IGTF
Interoperable Global Trust Federation
AP | EU | TAG

Building Trust and Security with AARC, IGTF, EOSC, & WISE

Enabling Communities through Trust, Identity, and Security in the Open Science era

David Groep
davidg@nikhef.nl

eugridpma Nikhef

part of the work programme of SURF - the Dutch National e-Infrastructure, GEANT 4-3 EnCo, EGI-ACE, and EOSC-Future

the work has received co-funding from the Horizon 2020 programme of the European Union

co-supported by Nikhef and the Dutch National e-Infrastructure coordinated by SURF

SURF

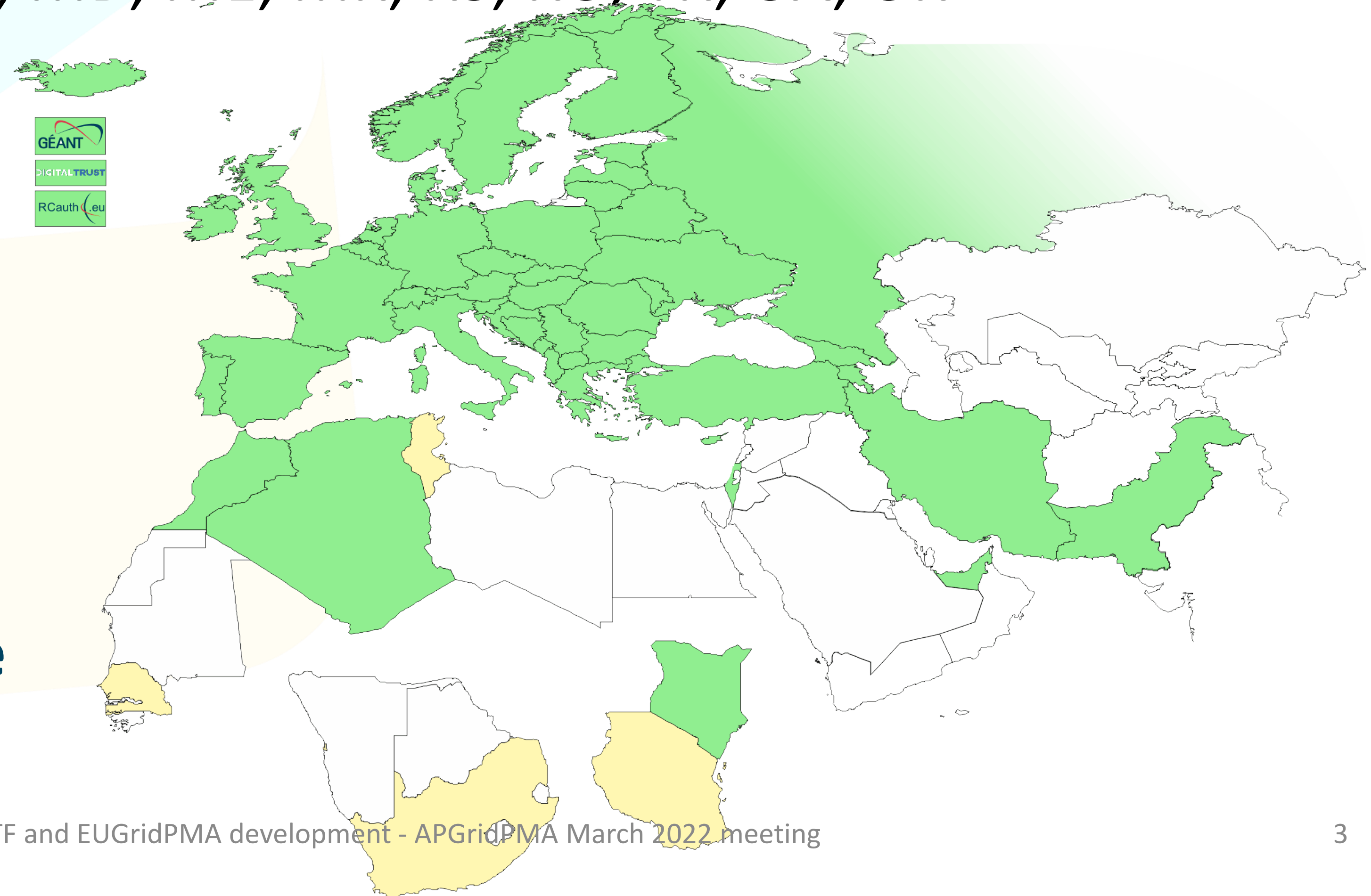
Meanwhile in the EUGridPMA+ …

- EUGridPMA constituency and profile developments
- European Open Science Cloud – Security Baseline
- Attribute Authority Operations guideline

- Simple highly-available services with anycast – and a stateful service
- Readiness and communications – the ‘SCCC-JWG’ and the IGTF RAT CC

IGTF EMEA area membership evolution

- Europe$^+$: GEANT TCS, and CZ, DE, DK(+FI+IS+NO+SE), FR, GR, HR, HU, NL, PL, PT, RO, SI, SK; AM, GE, MD, ME, MK, RS, RU, TR, UA, UK
- Middle East: AE, IR, PK
- Africa: DZ, KE, MA
- CERN, RCauth.eu, DigitalTrust (AE)

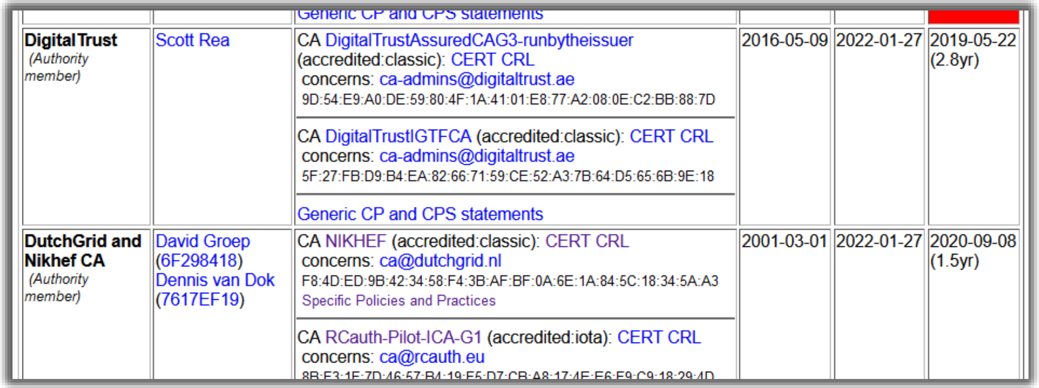


Emphasis on collaboration across the whole T&I space

Membership and other changes

- Identity providers: both reduction and growth
  - some migration to GEANT TCS is still ongoing *https://wiki.geant.org/display/TCSNT/TCS+Participants+Sectigo*
  - BCDR

- Self-audit review
  - Cosmin Nistor as review coordinator
  - Self-audits are slacking a bit – fewer CAs …



		Generic CP and CPS statements			🟥
DigitalTrust *(Authority member)*	Scott Rea	CA DigitalTrustAssuredCAG3-runbytheissuer (accredited:classic): CERT CRL concerns: ca-admins@digitaltrust.ae 9D:54:E9:A0:DE:59:80:4F:1A:41:01:E8:77:A2:08:0E:C2:BB:88:7D CA DigitalTrustIGTFCA (accredited:classic): CERT CRL concerns: ca-admins@digitaltrust.ae 5F:27:FB:D9:B4:EA:82:66:71:59:CE:52:A3:7B:64:D5:65:6B:9E:18 Generic CP and CPS statements	2016-05-09	2022-01-27	2019-05-22 (2.8yr)
DutchGrid and Nikhef CA *(Authority member)*	David Groep (6F298418) Dennis van Dok (7617EF19)	CA NIKHEF (accredited:classic): CERT CRL concerns: ca@dutchgrid.nl F8:4D:ED:9B:42:34:58:F4:3B:AF:BF:0A:6E:1A:84:5C:18:34:5A:A3 Specific Policies and Practices CA RCauth-Pilot-ICA-G1 (accredited:iota): CERT CRL concerns: ca@rcauth.eu 8B:F3:1F:7D:46:57:B4:19:F5:D7:CB:A8:17:4F:F6:F9:C9:18:29:4D	2001-03-01	2022-01-27	2020-09-08 (1.5yr)

- Next meeting in Garching, DE, May 23-25!

WLCG and server credentials study WG

- Increased use of automatic public cloud deployment (and at times lack of documentation) highlight the fact that in ‘conventional’ grid middleware server-trust and client-trust cannot be distinguished
- Similarly, while combined-assurance (DOGWOOD) is available for client-auth, there is no equivalent for server trust
- Although issues will change on introduction of ‘token-based’ access (which does distinguish client & channel trust), of limited help now

WLCG, with participants from the IGTF, set up a WG to study the issues
https://docs.google.com/document/d/1Sl0C_q-lGMCifChmFArHjsGzdnd-RM7O7jbpsGa8XRw

European Open Science Cloud

EOSC Security Baseline

Evolving the Policy Development Kit in WISE SCI

A SECURITY BASELINE
FOR DIVERSE INFRASTRUCTURES AND THE EOSC

European Open Science Cloud - Interconnecting communities

GÉANT

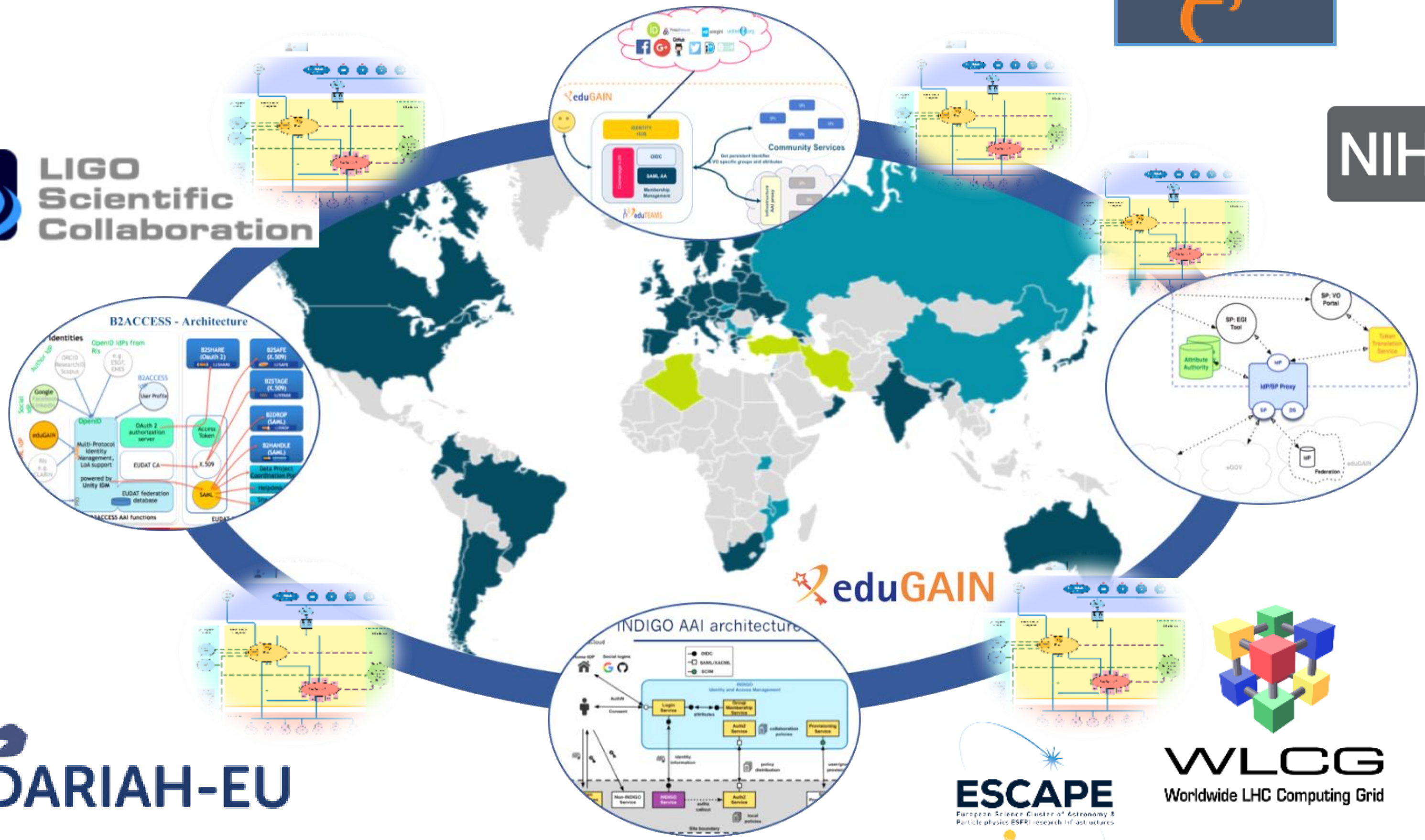
elixir

LSC LIGO Scientific Collaboration

NIH National Institutes of Health
Turning Discovery Into Health

EUDAT

egi



DARIAH-EU

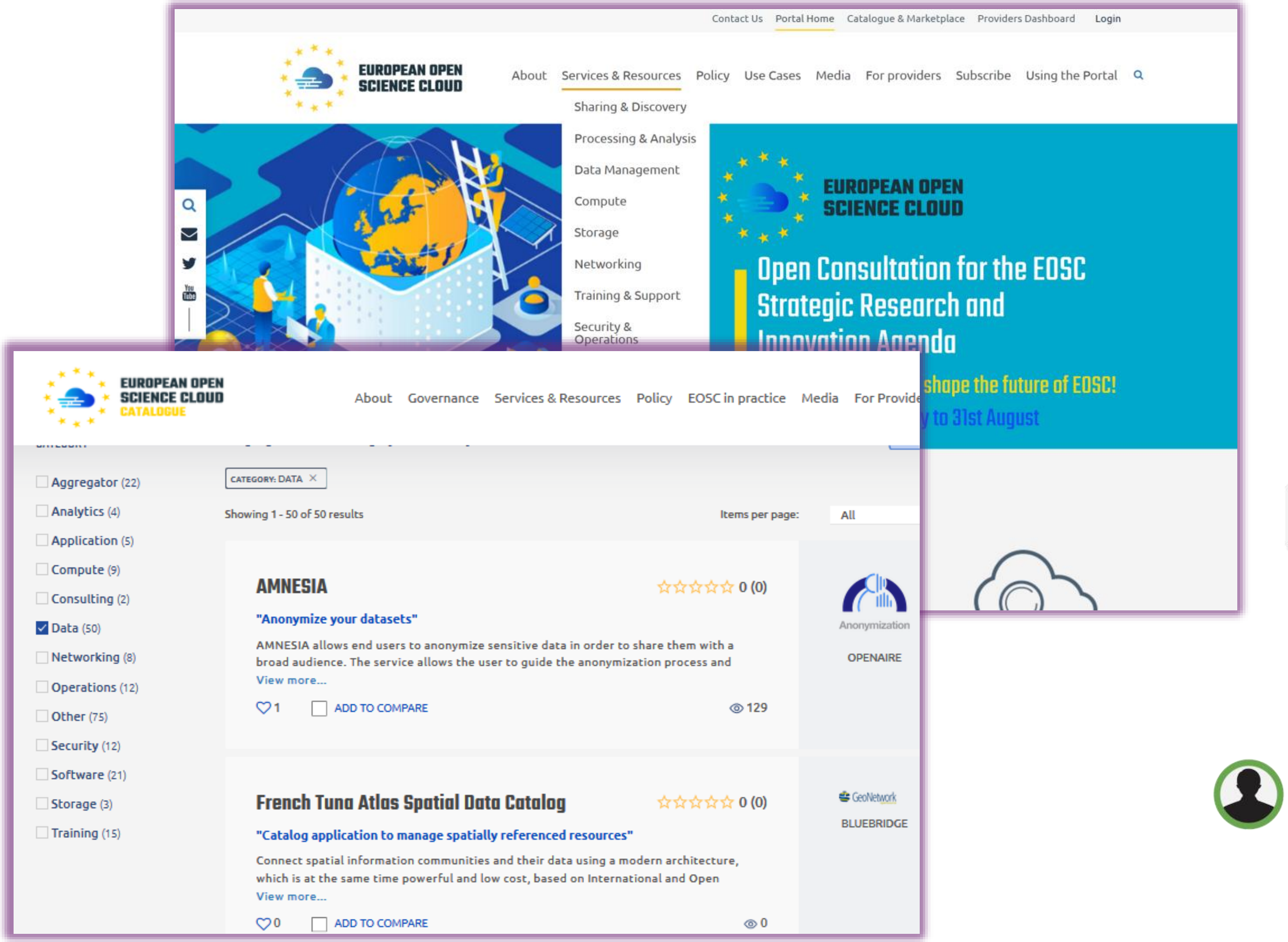
ESCAPE

WLCG
Worldwide LHC Computing Grid

INDIGO - DataCloud
Better Software for Better Science

https://aarc-community.org/about/aegis/

An ecosystem more than just the infrastructure



Contact Us | Portal Home | Catalogue & Marketplace | Providers Dashboard | Login

EUROPEAN OPEN SCIENCE CLOUD

About | Services & Resources | Policy | Use Cases | Media | For providers | Subscribe | Using the Portal

- Sharing & Discovery
- Processing & Analysis
- Data Management
- Compute
- Storage
- Networking
- Training & Support
- Security & Operations

EUROPEAN OPEN SCIENCE CLOUD

Open Consultation for the EOSC Strategic Research and Innovation Agenda

shape the future of EOSC!

to 31st August

EUROPEAN OPEN SCIENCE CLOUD CATALOGUE

About | Governance | Services & Resources | Policy | EOSC in practice | Media | For Provide

- □ Aggregator (22)
- □ Analytics (4)
- □ Application (5)
- □ Compute (9)
- □ Consulting (2)
- ☑ Data (50)
- □ Networking (8)
- □ Operations (12)
- □ Other (75)
- □ Security (12)
- □ Software (21)
- □ Storage (3)
- □ Training (15)

CATEGORY: DATA ×

Showing 1 - 50 of 50 results

Items per page: All

AMNESIA ☆☆☆☆☆ 0 (0)

"Anonymize your datasets"

AMNESIA allows end users to anonymize sensitive data in order to share them with a broad audience. The service allows the user to guide the anonymization process and

View more...

♡1 □ ADD TO COMPARE 129

Anonymization

OPENAIRE

French Tuna Atlas Spatial Data Catalog ☆☆☆☆☆ 0 (0)

"Catalog application to manage spatially referenced resources"

Connect spatial information communities and their data using a modern architecture, which is at the same time powerful and low cost, based on International and Open

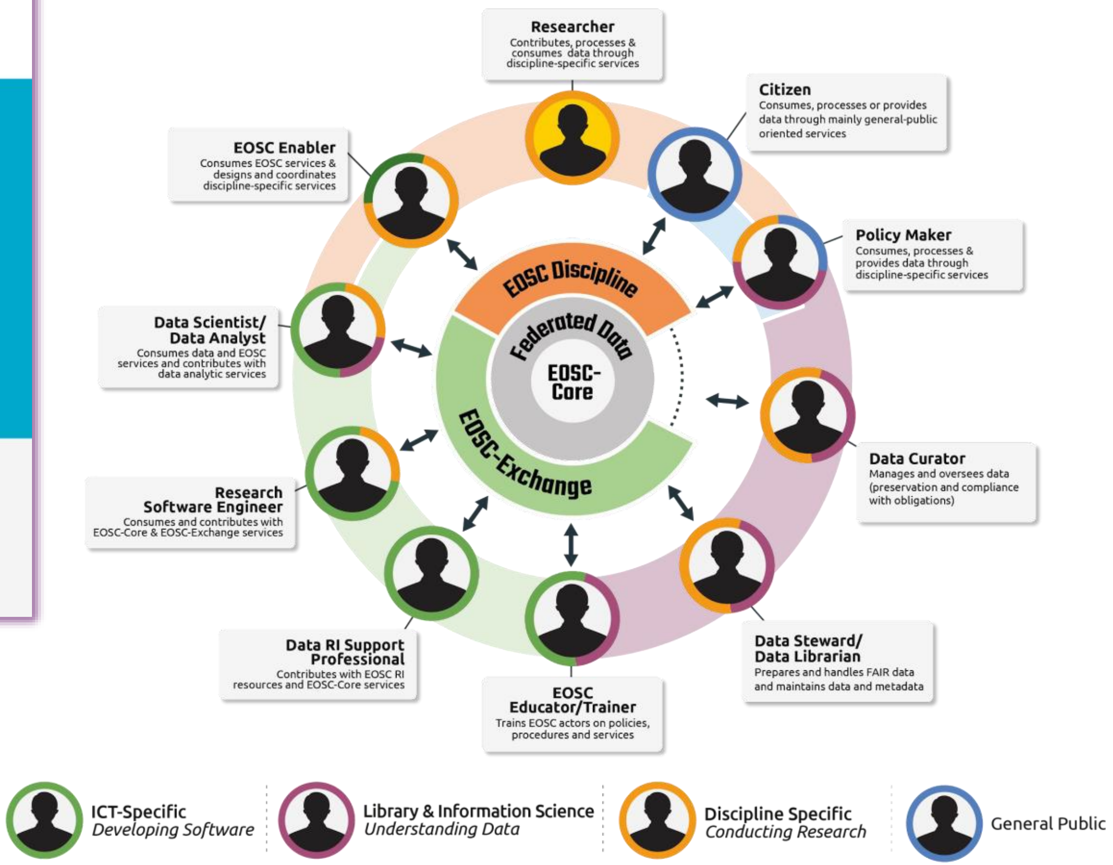
View more...

♡0 □ ADD TO COMPARE 0

GeoNetwork

BLUEBRIDGE

EOSC Portal (https://www.eosc-portal.eu/) – as built by EOSChub



Researcher Contributes, processes & consumes data through discipline-specific services

Citizen Consumes, processes or provides data through mainly general-public oriented services

EOSC Enabler Consumes EOSC services & designs and coordinates discipline-specific services

Policy Maker Consumes, processes & provides data through discipline-specific services

Data Scientist/ Data Analyst Consumes data and EOSC services and contributes with data analytic services

Data Curator Manages and oversees data (preservation and compliance with obligations)

Research Software Engineer Consumes and contributes with EOSC-Core & EOSC-Exchange services

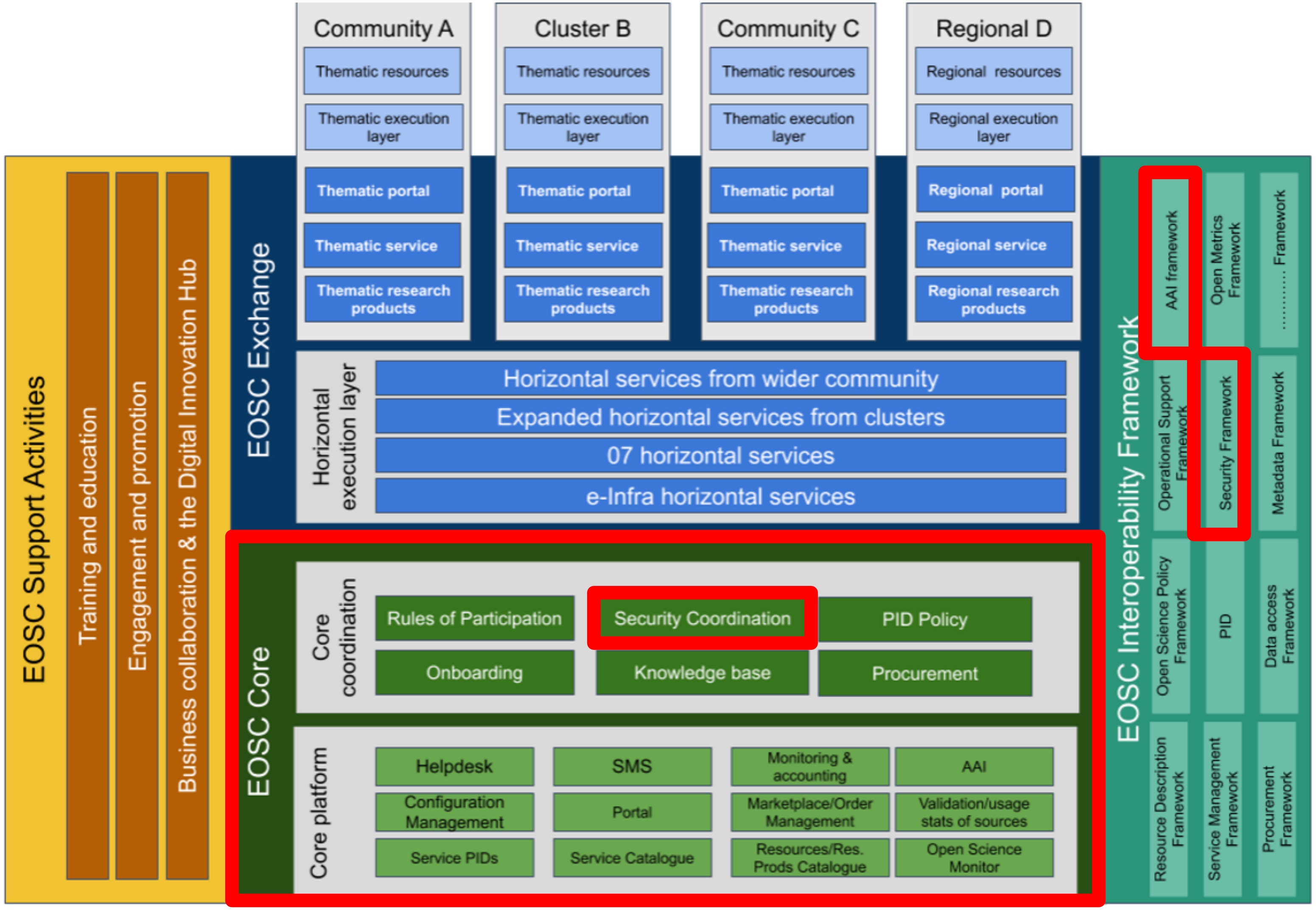
Data RI Support Professional Contributes with EOSC RI resources and EOSC-Core services

EOSC Educator/Trainer Trains EOSC actors on policies, procedures and services

Data Steward/ Data Librarian Prepares and handles FAIR data and maintains data and metadata

circle diagram: from Ignacio Blanquer's ISGC 2022 keynote
Digital Skills for FAIR and open science doi.org/10.2777/59065

The EOSC ecosystem – core and an ‘exchange’



Community A
Thematic resources
Thematic execution layer
Thematic portal
Thematic service
Thematic research products

Cluster B
Thematic resources
Thematic execution layer
Thematic portal
Thematic service
Thematic research products

Community C
Thematic resources
Thematic execution layer
Thematic portal
Thematic service
Thematic research products

Regional D
Regional resources
Regional execution layer
Regional portal
Regional service
Regional research products

EOSC Support Activities
Training and education
Engagement and promotion
Business collaboration & the Digital Innovation Hub

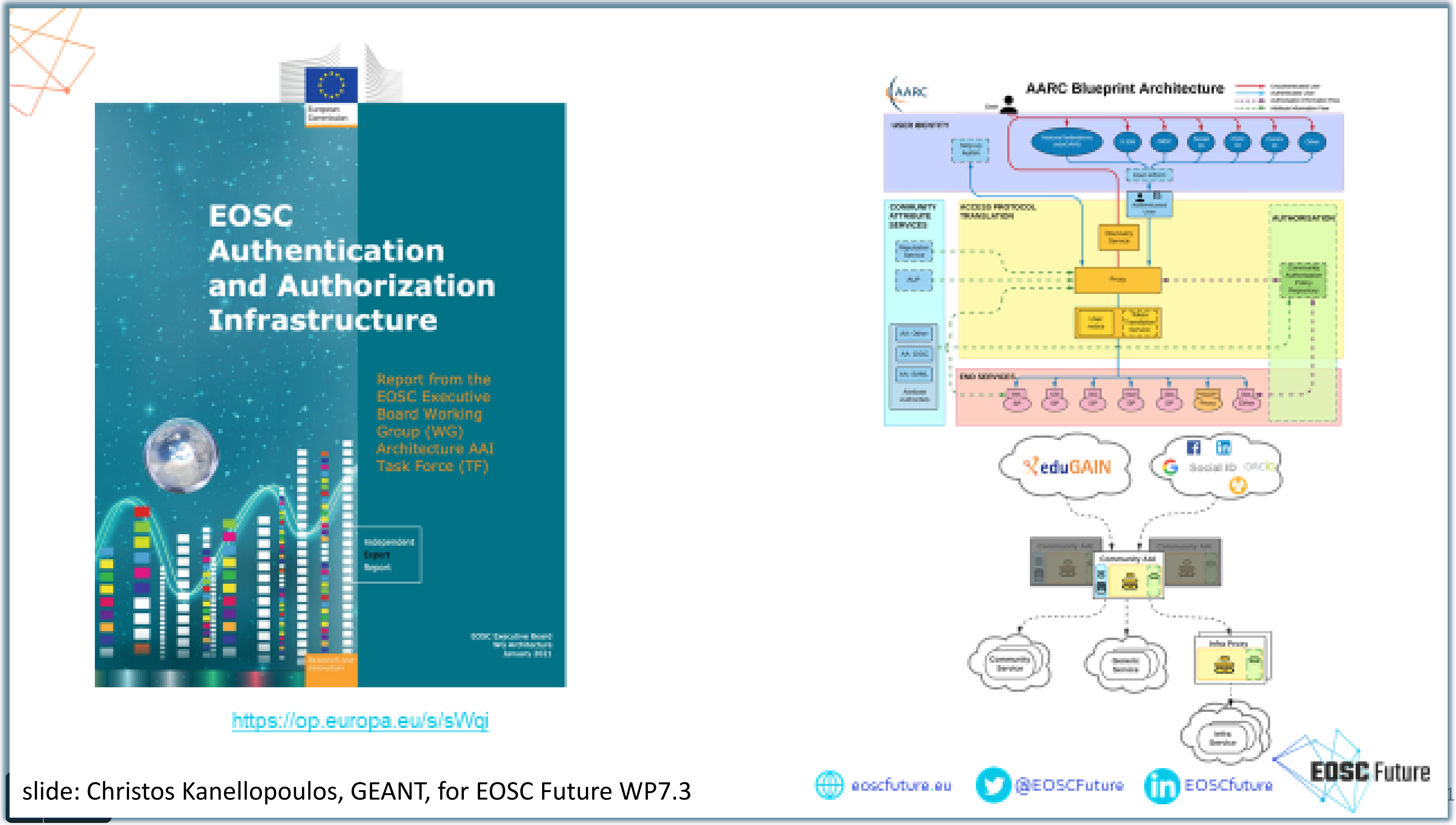
EOSC Exchange
Horizontal execution layer
Horizontal services from wider community
Expanded horizontal services from clusters
07 horizontal services
e-Infra horizontal services

EOSC Core
Core coordination
Rules of Participation
Security Coordination
PID Policy
Onboarding
Knowledge base
Procurement

Core platform
Helpdesk
SMS
Monitoring & accounting
AAI
Configuration Management
Portal
Marketplace/Order Management
Validation/usage stats of sources
Service PIDs
Service Catalogue
Resources/Res. Prods Catalogue
Open Science Monitor

EOSC Interoperability Framework
AAI framework
Open Metrics Framework
………… Framework
Operational Support Framework
Security Framework
Metadata Framework
Open Science Policy Framework
PID
Data access Framework
Resource Description Framework
Service Management Framework
Procurement Framework

EOSC Authentication and Authorization Infrastructure



EOSC Authentication and Authorization Infrastructure

Report from the EOSC Executive Board Working Group (WG) Architecture AAI Task Force (TF)

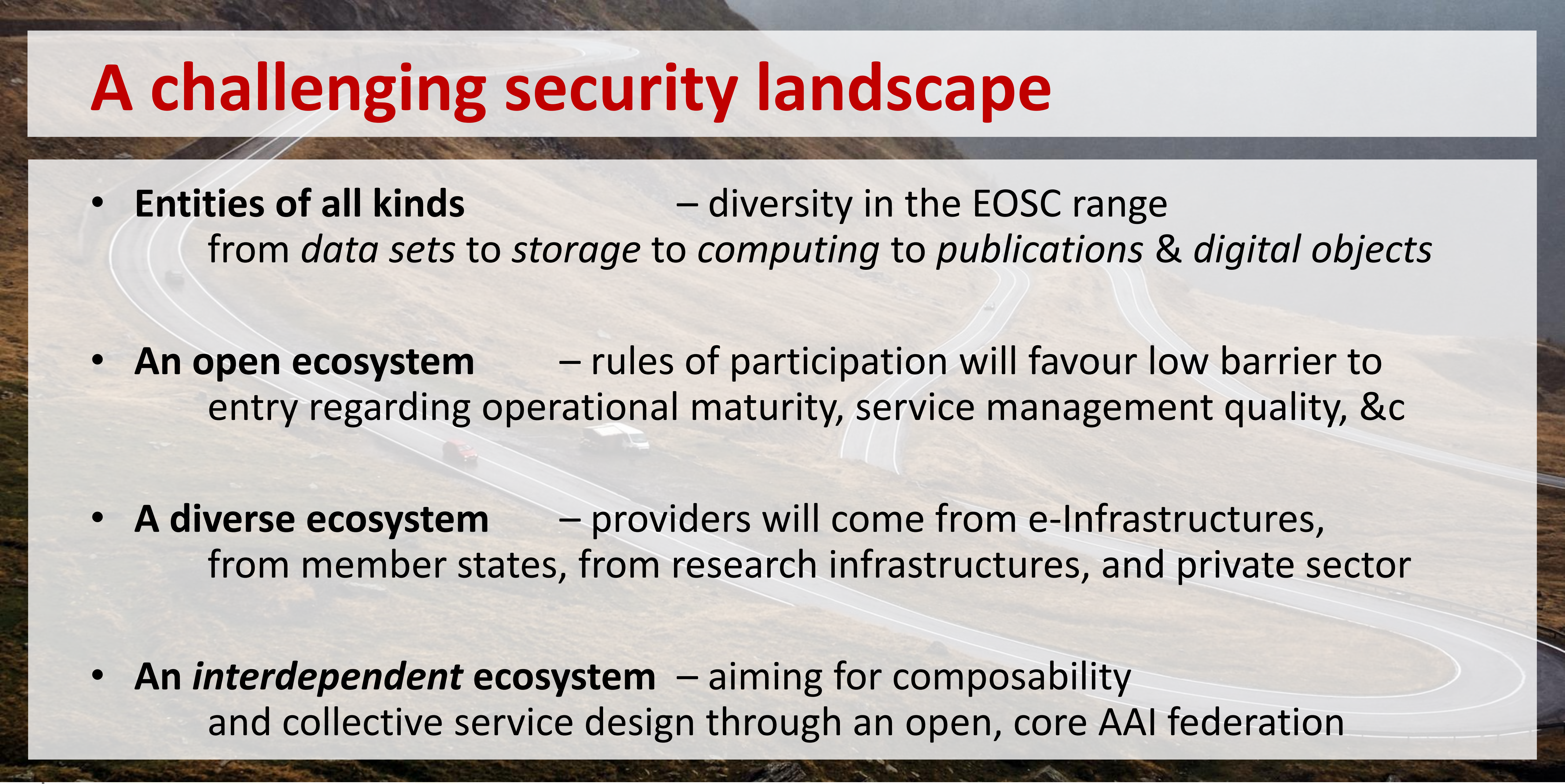
Independent Expert Report

https://op.europa.eu/s/sWqi

eoscfuture.eu @EOSCFuture EOSCfuture

EOSC Future

slide: Christos Kanellopoulos, GEANT, for EOSC Future WP7.3



A challenging security landscape

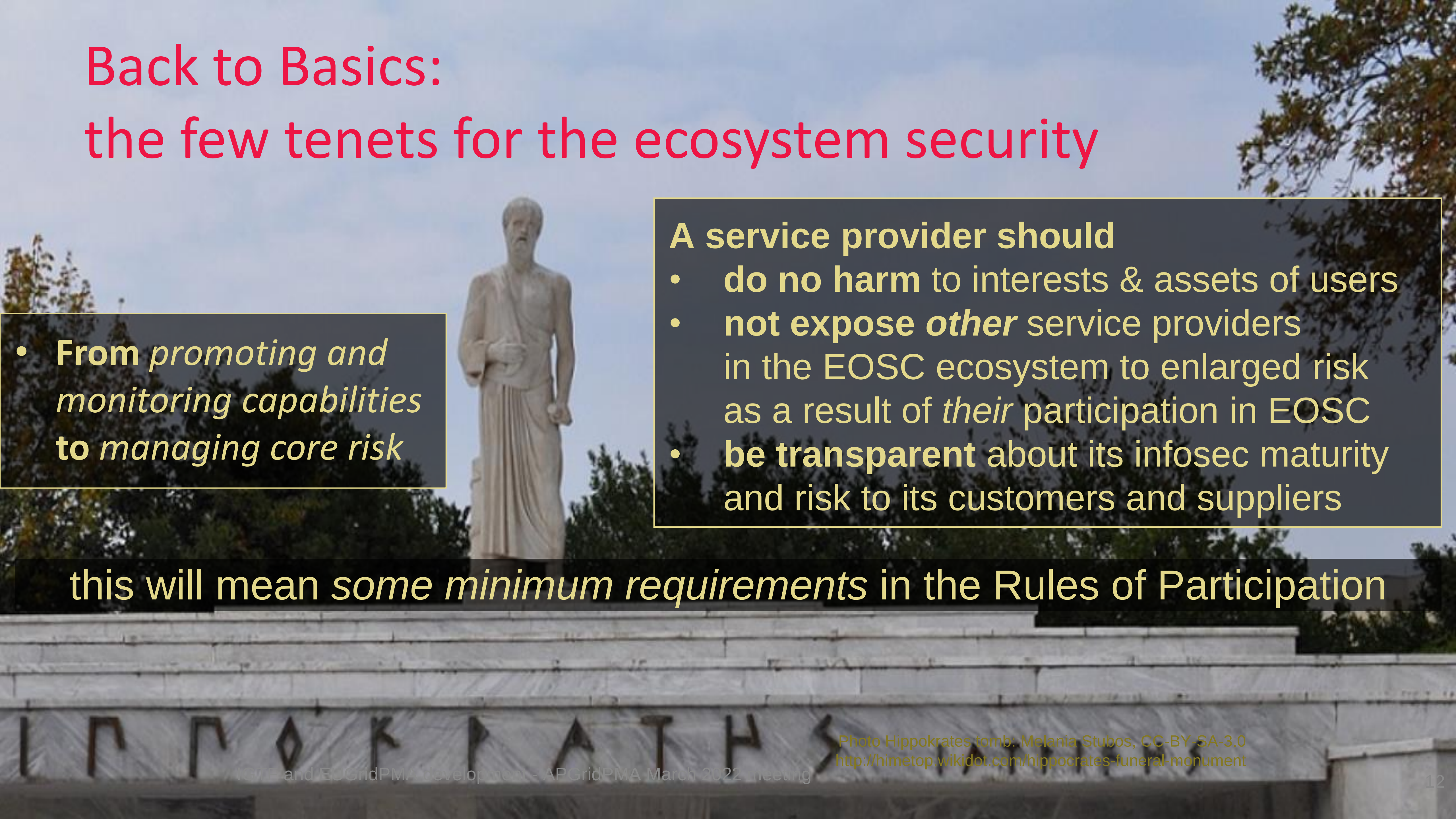
- **Entities of all kinds** – diversity in the EOSC range
  from *data sets* to *storage* to *computing* to *publications* & *digital objects*

- **An open ecosystem** – rules of participation will favour low barrier to
  entry regarding operational maturity, service management quality, &c

- **A diverse ecosystem** – providers will come from e-Infrastructures,
  from member states, from research infrastructures, and private sector

- **An *interdependent* ecosystem** – aiming for composability
  and collective service design through an open, core AAI federation

Back to Basics:
the few tenets for the ecosystem security



- **From** *promoting and monitoring capabilities* **to** *managing core risk*

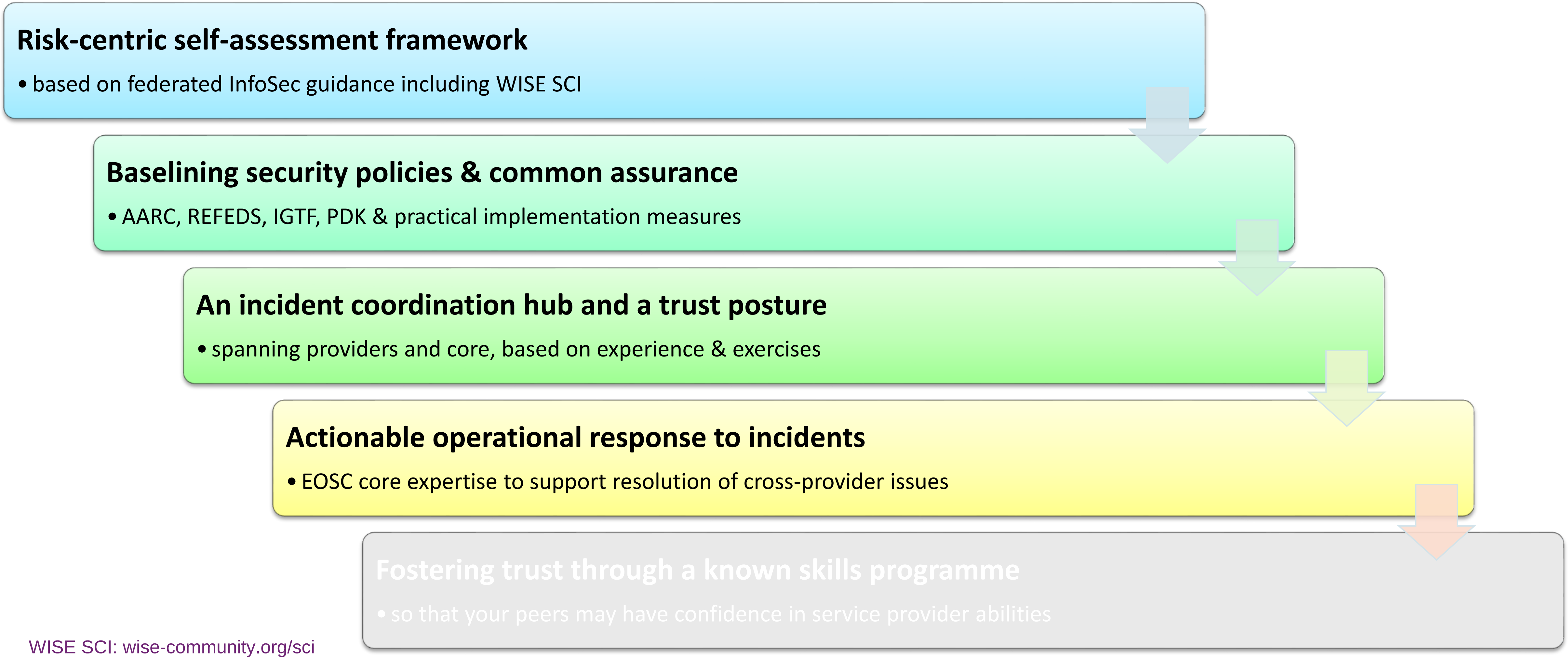
A service provider should

- **do no harm** to interests & assets of users
- **not expose *other*** service providers in the EOSC ecosystem to enlarged risk as a result of *their* participation in EOSC
- **be transparent** about its infosec maturity and risk to its customers and suppliers

this will mean *some minimum requirements* in the Rules of Participation

Photo Hippokrates tomb: Melania Stubos, CC-BY-SA-3.0
http://himetop.wikidot.com/hippocrates-funeral-monument

Making the EOSC a trusted place



Risk-centric self-assessment framework

- based on federated InfoSec guidance including WISE SCI

Baselining security policies & common assurance

- AARC, REFEDS, IGTF, PDK & practical implementation measures

An incident coordination hub and a trust posture

- spanning providers and core, based on experience & exercises

Actionable operational response to incidents

- EOSC core expertise to support resolution of cross-provider issues

Fostering trust through a known skills programme

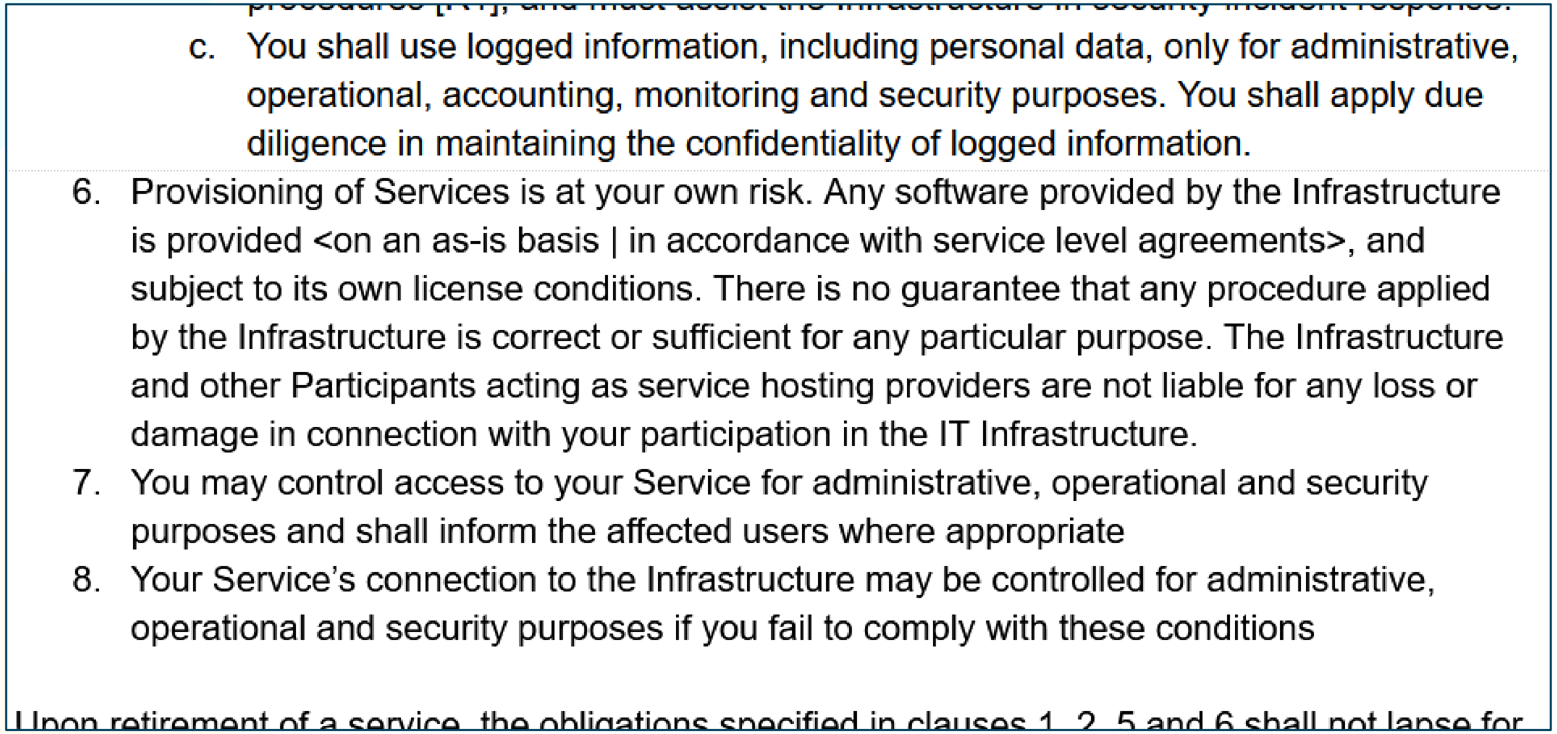
- so that your peers may have confidence in service provider abilities

WISE SCI: wise-community.org/sci
AARC&c: aarc-community.org, refeds.org, igtf.net
PDK: aarc-community.org/policies/policy-development-kit

From an infrastructure to an ecosystem view

Original AARC PDK version of “Service Operations” was rather prescriptive

- includes ‘service-internal’ operations and software
- embedded in the PDK document suite: does not work well as a ‘stand-alone’ document
- has built-in assumption of coherent and coordinated single infrastructure



procedures [R1], and must assist the Infrastructure in security incident response.

c. You shall use logged information, including personal data, only for administrative, operational, accounting, monitoring and security purposes. You shall apply due diligence in maintaining the confidentiality of logged information.

6. Provisioning of Services is at your own risk. Any software provided by the Infrastructure is provided <on an as-is basis | in accordance with service level agreements>, and subject to its own license conditions. There is no guarantee that any procedure applied by the Infrastructure is correct or sufficient for any particular purpose. The Infrastructure and other Participants acting as service hosting providers are not liable for any loss or damage in connection with your participation in the IT Infrastructure.
7. You may control access to your Service for administrative, operational and security purposes and shall inform the affected users where appropriate
8. Your Service’s connection to the Infrastructure may be controlled for administrative, operational and security purposes if you fail to comply with these conditions

Upon retirement of a service, the obligations specified in clauses 1, 2, 5 and 6 shall not lapse for

Evolving to the EOSC Security Baseline

In the EOSC ecosystem, more of the original assumptions no longer hold

- services provided are less coherent, and much more autonomous then every before

- need to accommodate providers with varying maturity levels - and different intentions!

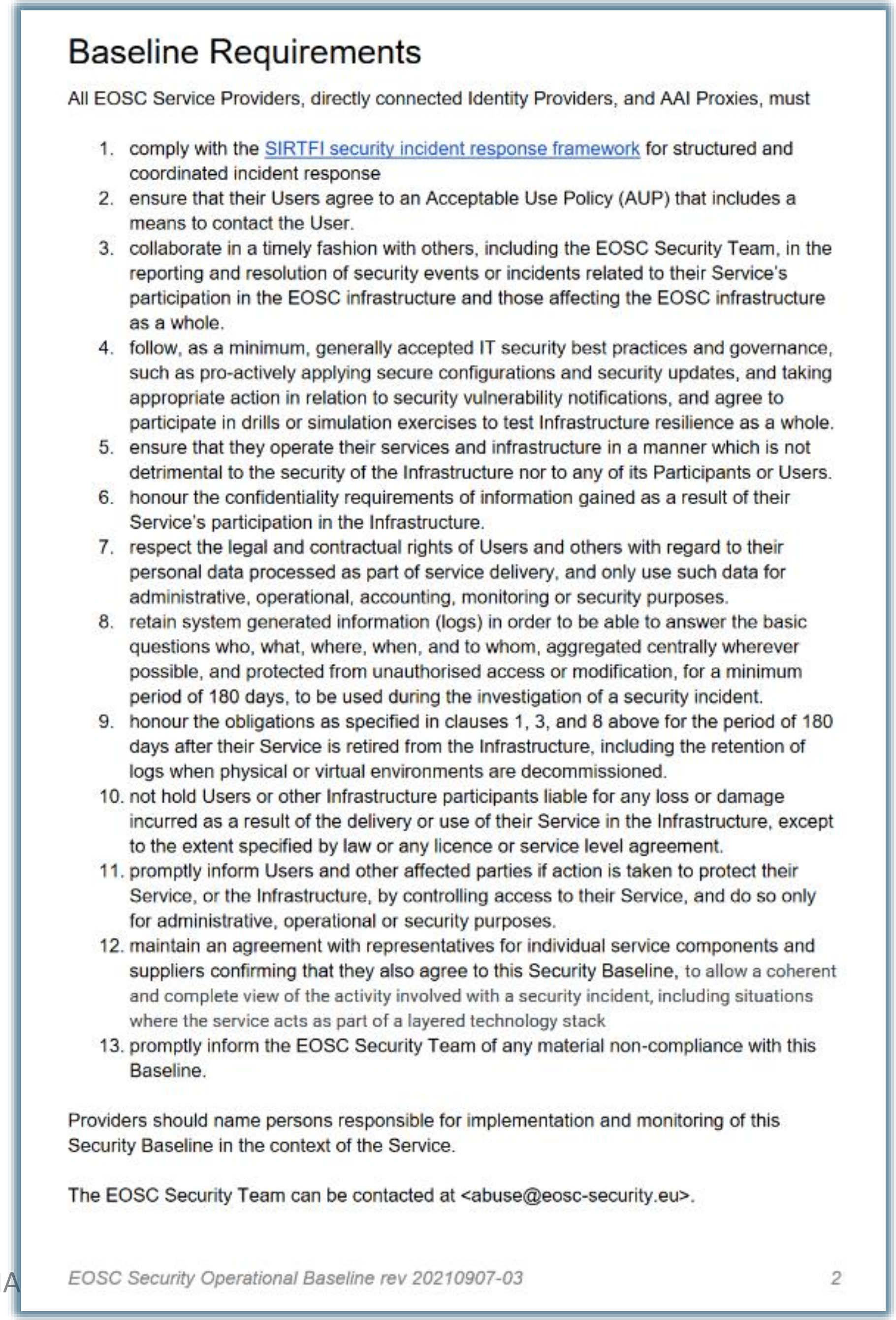
Baseline Process

Co-development of EOSC Future & AARC Policy Community

- version based on UK-IRIS evolution of the AARC PDK
- specifically geared towards the looser EOSC ecosystem
- mindful of urgent need for collective coherent response

AARC Policy team consultation -> AEGIS -> EOSC

- 13 itemised points - https://edu.nl/avfv4
- complemented by an 'FAQ' with guidance and refs
  (no new standards, there is enough good stuff out there)
- leverages *Sirtfi* framework
- connects to the Core Security Team



Baseline Requirements

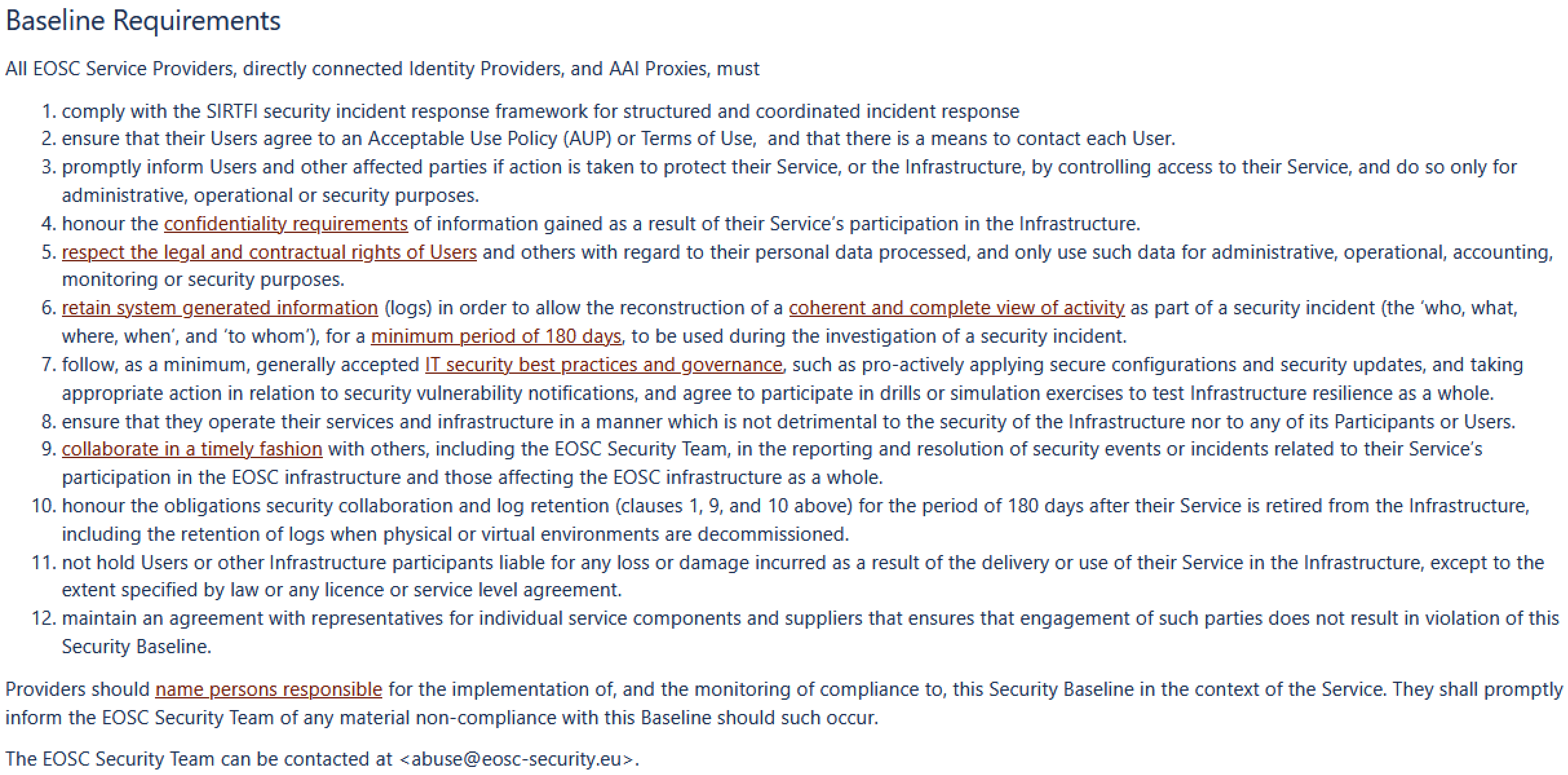
All EOSC Service Providers, directly connected Identity Providers, and AAI Proxies, must

1. comply with the [SIRTFI security incident response framework]() for structured and coordinated incident response
2. ensure that their Users agree to an Acceptable Use Policy (AUP) that includes a means to contact the User.
3. collaborate in a timely fashion with others, including the EOSC Security Team, in the reporting and resolution of security events or incidents related to their Service's participation in the EOSC infrastructure and those affecting the EOSC infrastructure as a whole.
4. follow, as a minimum, generally accepted IT security best practices and governance, such as pro-actively applying secure configurations and security updates, and taking appropriate action in relation to security vulnerability notifications, and agree to participate in drills or simulation exercises to test Infrastructure resilience as a whole.
5. ensure that they operate their services and infrastructure in a manner which is not detrimental to the security of the Infrastructure nor to any of its Participants or Users.
6. honour the confidentiality requirements of information gained as a result of their Service's participation in the Infrastructure.
7. respect the legal and contractual rights of Users and others with regard to their personal data processed as part of service delivery, and only use such data for administrative, operational, accounting, monitoring or security purposes.
8. retain system generated information (logs) in order to be able to answer the basic questions who, what, where, when, and to whom, aggregated centrally wherever possible, and protected from unauthorised access or modification, for a minimum period of 180 days, to be used during the investigation of a security incident.
9. honour the obligations as specified in clauses 1, 3, and 8 above for the period of 180 days after their Service is retired from the Infrastructure, including the retention of logs when physical or virtual environments are decommissioned.
10. not hold Users or other Infrastructure participants liable for any loss or damage incurred as a result of the delivery or use of their Service in the Infrastructure, except to the extent specified by law or any licence or service level agreement.
11. promptly inform Users and other affected parties if action is taken to protect their Service, or the Infrastructure, by controlling access to their Service, and do so only for administrative, operational or security purposes.
12. maintain an agreement with representatives for individual service components and suppliers confirming that they also agree to this Security Baseline, to allow a coherent and complete view of the activity involved with a security incident, including situations where the service acts as part of a layered technology stack
13. promptly inform the EOSC Security Team of any material non-compliance with this Baseline.

Providers should name persons responsible for implementation and monitoring of this Security Baseline in the context of the Service.

The EOSC Security Team can be contacted at <abuse@eosc-security.eu>.

EOSC Security Operational Baseline rev 20210907-03 2



Baseline Requirements

All EOSC Service Providers, directly connected Identity Providers, and AAI Proxies, must

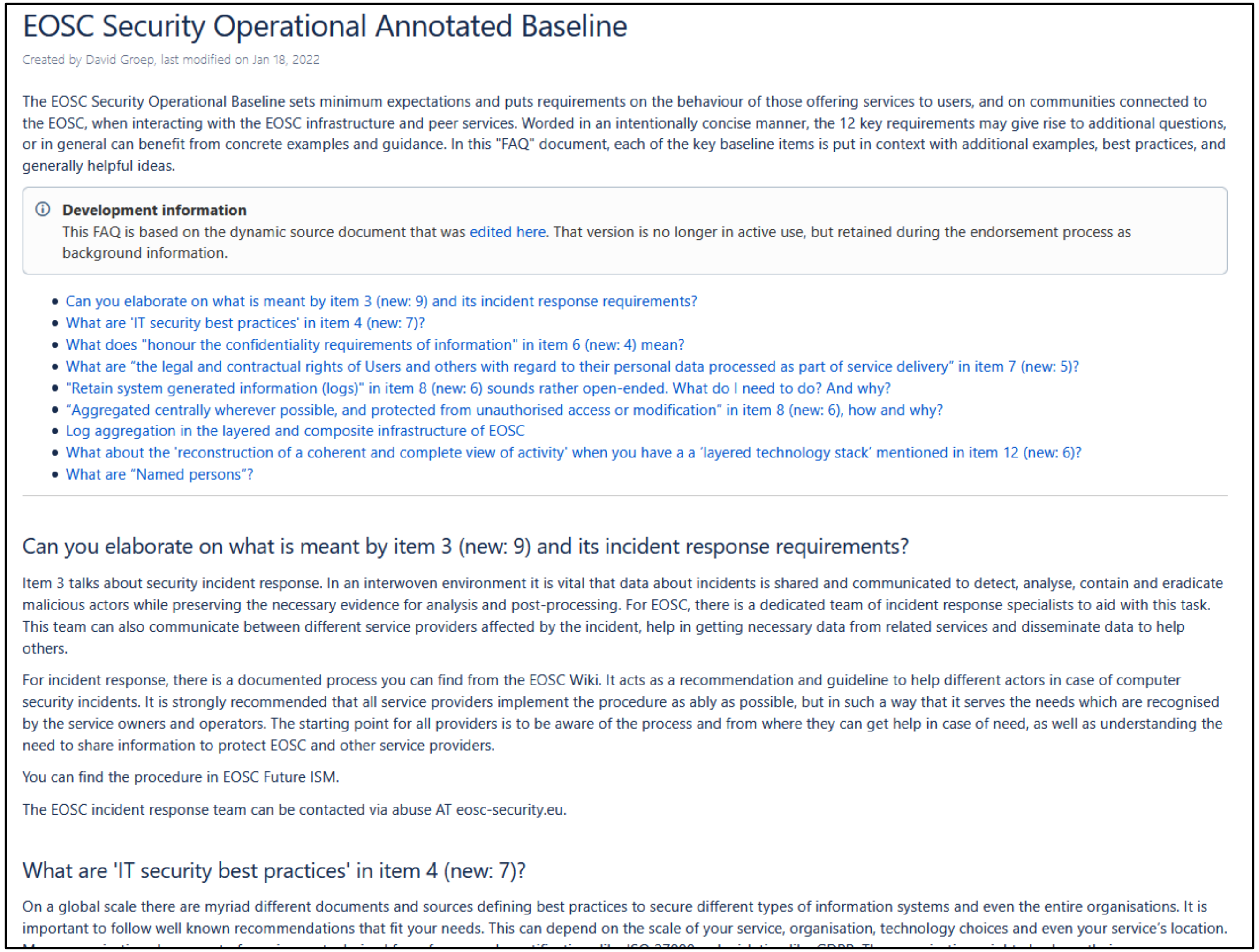
1. comply with the SIRTFI security incident response framework for structured and coordinated incident response
2. ensure that their Users agree to an Acceptable Use Policy (AUP) or Terms of Use, and that there is a means to contact each User.
3. promptly inform Users and other affected parties if action is taken to protect their Service, or the Infrastructure, by controlling access to their Service, and do so only for administrative, operational or security purposes.
4. honour the confidentiality requirements of information gained as a result of their Service's participation in the Infrastructure.
5. respect the legal and contractual rights of Users and others with regard to their personal data processed, and only use such data for administrative, operational, accounting, monitoring or security purposes.
6. retain system generated information (logs) in order to allow the reconstruction of a coherent and complete view of activity as part of a security incident (the 'who, what, where, when', and 'to whom'), for a minimum period of 180 days, to be used during the investigation of a security incident.
7. follow, as a minimum, generally accepted IT security best practices and governance, such as pro-actively applying secure configurations and security updates, and taking appropriate action in relation to security vulnerability notifications, and agree to participate in drills or simulation exercises to test Infrastructure resilience as a whole.
8. ensure that they operate their services and infrastructure in a manner which is not detrimental to the security of the Infrastructure nor to any of its Participants or Users.
9. collaborate in a timely fashion with others, including the EOSC Security Team, in the reporting and resolution of security events or incidents related to their Service's participation in the EOSC infrastructure and those affecting the EOSC infrastructure as a whole.
10. honour the obligations security collaboration and log retention (clauses 1, 9, and 10 above) for the period of 180 days after their Service is retired from the Infrastructure, including the retention of logs when physical or virtual environments are decommissioned.
11. not hold Users or other Infrastructure participants liable for any loss or damage incurred as a result of the delivery or use of their Service in the Infrastructure, except to the extent specified by law or any licence or service level agreement.
12. maintain an agreement with representatives for individual service components and suppliers that ensures that engagement of such parties does not result in violation of this Security Baseline.

Providers should name persons responsible for the implementation of, and the monitoring of compliance to, this Security Baseline in the context of the Service. They shall promptly inform the EOSC Security Team of any material non-compliance with this Baseline should such occur.

The EOSC Security Team can be contacted at <abuse@eosc-security.eu>.

https://wiki.eoscfuture.eu/display/EOSCSMS/EOSC+Security+Operational+Baseline

But an FAQ is almost mandatory



EOSC Security Operational Annotated Baseline

Created by David Groep, last modified on Jan 18, 2022

The EOSC Security Operational Baseline sets minimum expectations and puts requirements on the behaviour of those offering services to users, and on communities connected to the EOSC, when interacting with the EOSC infrastructure and peer services. Worded in an intentionally concise manner, the 12 key requirements may give rise to additional questions, or in general can benefit from concrete examples and guidance. In this "FAQ" document, each of the key baseline items is put in context with additional examples, best practices, and generally helpful ideas.

ⓘ **Development information**
This FAQ is based on the dynamic source document that was edited here. That version is no longer in active use, but retained during the endorsement process as background information.

- Can you elaborate on what is meant by item 3 (new: 9) and its incident response requirements?
- What are 'IT security best practices' in item 4 (new: 7)?
- What does "honour the confidentiality requirements of information" in item 6 (new: 4) mean?
- What are "the legal and contractual rights of Users and others with regard to their personal data processed as part of service delivery" in item 7 (new: 5)?
- "Retain system generated information (logs)" in item 8 (new: 6) sounds rather open-ended. What do I need to do? And why?
- "Aggregated centrally wherever possible, and protected from unauthorised access or modification" in item 8 (new: 6), how and why?
- Log aggregation in the layered and composite infrastructure of EOSC
- What about the 'reconstruction of a coherent and complete view of activity' when you have a a 'layered technology stack' mentioned in item 12 (new: 6)?
- What are "Named persons"?

Can you elaborate on what is meant by item 3 (new: 9) and its incident response requirements?

Item 3 talks about security incident response. In an interwoven environment it is vital that data about incidents is shared and communicated to detect, analyse, contain and eradicate malicious actors while preserving the necessary evidence for analysis and post-processing. For EOSC, there is a dedicated team of incident response specialists to aid with this task. This team can also communicate between different service providers affected by the incident, help in getting necessary data from related services and disseminate data to help others.

For incident response, there is a documented process you can find from the EOSC Wiki. It acts as a recommendation and guideline to help different actors in case of computer security incidents. It is strongly recommended that all service providers implement the procedure as ably as possible, but in such a way that it serves the needs which are recognised by the service owners and operators. The starting point for all providers is to be aware of the process and from where they can get help in case of need, as well as understanding the need to share information to protect EOSC and other service providers.

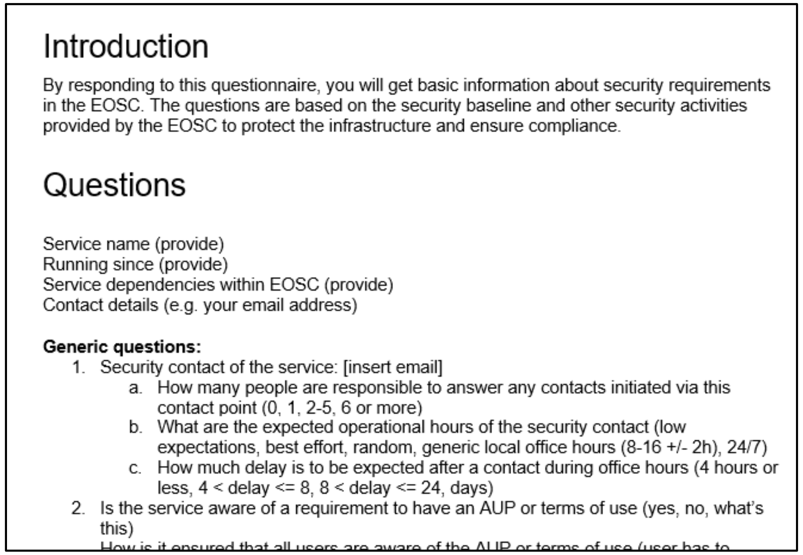
You can find the procedure in EOSC Future ISM.

The EOSC incident response team can be contacted via abuse AT eosc-security.eu.

What are 'IT security best practices' in item 4 (new: 7)?

On a global scale there are myriad different documents and sources defining best practices to secure different types of information systems and even the entire organisations. It is important to follow well known recommendations that fit your needs. This can depend on the scale of your service, organisation, technology choices and even your service's location.

and a way to both get the required information out of providers, gauge maturity, and raise awareness …



Introduction

By responding to this questionnaire, you will get basic information about security requirements in the EOSC. The questions are based on the security baseline and other security activities provided by the EOSC to protect the infrastructure and ensure compliance.

Questions

Service name (provide)
Running since (provide)
Service dependencies within EOSC (provide)
Contact details (e.g. your email address)

Generic questions:

1. Security contact of the service: [insert email]
   a. How many people are responsible to answer any contacts initiated via this contact point (0, 1, 2-5, 6 or more)
   b. What are the expected operational hours of the security contact (low expectations, best effort, random, generic local office hours (8-16 +/- 2h), 24/7)
   c. How much delay is to be expected after a contact during office hours (4 hours or less, 4 < delay <= 8, 8 < delay <= 24, days)
2. Is the service aware of a requirement to have an AUP or terms of use (yes, no, what's this)
   How is it ensured that all users are aware of the AUP or terms of use (user has to

Inspirational also for evolving the policy development kit

- Join the
  WISE SCI periodic meetings on Mondays (biweekly)

AARC-G071

IGTF AAOPS (https://www.eugridpma.org/guidelines/aaops/)

ATTRIBUTE AUTHORITY OPERATIONAL SECURITY

Taking proper care of trust sources

Protections for (IGTF) identity providers are known and documented

- RFC3647
- IGTF Guidelines
- Technical profiles

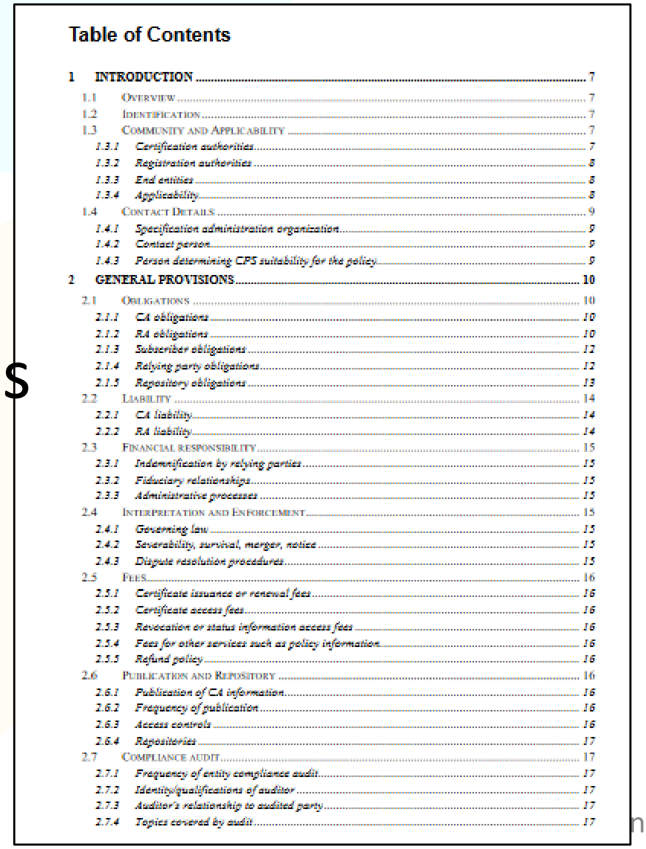
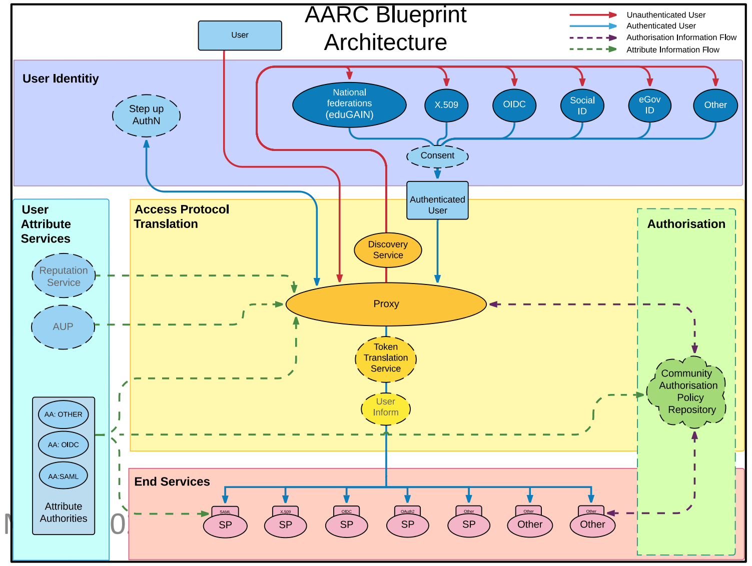


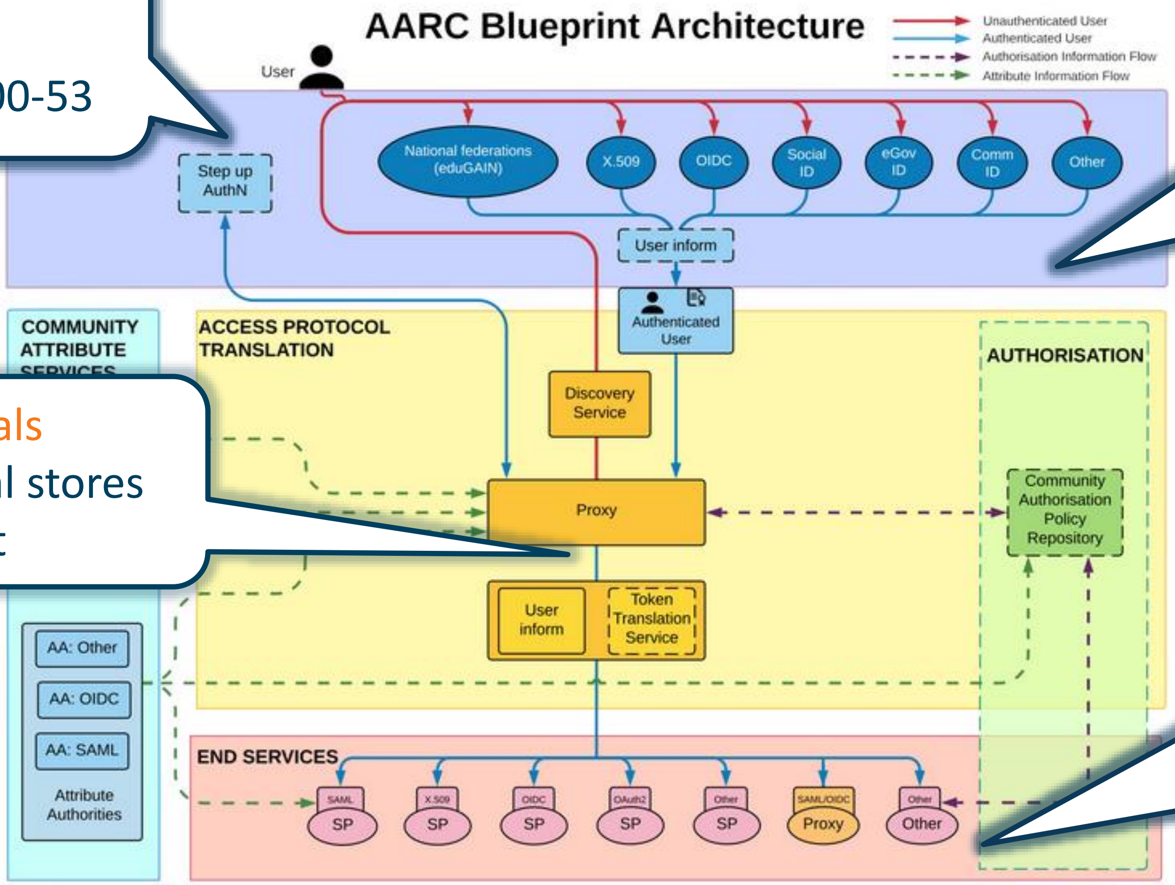
Table of Contents

The AAI relies also on other attribute sources, and on the hubs & AARC Proxies

- only generic guidance
- proxies fully hide ID source



Operational guideline landscape for - proxy or source - AAI components



RFC6238/4226
FIPS140
NISTSP800-53

Authentication/identity sources
Sirtfi
(eduGAIN) baselining, RAF
IGTF AP Profiles
NIST SP800-63
eduGAIN sec. team workflow

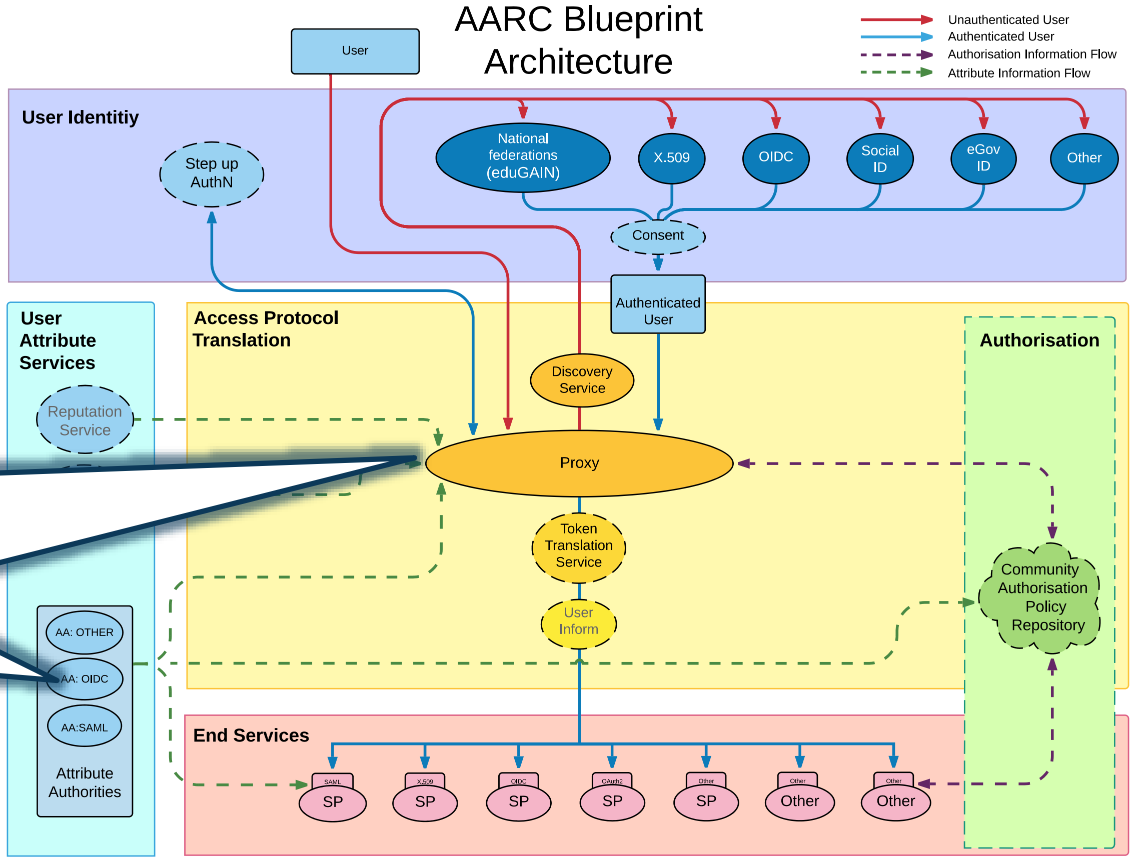
Ephemeral credentials
- trusted credential stores
- protection at rest

Service provider operations
ISO27k
Sirtfi
Infrastructure response plans

Operational security focus in the BPA: beyond just the IdPs

Community membership management directories and attribute authorities

- integrity of membership
- identification, naming and traceability
- site and service security
- protection on the network
- assertion integrity

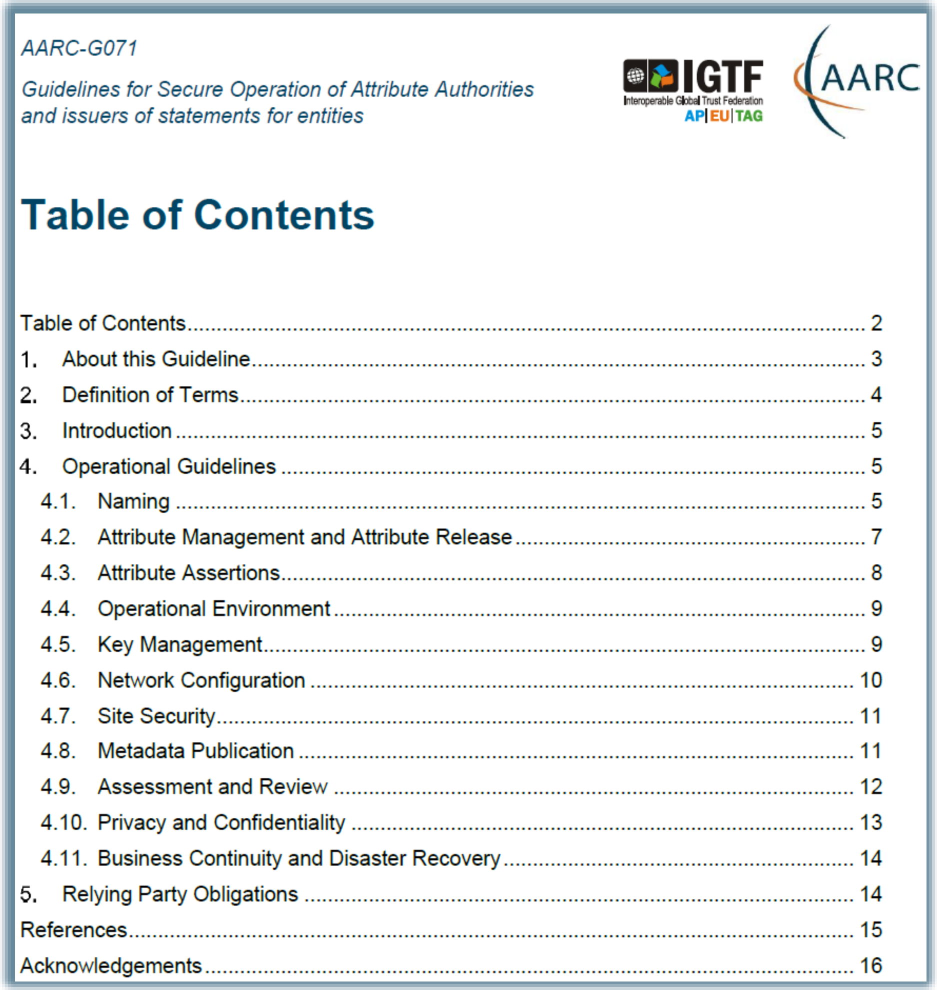


Guidelines for Secure Operation of Attribute Authorities and other issuers of access-granting statements *(AARC-I048, in collaboration with IGTF AAOPS)*

AARC-G071: keeping users & communities protected, moving across models

Structured around concept of “**AA Operators**”,
operating “**Attribute Authorities**”
(technological entities or proxies),
on behalf of, one or more, **Communities**, that are
trusted by **Relying Parties**

formerly AARC-G048bis



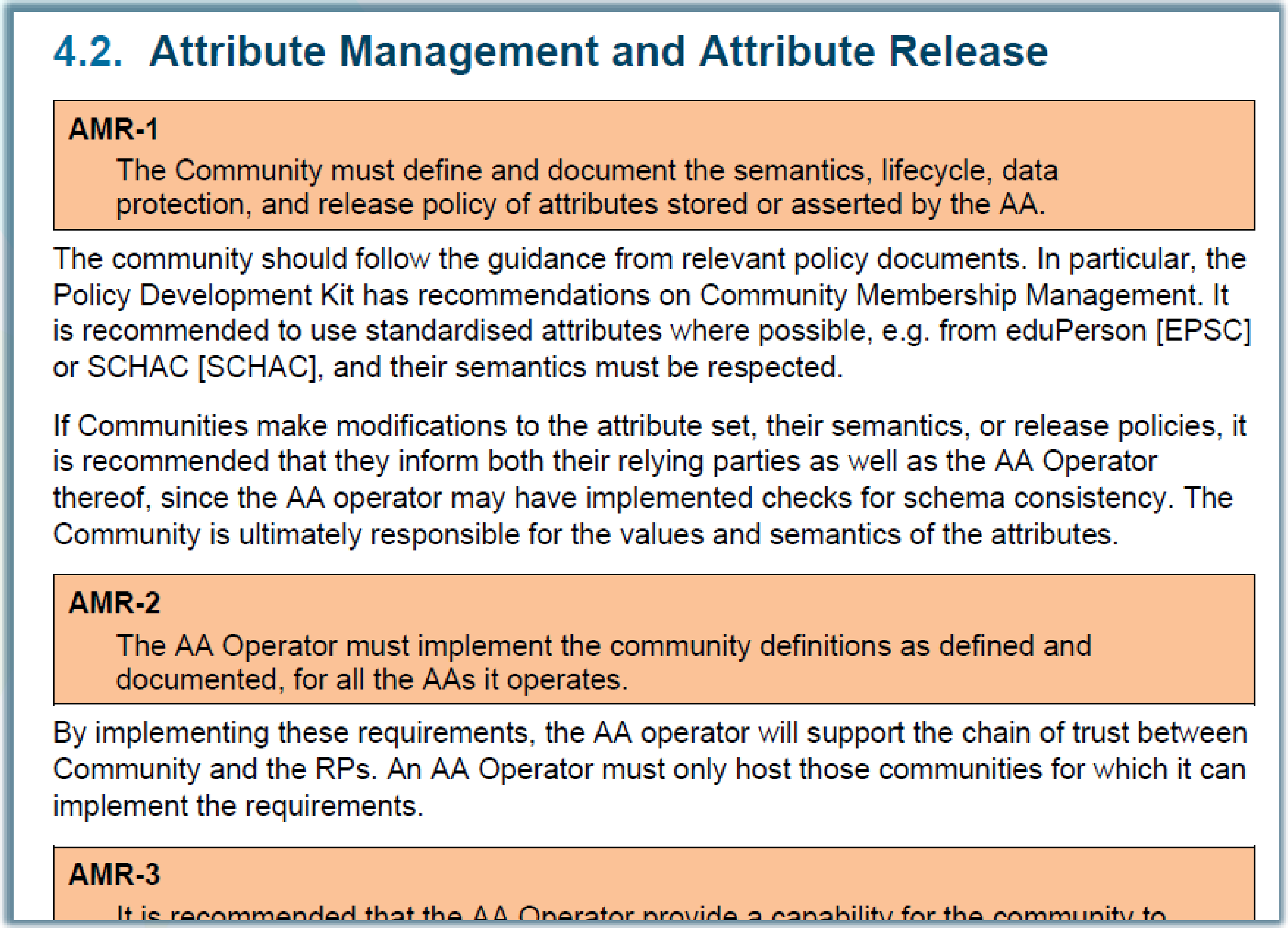
AARC-G071

Guidelines for Secure Operation of Attribute Authorities and issuers of statements for entities

Table of Contents

https://www.igtf.net/guidelines/aaops/ **https://aarc-community.org/guidelines/aarc-g071/**

Deployment guidance included …



4.2. Attribute Management and Attribute Release

AMR-1

The Community must define and document the semantics, lifecycle, data protection, and release policy of attributes stored or asserted by the AA.

The community should follow the guidance from relevant policy documents. In particular, the Policy Development Kit has recommendations on Community Membership Management. It is recommended to use standardised attributes where possible, e.g. from eduPerson [EPSC] or SCHAC [SCHAC], and their semantics must be respected.

If Communities make modifications to the attribute set, their semantics, or release policies, it is recommended that they inform both their relying parties as well as the AA Operator thereof, since the AA operator may have implemented checks for schema consistency. The Community is ultimately responsible for the values and semantics of the attributes.

AMR-2

The AA Operator must implement the community definitions as defined and documented, for all the AAs it operates.

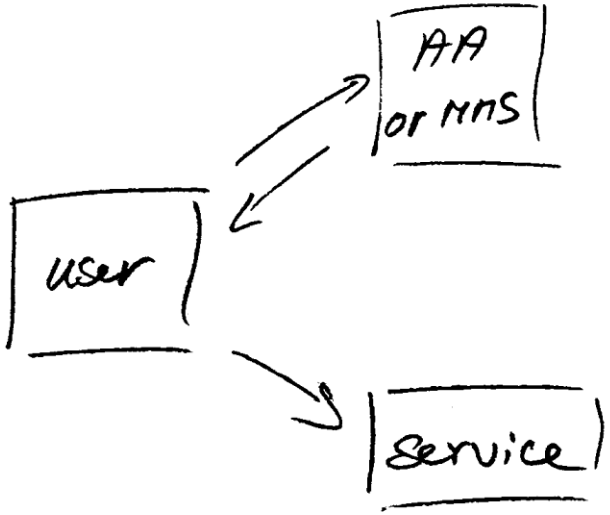
By implementing these requirements, the AA operator will support the chain of trust between Community and the RPs. An AA Operator must only host those communities for which it can implement the requirements.

AMR-3

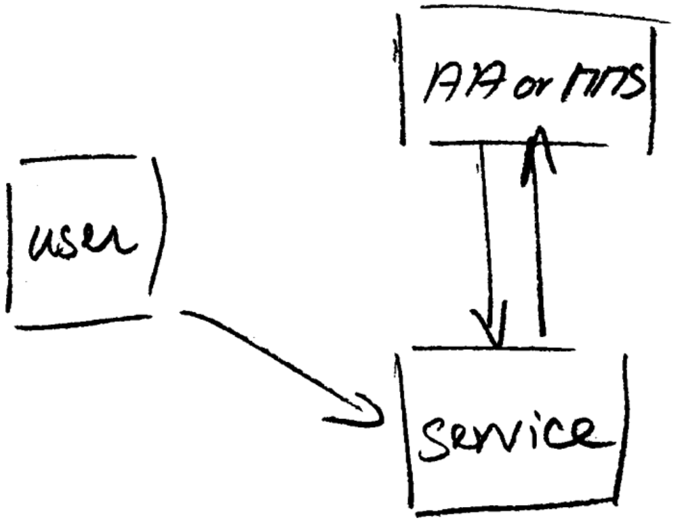
It is recommended that the AA Operator provide a capability for the community to

Protecting the community membership data and its proxy

Intentionally targeted broader than just the push model, since operational security spans
data centres and infrastructures using other forms of AA membership management
(SAML, OIDC, LDAP, ..)



push model – the common BPA method
(e.g. SAML AttributeStatement, VOMS AC)



pull model – common when using directories
(e.g. LDAP in PRACE, userinfo endpoint in OIDC)

push and pull model diagrams as per RFC2904 – the 3rd (agent) model is uncommon in research/collaboration scenarios except for provisioning

When the AA is in a managed environment …

Many of the recommendations are already implemented ‘implicitly’

- because common software implements it: e.g. signing SAML assertions and JWTs
- because a good data centre already has network monitoring and central logging in place
- because you signed up to Sirtfi (didn’t you?) – so you collaborate in incident response
- because you have trained IT operations personnel looking after the service

And some are intuitive best practice

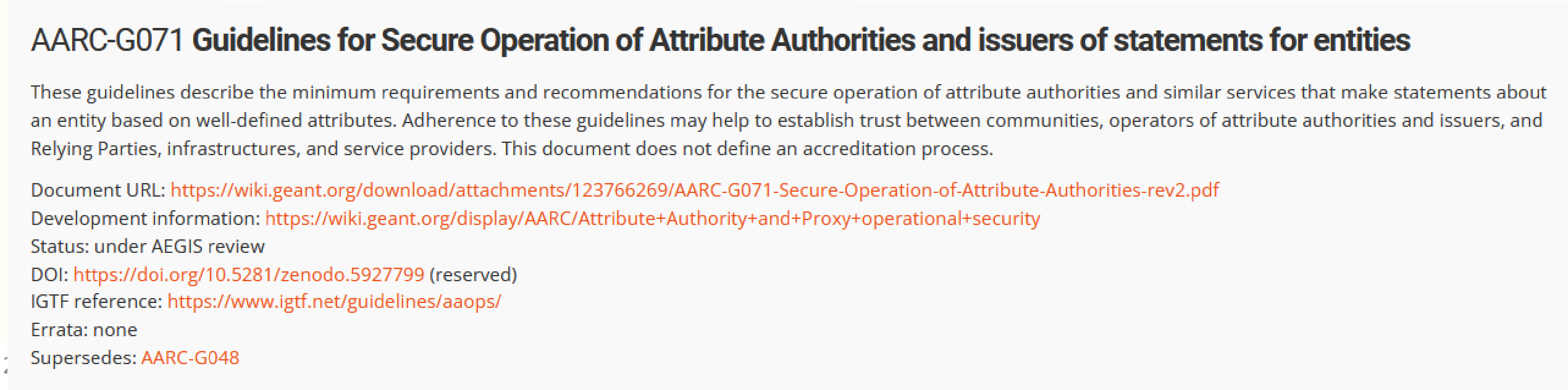
- like assigning a unique and lasting name to a group
- because implemented controls ought to be those that have been documented

Some items contain reminders about appropriate values and recommendations that are good practice - based on the relevant standards involved

Implementation of the AA Operations (“AAI proxy”) Security guidelines

1. Major RPs and Infrastructures reviewed it based on current use cases and models
2. Guideline aimed at both Infrastructure and Community use cases
3. Useful input to e.g. ‘EOSC’ connected proxies as a good practice guideline
4. Assessment or review process is separate – could be IGTF or an RP consortium, but does state what needs to be logged and saved to do a (self) assessment

https://aarc-community.org/guidelines/aarc-g071/



AARC-G071 **Guidelines for Secure Operation of Attribute Authorities and issuers of statements for entities**

These guidelines describe the minimum requirements and recommendations for the secure operation of attribute authorities and similar services that make statements about an entity based on well-defined attributes. Adherence to these guidelines may help to establish trust between communities, operators of attribute authorities and issuers, and Relying Parties, infrastructures, and service providers. This document does not define an accreditation process.

Document URL: https://wiki.geant.org/download/attachments/123766269/AARC-G071-Secure-Operation-of-Attribute-Authorities-rev2.pdf
Development information: https://wiki.geant.org/display/AARC/Attribute+Authority+and+Proxy+operational+security
Status: under AEGIS review
DOI: https://doi.org/10.5281/zenodo.5927799 (reserved)
IGTF reference: https://www.igtf.net/guidelines/aaops/
Errata: none
Supersedes: AARC-G048

multi-domain anycast

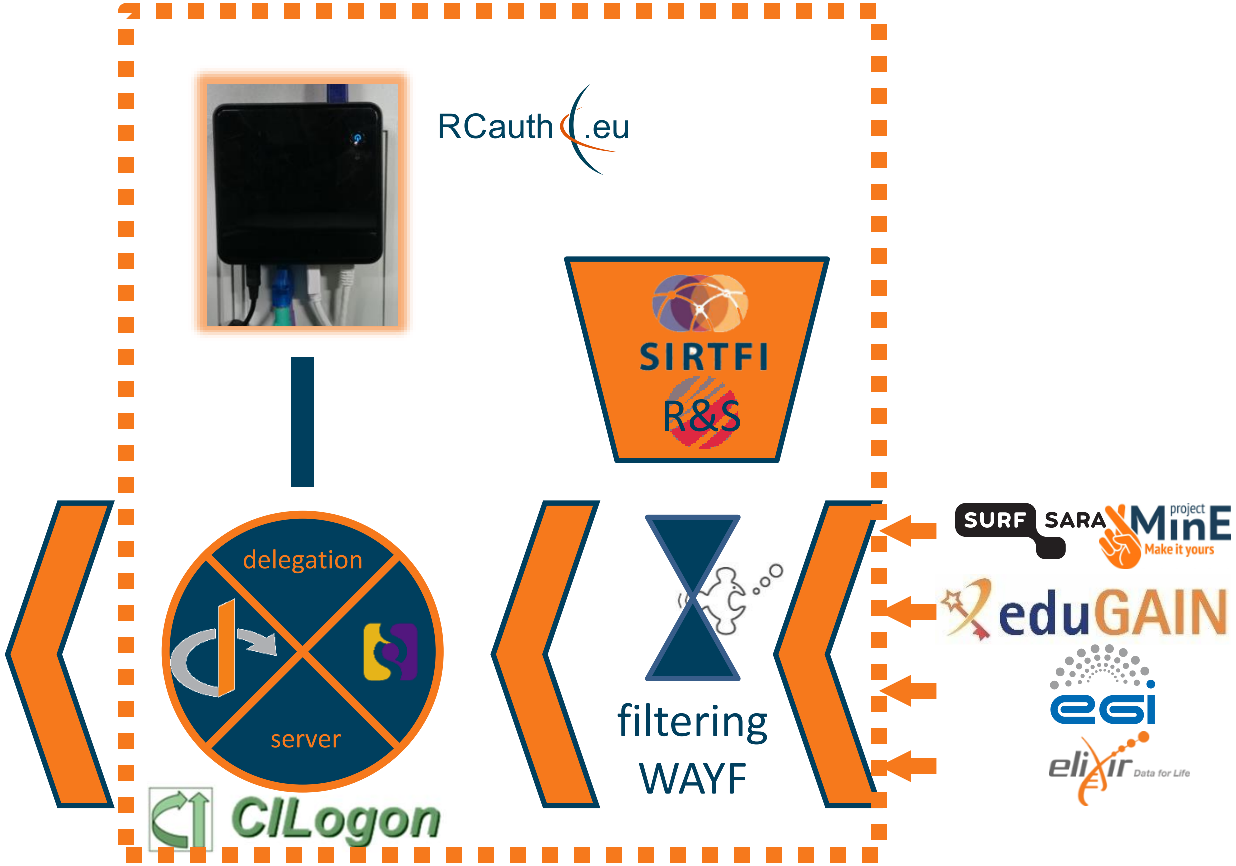
RCAUTH.EU – RESILIENCE AND HA

RCauth.eu – a ubiquitous federated IOTA

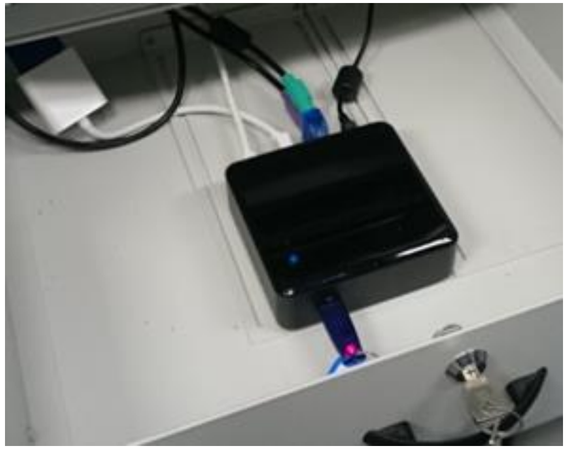
- RCauth is an IGTF accredited IOTA (DOGWOOD class) CA
  - Online credential conversion
  - Connected to eduGAIN (R&S+Sirtfi) plus direct, e.g. EGI Check-in and eduTEAMS
- Inspired by and leveraging the delegation service from CILogon
- EOSC Hub and EOSC Future implementing a High Availability setup across 3 sites

RCauth.eu

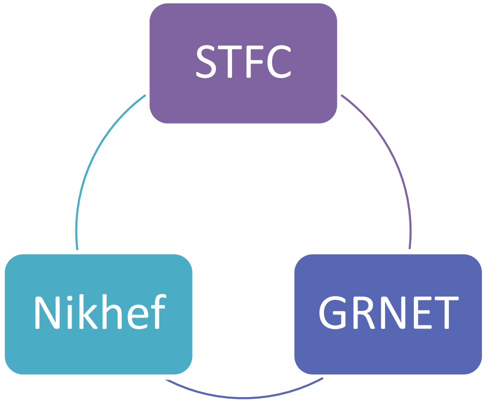
Long ago, in a drawer far, far away …

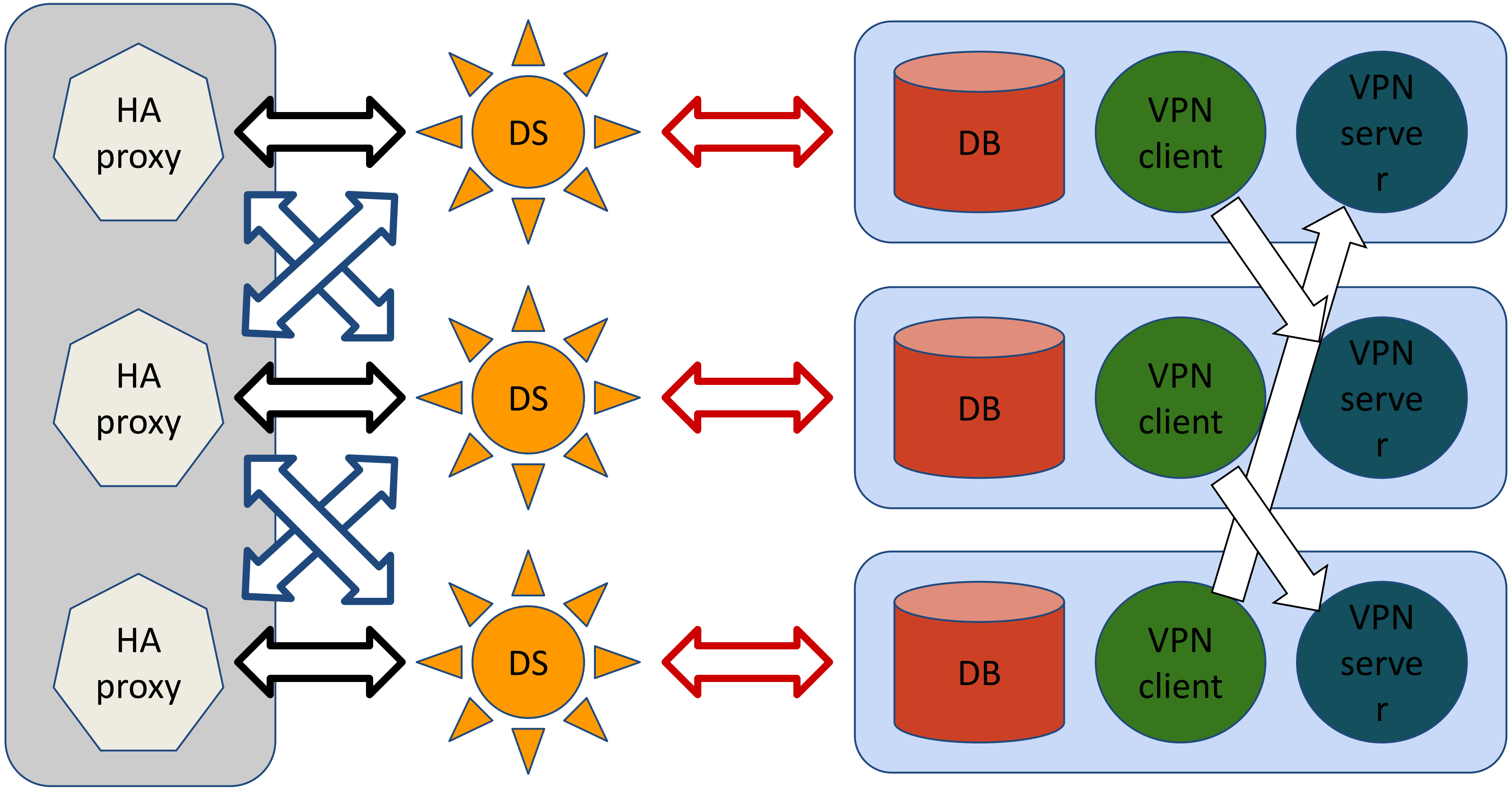


RCauth.eu



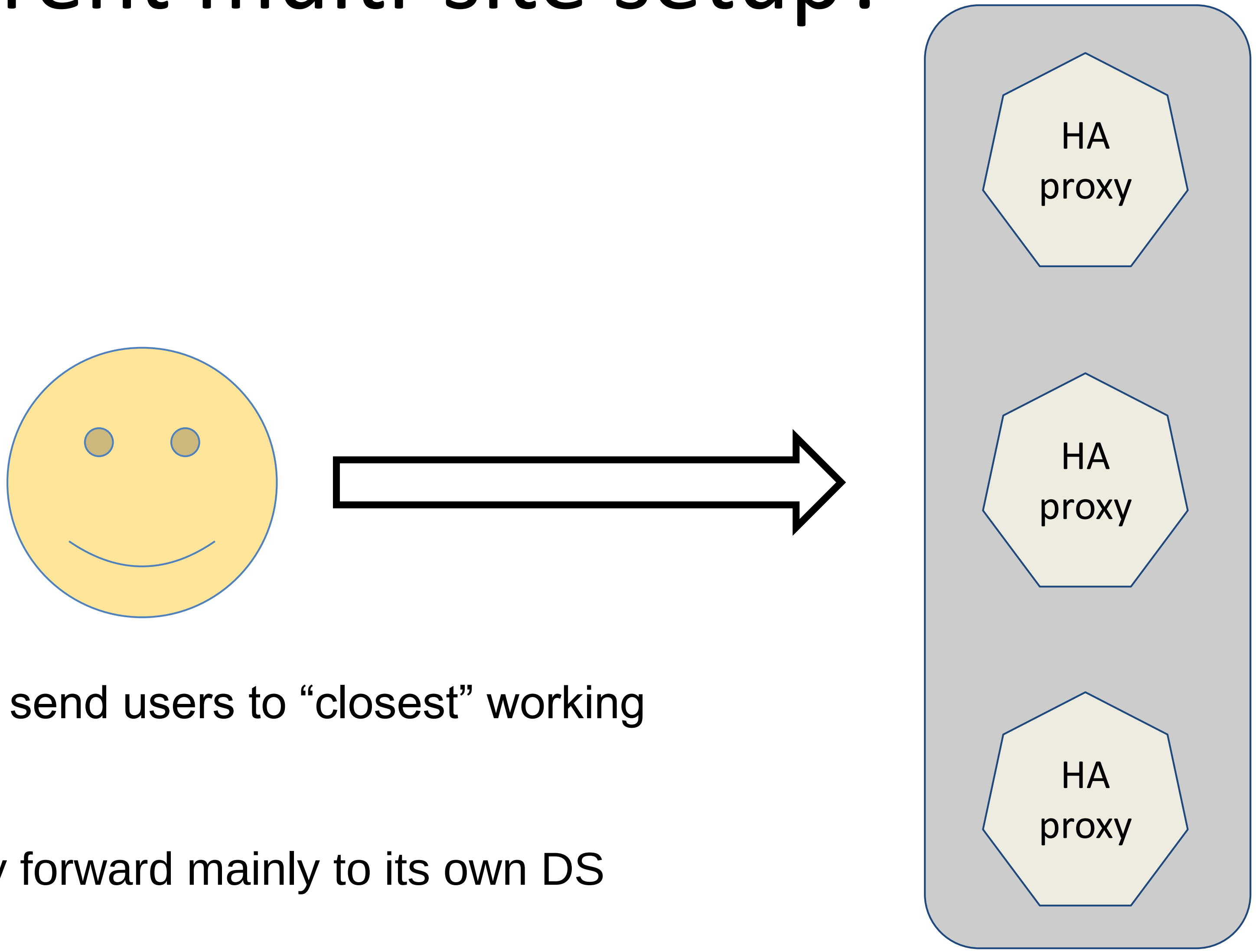
Distributed RCauth





selected imagery: Mischa Sallé, Jens Jensen, Nicolas Liampotis

A transparent multi-site setup?



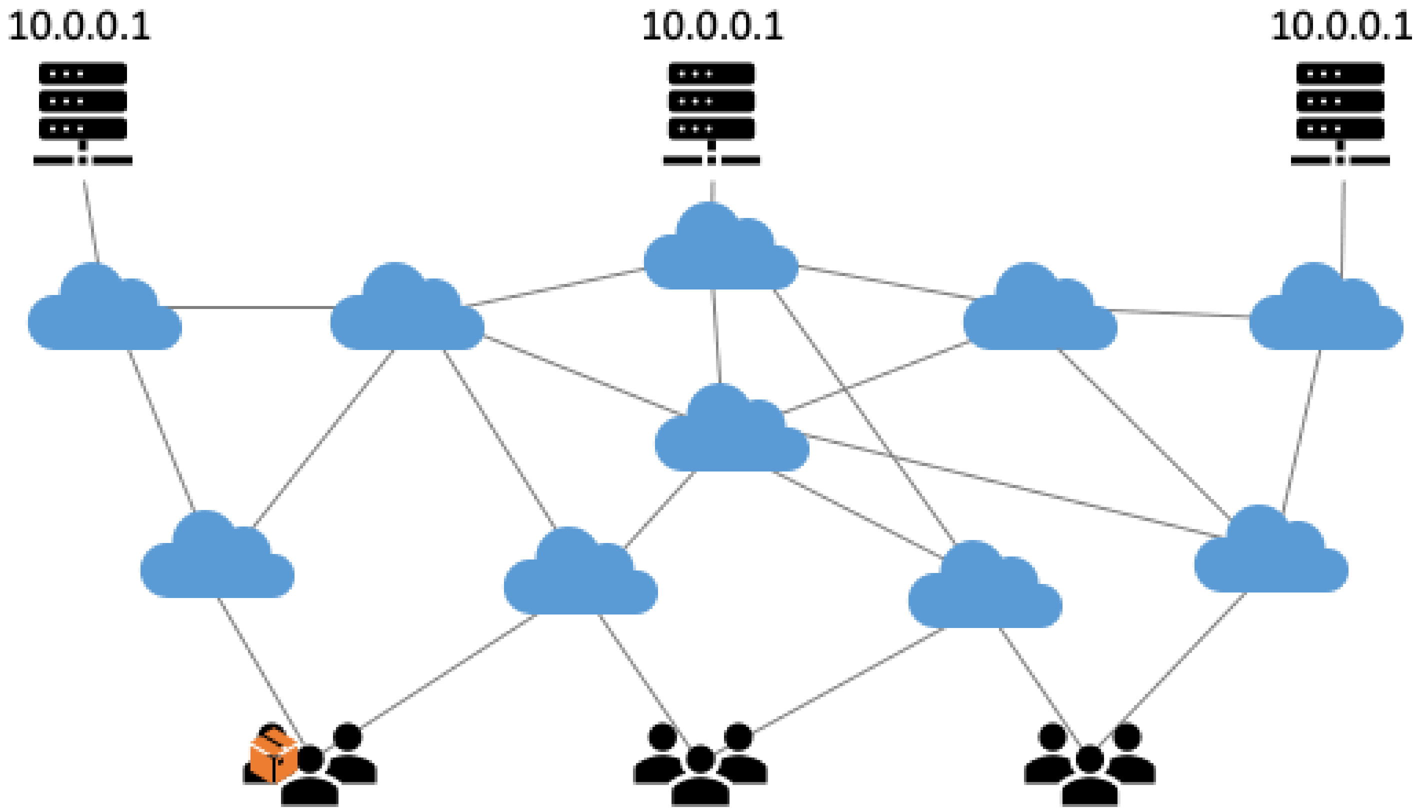
Need a way to send users to “closest” working service

Each HA proxy forward mainly to its own DS

If a HA loses its backend DS, it can still route to the other DSes

selected imagery: Mischa Sallé, Jens Jensen, Nicolas Liampotis

Use proven technology: ip anycast



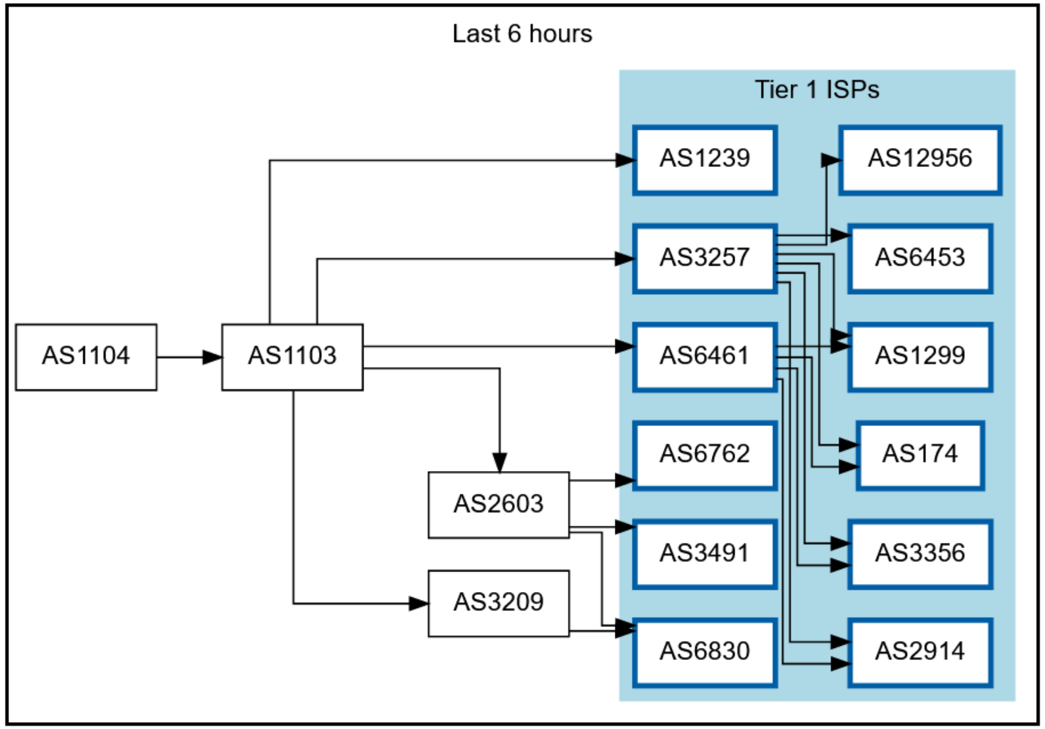
So we used

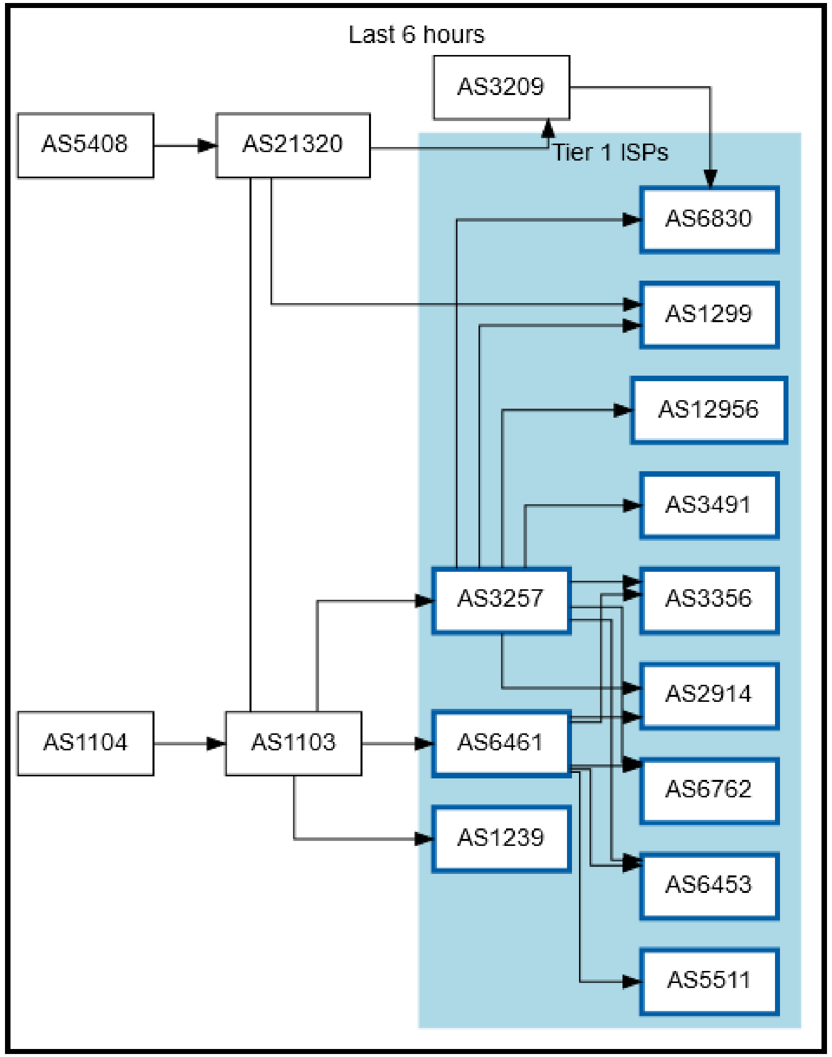
- 3 (now: 2) sites
- one VM at each site exposing 145.116.216.1
- smallest v4 subnet (/24)
- bird + a service probe
- each site’s own ASN
- some IRR DB editing
- v6 is similar, with a /48

and some monitoring

routing image: SIDNlabs - https://www.sidnlabs.nl/en/news-and-blogs/the-bgp-tuner-intuitive-management-applied-to-dns-anycast-infrastructure

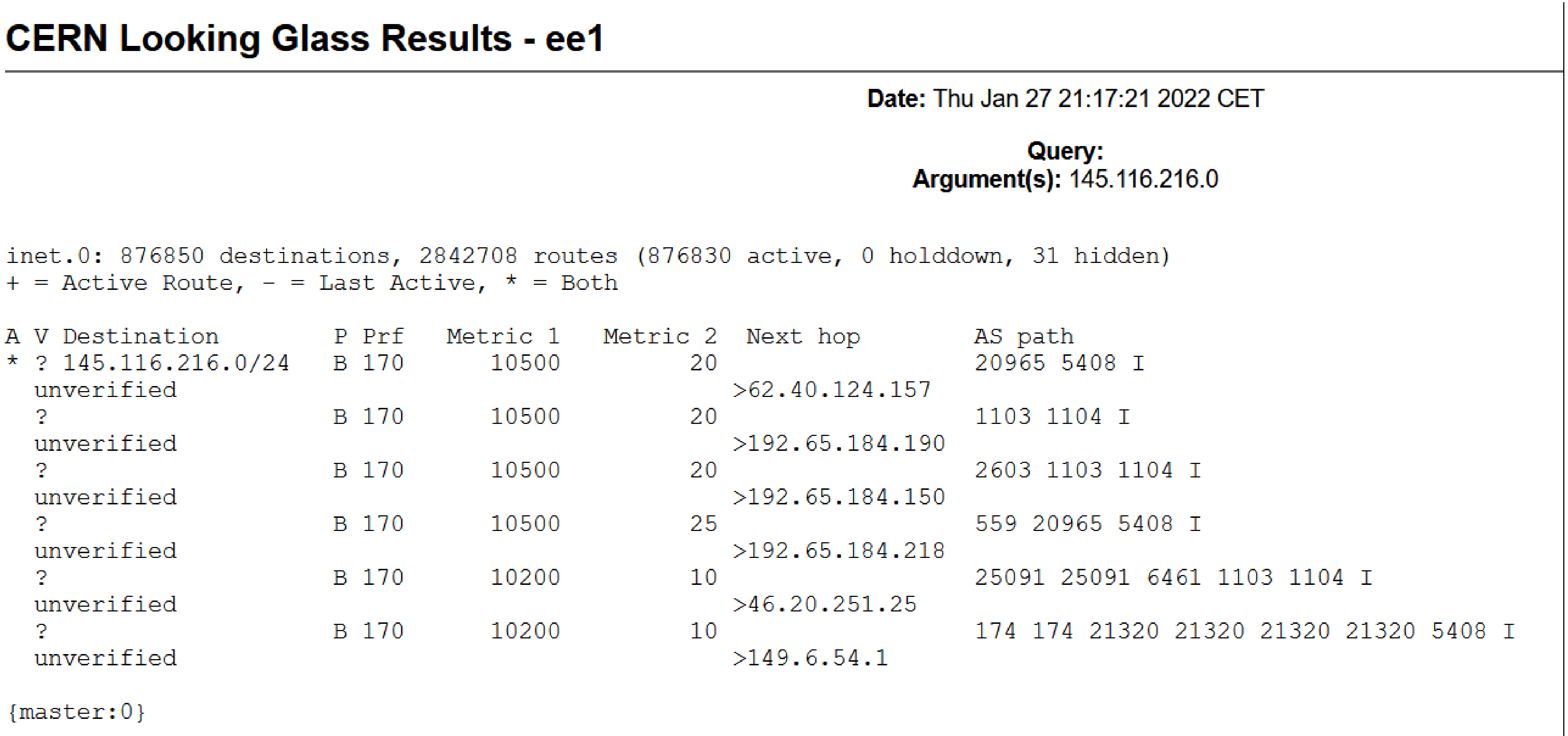
Getting 145.116.216.0/24 out there





route maps: bgp.tools for 145.116.216.0/24 – IPv6 would be similar

Same IP address, two AS paths ☺



CERN Looking Glass Results - ee1

Date: Thu Jan 27 21:17:21 2022 CET

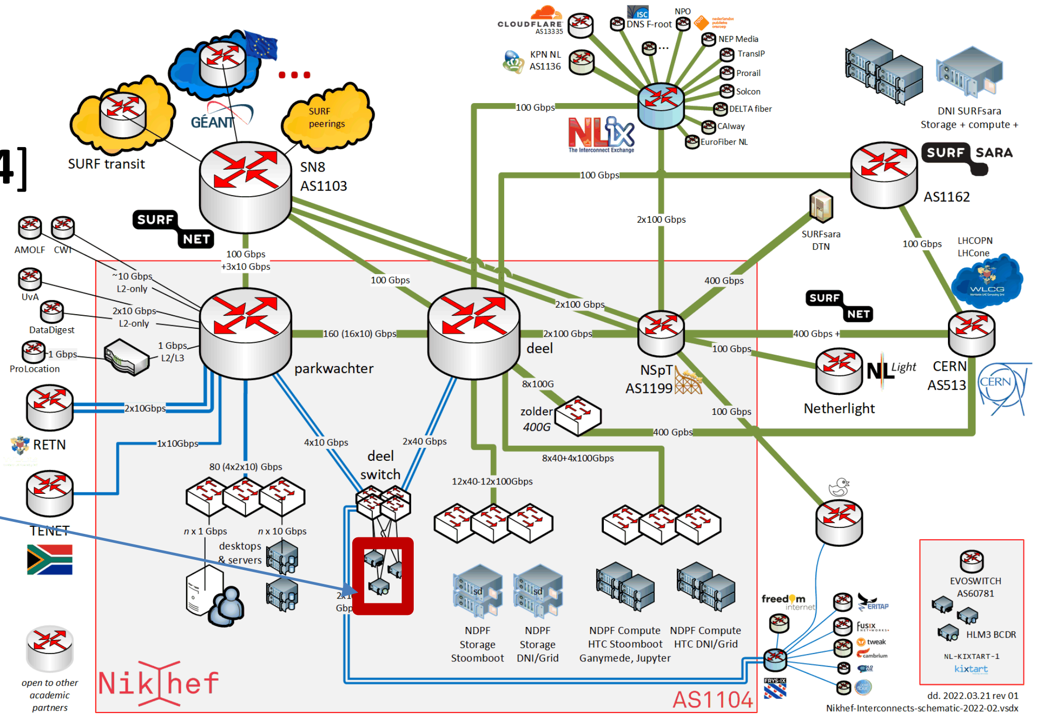
Query:
Argument(s): 145.116.216.0

```
inet.0: 876850 destinations, 2842708 routes (876830 active, 0 holdddown, 31 hidden)
+ = Active Route, - = Last Active, * = Both

A V Destination        P Prf   Metric 1   Metric 2  Next hop        AS path
* ? 145.116.216.0/24   B 170      10500         20                  20965 5408 I
  unverified                                        >62.40.124.157
  ?                    B 170      10500         20                  1103 1104 I
  unverified                                        >192.65.184.190
  ?                    B 170      10500         20                  2603 1103 1104 I
  unverified                                        >192.65.184.150
  ?                    B 170      10500         25                  559 20965 5408 I
  unverified                                        >192.65.184.218
  ?                    B 170      10200         10                  25091 25091 6461 1103 1104 I
  unverified                                        >46.20.251.25
  ?                    B 170      10200         10                  174 174 21320 21320 21320 21320 5408 I
  unverified                                        >149.6.54.1

{master:0}
```

Will take any shortest route in the default-free zone

```
[root@kwark ~]# traceroute -IA 145.116.216.1
traceroute to 145.116.216.1 (145.116.216.1), 30 hops max, 60 byte packets
 1  cmbr.connected.by.freedominter.net (185.93.175.234) [AS206238]
 2  connected.by.freedom.nl (185.93.175.240) [AS206238]
 3  et-0-0-0-1002.core1.fi001.nl.freedomnet.nl (185.93.175.208) [AS206238]
 4  as1104.frys-ix.net (185.1.203.66) [*]
 5  parkwachter.nikhef.nl (192.16.186.141) [AS1104]
 6  gw-anyc-01.rcauth.eu (145.116.216.1) [AS786/AS5408/AS1104]
```

rcauth.eu HA proxy



Network graphic: https://www.nikhef.nl/pdp/doc/facility

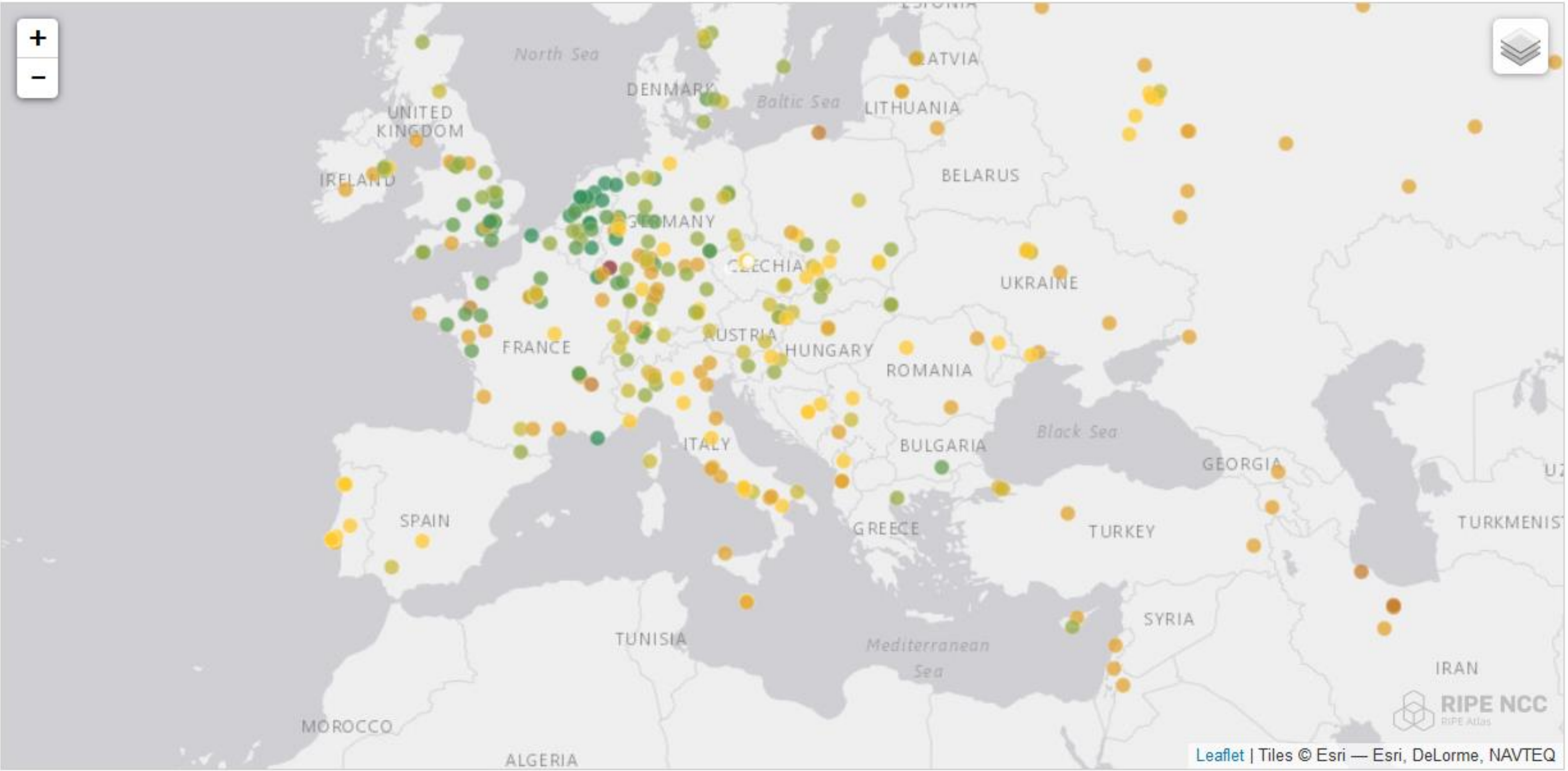
Prerequisites are relatively simple

- an IPv4 /24 netblock (and, or) an IPv6 /48
- your own, or a friendly AS
- a set of IRR route objects, and either none, or a correct RPKI VRP
  (easily done in your local RIR registry: APNIC, RIPE, ARIN, AfriNIC, LACNIC)
- bird, or quagga, with a monitoring plugin (to flap the route in case of downtime)

But you *don't* per-se need:

- a unique AS *just* for this anycast activity (it works equally well without it)
- a balanced AS path length (unless you want load balancing as well as redundancy)
- your own AS (if you have a friendly AS willing to re-announce your specific route)

And you get reasonable load balancing



🟩 < 10 ms: 29 | 🟩 < 20 ms: 46 | < 30 ms: 59 | < 40 ms: 54 | < 50 ms: 64 | < 100 ms: 113 | < 200 ms: 91 | < 300 ms: 26 | > 300 ms: 5 | No Data: 0

map: RIPE NCC RIPE Atlas- 500 probes, zoomed in on Europe

Other HA options

- Local HA with an HA proxy and pacemaker/CRM failover works on the local network – and can be meshed with two signing systems
this is the local Nikhef RCauth instance setup

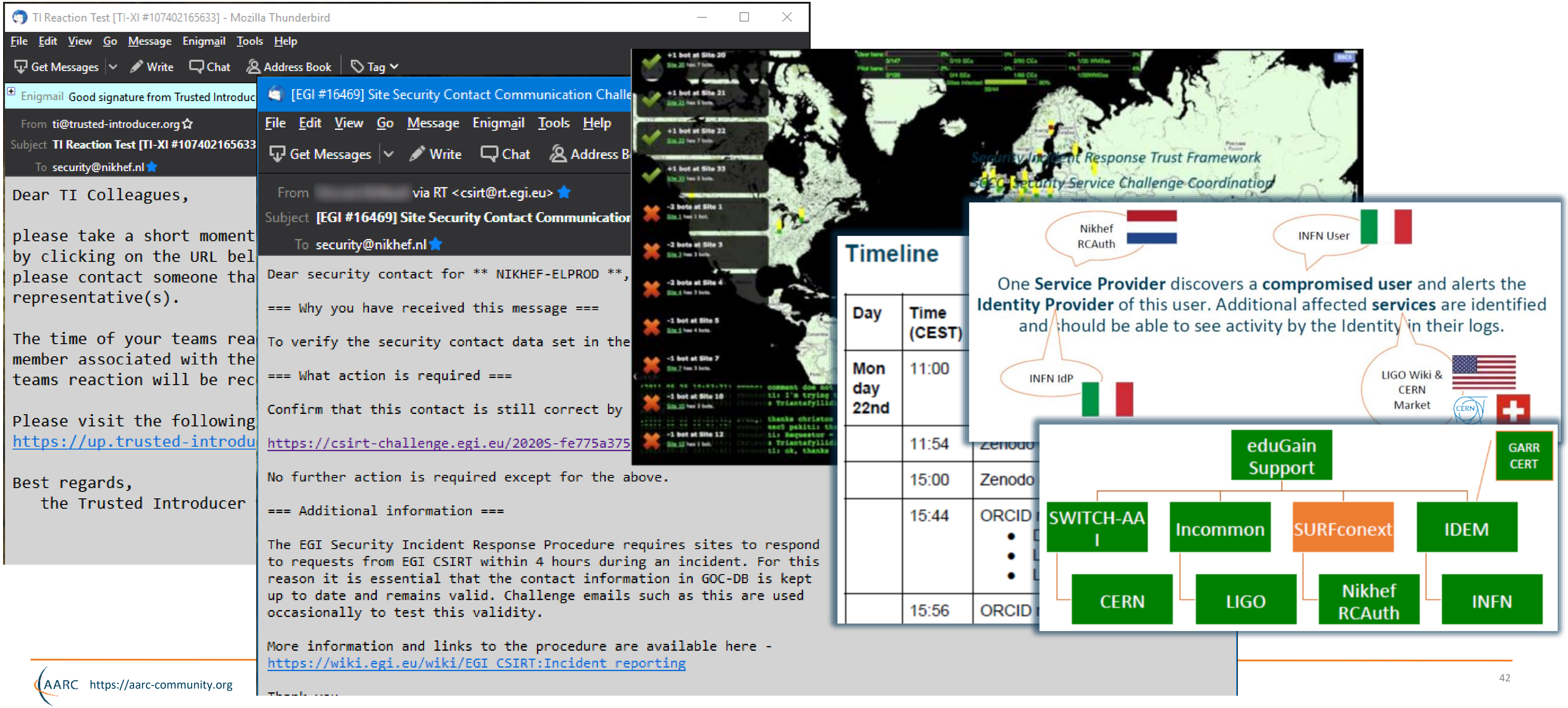
- DNS-based fast-failover – the method used for InAcademia
automatic updating of DNS a distributed set of servers, auto-updating each other
*But does require that the DNS domain level operator remains available, since you need *very* short TTLs (and of course your ccTLD/gTLD as well)*

- Add a dedicated HA link for the back-end databases
e.g. multiple redundant circuits over an MPLS cloud

From IGTF RAT CC to ‘Security Communications Challenge Coordination’ - SCCC

AND FINALLY … WHAT ABOUT AN IGTF RAT CC AGAIN?

Communications Challenges – who picks up the call?



TI Reaction Test [TI-XI #107402165633] - Mozilla Thunderbird

Enigmail Good signature from Trusted Introduc

From ti@trusted-introducer.org
Subject TI Reaction Test [TI-XI #107402165633
To security@nikhef.nl

```
Dear TI Colleagues,

please take a short moment
by clicking on the URL bel
please contact someone tha
representative(s).

The time of your teams rea
member associated with the
teams reaction will be rec

Please visit the following
https://up.trusted-introdu

Best regards,
   the Trusted Introducer
```

[EGI #16469] Site Security Contact Communication Challe

From [redacted] via RT <csirt@rt.egi.eu>
Subject [EGI #16469] Site Security Contact Communication
To security@nikhef.nl

```
Dear security contact for ** NIKHEF-ELPROD **,

=== Why you have received this message ===

To verify the security contact data set in the

=== What action is required ===

Confirm that this contact is still correct by

https://csirt-challenge.egi.eu/2020S-fe775a375

No further action is required except for the above.

=== Additional information ===

The EGI Security Incident Response Procedure requires sites to respond
to requests from EGI CSIRT within 4 hours during an incident. For this
reason it is essential that the contact information in GOC-DB is kept
up to date and remains valid. Challenge emails such as this are used
occasionally to test this validity.

More information and links to the procedure are available here -
https://wiki.egi.eu/wiki/EGI_CSIRT:Incident_reporting

Thank you
```

Security Incident Response Trust Framework

SCCC Security Service Challenge Coordination

Timeline

Day	Time (CEST)	
Mon day 22nd	11:00	
	11:54	Zenodo
	15:00	Zenodo
	15:44	ORCID
	15:56	ORCID

Nikhef RCAuth

INFN User

One **Service Provider** discovers a **compromised user** and alerts the **Identity Provider** of this user. Additional affected **services** are identified and should be able to see activity by the Identity in their logs.

INFN IdP

LIGO Wiki & CERN Market

eduGain Support

GARR CERT

SWITCH-AAI

Incommon

SURFconext

IDEM

CERN

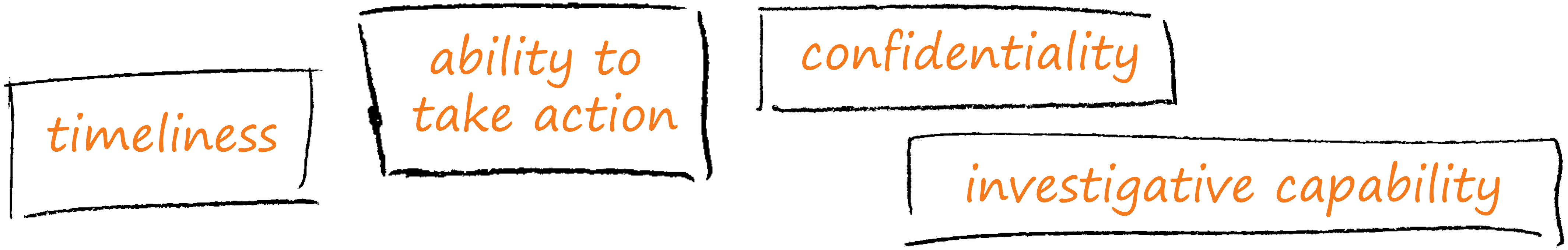
LIGO

Nikhef RCAuth

INFN

Challenge elements – what is valued or expected might differ …

A single test and challenge can answer one **or more** of these questions



timeliness

ability to take action

confidentiality

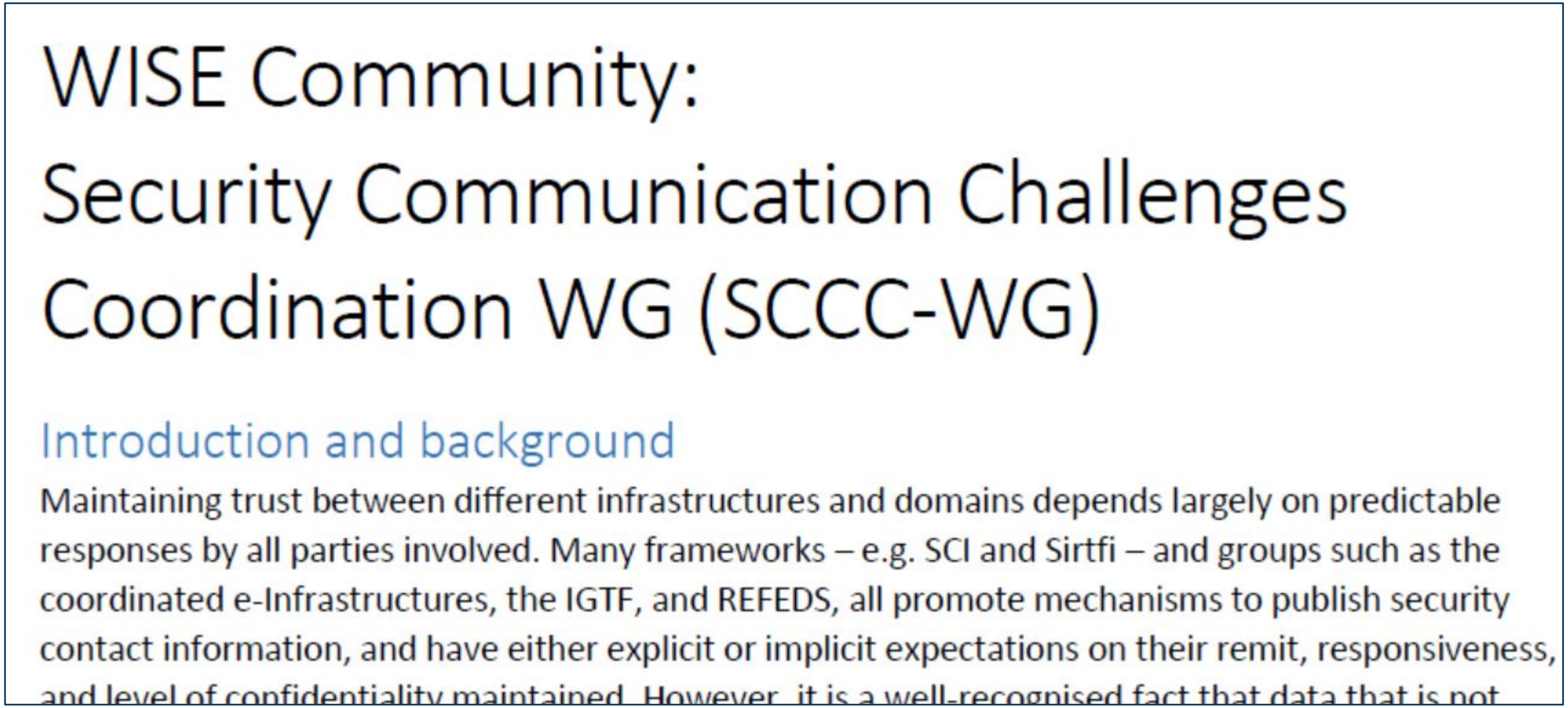
investigative capability

- when data available: infrastructure can set its *own level* of expectancy and gives *deep trust*
- assessment supported with community controls (suspension) gives a *baseline compliance*

Communications challenges build ‘confidence’ and trust – an important social aspect!

- different tests bring complementary results: responsiveness vs. ability act , or do forensics
- unless you run the test yourself, you may not be growing more trust in the entities tested
- for a ‘warm and fuzzy feeling of trust’, share results: but this is sociologically still challenging …

Continued engagement and coordination: WISE SCCC JOINT WG



WISE Community: Security Communication Challenges Coordination WG (SCCC-WG)

Introduction and background

Maintaining trust between different infrastructures and domains depends largely on predictable responses by all parties involved. Many frameworks – e.g. SCI and Sirtfi – and groups such as the coordinated e-Infrastructures, the IGTF, and REFEDS, all promote mechanisms to publish security contact information, and have either explicit or implicit expectations on their remit, responsiveness, and level of confidentiality maintained. However, it is a well-recognised fact that data that is not

WISE

SIG-ISM

REFEDS

IGTF

https://wiki.geant.org/display/WISE/SCCC-JWG

Subsidiary aim: make security contacts less 'scary'

The most basic response is to (sorry!) click on a harmless link: making it a challenge to respond 'as fast as possible' – a bit like a competition

Ask also a very simple 'question' to raise awareness,

> 'for security contacts, do you want to be (proactively) informed if we have security information relevant to your organisation?'

***esp.* if the contact is the technical rep, i.e. there is no *Sirtfi* contact**

> 'you got this message because there is no designated security contact for your organisation. Would you want to receive security information, or who (if not you) should be your security contact?
> Are you aware of Sirtfi?'

And we can add some ads for Sirtfi, although having *any* kind of contact is better than none …

Would *you* like to be contacted?

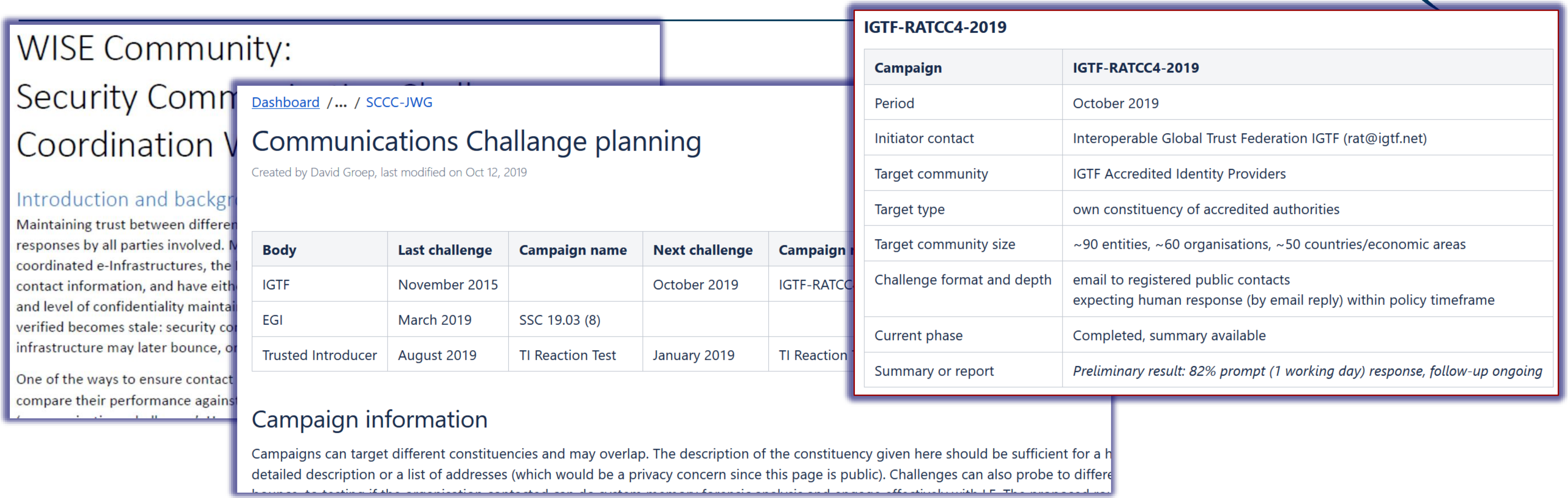
1. Do you have a security contact listed for your organisation?
   Is your CERT contact public?

2. Do you run (or control) an IdP, and do you support *Sirtfi*?

SIRTFI
Security Incident Response Trust Framework for Federated Identity

3. What kind of communications would *you* like to receive there?
   - information about **incidents in connected services**, where your users are actively involved?
   - information about incidents that are **currently affecting institutions like yours** and are spreading and attacking you soon?
   - information that **people with an email address** from your domain are using non-federated services?
   - **communications challenges**, to see whether you're awake?
   - **surveys** and questionnaires? ☺

WISE SCCC-WG – participate!



WISE Community:
Security Comm
Coordination V

Introduction and backgr

Maintaining trust between differen
responses by all parties involved. M
coordinated e-Infrastructures, the
contact information, and have eith
and level of confidentiality maintai
verified becomes stale: security co
infrastructure may later bounce, o

One of the ways to ensure contact
compare their performance agains

Dashboard / ... / SCCC-JWG

Communications Challange planning

Created by David Groep, last modified on Oct 12, 2019

Body	Last challenge	Campaign name	Next challenge	Campaign r
IGTF	November 2015		October 2019	IGTF-RATCC
EGI	March 2019	SSC 19.03 (8)		
Trusted Introducer	August 2019	TI Reaction Test	January 2019	TI Reaction

Campaign information

Campaigns can target different constituencies and may overlap. The description of the constituency given here should be sufficient for a h
detailed description or a list of addresses (which would be a privacy concern since this page is public). Challenges can also probe to differe

IGTF-RATCC4-2019

Campaign	IGTF-RATCC4-2019
Period	October 2019
Initiator contact	Interoperable Global Trust Federation IGTF (rat@igtf.net)
Target community	IGTF Accredited Identity Providers
Target type	own constituency of accredited authorities
Target community size	~90 entities, ~60 organisations, ~50 countries/economic areas
Challenge format and depth	email to registered public contacts expecting human response (by email reply) within policy timeframe
Current phase	Completed, summary available
Summary or report	*Preliminary result: 82% prompt (1 working day) response, follow-up ongoing*

WISE, SIGISM, REFEDS, TI joint working group

see wise-community.org wiki and join!

https://wiki.geant.org/display/WISE/SCCC-JWG

co-chairs: Hannah Short (CERN) and David Groep (Nikhef)

Questions?

BUILDING A GLOBAL TRUST FABRIC

this work is co-supported by the Trust and Identity workpackage of the GEANT4 project - phase 3

Thank you

davidg@nikhef.nl

Networks · Services · People
www.geant.org

with material also from Christos Kanellopoulos, Hannah Short, Pinja Koskinen, Maarten Kremers, David Crooks, Dave Kelsey, Nicolas Liampotis, Mischa Sallé, Jens Jensen, and others

This work IS ALSO SUPPORTED BY A project that has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).