Authentication and Authorisation for Research and Collaboration

News from the world of Federated Identity Management and AAI

David Kelsey

STFC – UK Research and Innovation

Co-authors: David Groep (Nikhef) and Hannah Short (CERN)

HEPiX Workshop, Madison WI

15 May 2018

Overview

- *The vision*: Researchers should have a single electronic identity that can be used to access all distributed IT resources around the world as required
- For the past 18 years the IGTF X.509 certificates together with VOMS Attribute Certificates have done an excellent job!
- BUT things move on
  - Many researchers find handling certificates too difficult
  - Many future services will be based on other AuthN/AuthZ technologies
  - Would like to use Federated Identities coming from (SAML) Home Institutes and eduGAIN
- In this talk, cover 3 topics (very quickly!)
  - FIM4R (David Kelsey)
  - OIDC Federation for Infrastructures (IGTF) (David Groep)
  - WLCG Authorisation Working Group (Hannah Short)
- Many thanks to my two co-authors
  - Their slides have been modified by me – mistakes are mine!

Authentication and Authorisation for Research and Collaboration

FIM4R - Requirements

Federated Identity Management for Research

David Kelsey
AARC2 Community Engagement/Policy and Best Practice Harmonisation
STFC – UK Research and Innovation

https://fim4r.org

Internet2 Global Summit, San Diego
9 May 2018

What is FIM4R?

- Founded in 2011, FIM4R (Federated Identity Management for Research) is a group of research communities (and some infrastructures)
  - collects requirements on technical architecture, functionality and operational policies
  - These requirements may apply to R&E Federations or to the Research/e-Infrastructures

Research Fields include

- Arts and Humanities
- Astronomy
- Climate Science
- Earth Observation
- European Neutron and Photon Facilities
- Gravitational Wave Astronomy
- High Energy Physics
- Infectious Disease Research
- Ionospheric and Atmospheric Science
- Life Sciences
- Linguistics
- Nuclear Physics
- Virtual Atomic and Molecular Data Centre

FIM4R – Version 1 white paper

FIM4R

- Published a whitepaper in 2012 that guided the direction of identity federation for research *https://fim4r.org/documents/*
- Specified a common vision together with common requirements and recommendations
- Revised (just to specify priorities) in 2013

Federated Identity Management for Research Collaborations

Paper Type: Research paper

Date of this version: 28 August 2013

Abstract

Federated identity management (FIM) is an arrangement that can be made among multiple organisations that lets subscribers use the same identification data to obtain access to the secured resources of all organisations in the group. Identity federation offers economic advantages, as well as convenience, to organisations and their users. For example, multiple institutions can share a single application, with resultant cost savings and consolidation of resources. In order for FIM to be effective, the partners must have a sense of mutual trust.

A number of laboratories including national and regional research organizations are facing the challenge of a deluge of scientific data that needs to be accessed by expanding user bases in dynamic collaborations that cross organisational and national boundaries.

Driven by these needs, representatives from a variety of research communities, including photon/neutron facilities, social science & humanities, high-energy physics, atmospheric science, bioinformatics and fusion energy, have come together to discuss how to address these issues with the objective to define a common policy and trust framework for Identity Management based on existing structures, federations and technologies.

This paper will describe the needs of the research communities, the status of the activities in the FIM domain and highlight specific use cases. The common vision for FIM across these communities will be presented as well the key stages of the roadmap and a set of recommendations intended to ensure its implementation.

Keywords
federated identity management, security, authentication, authorization, collaboration, community

CERN-OPEN-2012-006
28/08/2013

Introduction

Federated identity management (FIM) is an arrangement that can be made among multiple organisations that lets subscribers use the same identification data to obtain access to the secured resources of all organisations in the group. Identity federation offers economic advantages, as well as convenience, to organisations and their users. For example, multiple institutions can share a single application, with resultant cost savings and consolidation of resources. In order for FIM to be effective, the partners must have a sense of mutual trust.

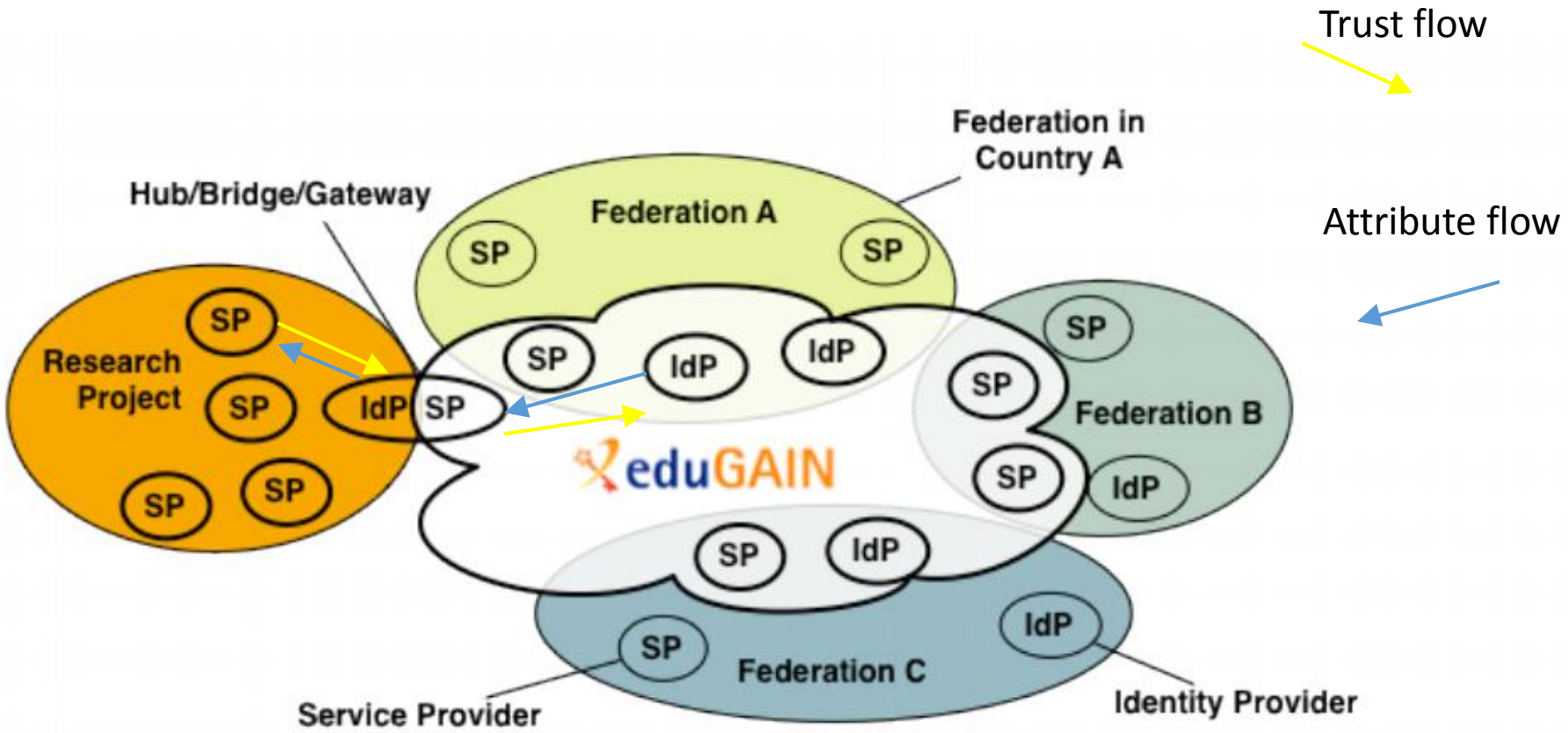
A number of laboratories including national and regional research organisations are facing the challenge of a deluge of scientific data that needs to be accessed by expanding user bases in dynamic collaborations that cross organisational and national boundaries. Many of the users have accounts at several research organisations and will need to use services provided by yet more organisations involved in research collaborations. All these identities and services need to be able work together without the users' being obliged to remember a growing number of accounts and passwords. As the user communities served by these organizations are growing they are also becoming younger and this younger generation has little tolerance for artificial barriers, many being the relics of technology and policies that could, if reasoned, also evolve. This "Facebook" generation [1] has triggered a change in the attitude towards IT tools. One expects to be able to share data, software, results, thoughts and emotions with whom they choose, when they choose. The boundaries between work and social life are less sharp, and it is expected that tools blend into this environment seamlessly. The interaction with commercial services such as the social networks must not imply that the users and research communities relinquish control over access to resources and security policies. The frequency of use will vary between the different users. Some will use these new tools continuously each day while others will log in a few times per year. This implies that operation has to be very intuitive, preferentially in a style known from common commercial devices and applications (PCs, smart phones, tablets etc).

Successes since FIM4R version 1 – but need an update (version 2)

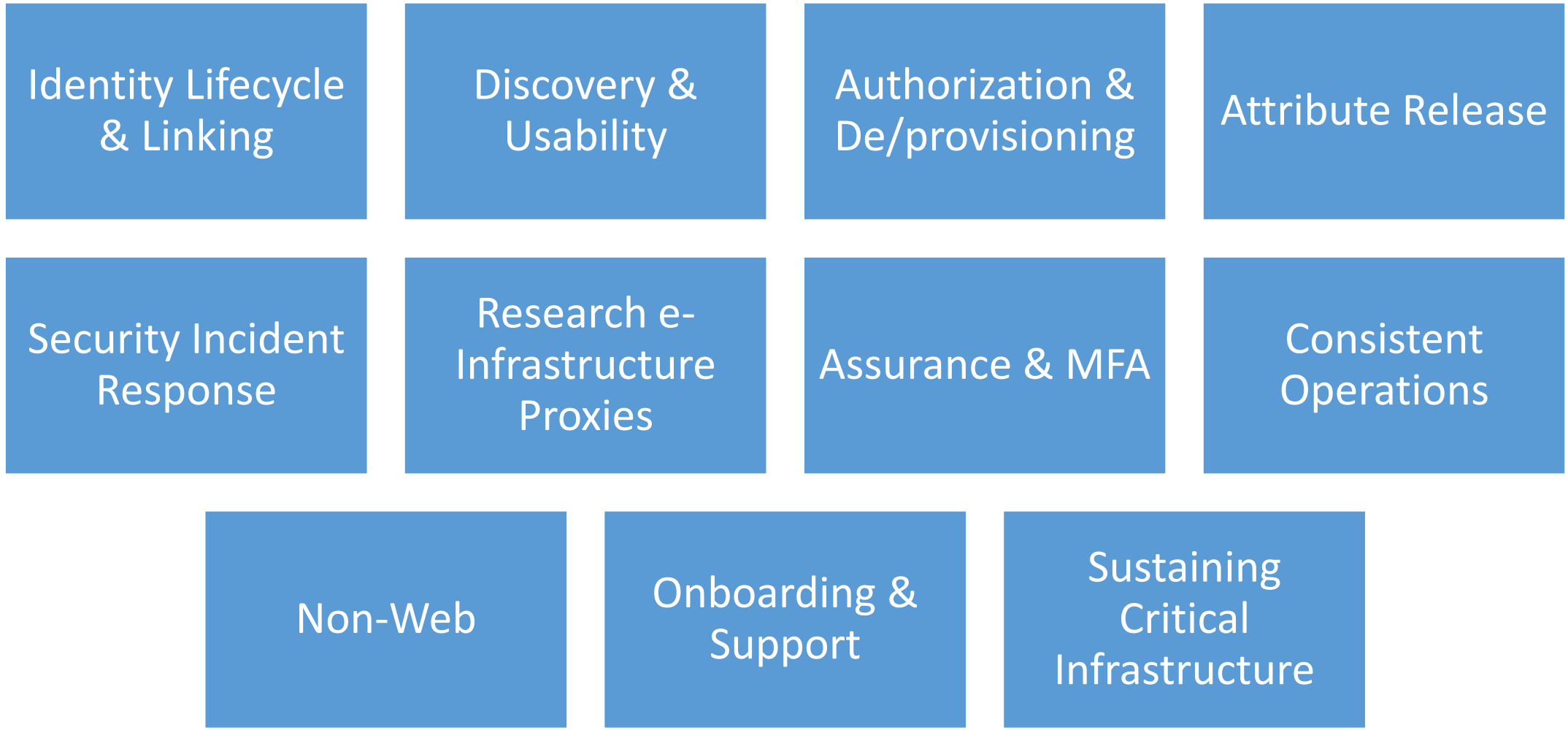
Much has changed since 2012 – AAI now more mature and many successes

- FIM4R 2012 paper was taken seriously
  - E.g. European Commission funding (H2020) for the AARC/AARC2 projects
- eduGAIN evolving slowly towards an operational infrastructure
- Emergence of a “proxy” architecture (The AARC Blue Print Architecture)
- eduGAIN (as an Authentication infrastructure) – Authorisation by Communities
- e-Infrastructures deploying AAI services (EGI, EUDAT, GÉANT, EOSC-hub, …)
  - e.g. for Life Sciences
- Specific successes include: the Sirtfi and Snctfi trust frameworks
- **But still many ongoing issues** – including Data Privacy and EU GDPR
  - Waiting for finalised GEANT Data Protection Code of Conduct V2
  - better data access and privacy expectations need to be balanced
  - E.g. ELIXIR Human Data resources are potentially liable for breaches

AARC Blueprint Architecture incudes an SP/IdP Proxy



FIM4R Version 2 – Frozen draft on 1st March 2018
https://fim4r.org/documents/ (11 groups, 39 requirements)



FIM4R - Next steps

- Complete and publish the version 2 white paper (in the coming weeks)
- This will include high-level Recommendations aimed at various Stakeholders
  - The highest priority/ most important requirements and other recommendations
  - Research Communities, e-Infrastructures, Federation Operators, IDP operators (Universities), Funding Agencies & other Sponsors

Thank you

Any Questions?

David.Kelsey@stfc.ac.uk

https://aarc-project.eu

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 730941 (AARC2).

OIDC Federation for Infrastructures

EUGridPMA 42

Prague, CZ

Nikhef

David Groep

davidg@nikhef.nl

Interoperable Global Trust Federation

IGTF "establishes common policies and guidelines that enable interoperable, global trust relations between providers of e-Infrastructures and cyber-infrastructures, identity providers"

- technology-agnostic assurance profiles (see IANA registry)
- with specific renderings – PKIX, Attribute Authorities, …

How can we help support RI and e-Infrastructure use cases?

- technology bridges: TCS, RCauth.eu, IGTF-eduGAIN bridge, …
- native SAML R&E federation most effective through REFEDS now
- behind the bridges for research & collaboration, OIDC prominence!

OIDC Federation Task Force

The IGTF task force for OIDC Federation will

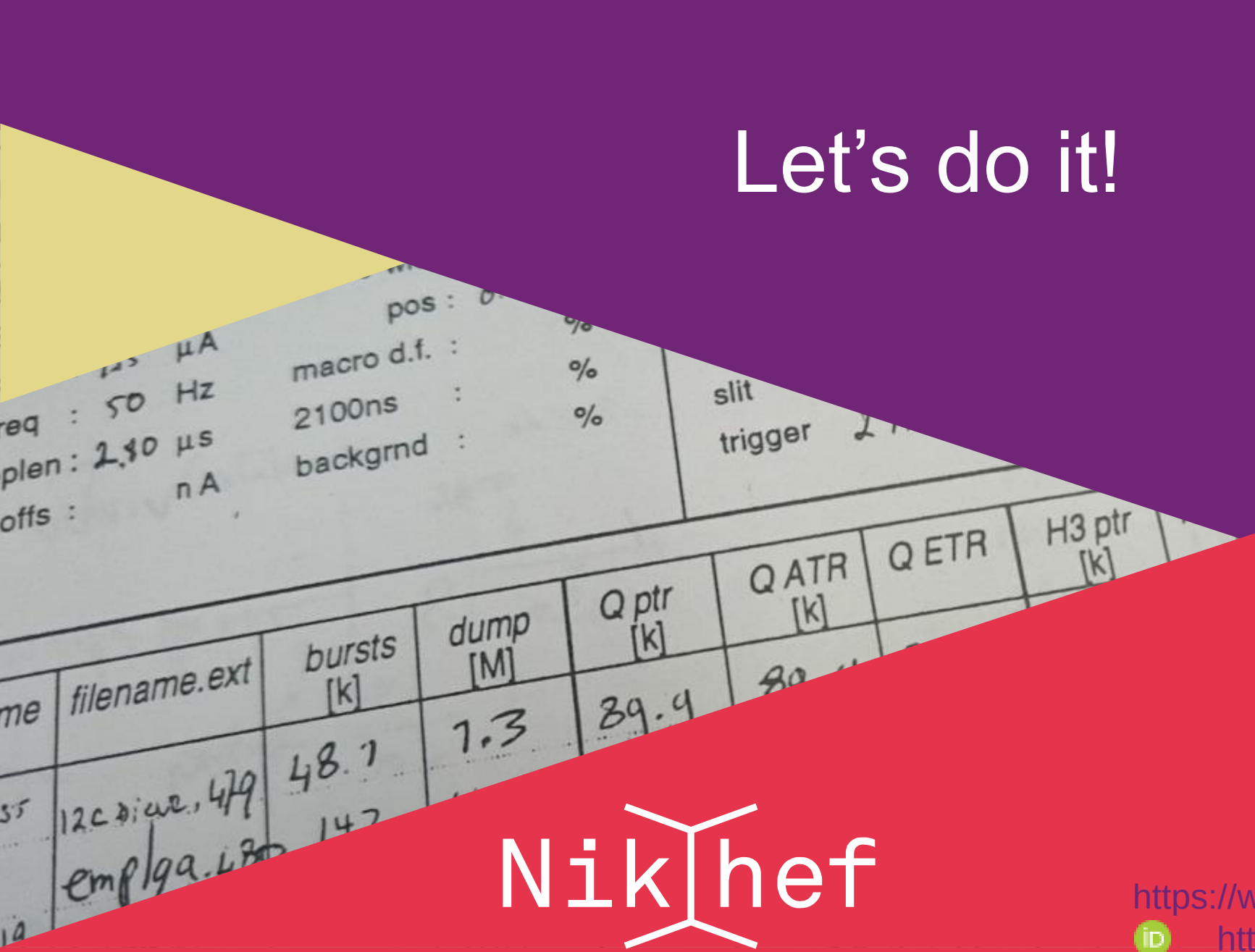
- identify specific objectives
- **scope needs and requirements for R/E infrastructure OIDC Fed**
- verify compatibility of IGTF Assurance Profile framework
  for ‘technology-agnosticity’ with OpenID Providers (proxies) and RPs
- test a OIDCFed scenario
  e.g. starting with use cases: WLCG, RCauth.eu, … ELIXIR, EGI CheckIn
- assess structure and needed meta-data in a ‘trust anchor service’,
  - how to address RPDNC (Name Constraints)
  - links it with (dynamic) client registration
- liaise with OIDC Fed efforts in AARC, GEANT and Roland Hedberg

OIDC Fed ‘policy’

IGTF “RP oriented” OIDC Fed can leverage existing framework

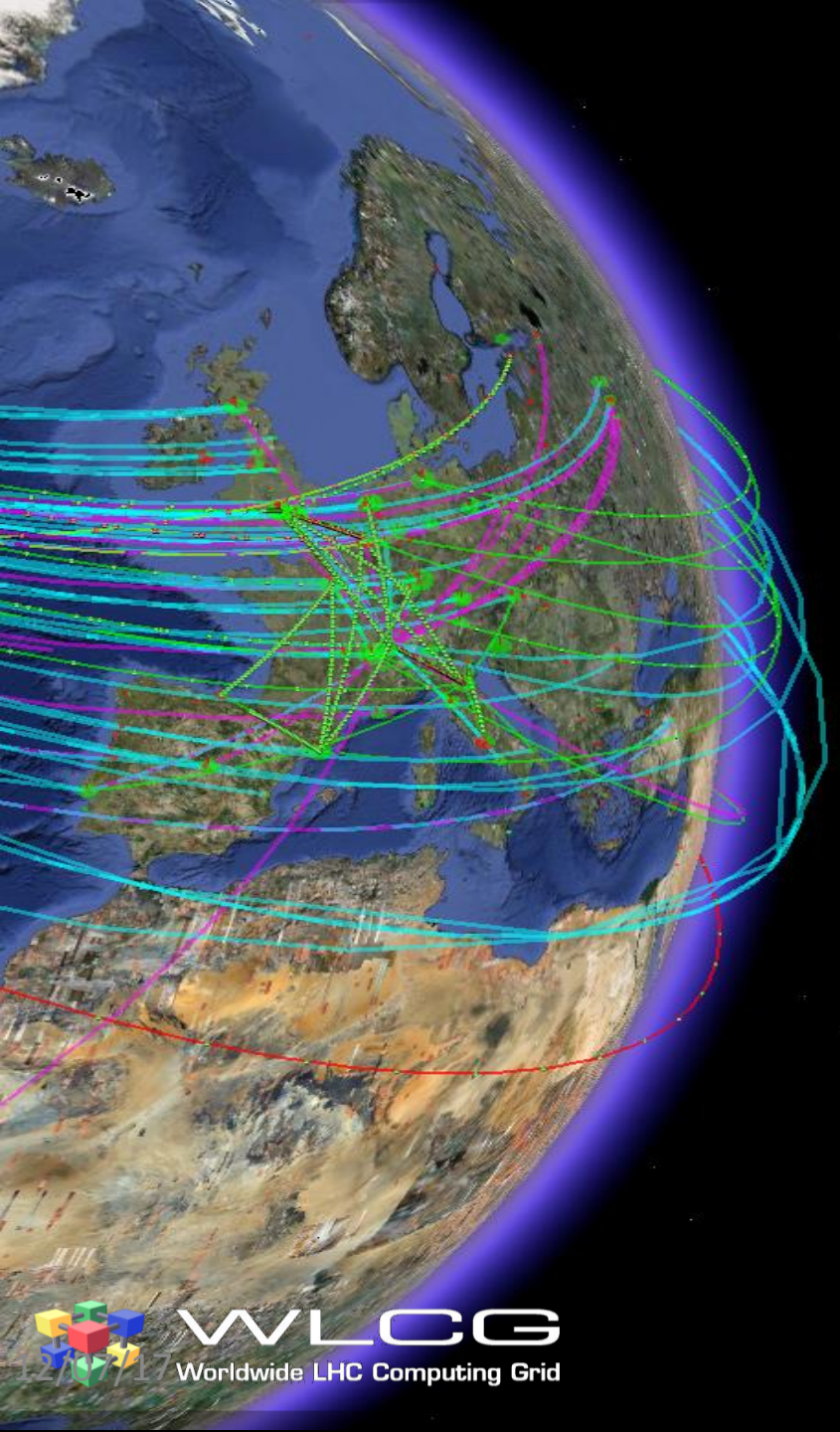
- connect RPs from infrastructures that are IGTF members (EGI, HPCI, OSG, WLCG, GEANT, PRAGMA, PRACE, XSEDE, …) and new IGTF RP members can join of course!
- Accreditation process and membership guidelines in place
- OPs in the federation (RI/EI IdP-SP-Proxies) use IGTF APs and Snctfi framework where needed
- RPs in the federation become the responsibility of their member representatives
- regional (‘national’) RP groups via their existing authority member

Let’s do it!



Nikhef

David Groep
davidg@nikhef.nl
https://www.nikhef.nl/~davidg/presentations/
https://orcid.org/0000-0003-1026-6606



WLCG Authorization Working Group

Hannah Short, CERN

WLCG Worldwide LHC Computing Grid

Motivation for WLCG Authorization WG

- Evolving Identity Landscape
  - User-owned x.509 certificates -> federated identities
  - Current grid middleware does not support federated identities
  - How can we shield users from the complexities of X.509 certificate management ?
  - Token-based authorization widely adopted in commercial services and increasingly by R&E Infrastructures
- Data Protection
  - Tightening of data protection (GDPR) requires fine-grained user level access control, certain provisioning practices may need to be adjusted

Objective: Understand & meet the requirements of a future-looking AuthZ service for WLCG experiments

Authorization WG Objectives

- Objectives have become clear over past 6 months:
  - Gather requirements for a WLCG AAI to provide Membership Management & Token Translation services
    - To facilitate transition to token-based credentials
  - Guide the development of AAI Pilot Projects
    - INDIGO IAM (pilot supported e.g. by EOSC-Pilot & AARC)
    - EGI Check-in & COmanage (pilot supported e.g. by AARC)
  - Define a JSON Web Token (JWT) Schema for Authorization and agree to its use among WLCG Participants
  - Assess the AAI Pilot Projects against our requirements and move towards production deployment on a per-VO basis

What is the AuthZ WG doing?

Winter 2017

- WLCG AAI Requirements Gathering
- Identify Possible Solutions and launch WLCG AAI Pilots

Spring 2018

- Define authorisation token schema for use by infrastructures and VOs
- Monitor WLCG AAI Pilots

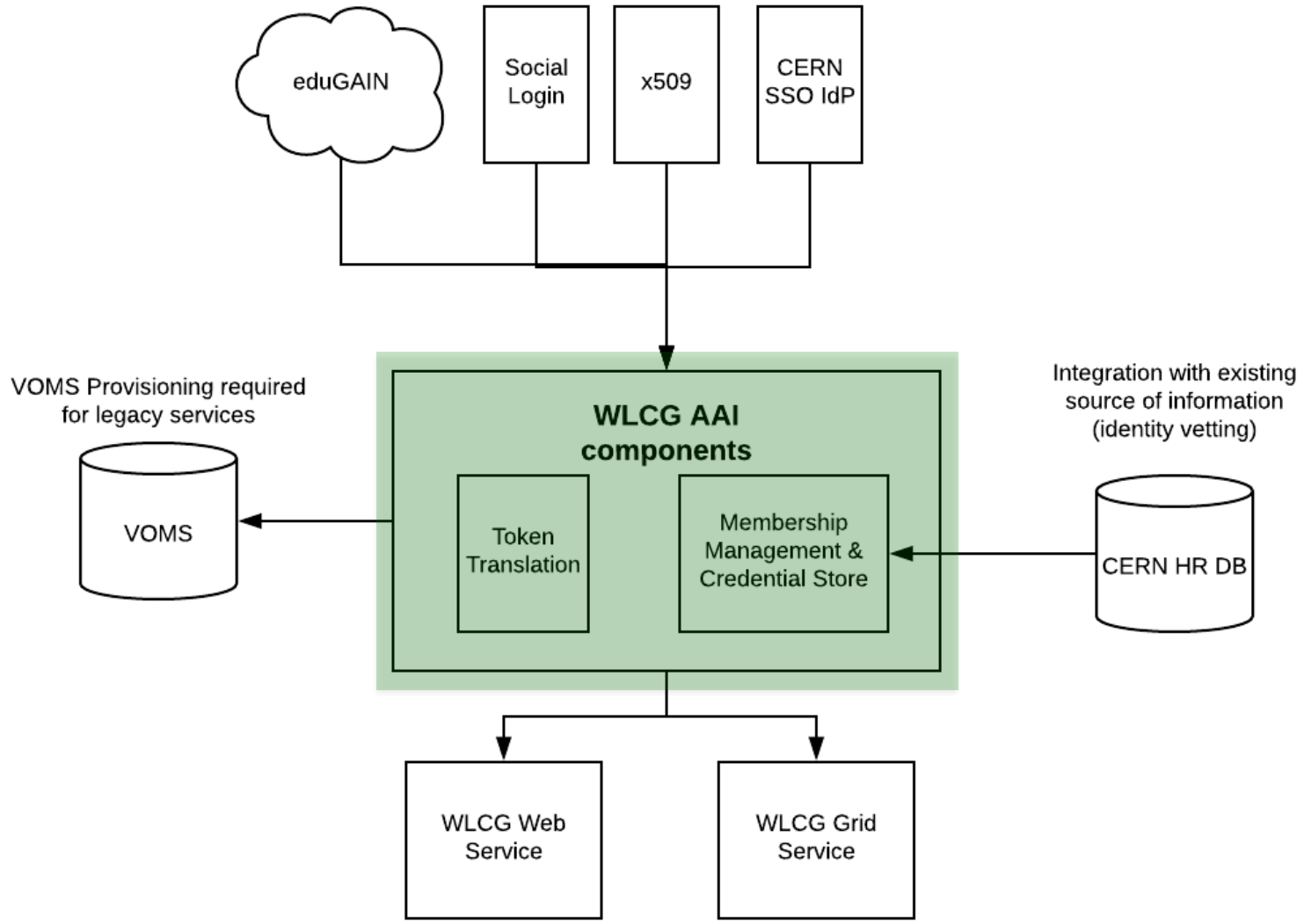
Autumn 2018

- Fully analyse operational impact
- Further liaison with VO management

Winter 2018

- Assess WLCG AAI Pilots

Solution Design

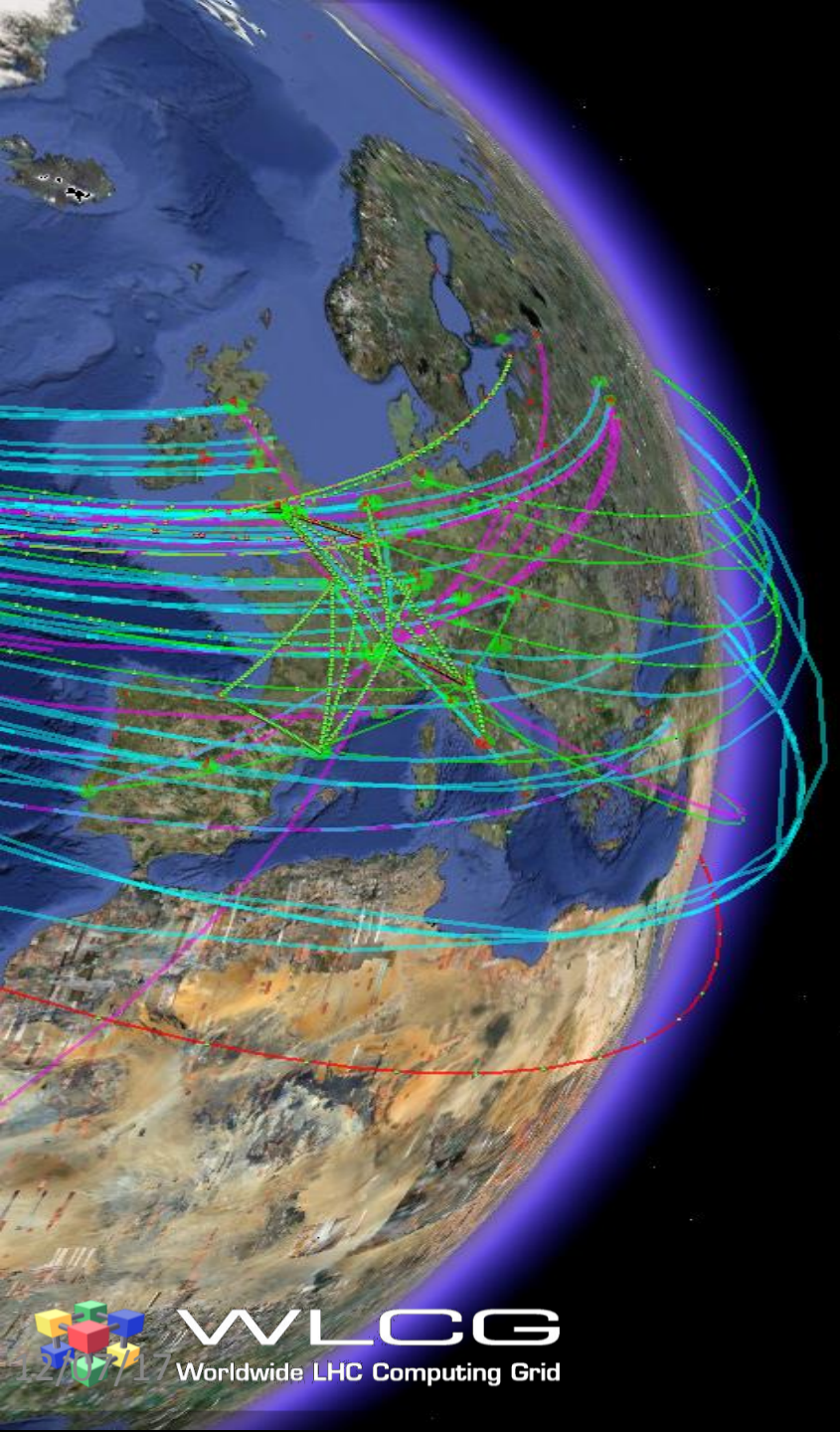


How to participate

Participation in the WG is welcome!

E-group: project-lcg-authz@cern.ch

Twiki: https://twiki.cern.ch/twiki/bin/view/LCG/WLCGAuthorizationWG



Questions?