AARC Authentication and Authorisation for Research and Collaboration

Interoperable AAI: blueprint, technology, policy in an interconnected world

David Groep

AARC Policy and Best Practice Activity Lead

Nikhef

APGridPMA IGTF Spring meeting at ISGC
March 2018
Taipei, TW

In collaboration with and co-supported by EOSC-HUB

Supported by the Dutch National e-Infrastructure coordinated by SURF

Research Communities

- How researchers collaborate varies significantly from community to community
- Ability to access and share resources is crucial for the success of any collaboration
  research -and education- depends on IT Infrastructure
- AAI becomes more diverse: different authentication, authorization, and community management models
- With user-managed, home-institute-, and social IDs

About the tour

- Federated identity and the research infrastructure: proxies in the **AARC Blueprint Architecture**
- Bridging policy across the proxy: **assurance profiles and assessment and operational trust**
- **Translating tokens and credentials**: TCS and RCauth.eu - on uniqueness and ‘trust marks’ in FIM
- Supporting connected services: **scalable trust in OIDC**

Identified common challenges

Communities / e-infrastructures surveyed in AARC

BBMRI
Biobanking and Biomolecular Resources Research Infrastructure
CORBEL
instruct
Integrating Biology
LIGO PROJECT
elixir
EPOS
EUROPEAN PLATE OBSERVING SYSTEM
CLARIN
LifeWatch
INFRAFRONTIER
umbrella
BioVeL
cta
cherenkov telescope array
WLCG
Worldwide LHC Computing Grid
DARIAH-EU
HP
ARIADNE
EISCAT 3D
PRACE
EUDAT
egi
GÉANT
CERN
HELIX NEBULA
THE SCIENCE CLOUD

Homeless users

User friendliness

PII Data Protection

Community based AuthZ

SP friendliness

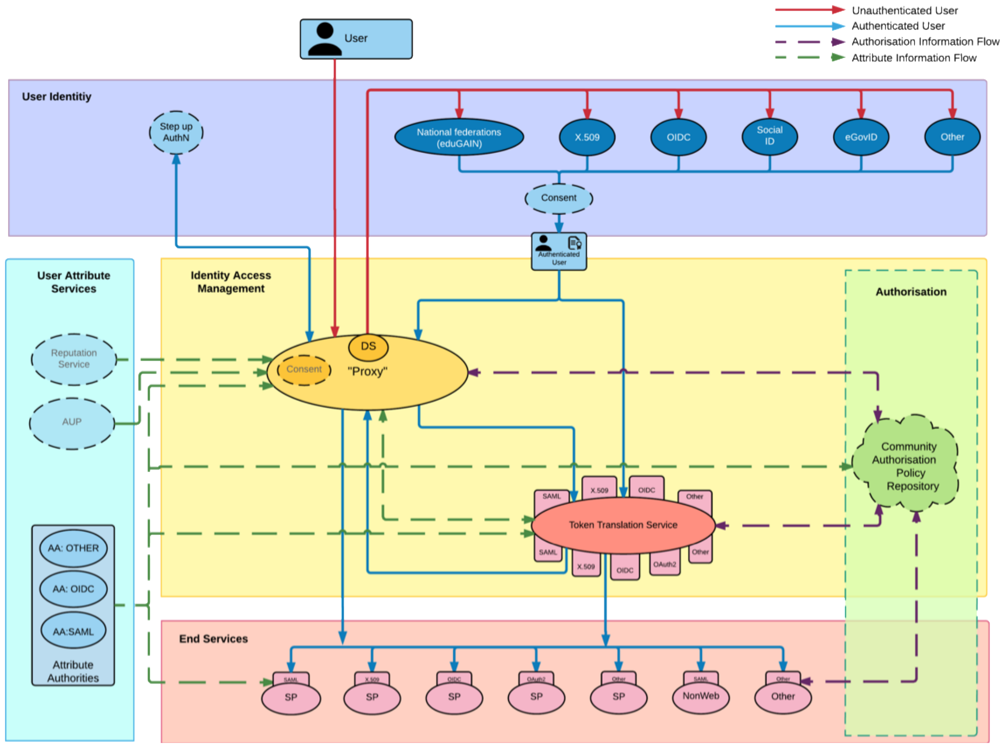
Credential translation

Bridging Communities

Engaging SPs

AARC Blueprint Process

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



Guidelines and supporting documents

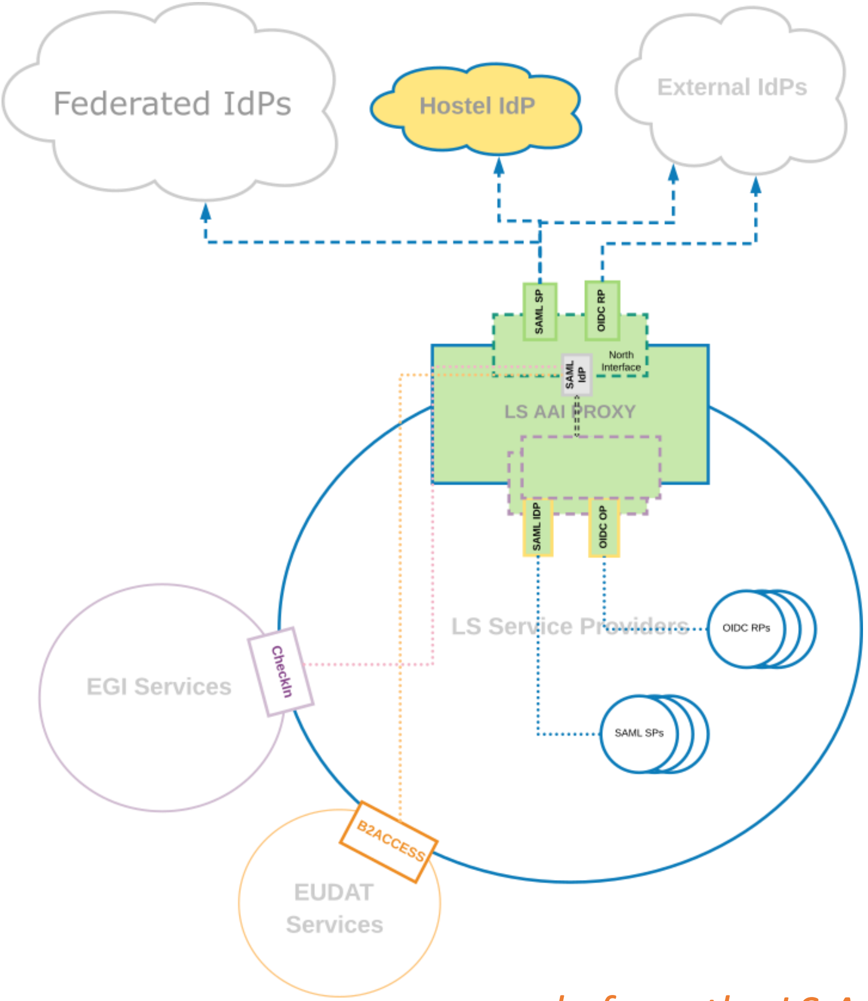
- *reference architecture*
- *conventions and community standards*
- *best policy practices*
- *implementation hints*
- *training for 'FIM' communities*

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

The IdP-SP-Proxy Design Pattern

Challenges addressed by the proxy model

- *attribute release, identity provider heterogeneity, and pervasiveness*
- *attribute aggregation, community based authorization, & persistent unique identifiers*
- *guest users, social, and eGov ID*
- *assurance aggregation and 'step-up'*
- *user friendliness and WAYF*
- *token translation, non-web, and delegation*
- *provider-friendliness and connection options*



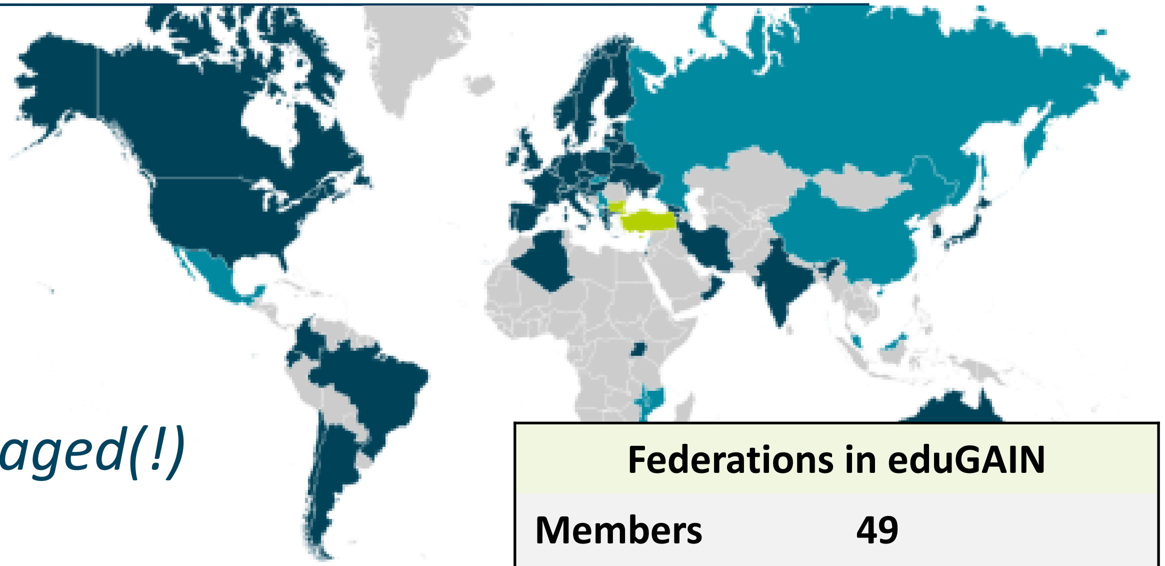
example from the LS AAI

Identity providers – eduGAIN, social, eGov, …

49 members – many different models?

- *architecture (hub-and-spoke vs mesh)*
- *baseline policies present or absent*
- *non-reassigned id and attributes:*
  'by default', optional, or sometimes discouraged(!)
- *tagging of entities and IdPs ('categories'):*
  open, limited, or needs implementation repeatedly
- *constituency: including or excluding e.g. private R&D*
- *paid option or part of* NREN *base services package*
- *support available for organisational IdP software (e.g. ADFS)*

and then there is social ID for (citizen) science, eGov IDs &c



Federations in eduGAIN	
Members	49
Voting-only	6
Candidates	13
Entities in eduGAIN	
All	4538
IdPs	2654
SPs	1888
Standalone AAs	5

data: technical.edugain.org as of 11 March 2018

Harmonisation at the proxy – the technical bits
user identity layer and attribute services

To harmonise incoming attributes, the proxy will need *state*

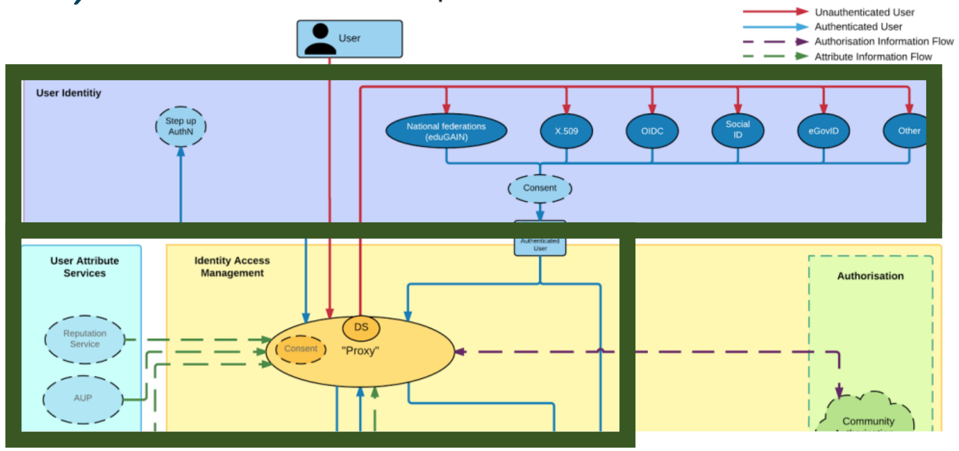
Long term state

- assignment of infrastructure-specific unique identifier
  current recommendation: eduPersonUniqueID or *sub* (type: public)
- heuristics to determine 'unexpected' changes in source IdPs
  even SAML NameID and eduPersonTargetedId may be suspect, and ePPN is not guaranteed
  *– see REFEDS R&S spec **and also LIGO** for algorithm*
- account linking

Ephemeral state

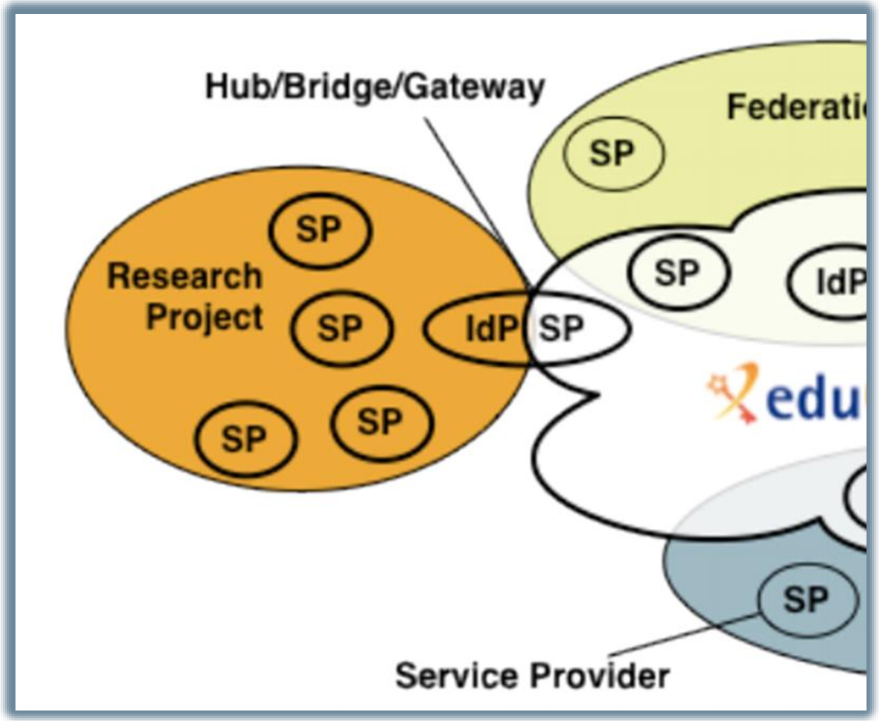
- SSO caching
- optional step-up authentication done for this session
- assurance profile based on linked authentications

AARC Blueprint Architecture



https://aarc-project.eu/guidelines/#architecture

Bridging more than just protocol and technology



https://aarc-project.eu/guidelines/#policy

Baseline capabilities in the IdPs

- Incident response collaboration
- Assurance
- non-reassignment of an identifier
- minimal release of attributes for collaboration

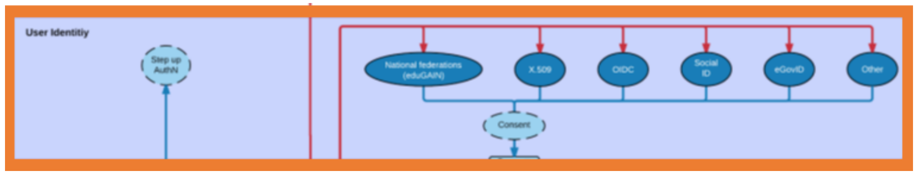
Baseline capabilities in the Infrastructure

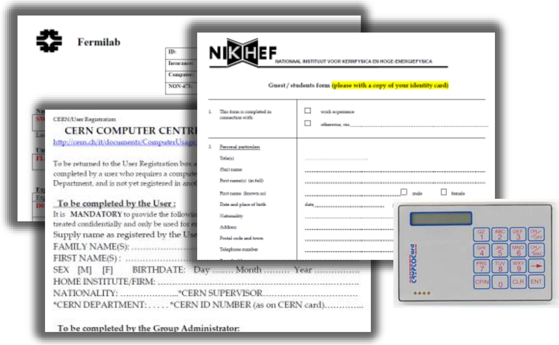
- Protection of Personal Data (“PII”) and Acceptable Use
- Define purpose and scope of attribute use
- User and community management
- Risk assessment and assurance needs

Graphics inset: Ann Harding and Lukas Hammerle, GEANT and SWITCH

Assurance: from federation to infrastructure

Trusting the User’s Authentication




Fermilab
ID:
Insurance:
Computer:
NON-473:
NIKHEF
NATIONAAL INSTITUUT VOOR KERNFYSICA EN HOGE-ENERGIEFYSICA
CRYPTOCard
QZ 1
ABC 2
DEF 3
ON/OFF
GHI 4
JKL 5
MNO 6
CH/MAC
PRS 7
TUV 8
WXY 9
CPIN
0
CLR
ENT

Guest / students form (please with a copy of your identity card)

1. This form is completed in connection with:
□ work experience
□ otherwise, viz. ……

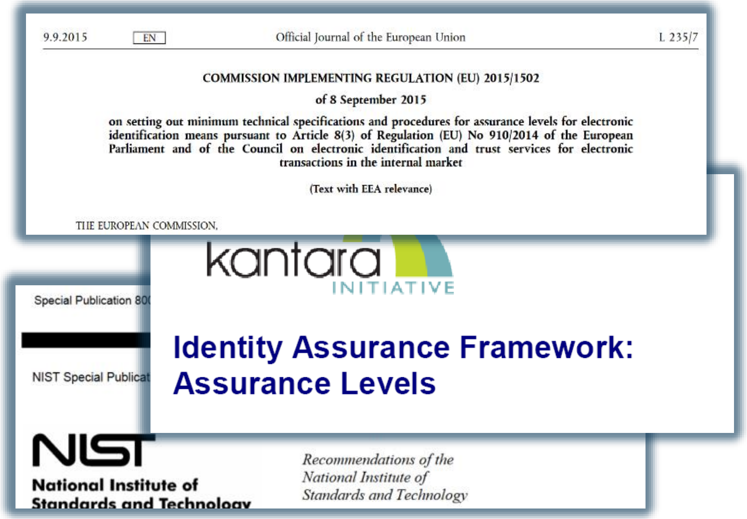
2. Personal particulars
Title(s)
(Sur) name
First name(s) (in full)
First name (known as) □ male □ female
Date and place of birth date……
Nationality
Address
Postal code and town
Telephone number

CERN/User Registration
CERN COMPUTER CENTR
http://cern.ch/it/documents/ComputerUsage

To be returned to the User Registration box a
completed by a user who requires a compute
Department, and is not yet registered in ano

To be completed by the User :
It is MANDATORY to provide the followin
treated confidentially and only be used for e
Supply name as registered by the Use
FAMILY NAME(S): ……
FIRST NAME(S) : ……
SEX [M] [F] BIRTHDATE: Day …… Month …… Year ……
HOME INSTITUTE/FIRM: ……
NATIONALITY: ……*CERN SUPERVISOR……
*CERN DEPARTMENT: . . . . . *CERN ID NUMBER (as on CERN card)……

To be completed by the Group Administrator:



9.9.2015 EN Official Journal of the European Union L 235/7

COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502

of 8 September 2015

on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

kantara INITIATIVE

Identity Assurance Framework: Assurance Levels

Special Publication 800

NIST Special Publicat

NIST
National Institute of Standards and Technology

Recommendations of the National Institute of Standards and Technology

Many layered models (3-4 layers)

but: specific levels don’t match needs of Research- and e-Infrastructures:

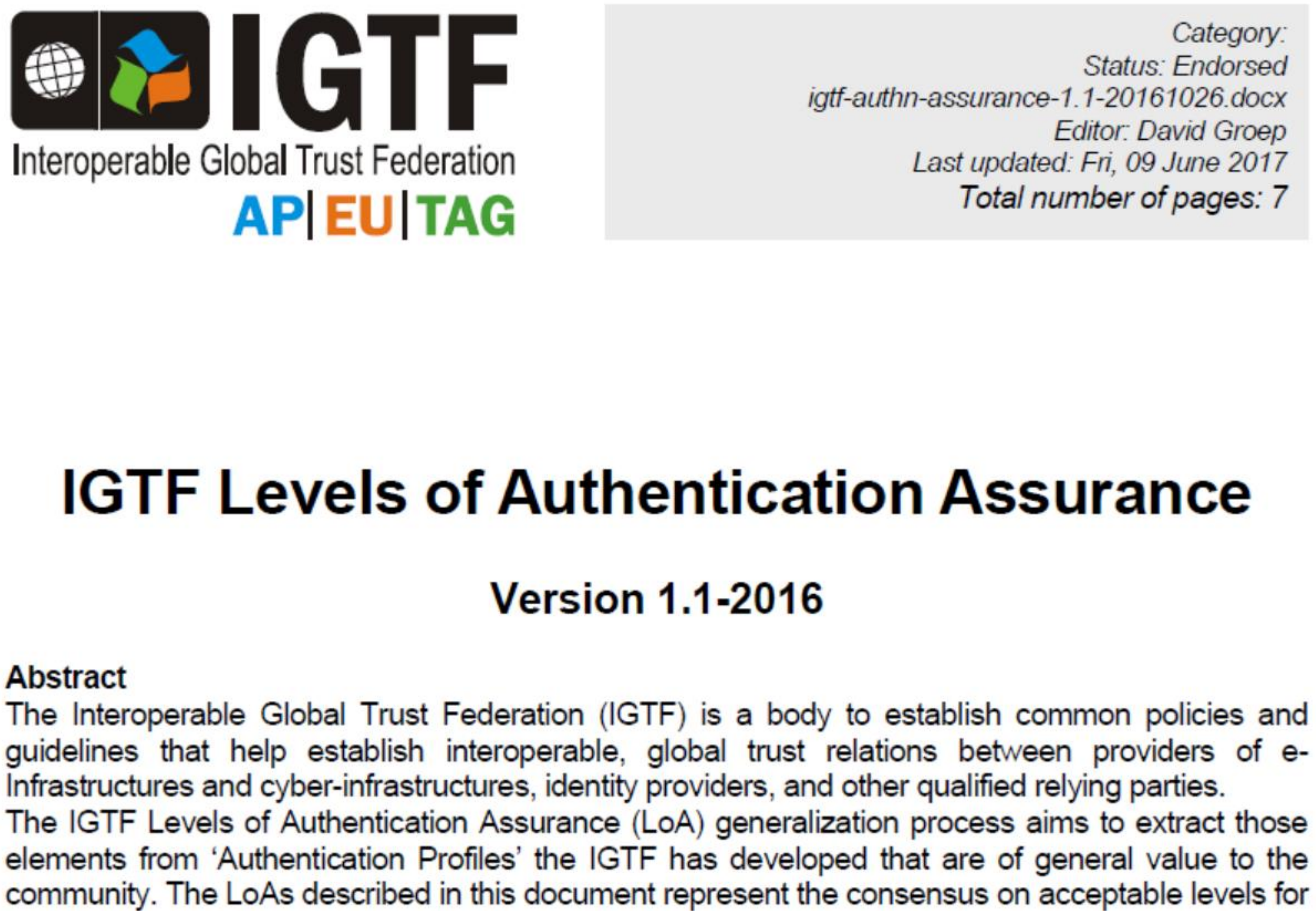
- Specific combination ‘authenticator’ and ‘vetting’ assurance doesn’t match research risk profiles
- Disregards existing trust model between federated R&E organisations
- Cannot accommodate distributed responsibilities

As a result, in R&E federation there was in practice hardly any documented and agreed assurance level

Beyond uncontrolled identifiers:

***baseline* assurance for research use cases**

The need for guidance



IGTF
Interoperable Global Trust Federation
AP | EU | TAG

Category:
Status: Endorsed
igtf-authn-assurance-1.1-20161026.docx
Editor: David Groep
Last updated: Fri, 09 June 2017
Total number of pages: 7

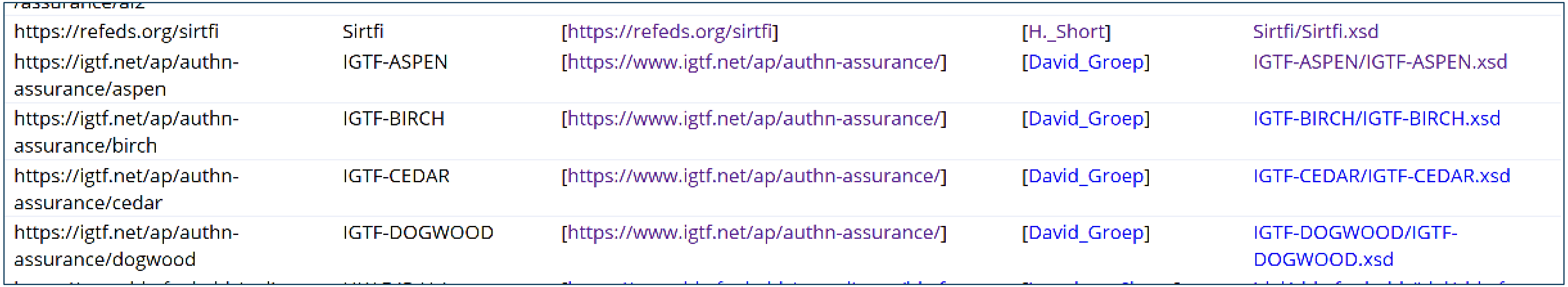
IGTF Levels of Authentication Assurance

Version 1.1-2016

Abstract
The Interoperable Global Trust Federation (IGTF) is a body to establish common policies and guidelines that help establish interoperable, global trust relations between providers of e-Infrastructures and cyber-infrastructures, identity providers, and other qualified relying parties.
The IGTF Levels of Authentication Assurance (LoA) generalization process aims to extract those elements from 'Authentication Profiles' the IGTF has developed that are of general value to the community. The LoAs described in this document represent the consensus on acceptable levels for

IGTF Assurance Levels: ASPEN to DOGWOOD

specifically targeted at the risk profile of the e-Infrastructures



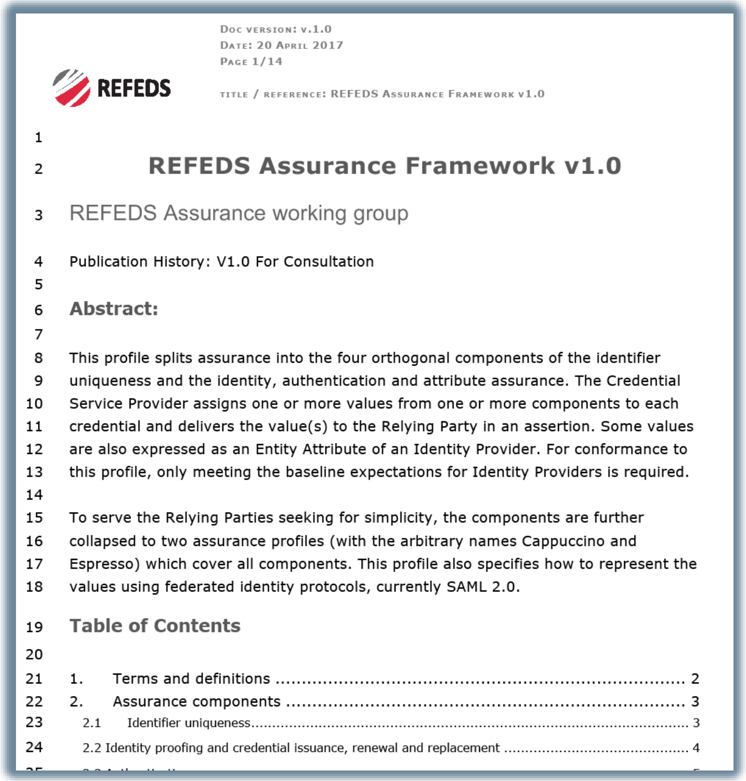
/assurance/al2				
https://refeds.org/sirtfi	Sirtfi	[https://refeds.org/sirtfi]	[H._Short]	Sirtfi/Sirtfi.xsd
https://igtf.net/ap/authn-assurance/aspen	IGTF-ASPEN	[https://www.igtf.net/ap/authn-assurance/]	[David_Groep]	IGTF-ASPEN/IGTF-ASPEN.xsd
https://igtf.net/ap/authn-assurance/birch	IGTF-BIRCH	[https://www.igtf.net/ap/authn-assurance/]	[David_Groep]	IGTF-BIRCH/IGTF-BIRCH.xsd
https://igtf.net/ap/authn-assurance/cedar	IGTF-CEDAR	[https://www.igtf.net/ap/authn-assurance/]	[David_Groep]	IGTF-CEDAR/IGTF-CEDAR.xsd
https://igtf.net/ap/authn-assurance/dogwood	IGTF-DOGWOOD	[https://www.igtf.net/ap/authn-assurance/]	[David_Groep]	IGTF-DOGWOOD/IGTF-DOGWOOD.xsd

https://www.iana.org/assignments/loa-profiles/

Gaining global federation adoption: REFEDS Assurance Framework

https://wiki.refeds.org/display/GROUPS/Assurance+Working+Group

- open, international forum for R&E FIM federations (and a few IdPs)
- has links to identity federations –
  adoption needs IdP to act and federations to communicate
- add new eduGAIN *metadata* and new *attributes* for IdPs
- implementation guidance in normative form helps



Doc version: v.1.0
Date: 20 April 2017
Page 1/14

REFEDS

title / reference: REFEDS Assurance Framework v1.0

REFEDS Assurance Framework v1.0

REFEDS Assurance working group

Publication History: V1.0 For Consultation

Abstract:

This profile splits assurance into the four orthogonal components of the identifier uniqueness and the identity, authentication and attribute assurance. The Credential Service Provider assigns one or more values from one or more components 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 Provider. For conformance to this profile, only meeting the baseline expectations for Identity Providers is required.

To serve the Relying Parties seeking for simplicity, the components are further collapsed to two assurance profiles (with the arbitrary names Cappuccino and Espresso) which cover all components. This profile also specifies how to represent the values using federated identity protocols, currently SAML 2.0.

Table of Contents

Focus on federation and identity provider feasibility

- leveraging REFEDS single* and multi-factor authentication specs
- *component-based* approach allows much flexibility for IdPs to express what they can do

… **but** - *by account linking or Infrastructure specification* - **assurance profiles can be more powerful**

Assurance between Infrastructure AAI Proxies

Assurance derived from several sources

- R&E federation IdPs
- linked (social) IDs
- user-managed credentials
- community registry processes

-> effective assurance level

Prevent *recomputation* of assurance when crossing infrastructures, or
when connecting to pre-arranges groupings of services (‘infrastructure services’)

- share common use cases and their risk assessment, so *assurance profiles* can take precedence
- ease flow of information *between* infrastructures, where more detail is often superfluous
- *augment* the basic REFEDS RAF profiles with infrastructure-specific profiles

Five Profiles: two imported from REFEDS RAF, two from IGTF, one new

Name	REFEDS RAF Assurance Profile Cappuccino

Name	REFEDS RAF Assurance Profile Espresso

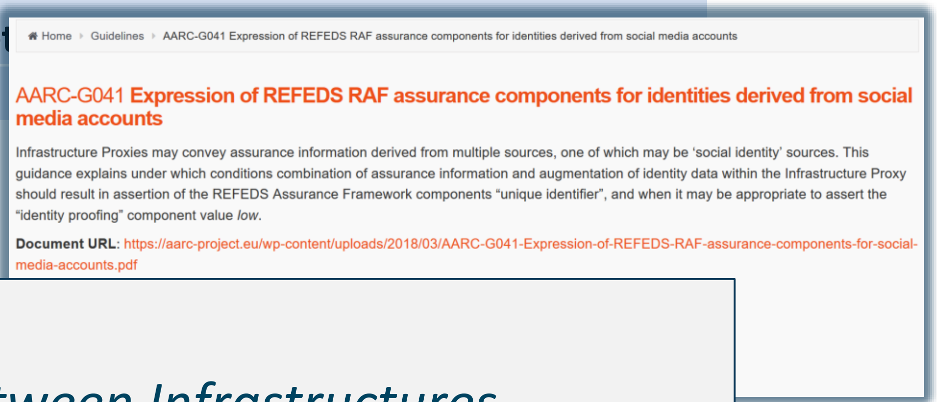
Name	IGTF BIRCH

Name	IGTF DOGWOOD

Name	AARC Assam
SAML Identifier	https://aarc-project.eu/policy/authn-assurance/assam
Other identifier(s)	AARC-Assam
Description	Identity substantially derived from social media or self-signup identity providers (outside the R&E community) on which no further policy controls or qualities are … e substantially derived from upstream … rastructure. **The Infrastructure ensures** … riet

this is a challenging profile, since many of its qualities are outside the control of the Infrastructure Proxy

See AARC-G041
for considerations on "ID/unique" compliance



Home
Guidelines
AARC-G041 Expression of REFEDS RAF assurance components for identities derived from social media accounts

AARC-G041 **Expression of REFEDS RAF assurance components for identities derived from social media accounts**

Infrastructure Proxies may convey assurance information derived from multiple sources, one of which may be 'social identity' sources. This guidance explains under which conditions combination of assurance information and augmentation of identity data within the Infrastructure Proxy should result in assertion of the REFEDS Assurance Framework components "unique identifier", and when it may be appropriate to assert the "identity proofing" component value *low*.

Document URL: https://aarc-project.eu/wp-content/uploads/2018/03/AARC-G041-Expression-of-REFEDS-RAF-assurance-components-for-social-media-accounts.pdf

AARC-G021

Exchange of specific assurance information between Infrastructures

https://aarc-project.eu/guidelines/aarc-g021/ and https://doi.org/10.5281/zenodo.1173558

Combined assurance: EGI example

EGI – by design - supports loose and flexible user collaboration

- 300+ communities
- Many established ‘bottom-up’ with fairly light-weight processes
- Membership management policy* is deliberately light-weight
- Most VO managers rely on naming in credentials to enroll colleagues

Only a few VOs are ‘special’

- LHC VOs: enrolment is based on the users’ entry in a special (CERN-managed) HR database, based on a separate face-to-face vetting process and eligibility checks, including government photo ID + institutional attestations
- Only properly registered and active people can be listed in VOMS

Developing an assessment framework

SPG:Drafts:Assessment Community IDvetting adequacy

Authentication and identification is considered adequate, for each User authorised to access Services, if the combined assurance level provided by the end-user credential issuing authority, and either the e-Infrastructure registration service and/or the VO registration service, meets or exceeds the requirements of the approved IGTF authentication assurance profiles [AAP].

The Community or e-Infrastructure wishing to prove the adequacy of its identity vetting, in order to use its members' credentials in conjunction with the IGTF Assurance Profile DOGWOOD, must submit a request for assessment by the EGI Security Policy Group to EGI operations.

The request shall include the following information:

- a statement of their compliance with the Community Membership Management Policy
- a statement of their compliance with the Community Operations Security Policy
- a documented description of the membership life cycle process and practices meeting the requirements of the IGTF BIRCH, CEDAR (or ASPEN) assurance level, in which
    - the *credential* of the user is the membership registration data and community-issued assertions
    - the *Issuing Authority* is the collection of membership management and assertion-issuing systems and services
    - the *credential life time* corresponds to the renewal periods as defined in the Community Membership Management Policy
- a description of the method of binding between the membership information and the DOGWOOD user credential

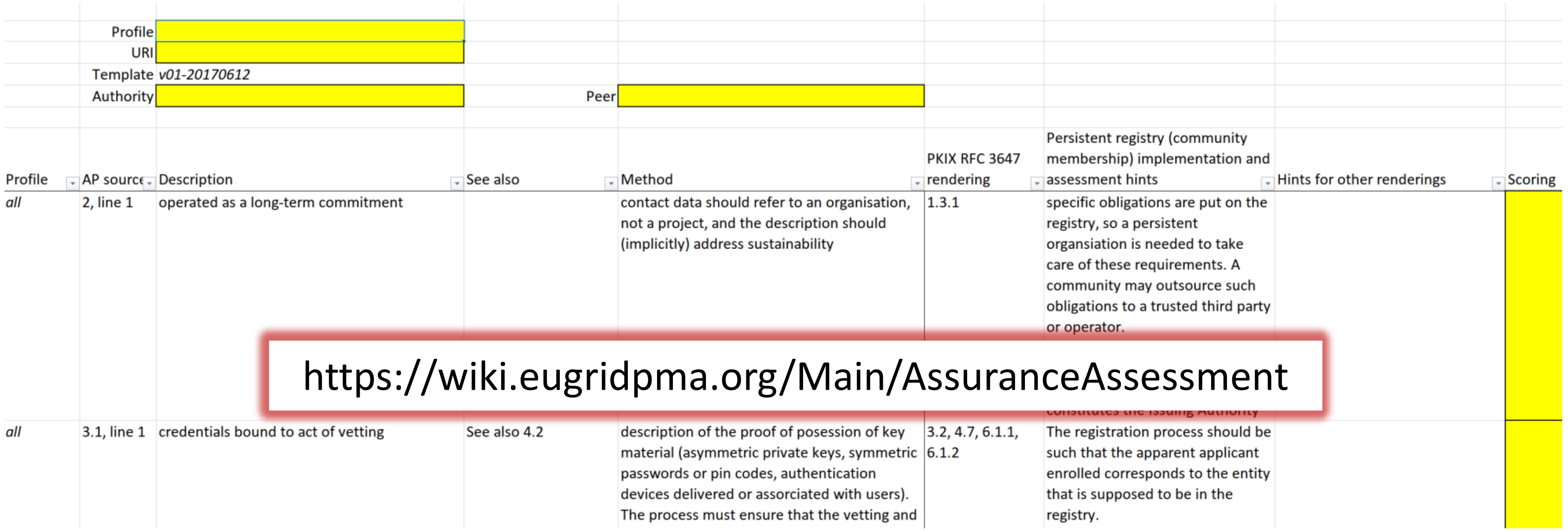
Based on this information, the EGI SPG shall advise the EGI Operations Management Board with respect to suitability of the Community or e-Infrastructure for such combined adequacy in accordance with the Policy on Acceptable Authentication Assurance.

The SPG may make available an evaluation matrix. Applicant communities are welcome to use the assurance evaluation matrix to prepare the requisite documents, bearing in mind the evaluation *Method* and the *Persistent registry (community membership) implementation and assessment hints*. The most relevant community assurance profiles for the joint adequacy purpose are BIRCH and CEDAR. Registries and membership services at ASPEN level are strongly discouraged. The credential (registration) life time of 11 days necessitates re-registering members with this frequency, and re-validating their eligibility. This model is likely to both confuse and upset members.

https://wiki.egi.eu/wiki/SPG:Drafts:Assessment_Community_IDvetting_adequacy

Assessment Matrix

- Mapping for PKIX/RFC3647 is trivial
- How to apply out BIRCH/CEDAR guidance to community registries?



Profile				
URI				
Template	*v01-20170612*			
Authority			Peer	

Profile	AP source	Description	See also	Method	PKIX RFC 3647 rendering	Persistent registry (community membership) implementation and assessment hints	Hints for other renderings	Scoring
all	2, line 1	operated as a long-term commitment		contact data should refer to an organisation, not a project, and the description should (implicitly) address sustainability	1.3.1	specific obligations are put on the registry, so a persistent organsiation is needed to take care of these requirements. A community may outsource such obligations to a trusted third party or operator. constitutes the issuing Authority		
all	3.1, line 1	credentials bound to act of vetting	See also 4.2	description of the proof of posession of key material (asymmetric private keys, symmetric passwords or pin codes, authentication devices delivered or associated with users). The process must ensure that the vetting and	3.2, 4.7, 6.1.1, 6.1.2	The registration process should be such that the apparent applicant enrolled corresponds to the entity that is supposed to be in the registry.		

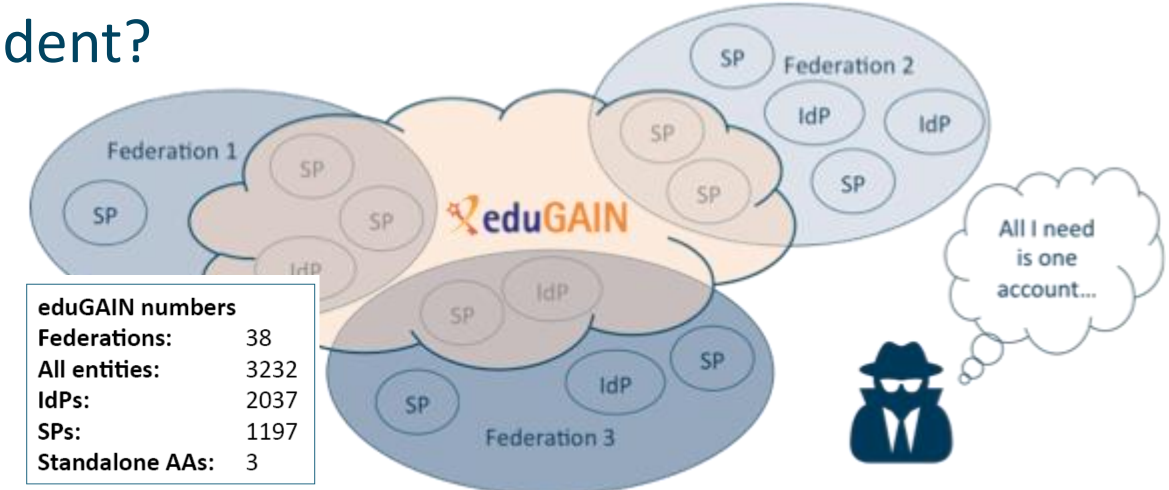
https://wiki.eugridpma.org/Main/AssuranceAssessment

- Relevant for COmanage & VOMS communities, and potentially much wider

Trusted Operational Security and Incident Response

Security Incident Response in the Federated World

- How could we determine the scale of the incident?
  - Do useful logs exist?
  - Could logs be shared?
- Who should take responsibility for resolving the incident?
- How could we alert the identity providers and service providers involved?



eduGAIN numbers	
Federations:	38
All entities:	3232
IdPs:	2037
SPs:	1197
Standalone AAs:	3

Data valid as of May 2016

- Could we ensure that information is shared confidentially, and reputations protected?

Security Incident Response Trust Framework for Federated Identity

Sirtfi – *based on Security for Collaborating Infrastructures (SCI) & FIM4R Recommendations*

A Security Incident Response Trust Framework – Sirtfi summary

Operational Security

- Require that a security incident response capability exists with sufficient authority to mitigate, contain the spread of, and remediate the effects of an incident.

Incident Response

- Assure confidentiality of information exchanged
- Identify trusted contacts
- Guarantee a response during collaboration

Traceability

- Improve the usefulness of logs
- Ensure logs are kept in accordance with policy

Participant Responsibilities

- Confirm that end users are aware of an appropriate AUP

Sirtfi adoption by authentication providers and services

IAM Online Europe

IAM Online Europe webinars are broug

51:17

iamonlineEU 001 Sirtfi

IamOnline

38 views • 4 days ago

https://refeds.org/SIRTFI

REFEDS > SIRTFI

Response Trust Framework for Federated Identity (Sirtfi) aims to enable the coordination of incident response nisations. This assurance framework comprises a list of assertions which an organisation can attest in order ompliant. Visit our Wiki to discover how your organisation can prepare itself for Federated Incident Response

Group has been active since 2014 and combines expertise in operational security and incident response pol- FEDS community. Work to publish and implement the Sirtfi Trust Framework is supported by the AARC

Benefits

Why should I join? What are the Benefits?

Sirtfi v 1.0

View the Sirtfi Framework

FAQs

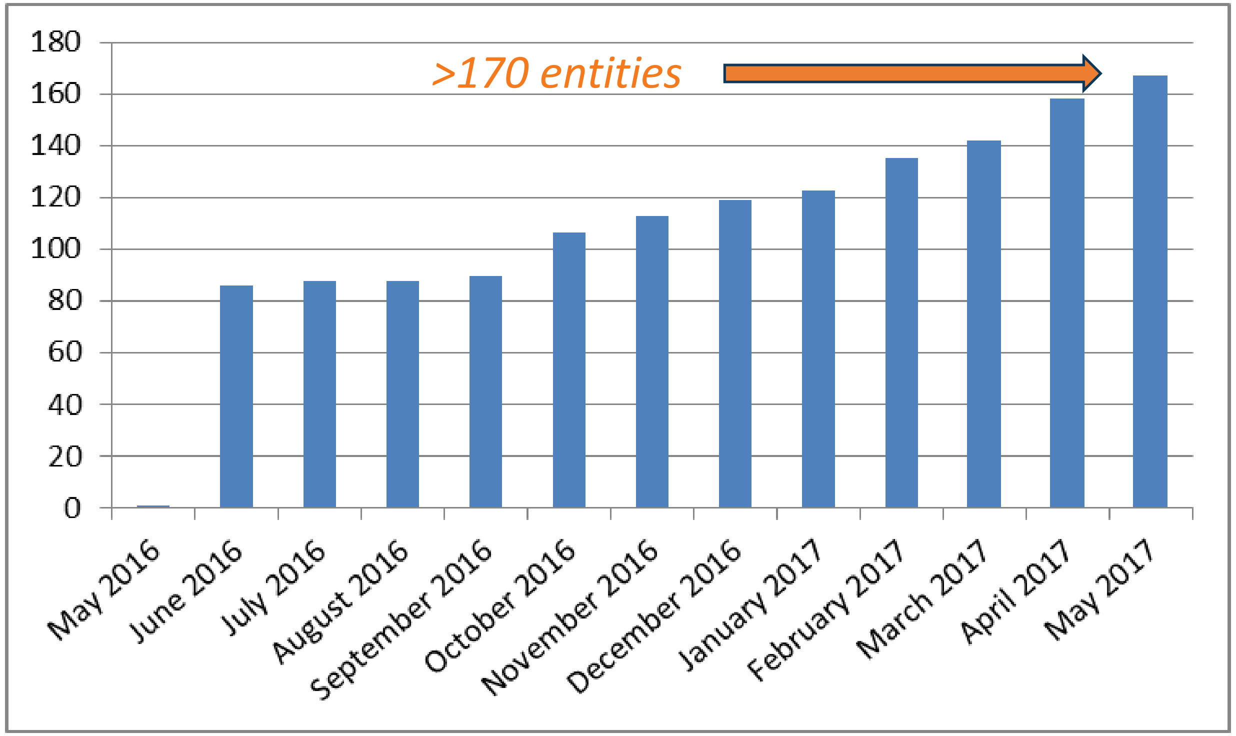
Need help?

- adds **security contact** meta-data in eduGAIN

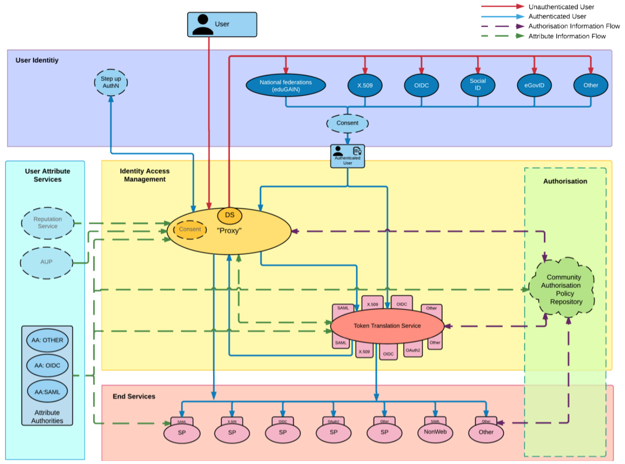
- with R&S meets **baseline assurance** and IGTF “assured identifier” profile
  … *IGTF-to-eduGAIN bridge asserts R&S+Sirtfi*

Used for filtering (with R&S) by proxies & services

EGI operational services, RCauth.eu bridge, CERN SSO, CILogon Basic services, …



Combine with 407 REFEDS R&S IdPs (May ’17)



Linking FIM AAI to PKIX technology: TCS and RCauth

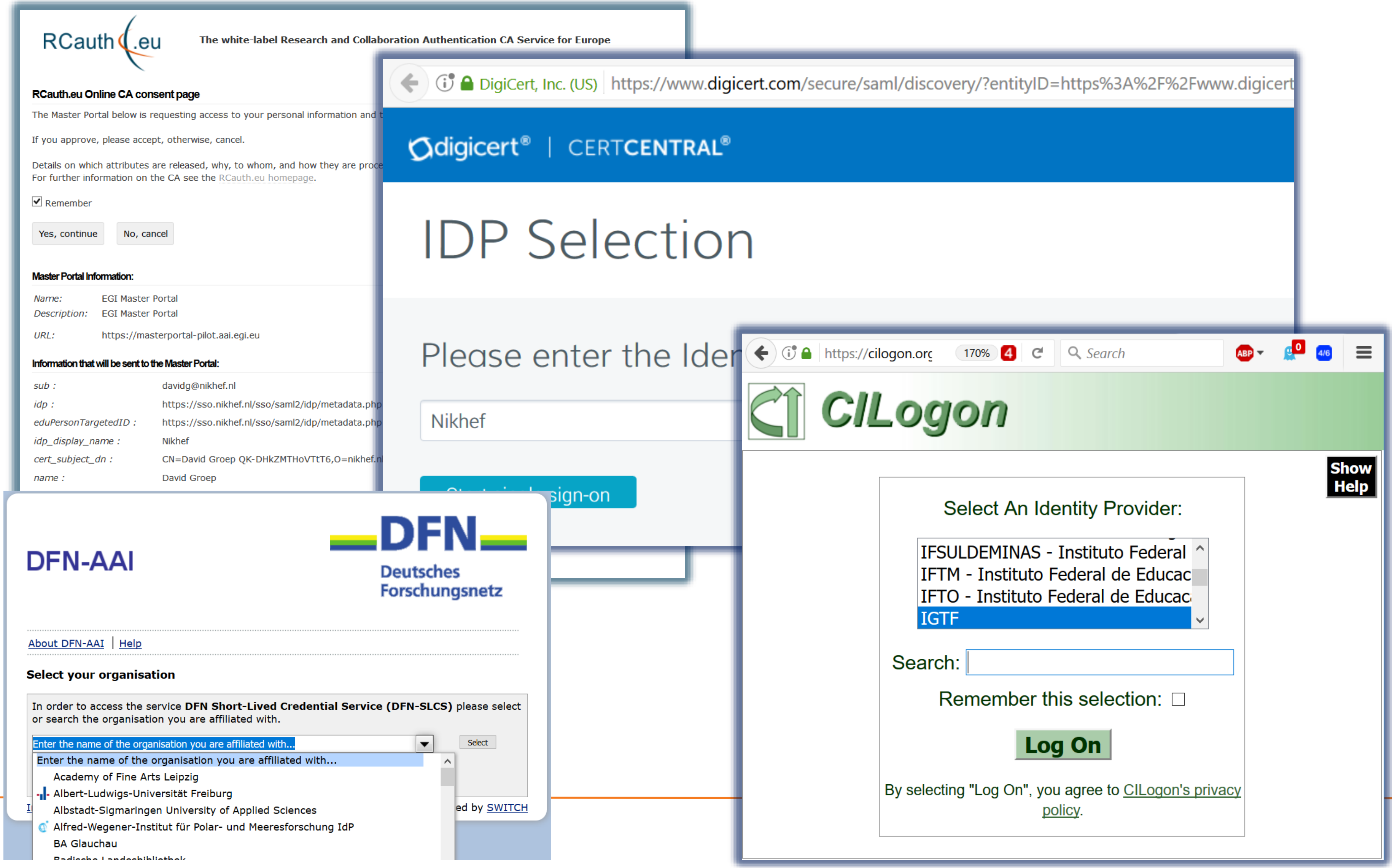
The AAI evolution of e-Infrastructures and Research Infrastructures

- Most infrastructures move to completely hiding PKIX from the end-user
  - Less credentials to manage, appearing ‘simpler’ to the user, but …
  - EEPKI + RFC3820 proxies **did solve both the CLI and delegation use case rather nicely!**

- Bridging and translation is the pragmatic approach
  - Does not require major technical changes in existing R&E federations
  - Allows for community-centric identities-of-last-resort (or first resort, for that matter!)
  - Time line is more predictable, because fewer entities are involved – and those entities have a stake in and the benefits off the results

- Emerging as a pattern in many Research Infrastructures that use CLI or brokerage
  - ELIXIR, UMBRELLA, WLCG, INDIGO DC
  - SAML->OIDC, SAML->X509, X509->OIDC, X509->SAML, OIDC->X509, …

Bridges everywhere: TCS – CILogon – DFN SLCS – RCauth.eu



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 t

If you approve, please accept, otherwise, cancel.

Details on which attributes are released, why, to whom, and how they are proce
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
idp_display_name :	Nikhef
cert_subject_dn :	CN=David Groep QK-DHkZMTHoVTtT6,O=nikhef.n
name :	David Groep

DigiCert, Inc. (US) https://www.digicert.com/secure/saml/discovery/?entityID=https%3A%2F%2Fwww.digicert

digicert® | CERTCENTRAL®

IDP Selection

Please enter the Ider

Nikhef

sign-on

DFN-AAI

DFN Deutsches Forschungsnetz

About DFN-AAI | Help

Select your organisation

In order to access the service **DFN Short-Lived Credential Service (DFN-SLCS)** please select or search the organisation you are affiliated with.

Enter the name of the organisation you are affiliated with... | Select

- Enter the name of the organisation you are affiliated with...
- Academy of Fine Arts Leipzig
- Albert-Ludwigs-Universität Freiburg
- Albstadt-Sigmaringen University of Applied Sciences
- Alfred-Wegener-Institut für Polar- und Meeresforschung IdP
- BA Glauchau

ed by SWITCH

https://cilogon.org 170% Search

CILogon

Show Help

Select An Identity Provider:

- IFSULDEMINAS - Instituto Federal
- IFTM - Instituto Federal de Educac
- IFTO - Instituto Federal de Educac
- IGTF

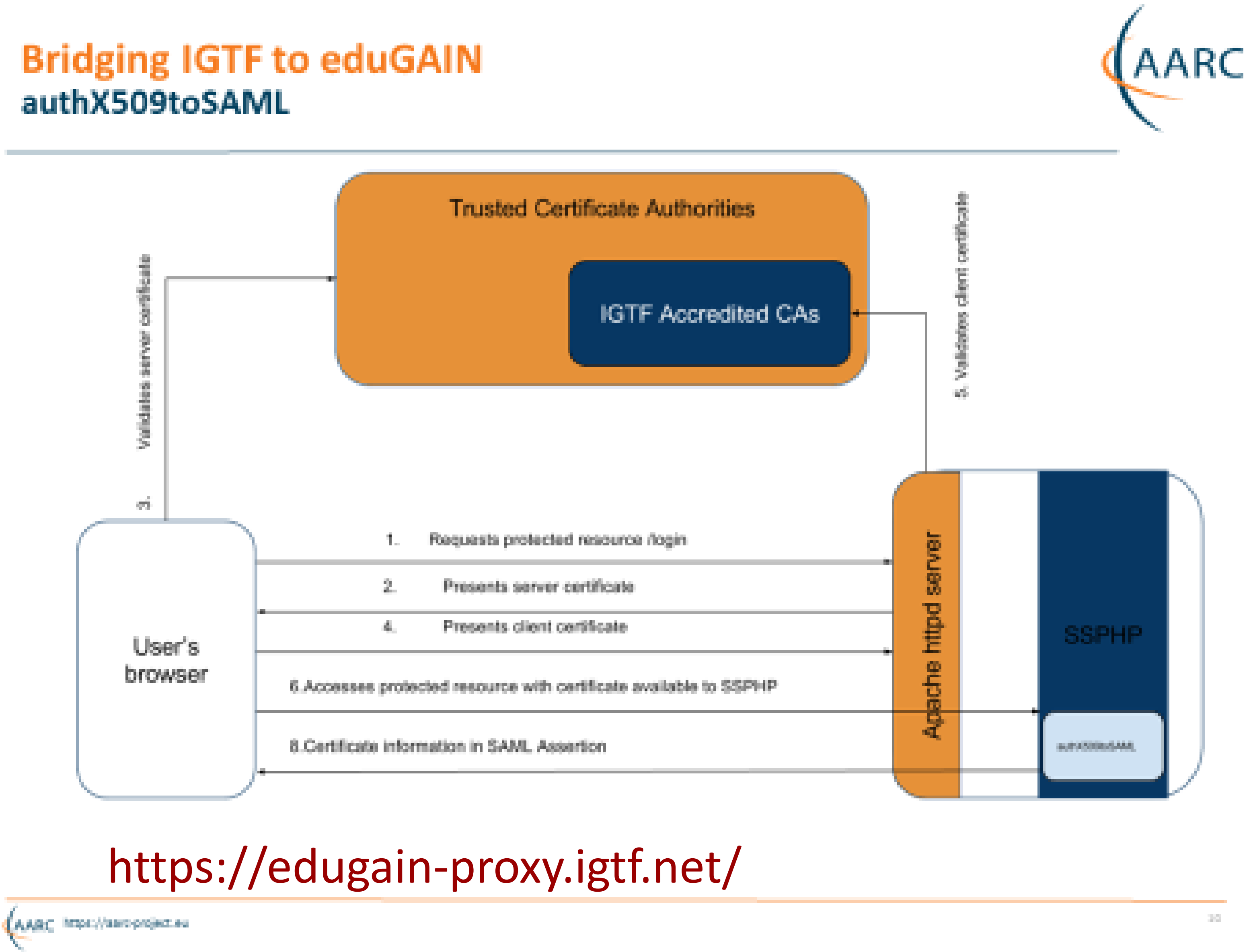
Search:

Remember this selection: □

Log On

By selecting "Log On", you agree to CILogon's privacy policy.

IGTF to eduGAIN



Bridging IGTF to eduGAIN

authX509toSAML

Trusted Certificate Authorities

IGTF Accredited CAs

3. Validates server certificate

5. Validates client certificate

User's browser

Apache httpd server

SSPHP

authX509toSAML

1. Requests protected resource /login

2. Presents server certificate

4. Presents client certificate

6.Accesses protected resource with certificate available to SSPHP

8.Certificate information in SAML Assertion

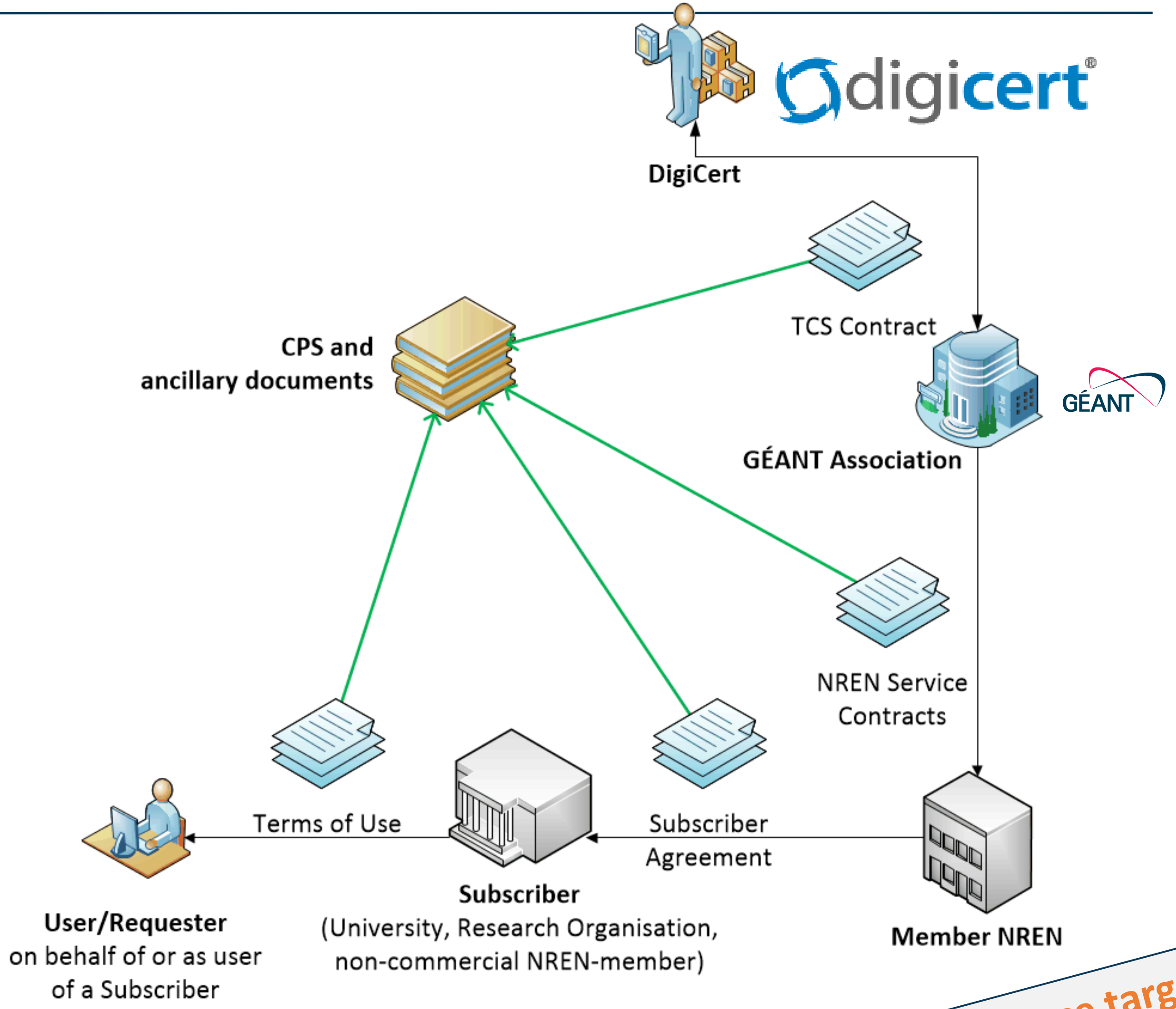
https://aarc-project.eu

https://edugain-proxy.igtf.net/

Work by Ioannis Kakavas and Nicolas Liampotis (GRNET) for the AARC project

TCS: Responsibility is built using contracts

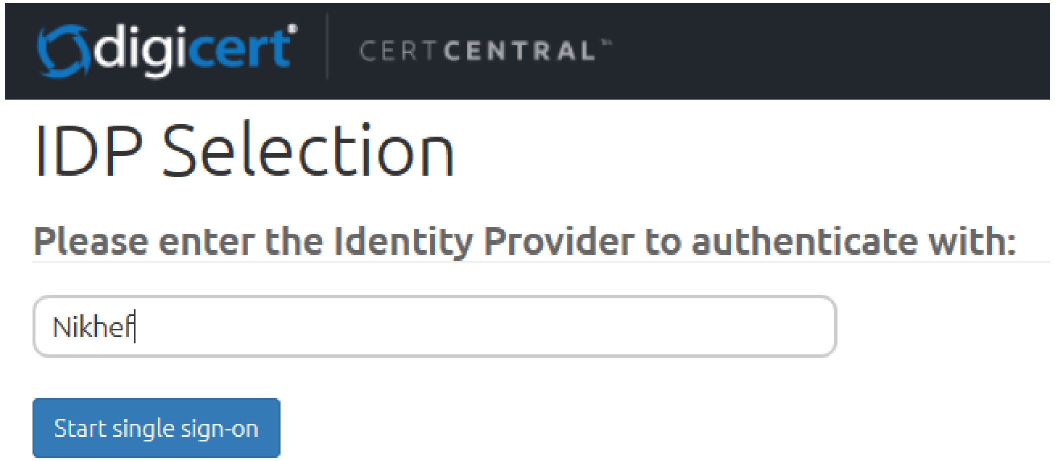
- scales well to large numbers of organisations and users
- assurance requirements on subscribers ensure quality ID
- bound through legal contracts
- listed in specific document and in the CPS



assurance target: BIRCH

SSO SAML portal now natively hosted by DigiCert

- Scope: **client certificates** (and client certificates only, sorry!)
- Assurance profile target BIRCH **and** public trust (S/MIME)
- DigiCert itself is now a ‘SAML2Int’ Service Provider
  <md:EntityDescriptor entityID="https://www.digicert.com/sso">
- visible to Federations and IdPs via the eduGAIN meta-data
- DigiCert will know about all IdPs in eduGAIN (via eduID.at)



IDP Selection

Please enter the Identity Provider to authenticate with:

Nikhef

Some scaling issues

Service is based on subscription – both by the NREN and the user's home institution

- impossible to connect non-NREN members, members outside GEANT scope, SMEs, &c
- sometimes entire countries opt out, for political or other reasons

Single, publicly-trusted, assurance level does not reflect current risk diversity

- all TCS trust anchors today are also publicly trusted
- works great for browser and S/MIME trust, but cannot address assurance composition by the Infrastructures and Proxies

Requires active work by the home organization for either FIM eligibility or specific enrolment

- and the specific enrolment options are not always clear, and technically more complex

Needs the user to keep managing credentials – an apparent obstacle for many communities

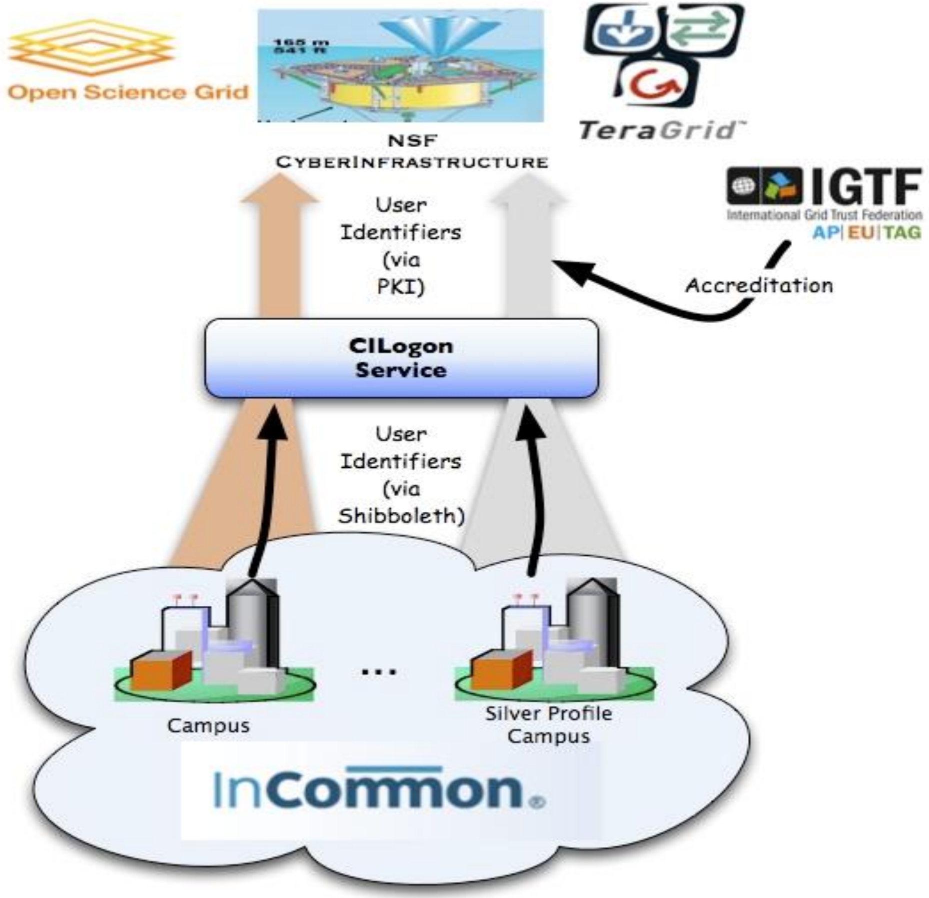
CILogon service and project (Jim Basney et al.)

CILogon Service

- Enable campus logon to CyberInfrastructure (CI)
  - Use researchers’ existing security credentials at their home institution
  - Ease credential management for researchers and CI providers

Multiple interfaces

- SAML/OpenID Web Browser SSO
  - PKCS12 certificate download
  - Certificate issuance via OAuth
  - OpenID Connect token issuance
  - SAML ECP for CLI issuance



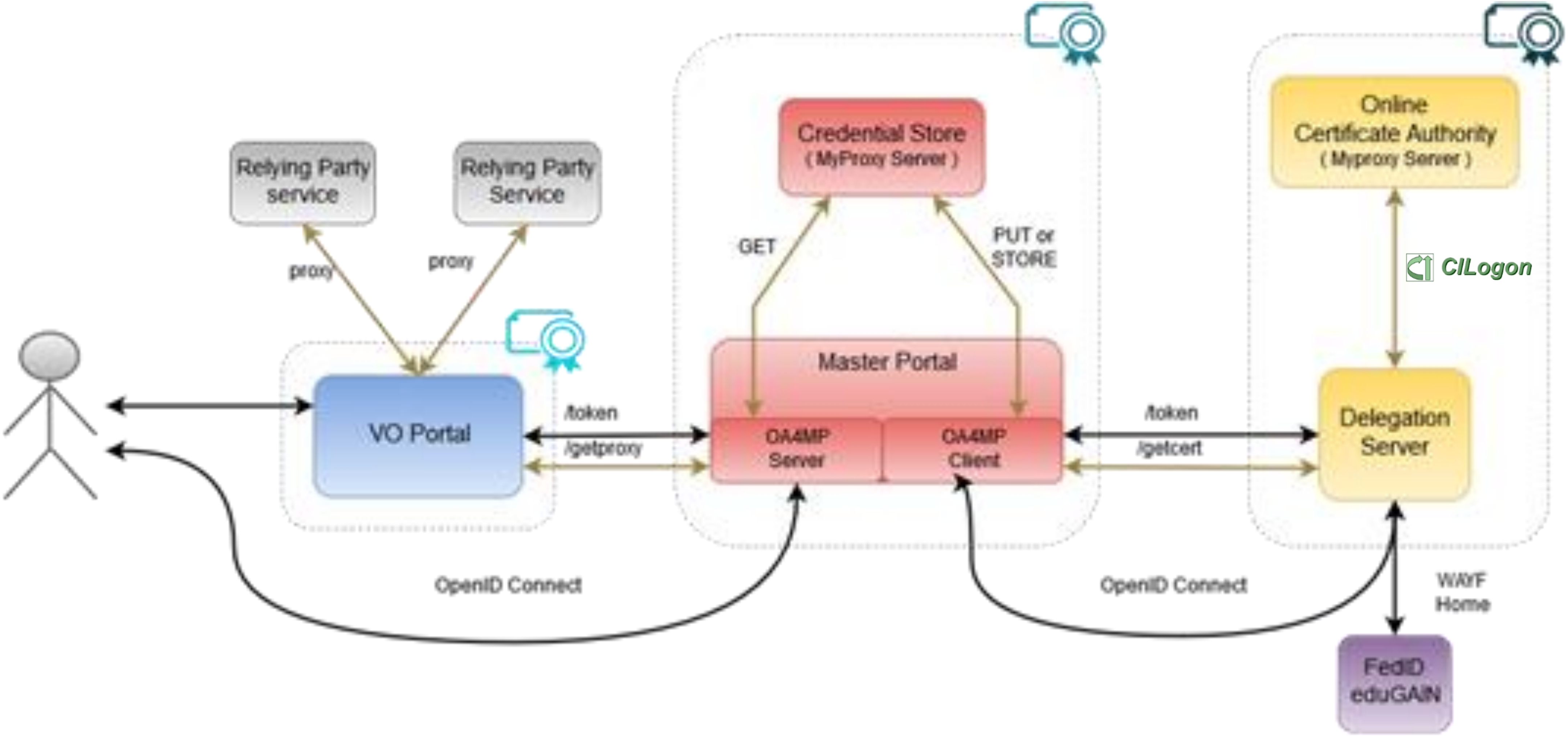
Slide content: Jim Basney, based on http://www.cilogon.org/docs/201106-cilogon-cern.pptx?attredirects=0&d=1 and http://www.cilogon.org/docs/20141030-basney-cilogon.pdf?attredirects=0&d=1

A CILogon-like Token Translations Service for Europe – RCauth.eu

- Ability to serve a large pan-European user base without national restrictions
  - without having to rely on specific national participation exclusively for this service
  - serving the needs of cross-national user communities that have a large but sparsely distributed user base
- Use existing resources and e-Infrastructure services
  - without the needs for security model changes at the resource centre or national level
- Allow integration of this system in science gateways and portals with minimal effort
  - only light-weight industry-standard protocols
- Permit the use of the (VOMS) community membership service
  - attributes for group and role management in attribute certificates
  - also for portals and science gateways access the e-Infrastructure
- Concentrate service elements that require significant operational expertise
  - not burden research communities with the need to care for security-sensitive service components
  - keep a secure credential management model
  - coordinate compliance and accreditation

assurance target: DOGWOOD

AARC CILogon-like TTS Pilot components



RCauth.eu – a white-label IOTA CA in Europe

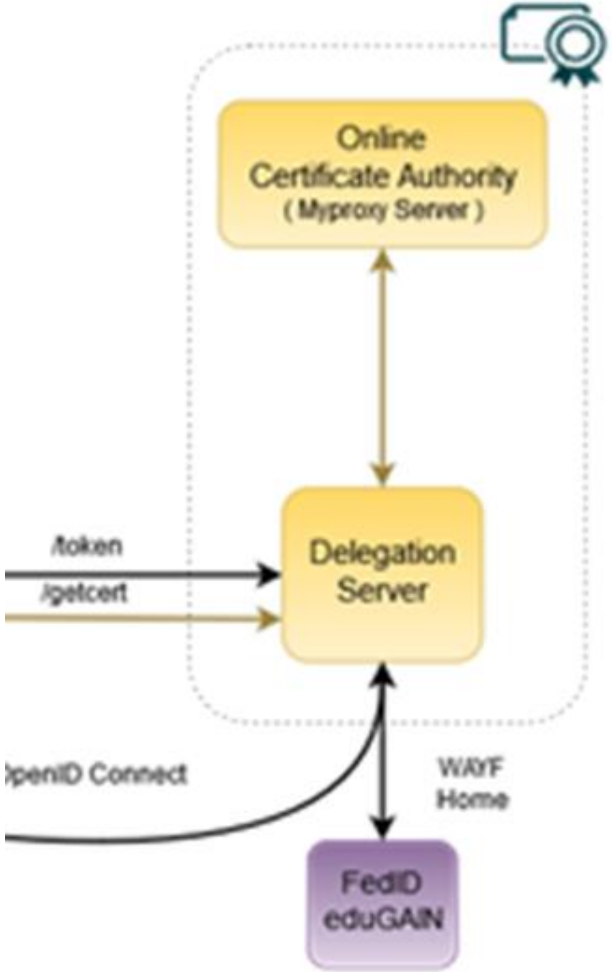
- Cover as much as R&E Federated Europe as possible
- Scoped to research and collaborative use cases
- In a scalable and sustainable deployment model

In the AARC Pilot we build a production-worthy pilot service

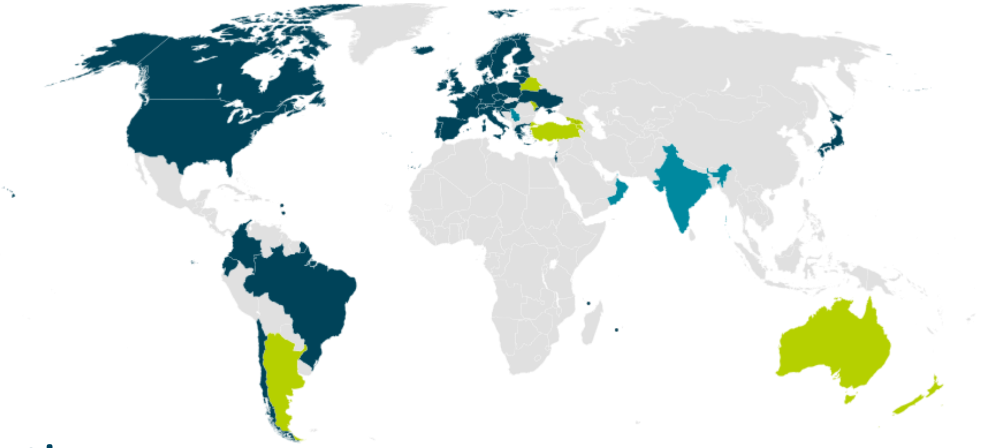
- which will operate for as long as necessary and useful
- supported by the Dutch National e-Infrastructure & Nikhef

… and that will in the subsequent phase be:

- taken up by sustained infrastructures (part supported by EOSC-HUB)
- a replicated redundant instance
- migrated to a new managing entity



Our Registration Authorities: all qualified Federated IdPs [1.3.2]



- RAs are the eligible IdPs connected through a Federated Identity Management System (FIMS)
- primarily: ensemble of IdPs in eduGAIN that meet the policy requirements of this CA
- Eligible applicants are all affiliated to an RA

Three eligibility models

1. Direct relationship CA-IdP, with agreement declaration
2. Rest of eduGAIN: – "**Sirtfi**" security incident response and OpSec capabilities plus
   – **REFEDS "R&S section 6"** non-reassigned identifiers and applicant name are required, and tested via statement in 'meta-data' and by releasing the proper attributes
3. *within the Netherlands: SURFconext Annex IX* compliance for all IdPs*

"IdPs within eduGAIN are deemed to have entered materially into an agreement with the CA"

Building RCauth - technically

Name uniqueness [3.1]

- Federations, with their distributed responsibility model, always face a consistency challenge
  - Release of any identifier associated with a individual person (‘privacy concerns’)
  - Guaranteeing non-reassignment of an identifier - has not played a major role *inside* any single org till now
  - Agreeing on how to name the name (attribute) of the authenticated user is different
  - Ability to trace an identifier to a person – and how to find the person at all

- We have to rely on the RAs (institutions) to provide an identifier that we can use - **even if** the institution itself does not consider RCauth.eu *on its own* worthy of specific attention

We can leverage grander schemes and agreements

- eduPerson schema – almost all federations use this, and most require specs compliance
- REFEDS Research and Scholarship (“R&S”) specification – aligns attribute release (and federation registrars check for minimal compliance
- Sirtfi – new standard to harmonize incident response and opsec capabilities and processes

Constructing a non-reassigned subjectName

/DC=eu/DC=rcauth/DC=rcauth-clients/O=*orgdisplayname*/CN=*commonName*

- All the uniqueness will be in the commonName – that will “contain sufficient information such that an enquiry via the issuer allows unique identification of the vetted entity”

- The orgdisplayname is used to “identify the identity management system via which the identity of this person was vetted” [IOTA 3.2]

So if – over time – the orgdisplayname may conflict, be re-used, or is ambiguous, we don’t need it: we will use the commonName to trace and ensure non-reassignment!

CommonName – the big challenge

Requirements

- Contain a representation of the real name of the applicant as asserted by the IdP
  the opaque option is not very friendly to downstream services
- Must be unique and non-reassigned
- Allow – via the issuer – unique identification of the entity in the stated IdP

So we construct it out of 2, but sometimes even 3, elements

1. Readable name of the applicant (max. 40 characters)
2. **Unique Shortened Representation** of the identifier provided by the IdP (16 characters)
3. *Optional:* ensured-uniqueness sequence number (max. 3 digits)

From eduGAIN IdPs, you can expect anything … rightfully!

```
$ java -cp icu4j-59_1.jar:. transliterate2 [...]
 "Jőzsi Bácsi" "Guðrún Ósvífursdóttir" "Χρηστος Κανελλοπουλος"
 "簡禎儀"
```

```
Input:   Jőzsi Bácsi
Output:  Jozsi Bacsi
Input:   Guðrún Ósvífursdóttir
Output:  Gudrun Osvifursdottir
Input:   Χρηστος Κανελλοπουλος
Output:  Christos Kanellopoulos
Input:   簡禎儀
Output:  jian zhen yi
```

Try yourself?
https://github.com/rcauth-eu/aarc-delegation-server/blob/master/delegation-server/src/main/java/org/delegserver/oauth2/generator/DNGenerator.java

But Unicode e.g. does not distinguish the *diaeresis* and the *umlaut*

- Paul Mühl → Paul Muhl   is wrong, should have been ‘Paul Muehl’
- reünie → reunie   is good, you definitely don’t want ‘reuenie’

As the so for stability, we keep Any-Latin here and treat all as a diaeresis

commonName – USR of the IdP identifier

Provides for issuer-assisted traceability of people. We pick and record the attribute used, preferring:

1. eduPersonUniqueID attribute (scoped) from the IdP (the ‘perfect’ attribute, available nowhere)
2. eduPersonPrincipalName (scoped) attribute from the IdP (a good attribute, OK 97% of the time)
3. eduPersonTargetedID constructed from IdP entityID and IdP-local (but targeted) opaque value

This is then pushed through the “Unique Shortened Representation”:

- first 16 characters of the base-64 encoded binary representation of the SHA-256 hash of the value, with any SOLIDUS (“/”) characters replaced by HYPHEN-MINUS (“-“) characters
- This **mapping leaves 96 bits of entropy of the hash and thus a mean collision probability <10**$^{-14}$

If the IdP gives	USR in CN RDN
40ea621a0a7355cf4fb1ca8d4f22a53d@nikhef.nl	uXmc85peL+35ONPO
davidg@nikhef.nl	Kydx8KT6xc1CHjD1
https://sso.nikhef.nl/sso/saml2/idp/metadata.php!02f7dfbb9605cf549e874bce55bfe0de030e9140	Wgt0ltSuF7BAA7FM

RCauth.eu Pilot ICA G1 – its initial single-site deployment

try some services at
https://rcdemo.nikhef.nl/
or use Project MinE, or ELIXIR, or …

Considerations

Part of the operations will be sustainably funded

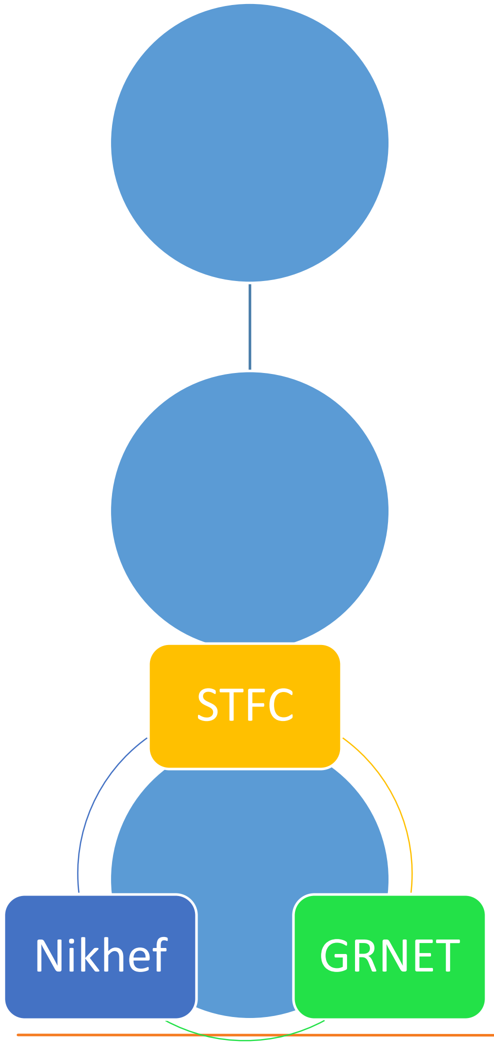
- by EOSC-HUB through its partners for the technical ops
- by SURF DNI for both support and operations
- in-kind for trusted network connectivity by GÉANT

and those who put in resources have a rightful say in where the resources go … up to a point

Core values and principles of RCauth.eu are beyond just those contributing stakeholders

- must be open to anyone for any acceptable work – we don’t want a fragmented community
- nobody to be ‘left out of the rain’ (unlike to TCS which depends on NREN policy and sign-up)
- usefulness to research and collaboration is paramount and must be the deciding factor

RCauth.eu Governance



Governance Board

Representatives (and one alternate) from each Materially Contributing Stakeholder
EGI.eu, EUDAT (ETFC), GÉANT, Nikhef (SURF)

RCauth PMA

Individuals drawn from the wide community […]
experts in the field of identity management
for research and collaboration,
PKI technology and identity bridging

Ops Coordination Team

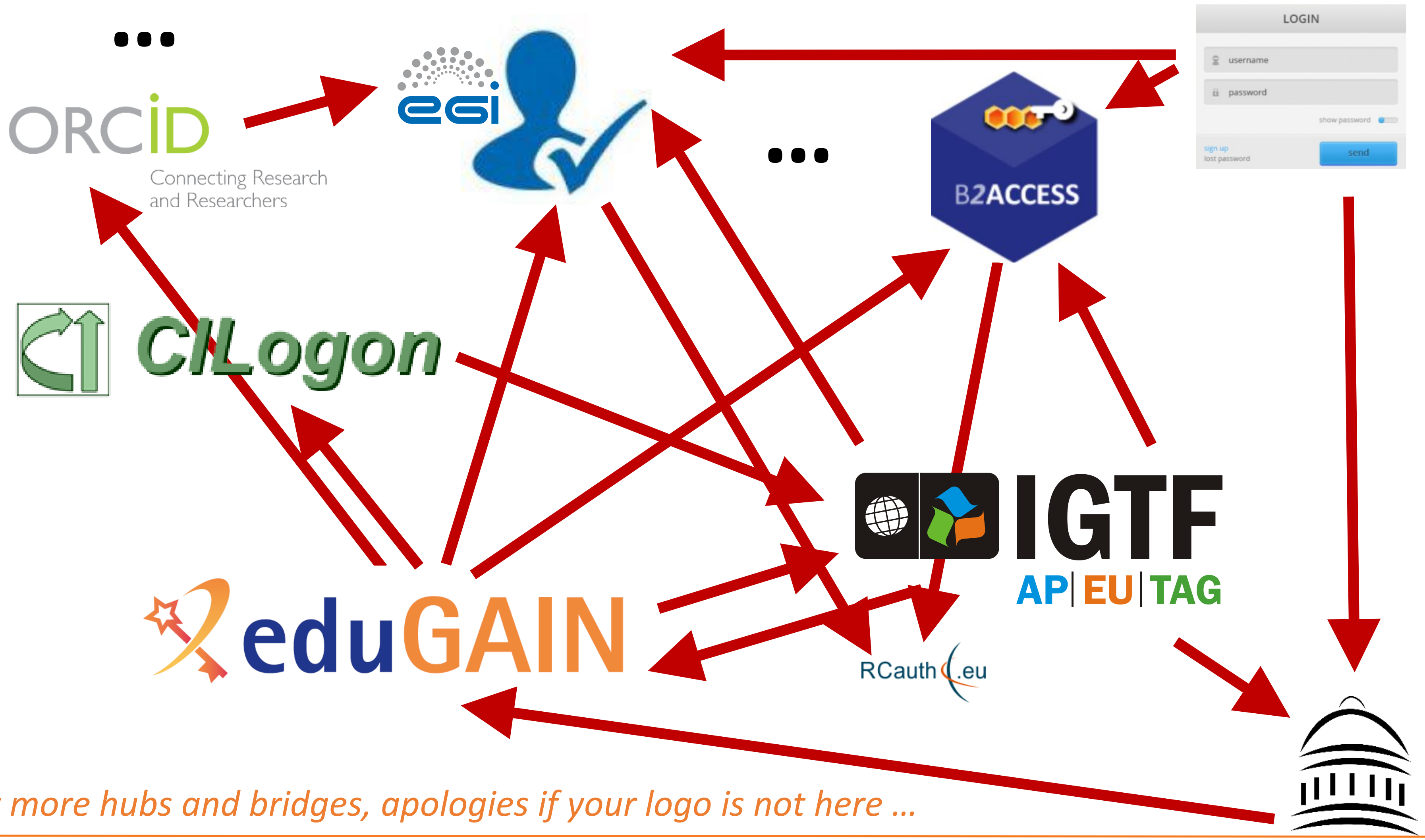
Operations people from each of the **hosting partners**
with a (copy of) the RCauth.eu signing key,
and those partners otherwise involved in OPS

How to manage distribution: two options

1. Most consistent external view – closest internal coordination and trust
   - Single RCauth.eu signing key
   - Securely distributed to each operational partner
   - Fully owned and managed by the PMA
   - Requires partners to accept stringent controls by the PMA to ensure trust
   - Fully transparent to users and external RPs

2. Most distributed and resilient view – with global user and RP impact on usability
   - Each partner gets a different RCauth.eu signing key
   - These will show up as independent ICAs in the IGTF distribution
   - Same Subject DN namespace, but different issuer names in parallel and simultaneously
   - Partners can join and leave, validity of ICA controlled through the CRL of upstream root
   - Allows PMA to control a leaving party without such party’s co-operation and without special measures
   - Floods IGTF distribution with multiple ICAs, and persistently exposes CA internal to VOMS and RPs

Everything meshed together … look for your favourite loop …



and many more hubs and bridges, apologies if your logo is not here …

- OIDC technology
- OIDC Federation
- IGTF OIDCfed AARC Pilot

Supporting the Infrastructures beyond PKIX & SAML

OpenID Connect

Web- and mobile-friendly (REST/JSON) identity layer on top of OAuth2

- OAuth2 authentication flow
- Claims REST interface for identity information

Probably known to you already

- many social logins: Google, Linked-In, MSFT, …
- part of many identity solutions products: Ping, NRI, …
- and one very .well-known from our own community: ORCID

https://www.eugridpma.org/meetings/2018-01/summary-eugridpma-2018-01-prague.txt

Building conections: Client ID and Client Secret

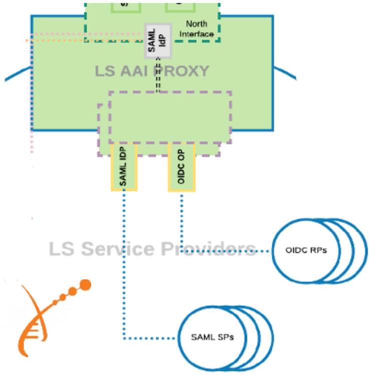
XSEDE
Extreme Science and Engineering Discovery Environment
CILogon

- Planning for Globus migration from X.509 to Globus Auth
- Maintain credential assurance for XSEDE users and systems
- Continue to benefit from IGTF trust community

RCauth.eu

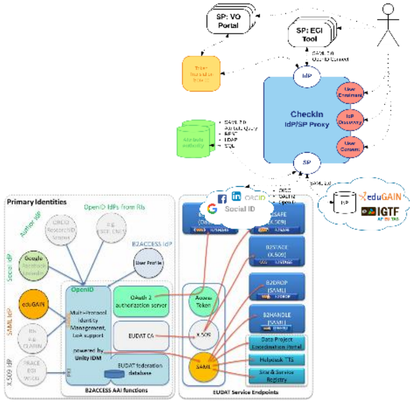
- WaTTS service
- EGI MasterPortal
- MinE Credential Hosting
- *… B2ACCESS, …*

- ELIXIR and LSAAI services
- e-Infra connections



Master Portal

- SSH Proxy CLI
- Prometheus WebDAV portal
- mkProxy service
- …



- EGI CheckIn
- B2ACCESS
- EOSC-HUB AAI
- Today < O(50) clients; next year O(100-1000)?

both technical trust (trust anchors) and aligned policies needed to make this scale

Assurance and trust frameworks

Identity Assurance Profiles for R/E-Infra risk scenarios (https://igtf.net/ap/loa/**)**

- "BIRCH" - good quality (federated) identity,
  "DOGWOOD" - identifier-only, but with traceability (*R&S+Sirtfi+a few bits)*
  RFC 6711 Registry: https://iana.org/assignments/loa-profiles
- technology-specific 'trust anchor' distribution services

Policy framework for Relying Parties ('SP-IdPs-Proxies')

- Snctfi - Community Trust Framework in Federated Infras
  https://igtf.net/snctfi

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

- technology bridges: TCS, RCauth.eu, IGTF-eduGAIN bridge, …
- behind the Infrastructure Proxies for research & collaboration, OIDC gains prominence

thanks to Davide Vaghetti (GARR) whose REFEDS Linz slide content I re-used

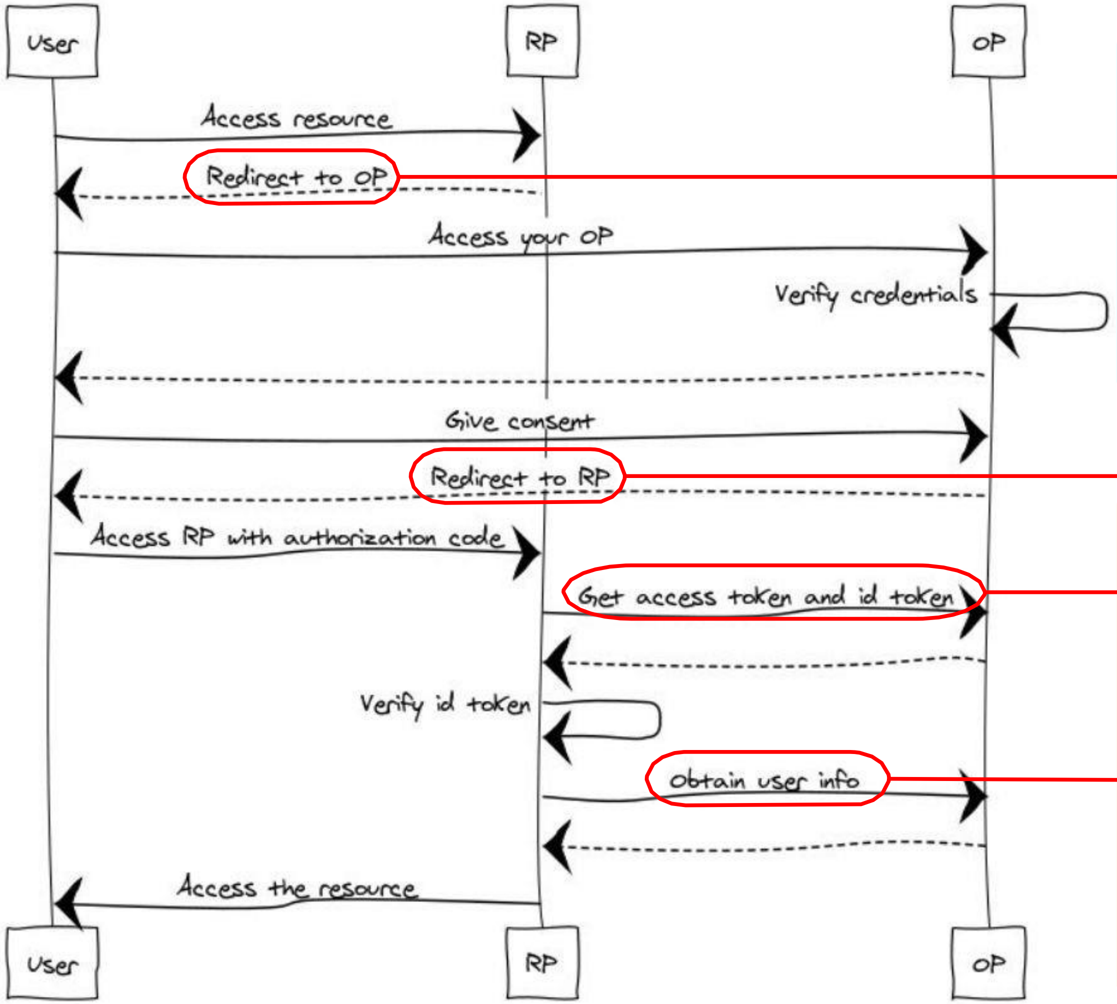
OIDC MECHANICS

OIDC Actors

- The **User** who wants to access a protected resource, either by himself or through an application.
- The **Relying Party** (often called the Client) is the entity that will request and use an access token.
- The **OIDC Provider** (OP) is the entity that will release the access token.

slide content thanks to Davide Vaghetti, GARR, for GN4-2-JRA3-T3.1.A

OIDC: OP and RP needs to know about each other



RP redirect the user to the OP's **authorization_endpoint**

OP redirect the user to the RP's **redirect_uri**

RP exchange the code for an access_token at the **token_endpoint** (and authenticate…)

RP requests user claims at the OP's **userinfo_endpoint**

slide content thanks to Davide Vaghetti, GARR, for GN4-2-JRA3-T3.1.A

OpenID Connect –
Discovery and Dynamic Client Registration

http://openid.net/specs/openid-connect-discovery-1_0.html

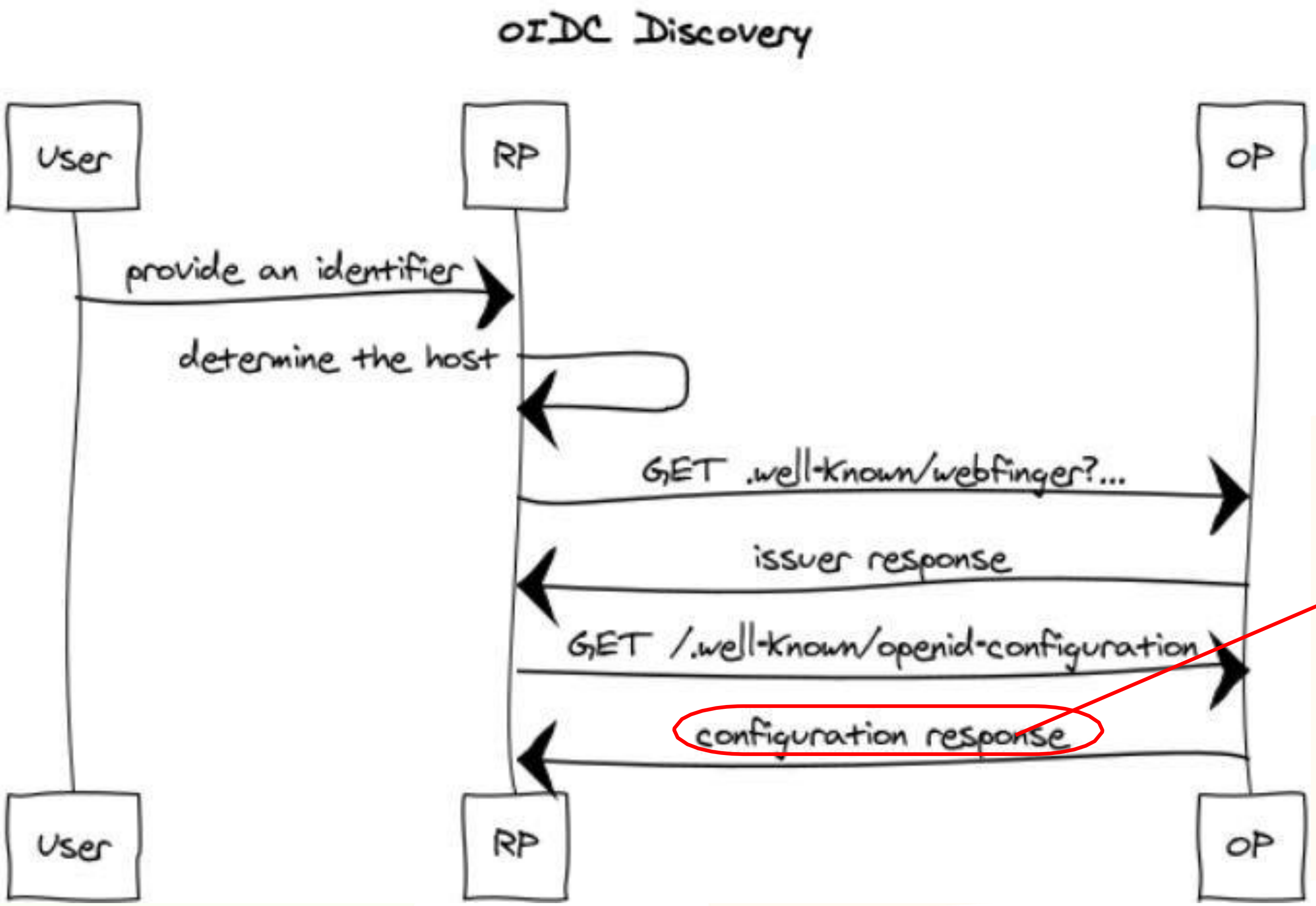
a mechanism for an OpenID Connect Relying Party to discover the End-User's OpenID Provider and obtain information needed to interact with it, including its OAuth 2.0 endpoint locations

http://openid.net/specs/openid-connect-registration-1_0.html

defines how an OpenID Connect Relying Party can dynamically register with the End-User's OpenID Provider, providing information about itself to the OpenID Provider, and obtaining information needed to use it, including the OAuth 2.0 Client ID for this Relying Party

slide content thanks to Davide Vaghetti, GARR, for GN4-2-JRA3-T3.1.A

OpenID Connect Discovery 1.0

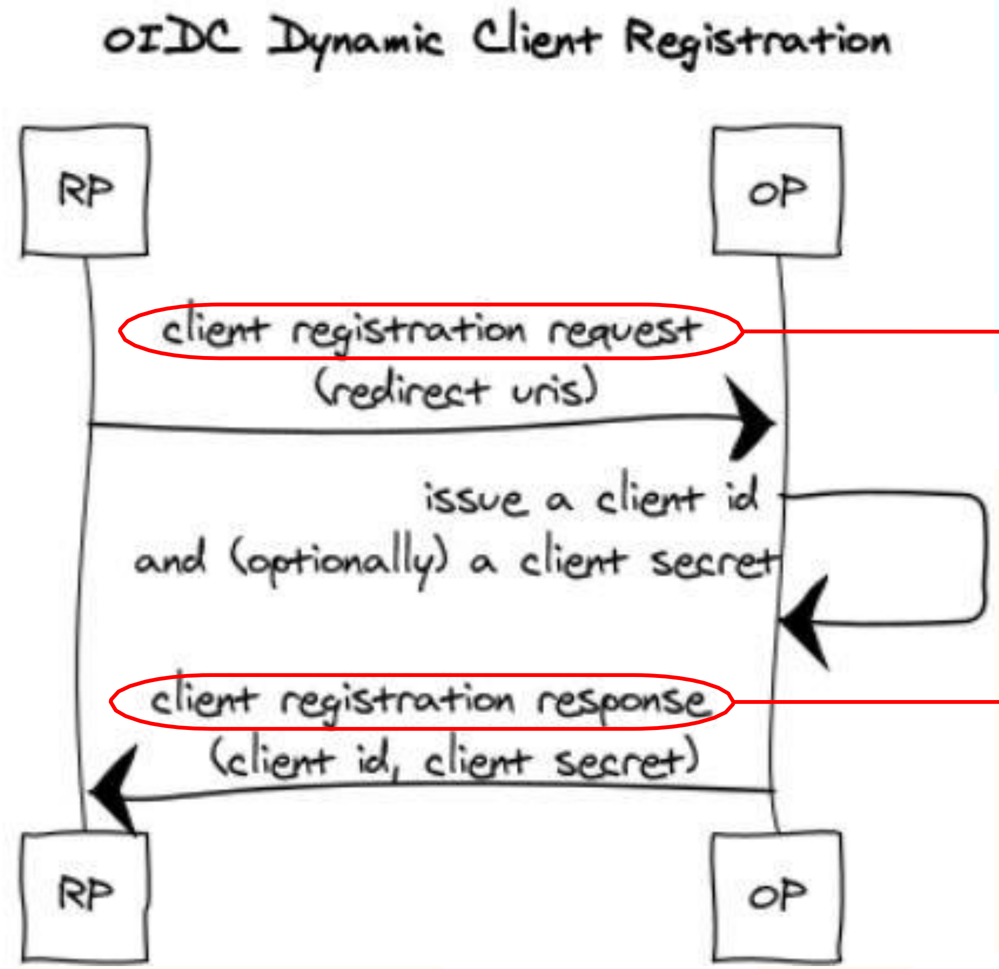


The **RP** receives and consumes the **OP** metadata (provider configuration).

No trust information is provided.

slide content thanks to Davide Vaghetti, GARR, for GN4-2-JRA3-T3.1.A

OpenID Connect Dynamic Client Registration 1.0


OIDC Dynamic Client Registration
RP
OP
client registration request
(redirect uris)
issue a client id
and (optionally) a client secret
client registration response
(client id, client secret)
RP
OP

The **OP** receives a client registration request from the **RP**.

No trust information is provided.

The **OP** sends a client registration response to the **RP**.

No trust information is provided.

slide content thanks to Davide Vaghetti, GARR, for GN4-2-JRA3-T3.1.A

Slides on general OIDC Fed work: Roland Hedberg, Ioannis Kakavas, Maarten Kremers

OIDC FEDERATION

OIDC Identity Federations – *The Specification*
Governing principals

- Allow dynamic discovery and registration without losing trust
- Enforcement of federation and organisation policies
- Allow delegation of entity registration
- Metadata transport and origin independent
- Self-contained metadata

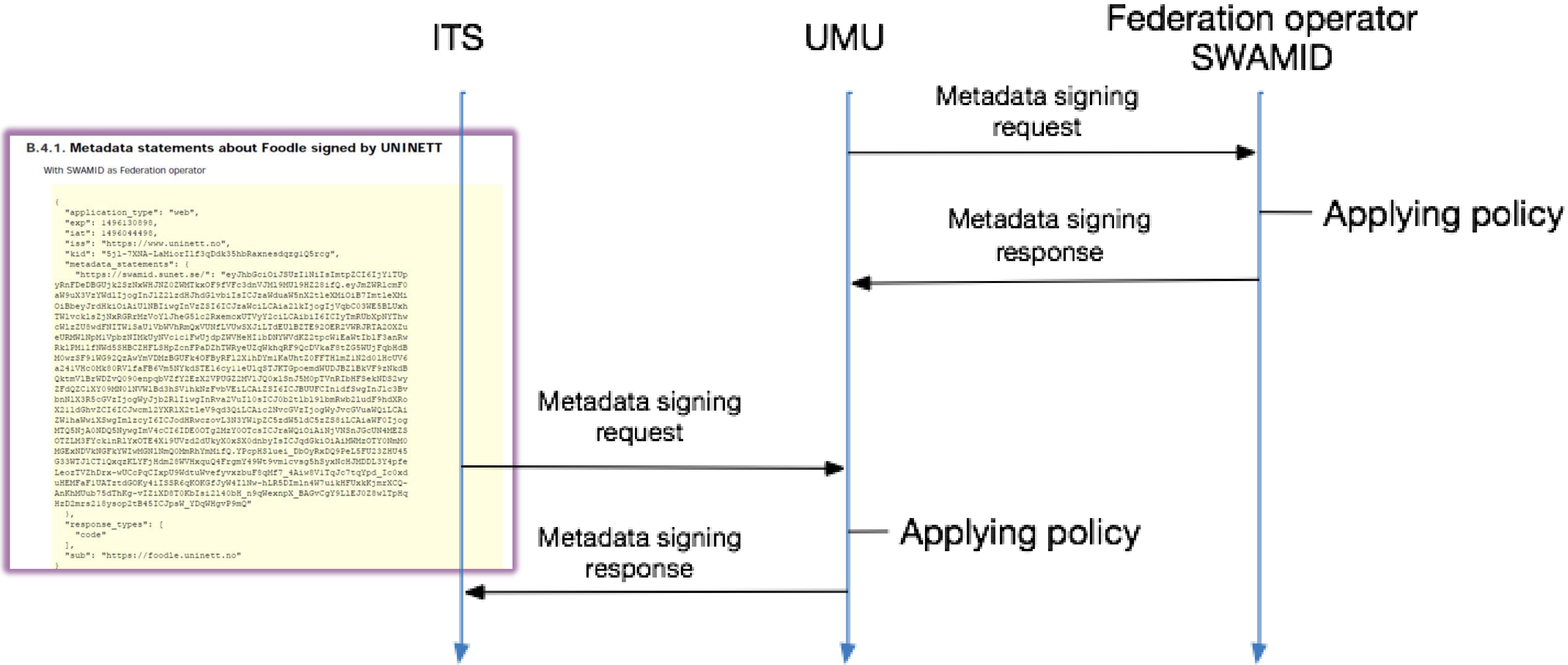
Slides content: Roland Hedberg, Ioannis Kakavas, Maarten Kremers

OIDC Identity Federations – *The Specification*
Building blocks

- Trusted 3rd party
- Chain of verifiable claims
- Compounded metadata

Slides content: Roland Hedberg, Ioannis Kakavas, Maarten Kremers

OIDC Identity Federations – *The Specification*
Metadata construction



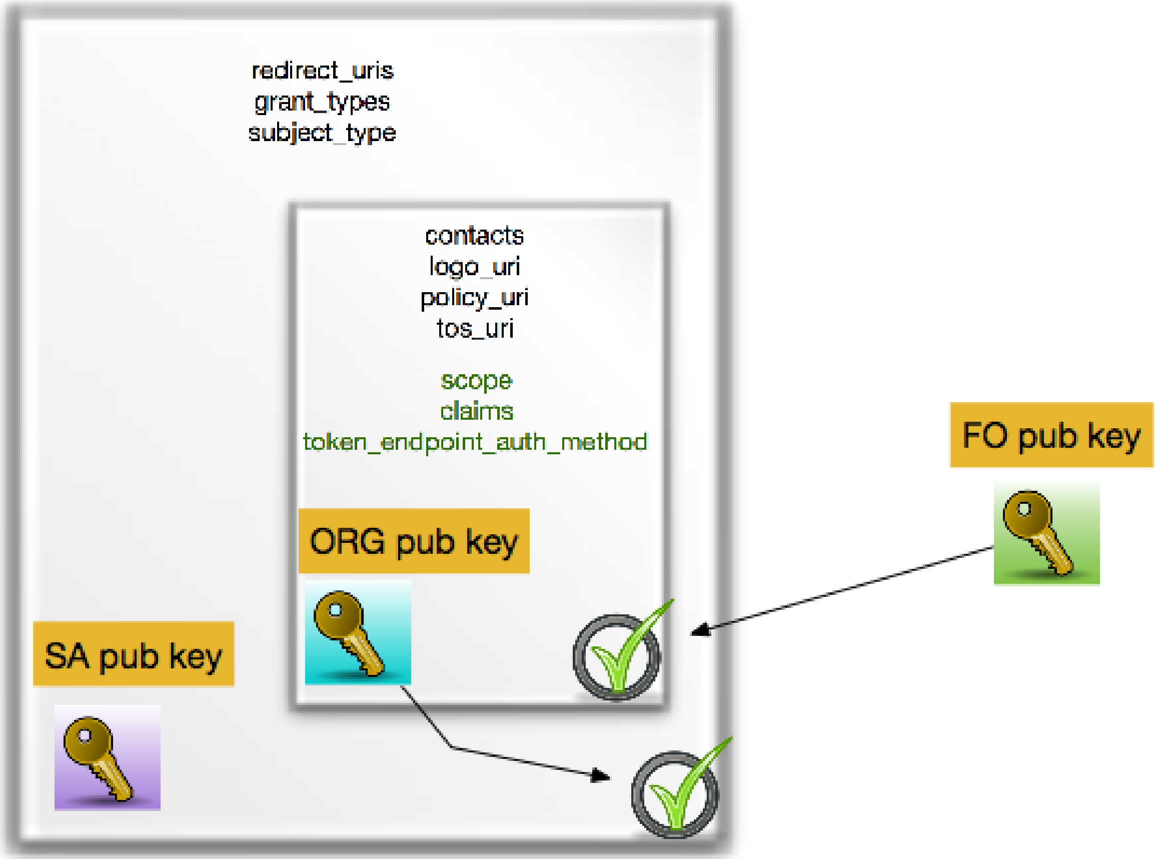
B.4.1. Metadata statements about Foodle signed by UNINETT

With SWAMID as Federation operator

```
{
  "application_type": "web",
  "exp": 1496130898,
  "iat": 1496044498,
  "iss": "https://www.uninett.no",
  "kid": "5jl-7XNA-LaMiorIlf3qDdk35hbRaxnesdqzgiQ5rcg",
  "metadata_statements": {
    "https://swamid.sunet.se/": "eyJhbGciOiJSUzI1NiIsImtpZCI6IjY1TUp
yRnFDeDBGUjk2SzNxWHJNZ0ZWMTkxOF9fVFc3dnVJMl9MUl9HZ28ifQ.eyJmZWRlcmF0
aW9uX3VzYWdlIjogInJlZ2lzdHJhdGlvbiIsICJzaWduaW5nX2tleXMiOiB7ImtleXMi
OiBbeyJrdHkiOiAiU1NBIiwgInVzZSI6ICJzaWciLCAia2lkIjogIjVqbC03WE5BLUxh
TWlvcklsZjNxRGRrMzVoYlJheG5lc2RxemcxUTVyY2ciLCAibiI6ICIyTmRUbXpNYThw
cWlzZU8wdFNITW1SaU1VbWVhRmQxVUNfLVUwSXJiLTdEU1BZTE92OER2VWRJRTA2OXZu
eURMW1NpM1VpbzNIMkUyNVc1c1FwUjdpZWVHeHI1bDNYWVdKZ2tpcW1EaWtIb1F3anRw
Rk1PM1lfNWd5SHBCZHFLSHpZcnFPaDZhTWRyeUZqWkhqRF9QcDVkaF8tZG5WUjFqbHdB
M0wzSF91WG92QzAwYmVDMzBGUFk4OFByRFl2X1hDYm1KaUhtZ0FFTHlmZ1N2d01HcUV6
a241VHc0Mk80RVlfaFB6Vm5NYkdSTEl6cy11eUlqSTJKTGpoemdWUDJBZ1BkVF9zNkdB
QktmVlBrWDZvQ090enpqbVZfY2EzX2VPUGZ2MVlJQ0xlSnJ5M0pTVnRIbHFSekNDS2wy
ZFdQZC1XY09MN01NVW1Bd3hSV1hkNzFvbVEiLCAiZSI6ICJBUUFCIn1dfSwgInJlc3Bv
bnNlX3R5cGVzIjogWyJjb2RlIiwgInRva2VuIl0sICJ0b2tlbl91bmRwb2ludF9hdXRo
X21ldGhvZCI6ICJwcml2YXRlX2tleV9qd3QiLCAic2NvcGVzIjogWyJvcGVuaWQiLCAi
ZW1haWwiXSwgImlzcyI6ICJodHRwczovL3N3YW1pZC5zdW5ldC5zZS8iLCAiaWF0Ijog
MTQ5NjA0NDQ5NywgImV4cCI6IDE0OTg2MzY0OTcsICJraWQiOiAiNjVNSnJGcUN4MEZS
OTZLM3FYcklnRlYxOTE4X19UVzd2dUkyX0xSX0dnbyIsICJqdGkiOiAiMWMzOTY0NmM0
MGExNDVkNGFkYWIwMGNlNmQ0MmRhYmMifQ.YPcpHSluei_DbOyRxDQ9PeL5FU23ZHU45
G33WTJlCT1QxqzKLYFjHdm28WVHxquQ4FrgmY49Wt9vmicvsg5hSyxNcHJMDDL3Y4pfe
LeozTVZhDrx-wUCcPqCIxpU9WdtuWvefyvxzbuF8qMf7_4Aiw8V1TqJc7tqYpd_Ic0xd
uHEMFaF1UATztdGOKy4iISSR6qKOKGfJyW4IlNw-hLR5DImln4W7uikHFUxkKjmrXCQ-
AnKhMUub75dThKg-vIZiXD8T0KbIsi2l40bH_n9qWexnpX_BAGvCgY9LlEJ0Z8wlTpHq
HzD2mrs218ysop2tB45ICJpsW_YDqWHgvP9mQ"
  },
  "response_types": [
    "code"
  ],
  "sub": "https://foodle.uninett.no"
}
```

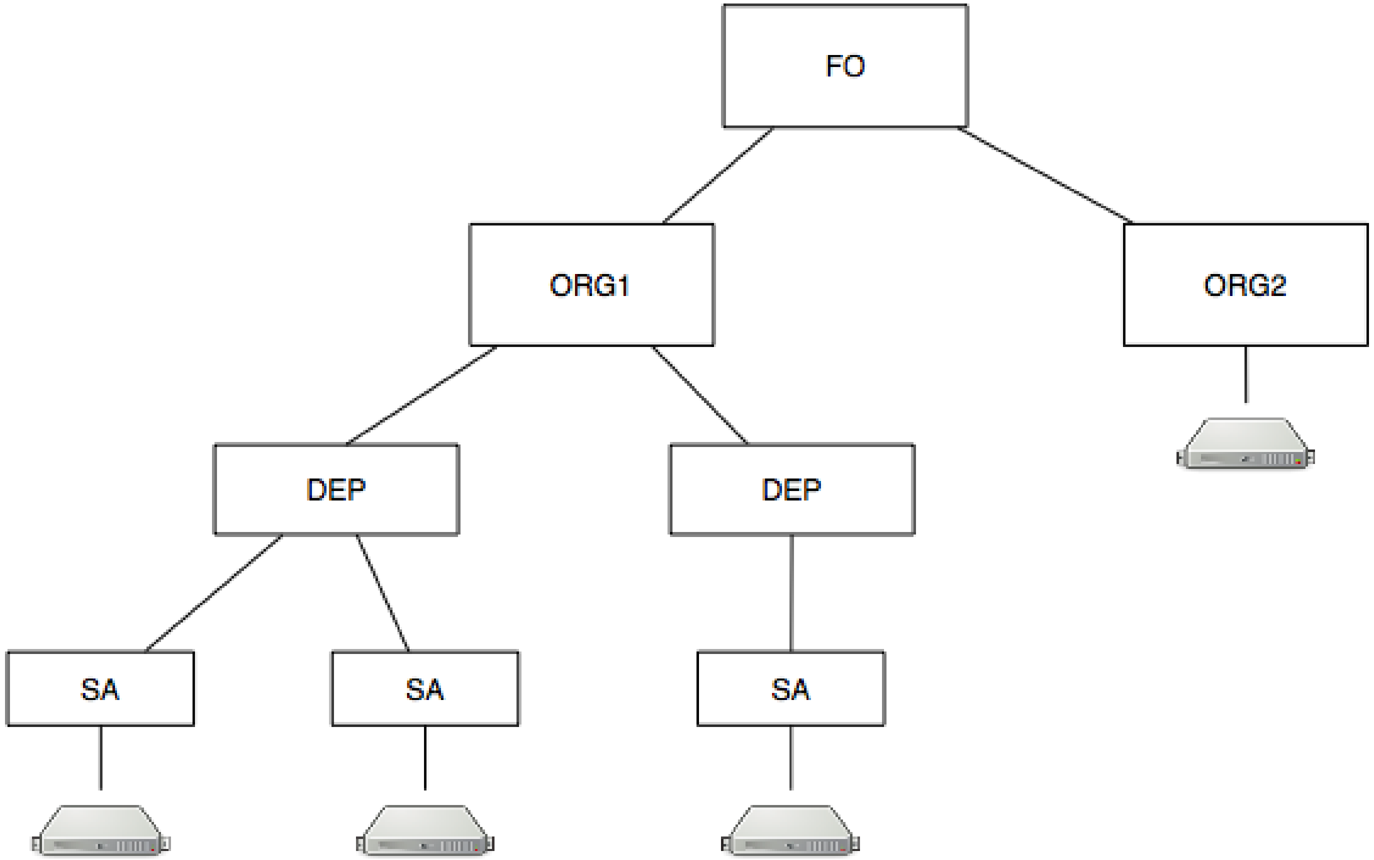
Slides content: Roland Hedberg, Ioannis Kakavas, Maarten Kremers

OIDC Identity Federations – *The Specification*
Compounded metadata statement



Slides content: Roland Hedberg, Ioannis Kakavas, Maarten Kremers

OIDC Identity Federations – *The Specification* Depth



Slides content: Roland Hedberg, Ioannis Kakavas, Maarten Kremers

OIDC Identity Federations – *Implementations & Tools*
Reference Implementation in Python

- https://github.com/OpenIDC/fedoidc
- Federation aware OpenID Connect Provider
- Federation aware Relying Party
- Support for Federation Operator related functionality

Slides content: Roland Hedberg, Ioannis Kakavas, Maarten Kremers

OIDC RP FEDERATION PILOT

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

for RP trust (more than today) re-use Sirtfi, WISE, and trust groups

Scoping and model discussions

ACAMP session nodes (see Wiki)

- do not over-complicate the initial set-up
- retain dynamics in the system by leveraging existing trust
- stick to OIDC core attributes makes life easier
- discovery – leave this for the RPs, but make our data available
- allow overlapping federations and be complementary (COIs)

Don’t boil the ocean

- scope to the expected $\mathcal{O}$(100) organisations
- leverage existing trust and current operational mechanisms

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

IGTF OIDC Federation Task Force

The IGTF task force for OIDC Federation will

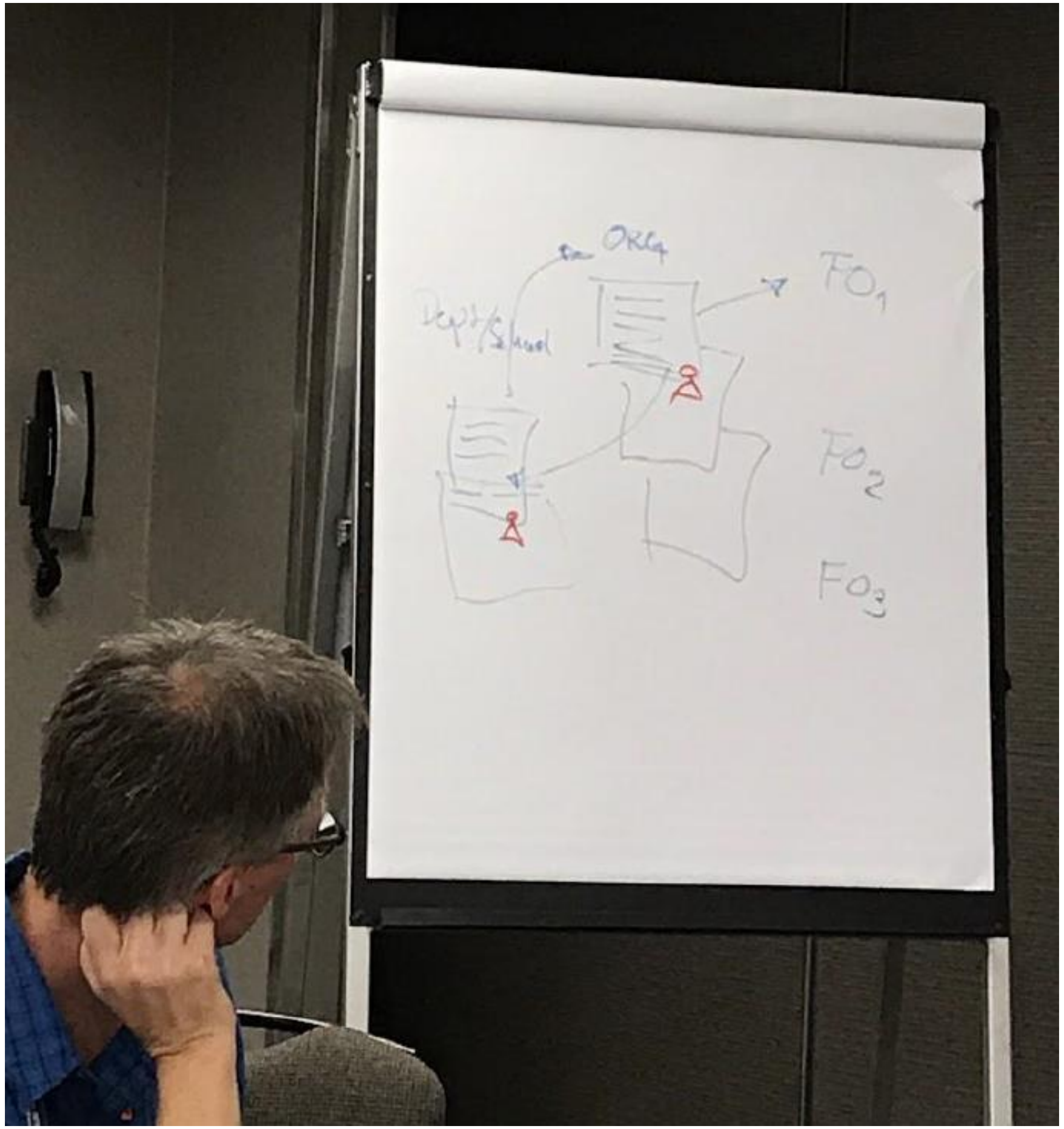
- identify specific objectives – *I2 TechEx*
- scope needs and requirements for R/E infrastructure OIDC Fed – *Prague EUGridPMA 42*
- verify compatibility of IGTF Assurance Profile framework for 'technology-agnosticity' with OpenID Providers (proxies) and RPs
- **test an OIDCFed scenario** ***e.g. starting with use cases: WLCG, RCauth.eu, ELIXIR/LS, EGI CheckIn, …***
- assess structure and needed meta-data in a 'trust anchor service',
  - how to address RPDNC
  - links it with (dynamic) client registration
- liaise with OIDC Fed efforts in AARC and GN*-*, and Roland Hedberg

OIDC Fed pilots

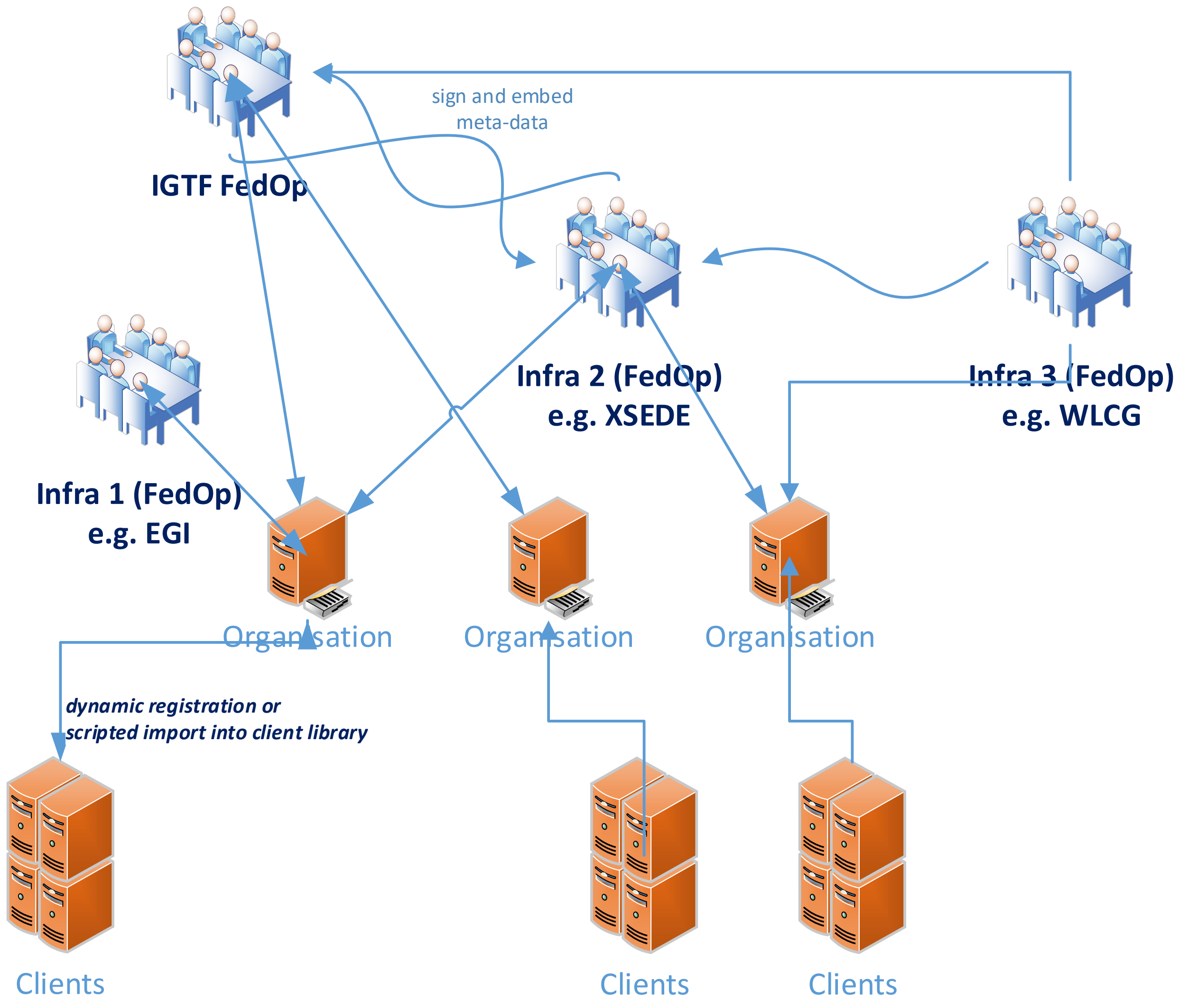
- Based on the spec by Roland Hedberg

- scoped to the RP + Proxy
  case is not very complex, actually
  Infrastructures can use trusty shortcuts that would be too costly at the general R&E scale

- leverage *existing policy and trust* framework
- 'pilot' RPs and proxies will be using scripting and glue to get integration with existing services, based on assessed trust framework
- we *can* leverage existing trust



Can we do without a single one to rule them all?



- today the RIs and EIs trust the IGTF trust anchors and
  may (but do rarely) add their own

- Can the 'federation' be the community and import a commonly trusted set?

- Can the IGTF allow devolved registration *provided* that the trusted organisations implement the same policy controls *Snctfi* and the proper *Assurance Profiles*?
  i.e. the IGTF runs an MDSS
  for the RPs and Proxies

For the benefit of Research Infras …

- IGTF membership process and *Snctfi* jointly give you the trust of Infra SPs (RPs)
- use peer-reviewed (self-)assessment as foundation of the ‘scientific process’ of trust
- technical details on how the IGTF FedOp will sign and distribute meta-data statements – subject to discussion at TIIME, AARC, and IGTF meetings
- new communities and (proxy) operators can join IGTF any time
  - there is no fee or something like that
  - but we request participation in the peer-review and assessment process …

Information sharing

Keeping in touch

- http://wiki.eugridpma.org/Main/OIDCFed
- oidcfed@igtf.net
(https://igtf.net/mailman/oidcfed)

but don’t forget everyone else!

- REFEDS, GEANT
- TIIME, TNC, TechEx, …

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

components of this work have been co-supported by:
the Dutch National e-Infrastructure coordinated by SURF,
EOSC-HUB – EOSC-hub receives funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 777536
AARC (2) – which has received funding from the European Union’s Horizon 2020 research and innovation programme under Grant Agreement No. 730941 (AARC2)

Thank you
Any Questions?

davidg@nikhef.nl

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).