Boosting AAI for research and collaboration

David Groep

NA3 – Policy Harmonisation and Best Practice coordinator

Nikhef

Nikhef

10th FIM4R Meeting

Vienna, 20-21 February 2017

Starting Point: Identified Requirements

Attribute Release

Attribute Aggregation

User Friendliness

SP Friendliness

User Managed Information

Persistent Unique Id

Credential translation

Credential Delegation

Levels of Assurance

Guest users

Step-up AuthN

Non-web-browser

Community based AuthZ

Best Practices

Social & e-Gov IDs

Incident Response

Addressing e-Research Requirements

Date: 6 March 2012

Authors: Licia Florio (TERENA), Nicole Harris (JISC Advance), Christoph Witzig
Mikael Linden (CSC), Ajay Daryanani (RedIRIS), Ann Harding (SWITCH),

Advancing Technologies and Federating Communities

A Study on Authentication and Authorisation Platforms for Scientific Resources in Europe

A pilot project for WLCG
eduGAIN
IdP
CERN SSO
STS
MYPROXY
IOTA CA
VOMS
SAML
X.509
The UK Access Management Federation
FOR EDUCATION AND RESEARCH
aconet
cafe
SWITCH aai
grnet
ID cz
SIFULAN
confia
AUSTRALIAN ACCESS FEDERATION
Belnet
R&E Federation
CILogon Service
Edu gate
Gaining Access to Education
SURF CONEXT
WAYF
Where are you from
IGTF
Interoperable Global Trust Federation
AP | EU | TAG
RCTSaai
REDE CIÊNCIA, TECNOLOGIA E SOCI
Carsi
eduGAIN
RENATER
CONNECTEUR DE SAVOIRS
学認 GakuNin
InCommon®
Colfire
Colombian Federation of Identity for Research and Education renata
TAAT
AAI @EduHr
Tuakiri
NEW ZEALAND ACCESS FEDERATION
arnes
eduID
SWAMID
Comunidad Federada REUNA

Common Scenario

- The scenario:
  - There is a **technical architect of a research community**
  - Her community is **distributed internationally**
  - **Increasing number of services** need authentication and authorization
  - She wants to **focus on research** and not reinvent the wheel
  - She starts googling and asking around
- So, there are some solutions available, but…

Think Global: the AARC project

Bring federated access to eResearch

Avoid a future in which new research collaborations develop independent AAIs

Build on existing tools and framework

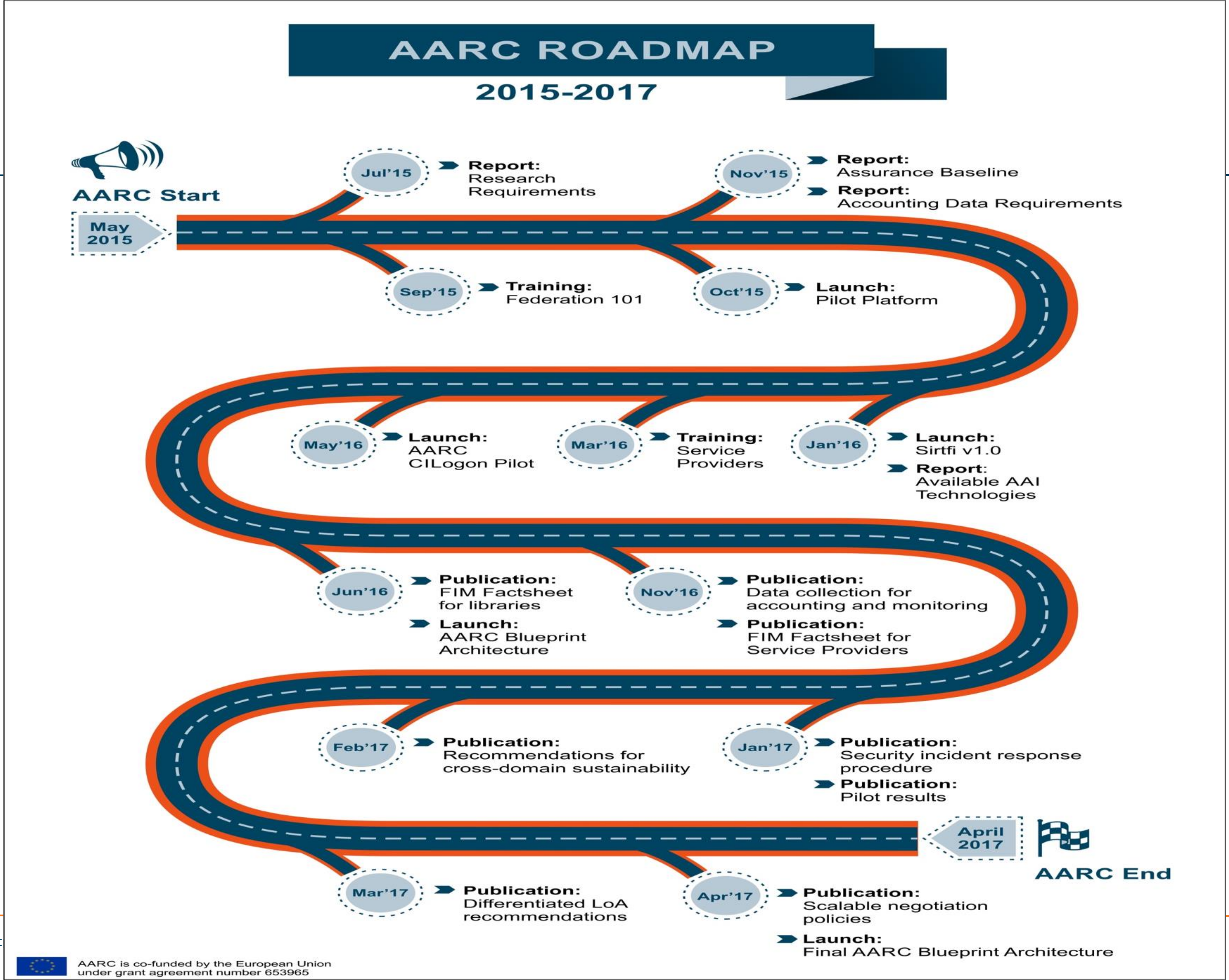
What AARC does want to change and how

- Improve usage of FIM – Promote usage of FIM and organise training to leverage identity providers outside the academic boundaries

- Address Research requirements – Design a technical Blueprint Architecture that builds on top of eduGAIN to add components required

- Offer support for global policies – Sponsor the development of key policy frameworks that aim to add additional ‘flavours’ to eduGAIN.

- Sustainability – Ensure that operations of components of the blueprint architecture and deployment of assurance, security and policy frameworks rest with r/e-infrastructures



AARC ROADMAP

2015-2017

AARC Start

May 2015

Jul'15
- **Report:** Research Requirements

Sep'15
- **Training:** Federation 101

Oct'15
- **Launch:** Pilot Platform

Nov'15
- **Report:** Assurance Baseline
- **Report:** Accounting Data Requirements

Jan'16
- **Launch:** Sirtfi v1.0
- **Report**: Available AAI Technologies

Mar'16
- **Training:** Service Providers

May'16
- **Launch:** AARC CILogon Pilot

Jun'16
- **Publication:** FIM Factsheet for libraries
- **Launch:** AARC Blueprint Architecture

Nov'16
- **Publication:** Data collection for accounting and monitoring
- **Publication:** FIM Factsheet for Service Providers

Jan'17
- **Publication:** Security incident response procedure
- **Publication:** Pilot results

Feb'17
- **Publication:** Recommendations for cross-domain sustainability

Mar'17
- **Publication:** Differentiated LoA recommendations

Apr'17
- **Publication:** Scalable negotiation policies
- **Launch:** Final AARC Blueprint Architecture

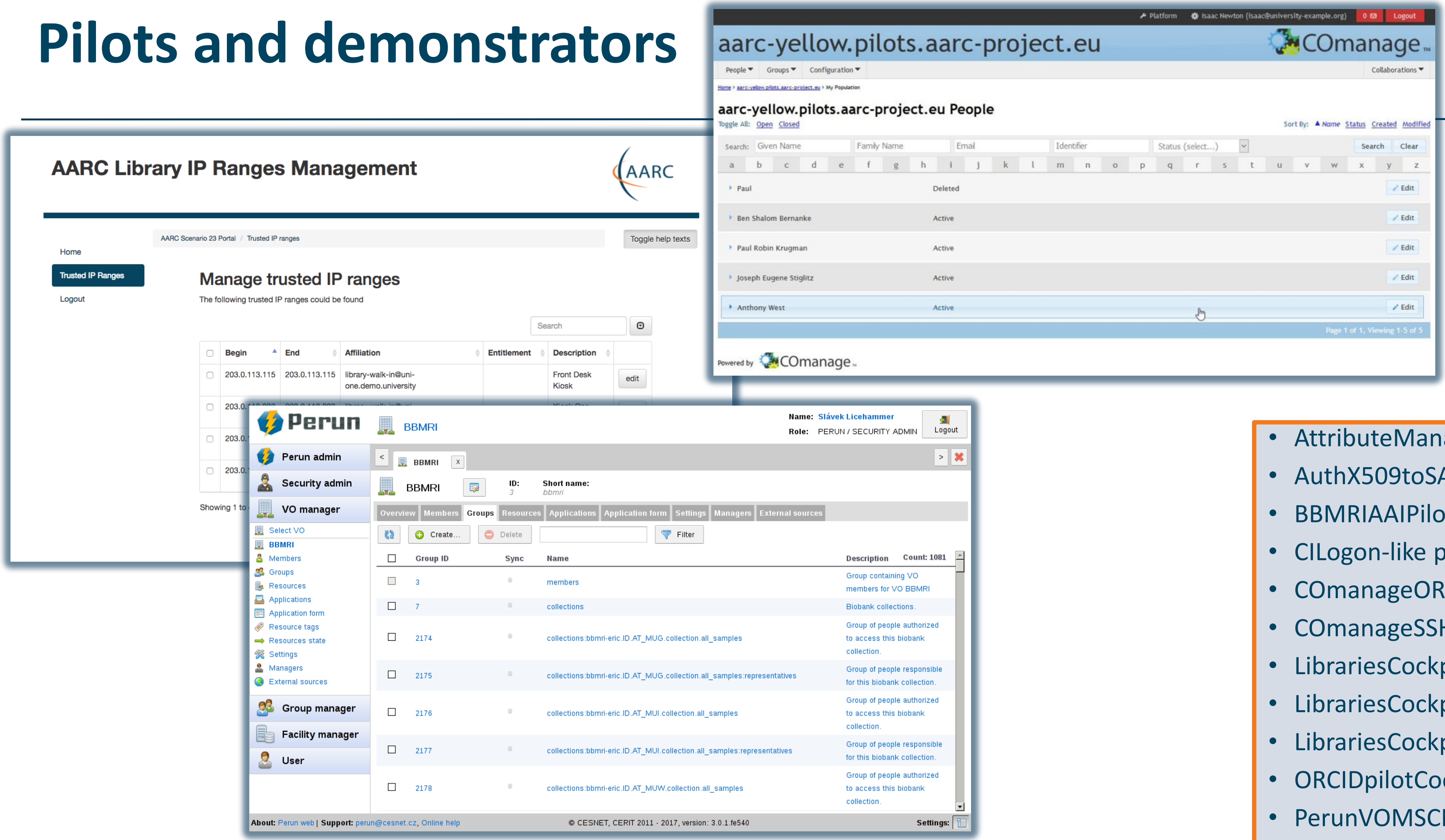
April 2017

AARC End

AARC is co-funded by the European Union under grant agreement number 653965

https://aarc-project.eu/achievements/

Pilots and demonstrators



AARC Library IP Ranges Management

AARC Scenario 23 Portal / Trusted IP ranges

Toggle help texts

- Home
- Trusted IP Ranges
- Logout

Manage trusted IP ranges

The following trusted IP ranges could be found

Search

☐	Begin	End	Affiliation	Entitlement	Description	
☐	203.0.113.115	203.0.113.115	library-walk-in@uni-one.demo.university		Front Desk Kiosk	edit
☐	203.0.					
☐	203.0.1					
☐	203.0.1					

Showing 1 to

Platform · Isaac Newton (isaac@university-example.org) · 0 · Logout

aarc-yellow.pilots.aarc-project.eu COmanage

People · Groups · Configuration · Collaborations

Home > aarc-yellow.pilots.aarc-project.eu > My Population

aarc-yellow.pilots.aarc-project.eu People

Toggle All: Open Closed — Sort By: Name Status Created Modified

Search: Given Name · Family Name · Email · Identifier · Status (select...) · Search · Clear

a b c d e f g h i j k l m n o p q r s t u v w x y z

Name	Status	
Paul	Deleted	Edit
Ben Shalom Bernanke	Active	Edit
Paul Robin Krugman	Active	Edit
Joseph Eugene Stiglitz	Active	Edit
Anthony West	Active	Edit

Page 1 of 1, Viewing 1-5 of 5

Powered by COmanage

Perun BBMRI

Name: Slávek Licehammer
Role: PERUN / SECURITY ADMIN
Logout

- Perun admin
- Security admin
- VO manager
  - Select VO
  - BBMRI
  - Members
  - Groups
  - Resources
  - Applications
  - Application form
  - Resource tags
  - Resources state
  - Settings
  - Managers
  - External sources
- Group manager
- Facility manager
- User

BBMRI — ID: 3 — Short name: bbmri

Overview · Members · Groups · Resources · Applications · Application form · Settings · Managers · External sources

Create... · Delete · Filter

☐	Group ID	Sync	Name	Description
☐	3		members	Group containing VO members for VO BBMRI
☐	7		collections	Biobank collections.
☐	2174		collections:bbmri-eric.ID.AT_MUG.collection.all_samples	Group of people authorized to access this biobank collection.
☐	2175		collections:bbmri-eric.ID.AT_MUG.collection.all_samples:representatives	Group of people responsible for this biobank collection.
☐	2176		collections:bbmri-eric.ID.AT_MUI.collection.all_samples	Group of people authorized to access this biobank collection.
☐	2177		collections:bbmri-eric.ID.AT_MUI.collection.all_samples:representatives	Group of people responsible for this biobank collection.
☐	2178		collections:bbmri-eric.ID.AT_MUW.collection.all_samples	Group of people authorized to access this biobank collection.

Count: 1081

About: Perun web | Support: perun@cesnet.cz, Online help © CESNET, CERIT 2011 - 2017, version: 3.0.1.fe540 Settings:

- AttributeManagementPilot
- AuthX509toSAMLDemo
- BBMRIAAIPilot
- CILogon-like pilot
- COmanageORCIDPilot
- COmanageSSHPilot
- LibrariesCockpitPanelConsortiumProxy
- LibrariesCockpitPanelEZproxy
- LibrariesCockpitPanelWalkInUsersPortal
- ORCIDpilotCockpitPanel
- PerunVOMSCILogonPilot
- SocialIDCockpitPanel

https://wiki.geant.org/display/AARC/Pilot+results+and+demos

AARC CILogon Pilot: A Token Translations Service for Europe

Use-cases:

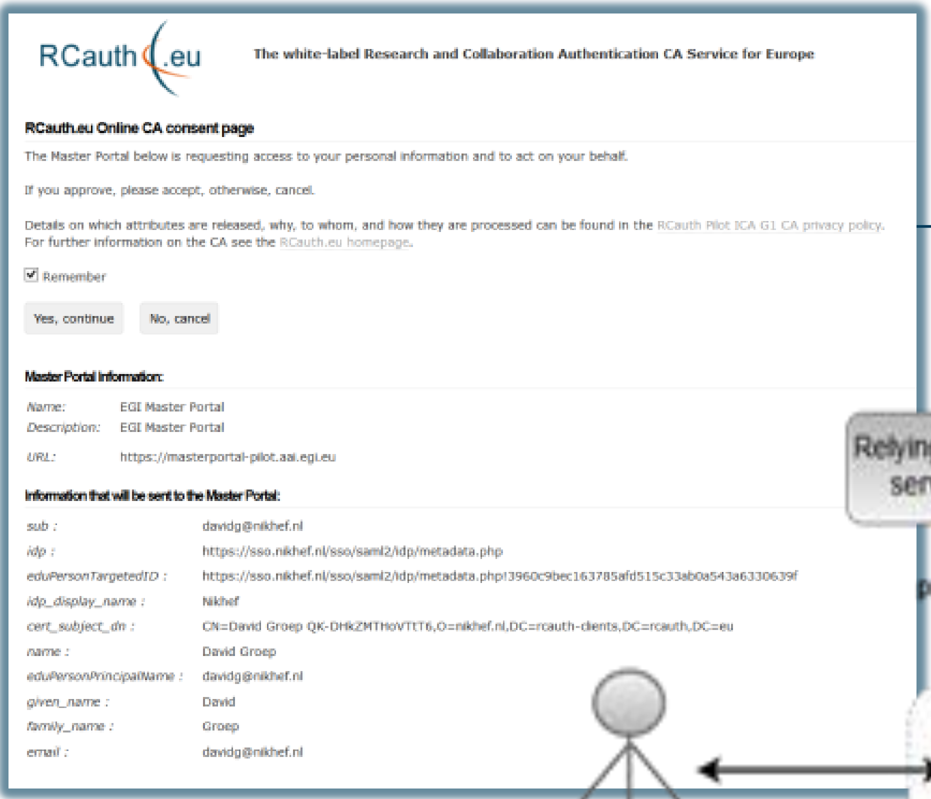
- Hide PKIX complexity from the users
- Federated Access to web and non-web resources
- Support different type of credentials and delegation
- Enables access to different resource via portal

Benefits:

- Allows for VO services, ie. VOMS
- Offered to research communities as service
- Managed security-sensitive components

Built on CILogon and MyProxy! www.cilogon.org CILogon

Flow for RCauth-like scenarios



RCauth.eu The white-label Research and Collaboration Authentication CA Service for Europe

RCauth.eu Online CA consent page

The Master Portal below is requesting access to your personal information and to act on your behalf.

If you approve, please accept, otherwise, cancel.

Details on which attributes are released, why, to whom, and how they are processed can be found in the RCauth Pilot ICA G1 CA privacy policy. For further information on the CA see the RCauth.eu homepage.

☑ Remember

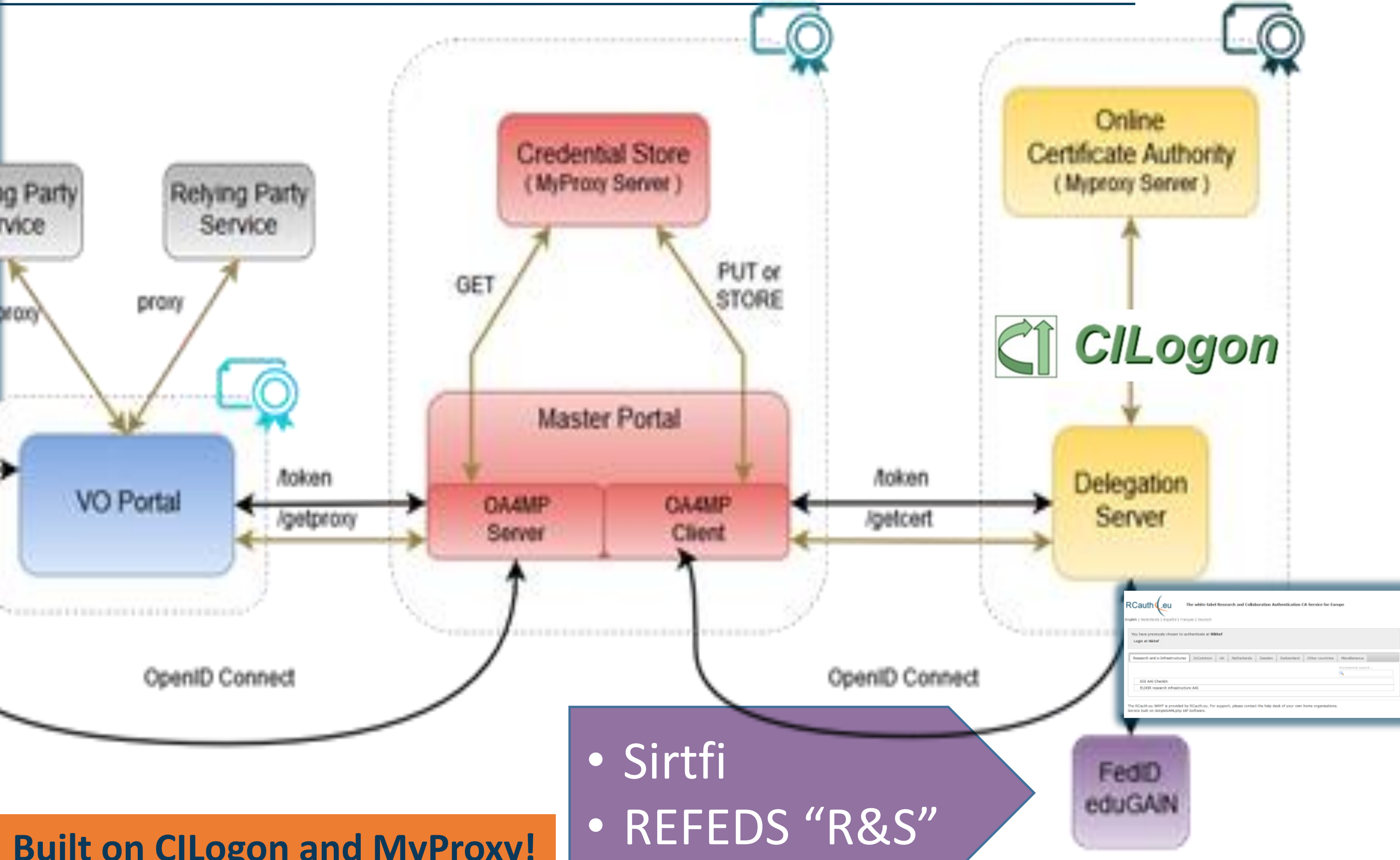
Yes, continue | No, cancel

Master Portal information:

Name:	EGI Master Portal
Description:	EGI Master Portal
URL:	https://masterportal-pilot.aai.egi.eu

Information that will be sent to the Master Portal:

sub :	davidg@nikhef.nl
idp :	https://sso.nikhef.nl/sso/saml2/idp/metadata.php
eduPersonTargetedID :	https://sso.nikhef.nl/sso/saml2/idp/metadata.php!3960c9bec163785afd515c33ab0a543a6330639f
idp_display_name :	Nikhef
cert_subject_dn :	CN=David Groep QK-DHkZMTHoVTtT6,O=nikhef.nl,DC=rcauth-clients,DC=rcauth,DC=eu
name :	David Groep
eduPersonPrincipalName :	davidg@nikhef.nl
given_name :	David
family_name :	Groep
email :	davidg@nikhef.nl



RCauth.eu The white-label Research and Collaboration Authentication CA Service for Europe

English | Nederlands | Español | Français | Deutsch

You have previously chosen to authenticate at **Nikhef**

Login at Nikhef

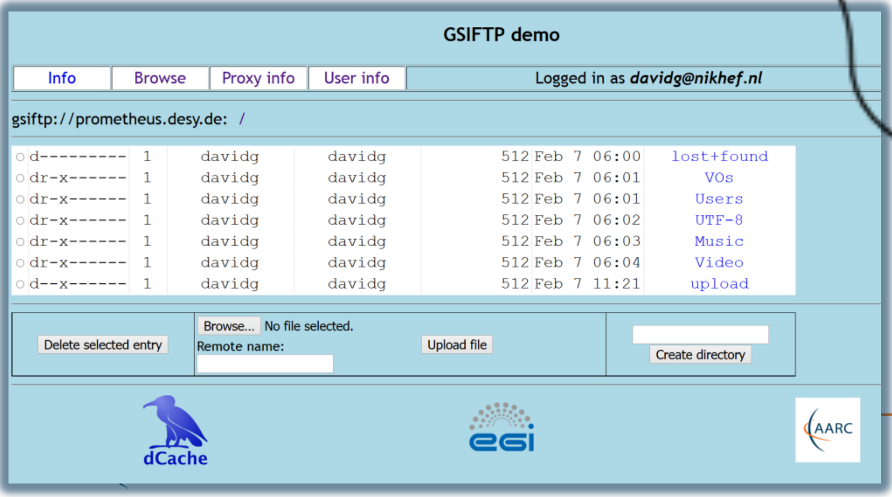
Research and e-Infrastructures | InCommon | UK | Netherlands | Sweden | Switzerland | Other countries | Miscellaneous

Incremental search...

EGI AAI CheckIn

ELIXIR research infrastructure AAI

The RCauth.eu WAYF is provided by RCauth.eu. For support, please contact the help desk of your own home organisations. Service built on SimpleSAMLphp IdP Software.



GSIFTP demo

Info | Browse | Proxy info | User info — Logged in as ***davidg@nikhef.nl***

gsiftp://prometheus.desy.de: /

```
○ d---------  1  davidg  davidg  512 Feb  7 06:00  lost+found
○ dr-x------  1  davidg  davidg  512 Feb  7 06:01  VOs
○ dr-x------  1  davidg  davidg  512 Feb  7 06:01  Users
○ dr-x------  1  davidg  davidg  512 Feb  7 06:02  UTF-8
○ dr-x------  1  davidg  davidg  512 Feb  7 06:03  Music
○ dr-x------  1  davidg  davidg  512 Feb  7 06:04  Video
○ d--x------  1  davidg  davidg  512 Feb  7 11:21  upload
```

Delete selected entry | Browse... No file selected. Remote name: | Upload file | Create directory

Built on CILogon and MyProxy!
www.cilogon.org

- Sirtfi
- REFEDS "R&S"

see also https://rcdemo.nikhef.nl/

First e-Infrastructure implementations for BPA & pilots

- EGI CheckIn Service

  https://wiki.egi.eu/wiki/AAI

- ELIXIR AAI

  https://www.elixir-europe.org/services/compute/aai

- EUDAT B2ACCESS

  https://www.eudat.eu/services/b2access

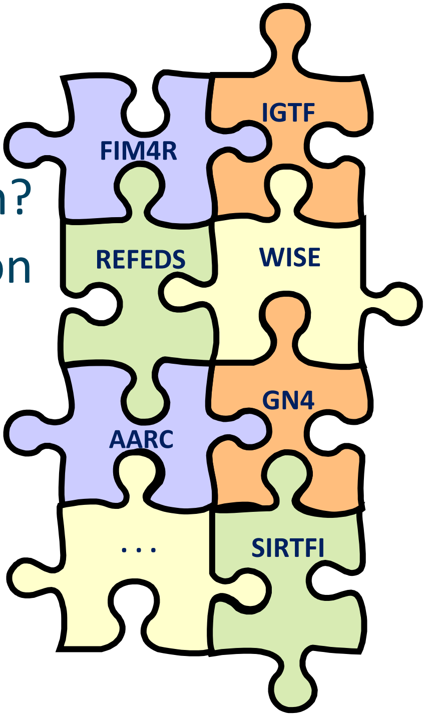
- GÉANT eduTEAMS

  https://www.eduteams.org

Solving the Policy Puzzle

Pushing forward best practices and like policies across many participants

- "Levels of Assurance"– baseline and differentiated profiles, capabilities and grouping
- "Incident Response" – beyond Sirtfi: a common understanding on operational security
- "Sustainability, Guest IdPs, use models" – how can a service be offered in the long run?
- "Scalable policy negotiation" – helping SPs move beyond bilateral discussion
- "Protection of (accounting) data privacy" – necessary aggregation without breaking the law too much



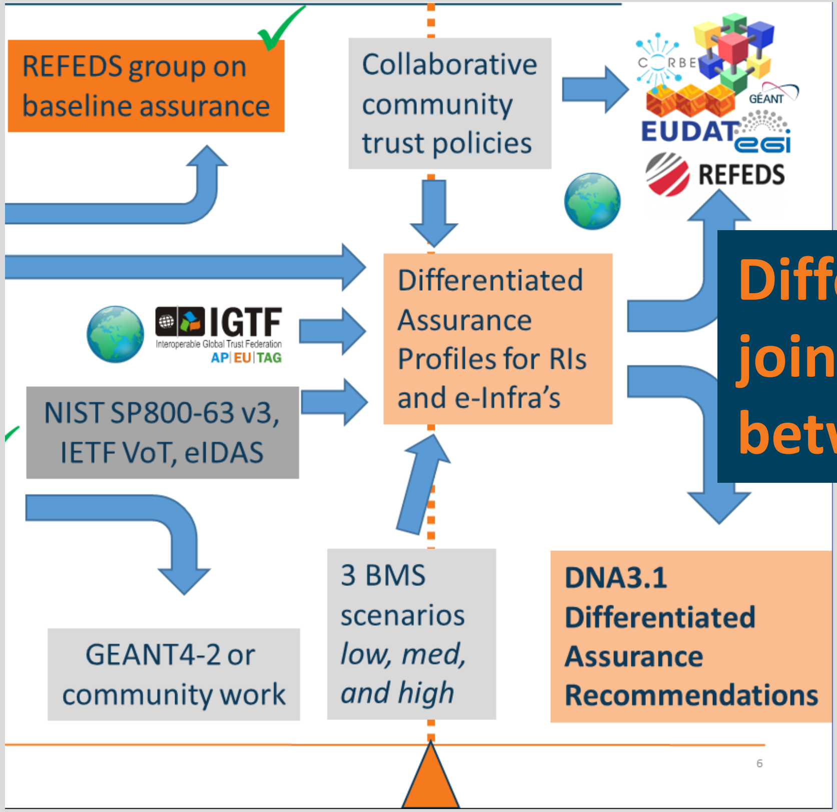
Strategy

to support and extend established and emergent groups

leverage their support base - and 'multiply' the effect of policy work from AARC

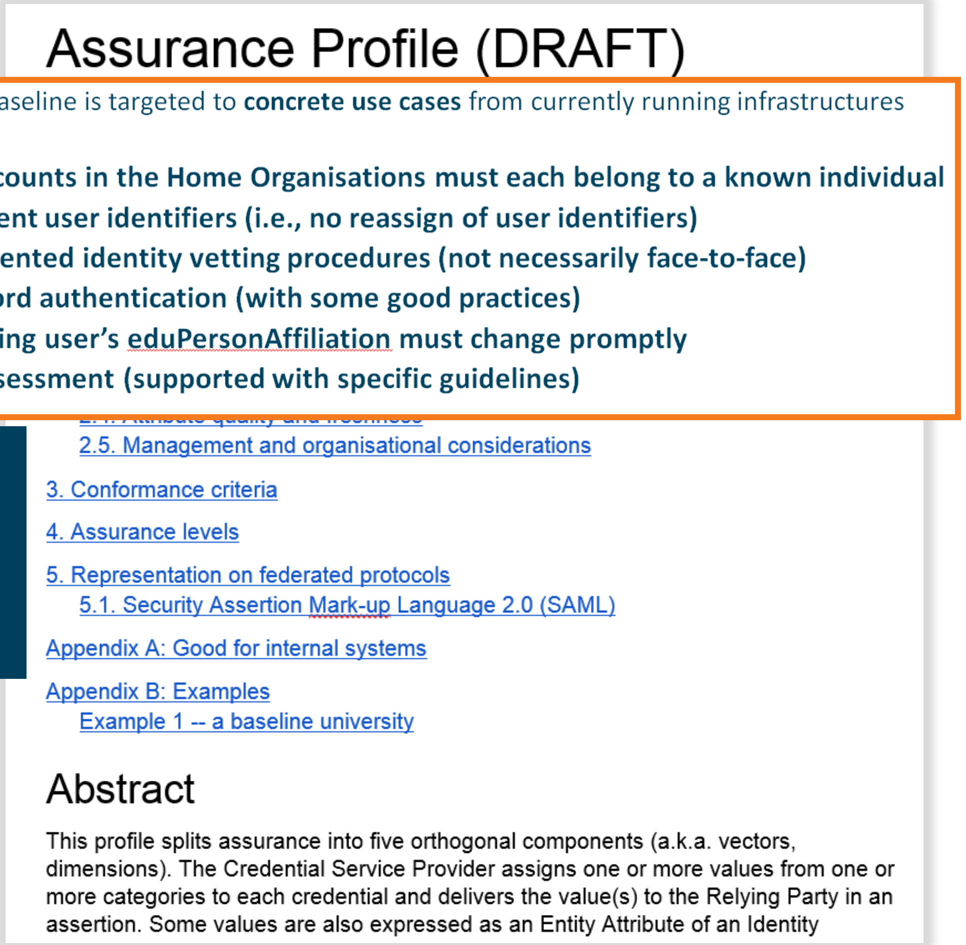
From Baseline to Differentiated Assurance

- REFEDS WG based on capabilities (‘vectors’ mainly for IdPs)
- Grouping of capabilities with our SPs into profiles


REFEDS group on baseline assurance
Collaborative community trust policies
CORBEL
EUDAT
GÉANT
egi
REFEDS
IGTF
Interoperable Global Trust Federation
AP | EU | TAG
Differentiated Assurance Profiles for RIs and e-Infra’s
NIST SP800-63 v3, IETF VoT, eIDAS
GEANT4-2 or community work
3 BMS scenarios *low, med, and high*
DNA3.1 Differentiated Assurance Recommendations
6

Minimum baseline is targeted to **concrete use cases** from currently running infrastructures

1. **The accounts in the Home Organisations must each belong to a known individual**
2. **Persistent user identifiers (i.e., no reassign of user identifiers)**
3. **Documented identity vetting procedures (not necessarily face-to-face)**
4. **Password authentication (with some good practices)**
5. **Departing user’s eduPersonAffiliation must change promptly**
6. **Self-assessment (supported with specific guidelines)**



Assurance Profile (DRAFT)

Abstract

This profile splits assurance into five orthogonal components (a.k.a. vectors, dimensions). The Credential Service Provider assigns one or more values from one or more categories to each credential and delivers the value(s) to the Relying Party in an assertion. Some values are also expressed as an Entity Attribute of an Identity

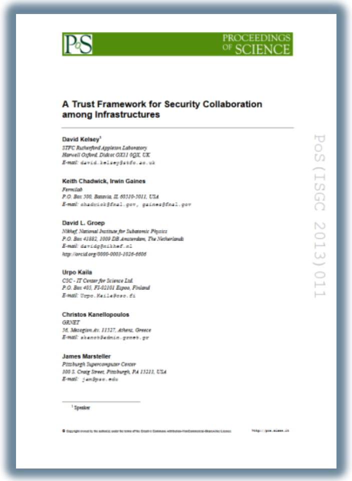
Different profiles and joint alignment of assurance between e-Infras ongoing …

@REFEDS: Assurance Components consultation early 2017 – simple structure
@FIM4R: useful grouping in assurance profiles – see Mikael’s talk

https://docs.google.com/document/d/15v65wJvRwTSQKViep_gGuEvxLl3UJbaOX5o9eLtsyBI

Developing scalable policy models in light of the Blueprint: Snctfi

- ✓ allow proxy operators to assert ‘trust marks’ based on known SP properties
- ✓ Develop framework recommendations for RIs for **coherent policy sets**



PROCEEDINGS OF SCIENCE

A Trust Framework for Security Collaboration among Infrastructures

David Kelsey[1]
STFC Rutherford Appleton Laboratory
Harwell Oxford, Didcot OX11 0QX, UK
E-mail: david.kelsey@stfc.ac.uk

Keith Chadwick, Irwin Gaines
Fermilab
P.O. Box 500, Batavia, IL 60510-5011, USA
E-mail: chadwick@fnal.gov, gaines@fnal.gov

David L. Groep
Nikhef, National Institute for Subatomic Physics
P.O. Box 41882, 1009 DB Amsterdam, The Netherlands
E-mail: davidg@nikhef.nl
http://orcid.org/0000-0003-1026-6606

Urpo Kaila
CSC - IT Center for Science Ltd.
P.O. Box 405, FI-02101 Espoo, Finland
E-mail: Urpo.Kaila@csc.fi

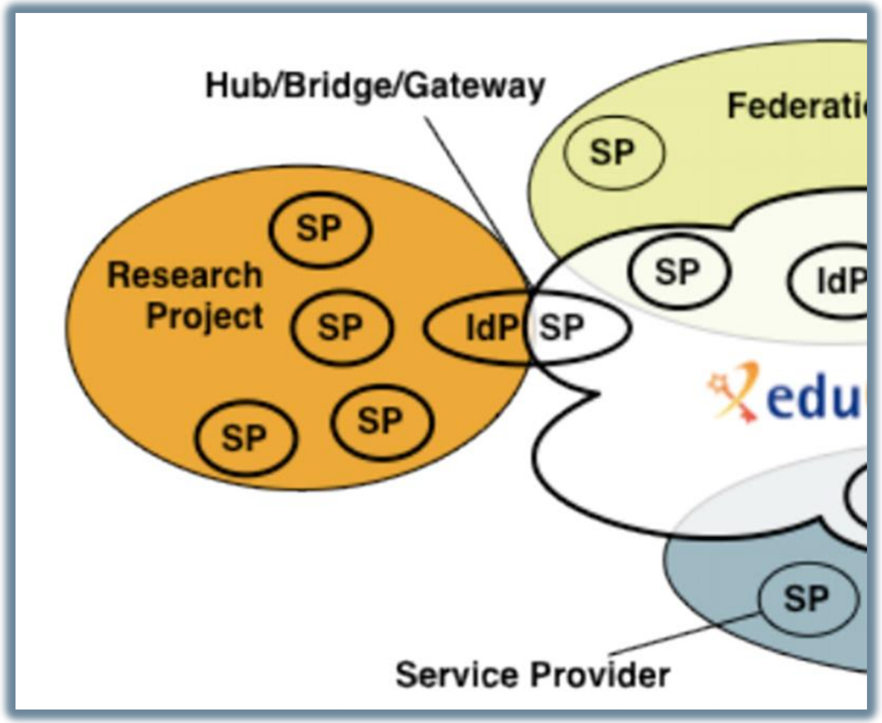
Christos Kanellopoulos
GRNET
56, Mesogion Av. 11527, Athens, Greece
E-mail: skanct@admin.grnet.gr

James Marsteller
Pittsburgh Supercomputer Center
300 S. Craig Street, Pittsburgh, PA 15213, USA
E-mail: jam@psc.edu

[1] Speaker

© Copyright owned by the author(s) under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike Licence. http://pos.sissa.it

PoS(ISGC 2013)011



evaluate with the SP-IdP-Proxies in pilots **based on the Blueprint Architecture**

Collaborate in **WISE, IGTF & FIM4R** to get endorsement

Complementary work:
Accounting Data Exchange
Protection for Infrastructures

Many SPs are alike

Policy frameworks for collective service providers
Shared use of and collaboration on reputation services, together in FIM4R

Graphics inset: Ann Harding, SWITCH

Proxying IdPs to SPs is part of the BPA, with e.g. the RCauth CPS as policy example

Inconsistency as our gravest risk? – towards AARC2

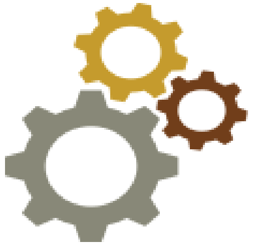
Reflected in updated AARC2 structure

- Operational security capabilities and Incident response in federations – beyond Sirtfi v1
- **Service-centric policies**: traceability & accounting, privacy, gateway operations & proxies
- **e-Researcher-centric policies**: alignment of AUPs and templates, authentication assurance, community attribute management models and provisioning
- Policy Engagement and Coordination: contributes to Community Engagement, provision of policy expertise to the Competence Centre, promotion of best practices globally (WISE, FIM4R, IGTF, REFEDS), easing **end-to-end coordination** across the chain
- Structuring the **exchange of information** amongst SP groups

AARC2 In three bullets

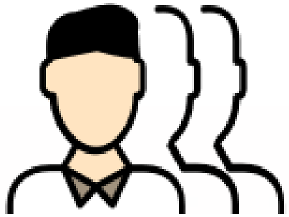
Support Use-driven approach

Enable federated access for a number of selected use-cases that meet data intensive and cross e-Infrastructures requirements



Deploy AARC/AARC2 Results

Support e-Infrastructures to deploy AARC/AARC2 results to enable service delivery across all of them



Continue the Training

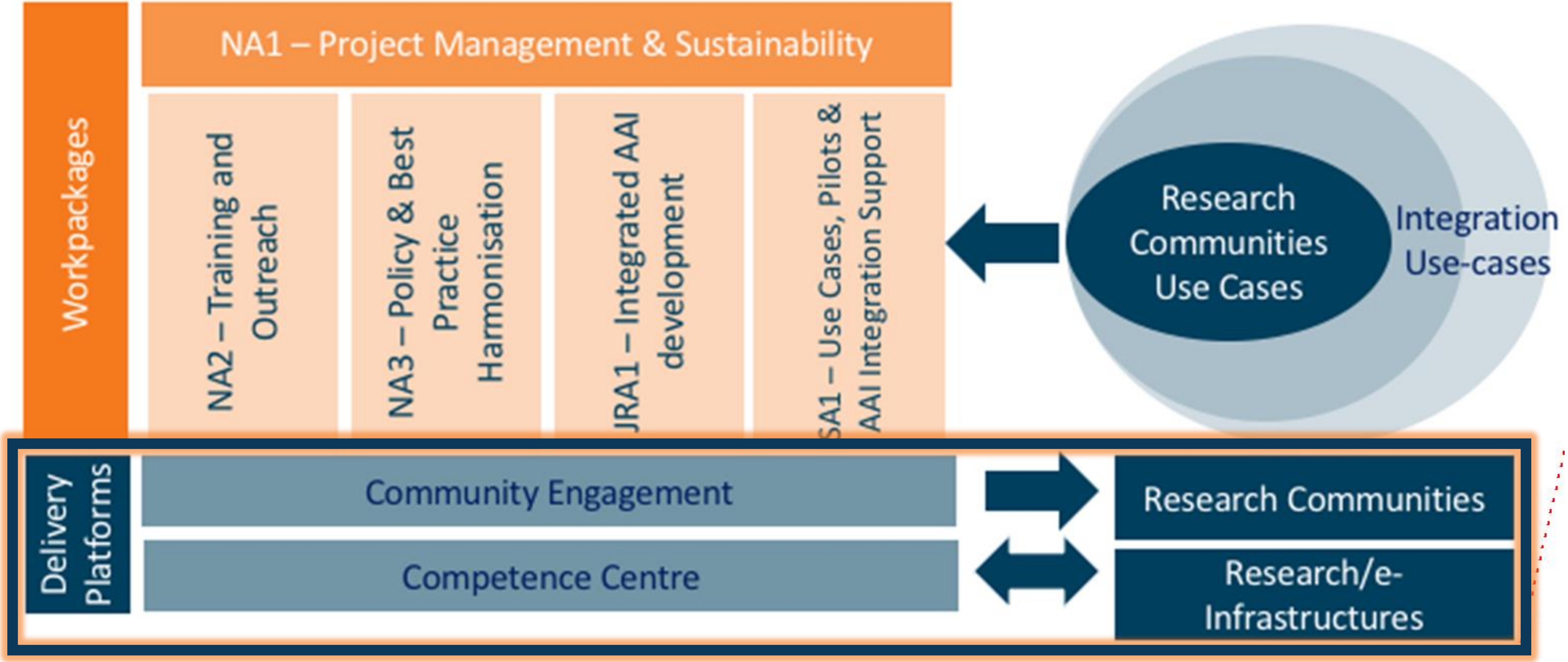
Offer different level of training to enable communities do use the underlying AAIs when building new services

AARC2 Focus on Pilots and eScience Engagement

- 8 Pilots with research communities:
  - CTA, EPOS, EISCAT_3D, LIGO, LifeWatch, WLCG, Biomedical Science Research, HNSciCloud

- Pilots to support interoperability among research & e-Infrastructures

Two new engagement mechanisms


Workpackages
NA1 – Project Management & Sustainability
NA2 – Training and Outreach
NA3 – Policy & Best Practice Harmonisation
JRA1 – Integrated AAI development
SA1 – Use Cases, Pilots & AAI Integration Support
Research Communities Use Cases
Integration Use-cases
Delivery Platforms
Community Engagement
Competence Centre
Research Communities
Research/e-Infrastructures

What AARC can do for you?

AARC/2 support for Research & e-Infrastructure collaborations

- **FIM4R as a community forum for AARC/2 work and pilots**
  including bilateral meetings as needed
- **Create a forum for Infrastructures: the competence centre**
  facilitate the exchange of information of every (AAI, security) sort

- Check the AARC blog for the latest information
  https://aarc-project.eu/news-blog/
- Get in touch: aarc-contacts@lists.geant.org

Thank you

Any Questions?

davidg@nikhef.nl

AARC

http://aarc-project.eu/

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 653965 (AARC).