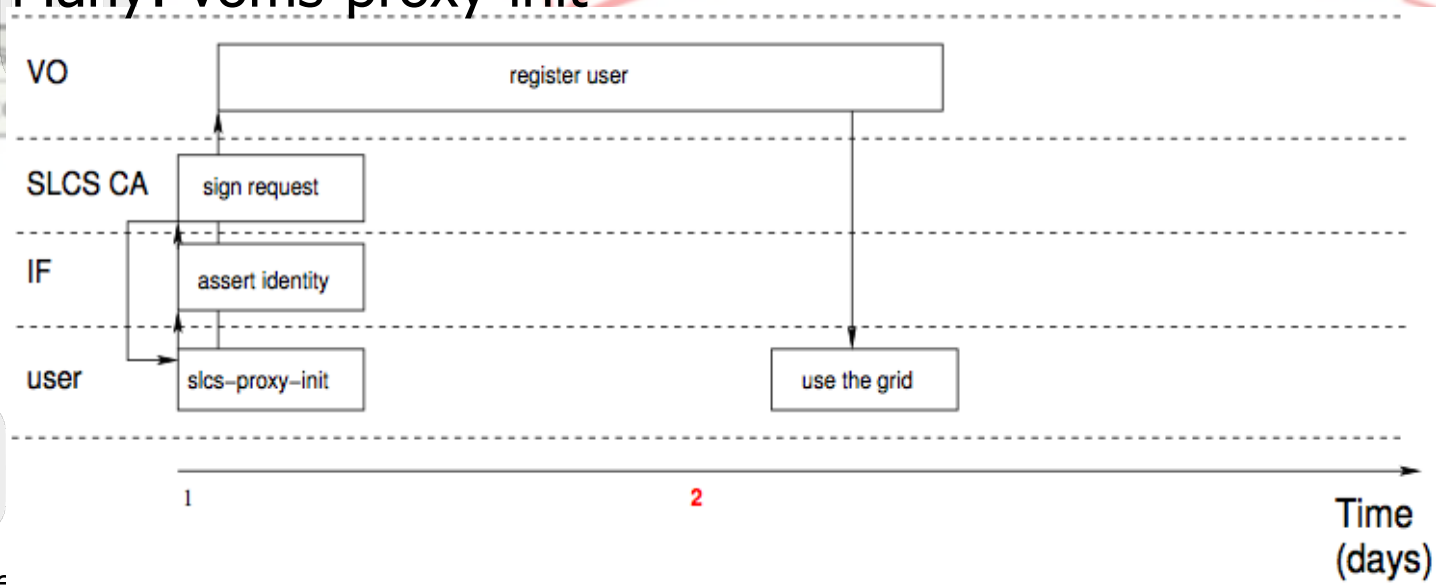
- Open Source Project based at UNINETT
- Contributions from UNINETT and NDGF
- Enables web as well as command line use
- Improves the procedure:
  - Once: grid-cert-req, vetting, voms-role-req
  - Many: voms-proxy-init



Confusa

- Open Source Project based at UNINETT
- Contributions from UNINETT and NDGF
- Enables web as well as command line use
- Improves the procedure:
  - Once: grid-cert-req, vetting, voms-role-req
  - Many: voms-proxy-init

COMPLICATED SLOW



Confusa

- Open Source Project based at UNINETT
- Contributions from UNINETT and NDGF
- Enables web as well as command line use
- Improves the procedure:
  - Once: grid-cert-req, vetting, voms-role-req
  - Many: voms-proxy-init

Accounting and Priorities

- We want to account to be able to control users priorities!
- This means that there is a loop between accounting and authorization
- And authorization, when it is variable, it is priority:
  - Less or More access to the resource
- Two kind of priority:
  - On / Off (quota or economy based)
  - Variable (ecological – use what is available)

Accounting Solutions

- In the Nordics the SGAS accounting system has been deployed
- SGAS v3 being deployed now supports
  - Account grid usage
  - Account pr DN and VO
  - Supports multiple databases to enable VO, site, and Country accounting

Accounting Solutions

- The DEISA accounting system works with:
  - UNICORE
  - Several LRMSes...
- It stores and presents OGF-UR!
- Enables accounting of other access patterns

DEISA
DISTRIBUTED EUROPEAN INFRASTRUCTURE FOR SUPERCOMPUTING APPLICATIONS

NDGF
Nordic DataGrid Facility

Capacity vs Quantity

NDGF
Nordic DataGrid Facility

Capacity vs Quantity

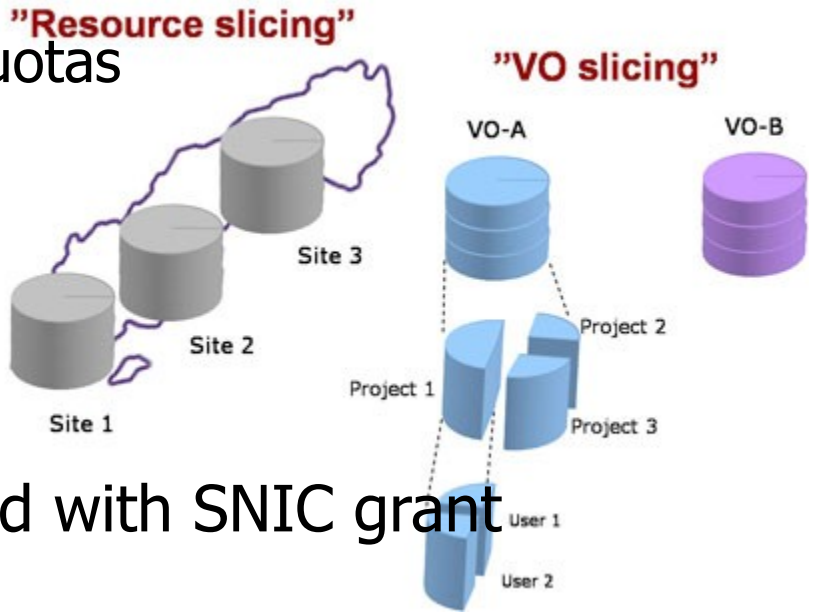
- Network is a capacity resource
- Storage is a quantity resource
  - But temporary storage (cache) is a capacity resource!
- Computing is capacity
  - But fixed allocations is a quantity resource!

- Economy works for Quantity resources
- Priority (like "fair share") works for Capacity resources

Grid wide fair share scheduling

Works with

- Hard quotas
- Max number of jobs allowed to run for user, groups, roles
- Fair share scheduling
  - Better utilization then hard quotas
  - Handles different use cases
  - Grid wide job priorities
- Support site policies
- Being implemented in SGAS
- Named FSGrid and coordinated with SNIC grant



Nordic Res. Sharing Framework

Problem I, II are solved and ready for deployment:

- SGAS/DEISA accounting (and FSGrid priorities)
- Federated IdPs, Confusa and TERENA Cert Service for prob. II

- Problem III:
  - DEISA accounting reporting modules
  - PAM modules being looked into.

Next Steps

- Resource Trading
  - Web tools for user priority ranking and policy settings
  - MoU between Nordic NGIs on the resource sharing / trading
- Promote an easy to administer resource usage loop:
  - Basic/new user – basic (low) priority
    - Apply for more resources based on use – higher priority
    - No/little use – lower priority
  - Similar to single resource use optimization – but infrastructure wide
- Possibility of using cross site / cross country usage in new resource funding considerations – exact policy to be determined

NDGF
Nordic DataGrid Facility