In Grid We Trust

New authentication mechanisms and their impact on trust relationships at the home organisation

ISGC 2011
David Groep
In Grid ...

where many participants have no a-priori relationship
... we trust
in identity and attributes delivered from many sources
Tusting and trustable parties

focus:  
- persistent unique ID
- traceability assurance

Home organisation or RA

Credentail Issuing Authority (Certification Authority)

VO (community) Membership Records (VOMS, LDAP)

Definitive Access Control

Resources: compute, storage, services, data

Site-level Authorization Database

IGTF
International Grid Trust Federation

voms admin for VO: alice Current user
VO management Subscriptions Config
AP Structure and Elements of Trust

- Identity Vetting (‘people ware’ LoA)
- Operational Requirements (‘what and how LoA’)
- Site security controls (‘implementation LoA’)
- Publication and disclosure (‘gaining trust’)
- Auditing (‘sustaining trust’)
- Privacy and confidentiality (‘securing trust’)
- Compromise and Disaster Recovery (‘recovering trust’)

- User responsibilities
  - this one deserves more attention in home organisation context, since direct & continuous contact with users can be maintained
Trust Relations in Classic CAs

CA Policy Document

User Community or Virtual Organisation

CA

RA (local to user)

Photo ID
Example: Classic Authority using Secured Infrastructure

- Aimed at long-lived identity assertions
- Identity vetting procedures
  - Based on (national) photo ID’s, face-to-face verification of applicants via distributed network of Registration Authorities or ‘Trusted’ Registrars
  - Periodic rekeying once every year, using fresh key material
  - Appropriate representation of the person’s real name in the credential
  - validate all rekeying against pre-existing credential identifiers
- Secured operations
  - dedicated rooms with monitored access, vault, and audit trails
  - off-line signing key or HSM-backed on-line systems (FIPS 140.2 lvl 2)
- Response to incidents
  - Timely (<24hrs) revocation of compromised credentials
  - must issue an up-to-date list of revoked credentials
- Audit log retention and periodic re-assessment

https://www.eugridpma.org/guidelines/classic/
Policies supporting trust

- Classic AP’s ‘traditional ID vetting’
  - done by CA explicitly according to own practices
  - face-to-face after or at time of making request

- What does that bring?
  - pro – easy to describe
  - con – complicated for user and introduces delay
  - but even then
    in risk analysis for the end-to-end trust chain, ID is only a small element as verified in the ‘classic’ AP
We, the Grid, trust

- Vetting in classic CAs gives ‘warm and fuzzy feeling’
  - is easy to describe in a stand-alone document
  - which may be false
  - but is certainly fuzzy

- But grid is no longer alone: many others need trust
  - many other services inside and off-campus need ‘trusted identity’ in some way
  - relative lower value of many off-campus services previously did not require a lot of complexity in assurance level or trust
A new wave of federated CAs

- new trusted identity sources have emerged
  - R&E federations have been established
  - hosting more and higher-valued services
  - broad and increasing user base

we now leverage these for access to e-Infra resources
Enabling new scenarios

GridShib
graphic: Jim Basney, NCSA

Delegation options
- ‘hidden’ federated CAs
- Security Token Service
- semi-explicit instant CA

IMDI Browser (delegated corpus browsing)
graphic: Mischa Salle, Nikhef

SURFnet
Big Grid
the Dutch e-science grid

David Groep
Nikhef
Amsterdam
PDP & Grid
Trust Relations in a Federated CA (MICS) model
New CA models

Broader base for users brings challenges

- ‘warm and fuzzy’ trust has a scaling limit
- there will necessarily be some indirection
- but federated IdP’s are ‘closer’ to the user
  - more trustworthy and more close to any changes
  - IdP’s are further away from the ‘grid’, and thus less warm and fuzzy

this applies to ID attributes and other value-added attributes ... and should apply to the VO as well!
In Grid We Trust

- IGTF global trust features are not ‘default’ in many federations
  - persistent unique naming
  - higher-assurance level identity vetting

- Responsibilities have to be defined
  - these now rely on the IdPs – these are now ‘quality IdPs’ in well-recognised federations
  - contract mechanisms tie down responsibility
  - how can an organisation set up a trusted IdM & IdP?
Basic federation policies

Requirements (example from SURFfederatie)

- Give accurate organisational contact details
- End-user guidance document per organisation
  - netiquette, compliance with law, no damage to third parties
  - guidance should be ‘appropriately enforced’
- federation systems appropriately secured
- data complete and up to date, set of required attributes
- disclose procedures and practices on request

Enforcement and sanctions

- Suspension from the federation (nothing worse)
- Indemnify other participants from damages
Contract supported trust

‘We the Grid’ should now trust what the IdP says, and rely on that trust without ‘warm and fuzzy’ recourse

graphic: after Jan Meijer, UNINETT
## Elements of institutional IdM

<table>
<thead>
<tr>
<th></th>
<th>Ad Hoc</th>
<th>Focused</th>
<th>Standard</th>
<th>Integrated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single log-on</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authorization</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source systems</td>
<td></td>
<td></td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Policies</td>
<td></td>
<td>●</td>
<td></td>
<td>●</td>
</tr>
<tr>
<td>Documented processes</td>
<td></td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>IdP systems for federation</td>
<td></td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Quality Assurance</td>
<td></td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Process implementation</td>
<td></td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Security / Auditing</td>
<td></td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>

Source: SURFnet Identity Management Maturity Scan [http://www.surfnet.nl/](http://www.surfnet.nl/)
IGI Group [http://www.igi.nl/](http://www.igi.nl/)
At a random mid-size org ...

- To be trustworthy, each IdP in a federation should address the basic requirements for trusted identity and attributes

- Basically, this is
  - addressing the topics listed in the AP by the IGTF
  - user education and validation
  - organisational ‘culture’

and a bit of policy and technical expertise ...
Organisational elements

- **ICT**
  - trustworthy IdP implies that users are familiar with the IdP, and use it for everyday work (so no separate login or system)
  - when rolled out, gives usability advantages (less helpdesk calls) and better security enforcement (single kill switch)
  - many services can be linked to SSO services (usually via LDAP)

- **HR**
  - source of ‘validated’ ID attributes (registry)
  - likely has existing practices to comply with privacy, data retention & protection, and legal issues

- **Management**
  - buy-in to endorse policy and guarantee continuity
Join a federation with integrated IdM

- For mid-size org needed effort not very high
  - once there is common intent and purpose can be done within ~ 6 months (not full-time), using OSS tooling

- Work items
  - ensure buy-in
  - write up a draft policy (using the AP template)
  - set up (LDAP-capable) directory service
  - demonstrate some quick goodies: desktop login, link to no-policy test federation using simpleSAMLphp
  - review the policy 😊
  - join the full federation and give goodies to users
Federation services as incentive and driving force for users and organisational systems such as email as incentive for both ICT (less support load, better controls) and users (single password).
The harder bits

- Goodies gain momentum, then take the next step
  - convert ‘critical’ systems, such as email, self-services (travel request, budgeting, timesheets, ...)
  - implement your account & password expiration policy in automated processes if that was not yet standing procedure (test first!)
  - give reasonable grace period, say, 13 months
  - start disabling services that are not SSO enabled
So: What About the Policy?

- Used IGTF Authentication Profile template

- Missing elements related to user management
  - need for data protection and attribute release policies
  - additional user obligations (e.g. password changing)
  - expiration controls
  - differentiate between suspension and expiration
  - you cannot ‘delete’ users (must keep the key identifier)

- In section 3 (identity vetting) added ‘hardship clause’ – helps ease pain of policy faults by limited override

- Also Grid AUP and Site Ops Policy have useful elements

- Be prepared to disclose the policy – publicly, AFAIAC!
Side effects of linking the IdM

- Organisational interest in proper registration as a side-effect of the IdM introduction
  - ICT services are typically the main thing people (grad students, guests, visiting researchers) need – so they want to have these and will go a long way to pester people. Alongside with a room key
  - Other services (registration in a phone directory, a web picture gallery, room allocation system, insurance) for the applicant have lower priority
  - By linking the systems, overall quality improved:
    - guests/students pester IT for an account, who redirects to HR. The applicant will keep on top of it and helps ensure consistency
    - HR wants a complete registration, e.g. for insurance purposes, and has an interest in processing the application
Some lessons learnt

- Policy document – you really must have one
  - as high level as possible (no frequent change), but ...
  - enough to assess compliance with popular services (in federation and elsewhere)

- Separate out your documents
  - practices and implementation from policy
  - attribute listing for data protection purposes in separate document – however, will need re-approval

- Explain intent, not only practices, to help desk
... so from now on ...

- web-SSO federations have matured
- integration of ‘high-value grid’ & web federation now becomes reality

- large, complex orgs: integration with existing ERP system
- mid-size: try it yourself, with policy templates and SSO tools

- Significant benefits for grid & more
- federation peers and CAs rely on and trust home institutes to manage their users properly
- so that in Grid we may trust