Introducing Identity Management in a mid-size research organisation

From use cases to policy … the good, the bad and the ugly

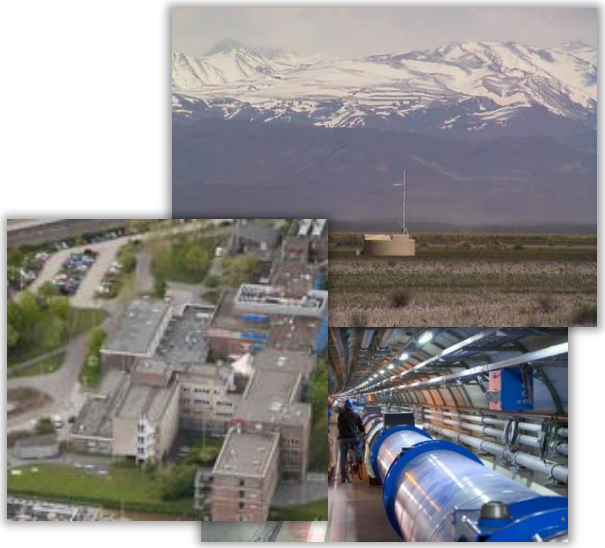
David Groep, Nikhef, Physics Data Processing Programme

Outline

- A few words about Nikhef
- Co-driving ID management adoption with research use cases
- Policy principles, document templates & structures
- The good, the bad and the ugly
- On sharing and engagement

David Groep
Nikhef
Amsterdam
PDP & Grid

About us, Nikhef



~ 260 employees

- 60 scientific staff
- 100 PhD & postdocs
- 80 engineers
- 20 support staff

+ many guests and students

… part of stichting FOM + 4 Universities (for employment administration)

And many national, European and global collaborations

listing only some ICT related ones here

BiG Grid
the dutch e-science grid

IGTF
International Grid Trust Federation
AP | EU | TAG

SURF SARA
National e-Infrastructure for Research

WLCG
Worldwide LHC Computing Grid

EMI
EUROPEAN MIDDLEWARE INITIATIVE

OGF

■ ■ ■

David Groep
Nikhef
Amsterdam
PDP & Grid

‘Why bother with policy?’

LSC VIRGO

Key ingredients when we started

PDP Research use cases ⇨ for our directorate

- Easier access to distributed e-Infrastructure via TCS eScience Personal (wLCG, EGI)
- Tempting access to federated services (LIGO/Virgo)

IT department use cases ⇨ for CT management

- Automate account clean-up: life cycle management
- Had to setup new mail service anyway, and …
- … users started requesting single password (beyond YP)

David Groep
Nikhef
Amsterdam
PDP & Grid

NIKHEF

Other key ingredient: cost

Being a mid-size organisation allowed us to introduce 'proper' IdM at very low cost as a *joint op* between the Nikhef research-IT (PDP) team and IT services group

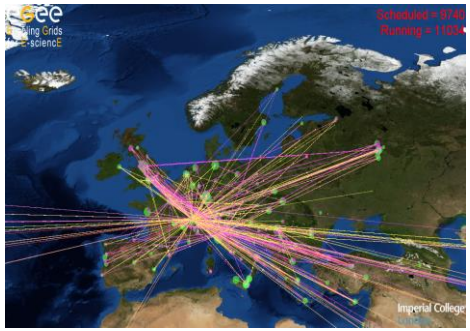
- All expertise existed in-house – mostly thanks to previous Grid & e-Infra work
  - Experience and good templates for policy
  - Existing central directory services for 'Grid' side
  - In-house expertise key technologies, if ~1-2 people
- Basic linkage to HRM systems had been done previously for a 'facebook' web gallery
- Flexible HR department (by good local proxy)

David Groep
Nikhef
Amsterdam
PDP & Grid

But: introducing Identity Management does not *save* you money!

Nothing new

Nobody actually wants to *read* policy, so tell in the exec-summary what target audience 'wants'



- For directorate, we promoted
  - Near-instant TCS certificates for wLCG
  - SURFspot (always a big selling point for federation, but *not* policy)
  - Elsevier/Scopus &c
- Convincing our CT group was fairly trivial
  - Auto-cleanup of accounts is a big plus – we lost 66% of our 'users' within a year ☺
  - SSO/LDAP integration for mail service (biggest head-ache till then)
- For 'DIY admins': ask how they deal with users in 10yrs

David Groep
Nikhef
Amsterdam
PDP & Grid

Graphic courtesy GridPP and EGEE: Real Time Monitor - *rtm.hep.ph.ic.ac.uk*

How to 'sell' a policy

- You don't! Policy is *not optional*, so don't even *suggest* anywhere you can work without one

Set up as *joint effort* of physics computing and IT services and got fairly quick directorate buy-in

- Stating we had to comply with TCS CP/CPS helped
- The 'IdM maturity scan' (SURFnet sponsored) helped
  … *that's external pressure working for you* ☺
- Writing one quickly – *and* not requesting effort up-front – helped
  … *could have been a draft to show where we were going*

David Groep
Nikhef
Amsterdam
PDP & Grid

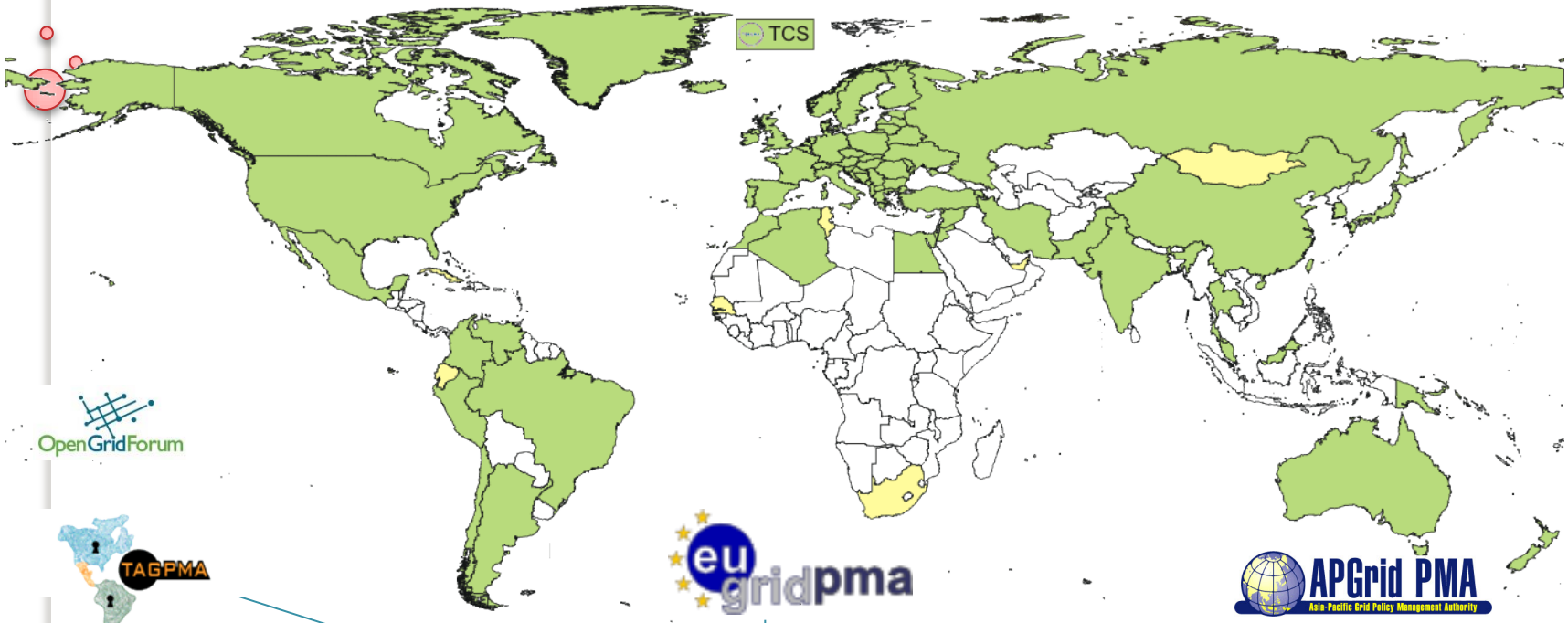
Writing it all up

- Use a template – there are many out there
  - Not too technology specific (e.g. RFC3647 is great, but too much PKI specific; NIST SP800 series too detailed)
  - Pick one which addresses federation concerns, and borrow from e.g. *REFEDS federation policy best practice approach* [2], the *Identity Federation Policy template document (TNC2013)* [3], &c…
  - And modify if there are missing elements
- We picked the Open Grid Forum "Requirements for Authentication Service Profiles" [1]
  - Technology agnostic, compact, and 'familiar' to us in the IGTF
  - Good list of 'things to address' (added just small things on end-user obligations, which in the IGTF are dealt with elsewhere)

David Groep
Nikhef
Amsterdam
PDP & Grid

[1] http://redmine.ogf.org/dmsf_files/29
[2] https://refeds.terena.org/index.php/Federation_Policy_Best_Practise_Approach
[3] Marina Vermezovic et al., https://tnc2013.terena.org/getfile/701

Borrowing from the IGTF



www.igtf.net

Global policy profile, based on 'minimum requirements', geared towards IdM for scattered, lone end-users

David Groep
Nikhef
Amsterdam
PDP & Grid

NIKHEF

Policy elements (from OGF template)

1. Authentication Service management
2. General architecture of the Service
3. Identity [*vetting, attributes, roles, life cycle management*]
4. Operational Requirements
5. Facility Security
6. Publication and Repository Responsibilities
7. Liability, Financial Reponsibilities, and Audits
8. Privacy and Confidentiality
9. Compromise and Disaster Recovery

- Added: Subscriber ('users') Obligations and Compliance

David Groep
Nikhef
Amsterdam
PDP & Grid

The Good …

- Make sure the policy *follows* working process, don't force reasonable processes to change
  - Spend time to understand processes elsewhere
  - Fix only 'worst bits' of process inconsistent with requirements
  - Introducing IdM policy is not an excuse for re-organisation: keep processes *and data* where they are
- Write to support exceptions: we have a hardship clause
- Follow organisational culture
  - Our basic premise: allow and promote use, preserve user privacy, *unless* it causes harm to Nikhef (like undue operational costs, non-compliance with external providers, legal hassle)
  - and do no harm towards our IdM consumers

David Groep
Nikhef
Amsterdam
PDP & Grid

example of its implementation

- So '*Following existing processes*' reflects in Sec. 3 "Identity"

  We defined all categories of account we identified in the old system
  - Users (those entities having registration data and vetting)
  - Generic Accounts (entities without independent registration data)
  - Automated system entities

- Vetting processes defined only for users
  - Thus: only Users get federated privileges
  - Actual F2F ID vetting done by HR dept only ('WBP-safe' ;-)
  - accounts with lower LoA ('affiliate') *can* be vetted by any (registered) employee: 'sponsor', *as long as registration data are kept*

- Registration is 'easy', but access to services controlled
- Complete account life cycle is defined, also for incidents

David Groep
Nikhef
Amsterdam
PDP & Grid

Good, cheap, or quick: pick any two

- Take your *calender* time – it took us ~ 2 years
  one year for establishment,
  plus one year for graceful roll-over
  - Awareness (TCS): early 2005, impetus early 2008
  - Initial maturity scan in Oct 2008 → still low
  - Took ~ 9mo calendar-time to get organisation aligned
  - Ready for prime time in December 2009
  - New IdM evaluated and audited Jan 2010
  - Graceful roll-over period complete January 2011

- Actual *effort* (policy + implementation) small: 2–3 PM
  - … but effort spent by few 'expensive' (=overcommitted) experts

David Groep
Nikhef
Amsterdam
PDP & Grid

… the bad …

- Training helpdesk personnel is never sufficient
  - you *will* be spending time dealing with exceptions, or otherwise with frustrated users
- Be prepared to 'educate' upstream providers

  "no, I don't need *to know everyone's pay grade nor a passport no. to determine if they're an employee"*
- Having a policy means there will be violations
  - Make sure the policy empowers you to take action
  - Be prepared to spend time on taking these actions
- You will have stay vigilant against the 'DIY admins'

David Groep
Nikhef
Amsterdam
PDP & Grid

… and the ugly

- Do *not* hurry too much – we made *that* mistake
  - Policy tends to become immutable,
    whilst practices may and will change
  - ***Take the advice of RFC3647 to heart***
    and take the time and *split* Policy and Practice statements
    we did not, and really ought to update the policy again
    and the policy SHOULD only have RFC2119 language in it, nothing else
- We really should have spent time doing RBAC
  but did not since most tooling was attribute-based
- It took us one more year to get a new AUP
  - since it involved monitoring capabilities, needed OR approval –
    and a works council is technically clueless

Getting there: share!

If you are inclined to 'duplicate' the process

- Find at least one research (read: business critical) case
  - to make it authoritative you'll need some top-down support
- Don't 'over-do' the policy
- Get involved in an IdM/policy community
  – having or breeding in-house experts helps
  - Go to SURF & SURFnet groups & network events …
  - TERENA taskforces TF-EMC2 and TNC
  - Go to the EuroCAMP meetings
  - Listen in to FIM4R workshops and REFEDS
  - **Talk, share, engage, ask & discuss!**

David Groep
Nikhef
Amsterdam
PDP & Grid

NIKHEF

Questions?

David Groep
Nikhef
Amsterdam
PDP & Grid