Evolving Assurance – going where?

Collaborative, distributed, and generalized assurance beyond just identity authentication

–

IGTF Generalized LoA, … and AARC!

With inputs from:
Interoperable Global Trust Federation IGTF
AARC – coordinated by the GEANT Association/TERENA
EGI SPG

David Groep
Nikhef
Amsterdam
PDP & Grid

Assurance Levels – both ways

- Risk based policies and assurance
- Focusing on the inputs
  - Assertions: identity, attributes
  - Release and Trust: policies on SPs, on IdPs, or both?
- Developing the composite AAI landscape
  - Authentication and Authorization for Research Collaborations

David Groep
Nikhef
Amsterdam

Risk

‘risk envelope’

Subject (ID/LoA) based

- Defined **identity assurance level**
- **Includes Community-given LoA**
- For given actions, resources, and acceptable residual risk, required ID assurance is a given

Action (app) based

- More constraint actions can lower need for identity LoA
- **(J)SPG VO Portal policy** does that: 4 levels of actions

Resource (value) based

- e.g. access to wireless network does not pose huge risks, so can live with a lower identity LoA (eduroam)

Residual Risk:

Determine the risk envelope

- What are you willing to accept?
  - Cost of monitoring to assess/retain systems integrity
  - Cost of recovery in case of incidents (time, money, consultancy costs)
  - Benefits of having more (paying) users
  - Benefits of appearing ‘low-barrier’
- Considerations include
  - Your ‘outside’ risk envelope should stay the same –
    determined by local regulation,
  - the AUPs of your (network) peers,
  - your (media) exposure and reputation status

David Groep
Nikhef
Amsterdam
PDP & Grid

Collaborative risk

In beyond, we have developed models shifting responsibilities within the risk envelope

- VO Portal Policy: offset lower ID vetting with restricting actions
- Consider lower-risk services (think eduroam)

Now incorporating collaborative subject attribute provisioning

- High-quality VO ID vetting (F2F)&IOTA identifiers (e.g. LHC)
- Mediated User Registration + actions containment + simple identifiers: LToS Specific Security Policy

David Groep
Nikhef
Amsterdam
PDP & Grid

Assurance in R&E federations

- For now focus has been largely on getting assurances *from the service providers,* e.g.
  - Data Protection Code of Conduct
  - developed Privacy Policy
  - Justification for each attribute requested
  - R&S Entity Category (for attribute release)

https://wiki.edugain.org/Recipe_for_a_Service_Provider

David Groep
Nikhef
Amsterdam
PDP & Grid

But EGI is (mostly) an SP

… so we need some assurance from IdPs and Federations …

- this is new for most IdPs!
  - Many (most) SPs have been ‘low-value’
    – now changing: also pressure from publishers worried about proxies
  - Focus of the IdP is to serve bulk users (students and admin staff),
    not typically researchers – there are too few!
  - The IdM folks are (typically) not the people doing IT Sec or CSIRT
  - and: not simple to get formal agreements really signed by an R&E institution (too many lawyers we don’t need get in the way)

- So we need some (‘R&E’ friendly) **IdP assurance**

David Groep
Nikhef
Amsterdam
PDP & Grid

Example: IGTF trust building method

- Accreditation process
  - Extensively documented *public* practices (CP/CPS, RFC3647)
  - Interviewing and scrutiny by peer group (the PMA)
  - Assessment against standards (LoA and APs)
  - Technical compliance checks (dependent on credential type)
- Periodic, peer-reviewed, self-audits
  - Based on Authentication Profiles, standard reference: GFD169
  - inspired by APs, LoA, and NIST SP800-53/ISO:IEC 27002
- Federated assessment methodology by region (IGTF)
  - keeps it scalable by ‘divide & conquer’

David Groep
Nikhef
Amsterdam
PDP & Grid

https://www.eugridpma.org/guidelines/accreditation

IGTF LoA Generalisation

http://wiki.eugridpma.org/Main/IGTFLoAGeneralisation

- Federation of major Relying Parties (RPs) and identity providers that jointly agree on achievable and sufficient assurance
  - RPs like PRACE, EGI, EUDAT, XSEDE, OSG, TERENA/ GÉANT, HPCI, … and many national representatives
  - Identity providers, both from R&E and beyond
- About 2-3 distinct levels (*not* the Kantara ones)

David Groep
Nikhef
Amsterdam
PDP & Grid

Generalised LoA

- IGTF ‘levels’ are useful classifying IdP assurance levels for distributed infrastructures
  - There is not exactly a hierarchy (so we used opaque names)
  - Is **technology agnostic** (PKI, SAML, OpenID/OAuth)

http://wiki.eugridpma.org/Main/IGTFLoAGeneralisation

  - ASPEN, BIRCH, CEDAR, DOGWOOD
  - Reflect trust level of SLCS, MICS, Classic, IOTA

David Groep
Nikhef
Amsterdam
PDP & Grid

Coming soon to a theatre near you: Compositional attributes & LoA

The future is bringing us attributes from many sources

- identifiers from R&E or external providers
- Attributes on community membership
- Eligibility attributes, social attributes, …

There are many, and quick, technical developments

- OpenConext, Grouper, PERUN, VOMS, HEXAA, …

But there's no (assurance level) collation mechanism yet …

- *How to compose policies?*

David Groep
Nikhef
Amsterdam
PDP & Grid

Making LoA useful

- For LoA to be useful, it needs to consider risk and e.g. incident response capability when all assertions are **combined** for a final AuthZ decision
  - Any source of attributes has an LoA (even if it is not yet expressed in readable form)
  - The end-to-end system collaboratively needs to address risk: identifiers, attributes, resource data
  - Example IGTF LoAs: The IGTF itself deals in identifiers, but the LoA framework could be applied to more attributes
- Decision based on attributes from multiple sources
  - Need to make the LoA more ‘visible’ to authZ

David Groep
Nikhef
Amsterdam

Expanding the work

Authentication and Authorization for Research Collaborations
AARC

David Groep
Nikhef
Amsterdam
PDP & Grid

Why AARC?

- On the technical side
  - address Single Sign On for non-web applications
  - authorisation side: attribute aggregation
  - integration of credential use

  Both these areas are rather complex and even if progresses have been made, there is still need for further work
- On the policy side
  - Consolidate initiatives where work is carried out
  - GÉANT project, EGI, IGTF, REFEDS, FIM4R, RDA,

David Groep
Nikhef
Amsterdam
PDP & Grid

Inputs to AARC

Organisational and legal (policy) work

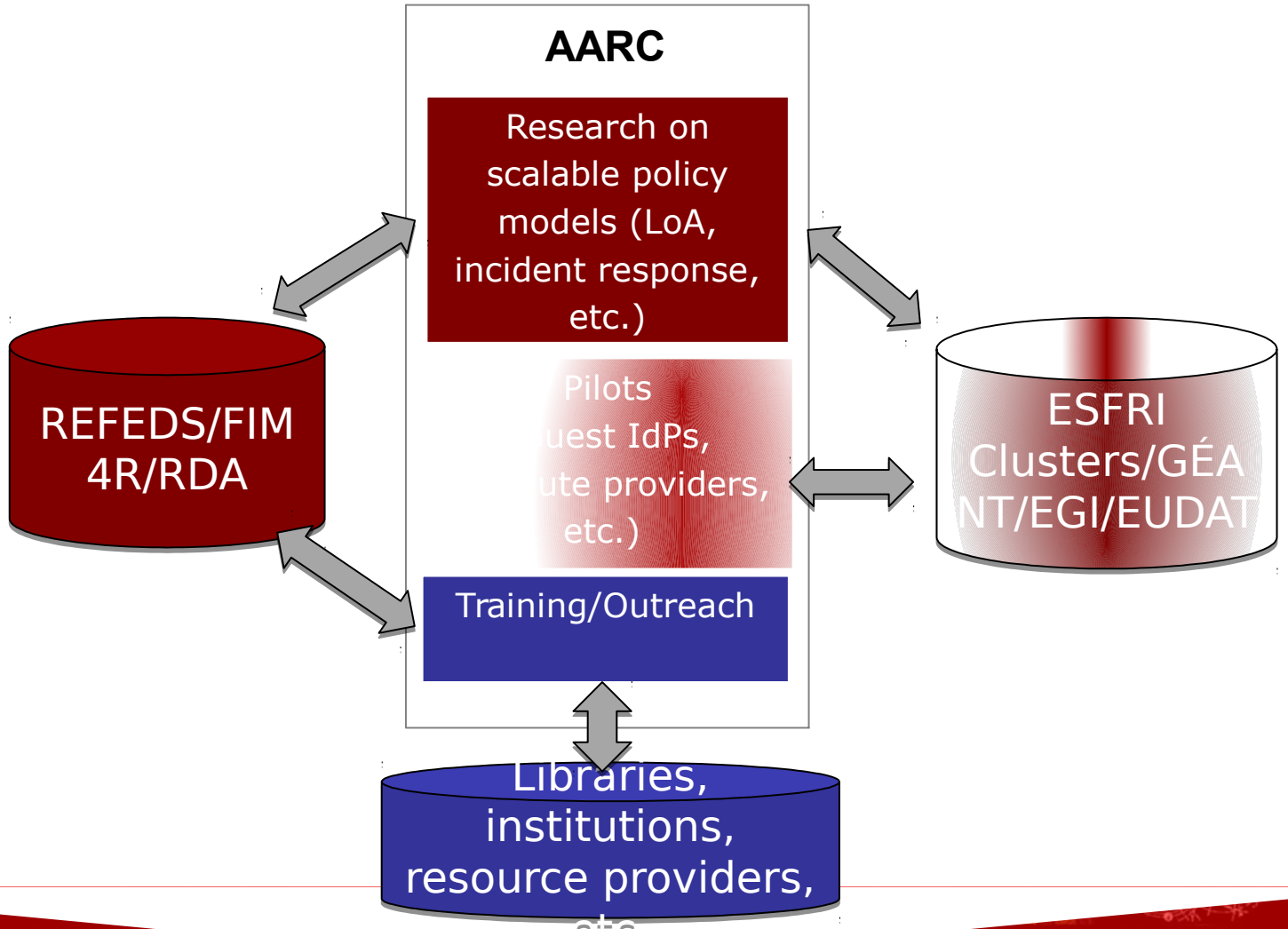
- eduGAIN
- REFEDS (R&S, CoC)
- IGTF RP (EGI, OSG, PRACE, XSEDE) LoA requirements

Technical work

- Various non-Web SSO techniques
- Credential translators (STS, Portals, SLCS CAs)

David Groep
Nikhef
Amsterdam
PDP & Grid

Part of an ecosystem



David Groep
Nikhef
Amsterdam
PDP & Grid

An open collaborative effort

- Although there are ‘only’ 20 project partners
  it is a pan-European effort!
  - work plan is to be co-developed collaboratively
  - communities are encouraged (in several ways)
    to attend workshops and express their requirements

TERENA, CERN, CESNET, CSC, DAASI, DFN, EGI, GARR, GRNET, JANET, FZJulich, KIT, LIBER, MZK/Brno, FOM-Nikhef, PSNC, RENATER, STFC/RAL, SURFNet, SURFsara

Your input is very welcome!

David Groep
Nikhef
Amsterdam
PDP & Grid