# Security in the Future of the European Open Science Cloud

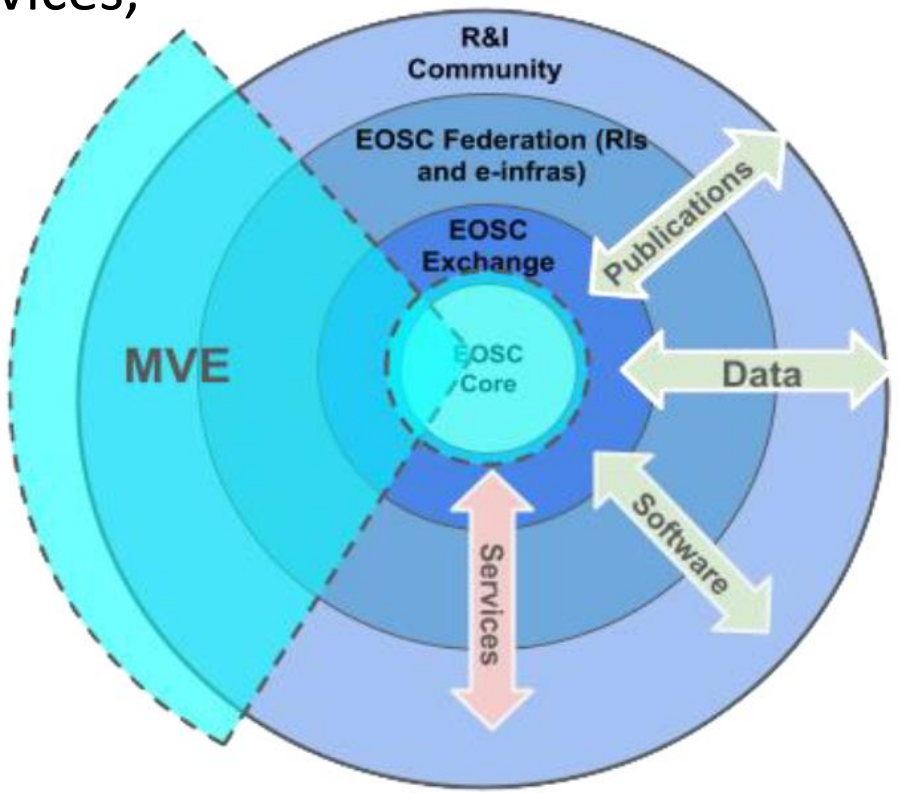
*WISE workshop, April 2022*


**David Groep – WP7.5 Security Operations and Policy lead**
*Nikhef Physics Data Processing programme*
*UM Faculty of Science and Engineering, DKE*

# Enabling an Interoperable & FAIR Research Ecosystem

Built as a sustainable ecosystem of FAIR research services, data, publications, and software for research:

- *based on the principle of openness*
- *aligned with FAIR principles*
- *interoperable architecture*
- *based on ethical research integrity*
- *users contribute to the 'federation'*
- *subject to guidelines and policies*
- *users properly reference all resources*




built in an incremental way ("Minimum Viable EOSC") way around common core



Image from: Licia Florio *et al.* Draft EOSC Architecture and Interoperability Framework, https://eosc-portal.eu/eosc-interoperability-framework-consultation

# Research and e-Infrastructures from all research areas




Images: logos of the ESFRI cluster projects, INFRAEOSC-07 awarded infrastructure projects, and the national and regional EOSC service development projects – retrieved from EOSC Future Open Day 1, https://eoscfuture.eu/library

# Core, Exchange, and composite services

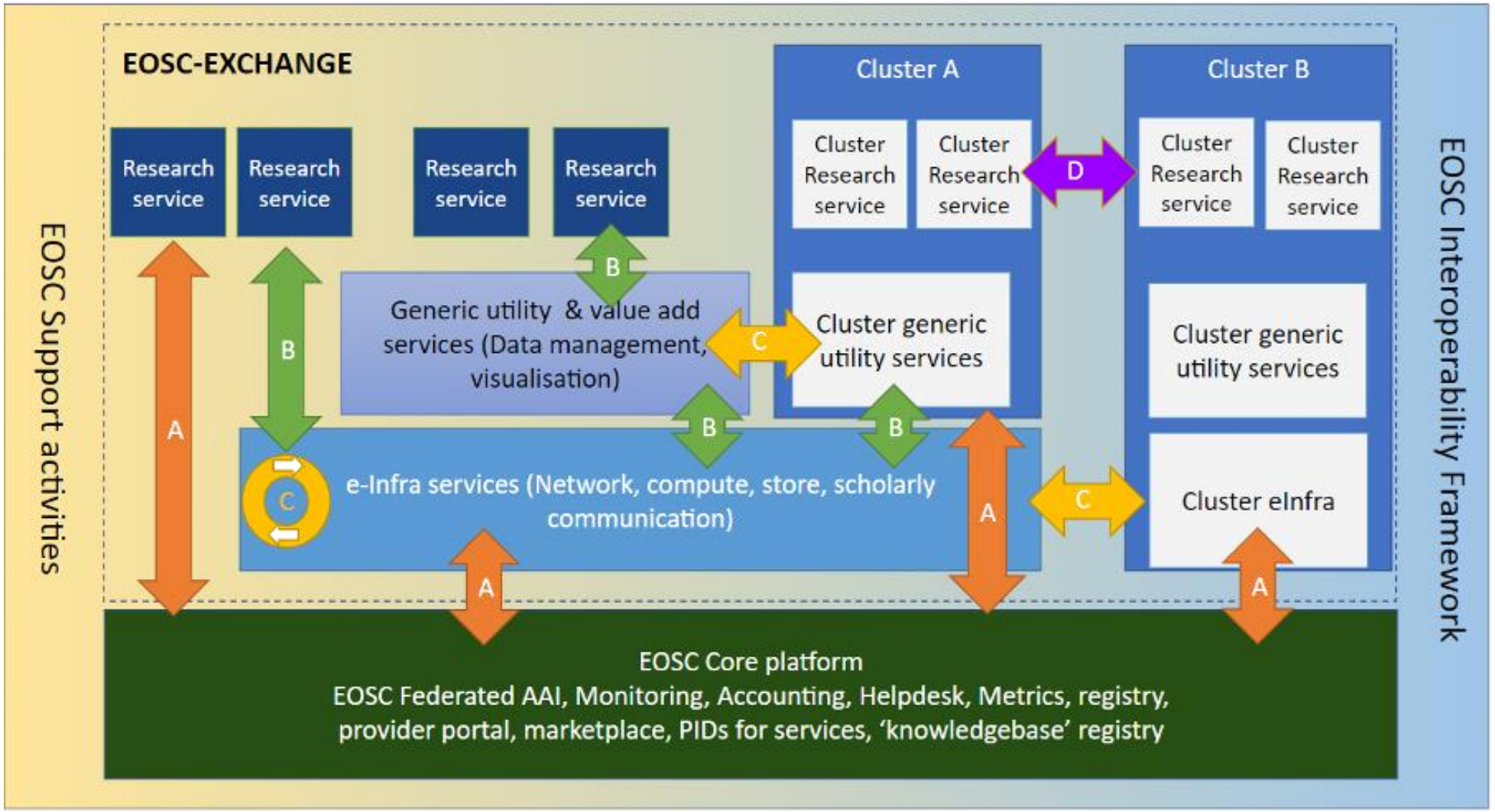





Image: EOSC Architecture WG

# A challenging landscape ahead!

doi:10.2777/8702 – ISBN 978-92-76-28113-9

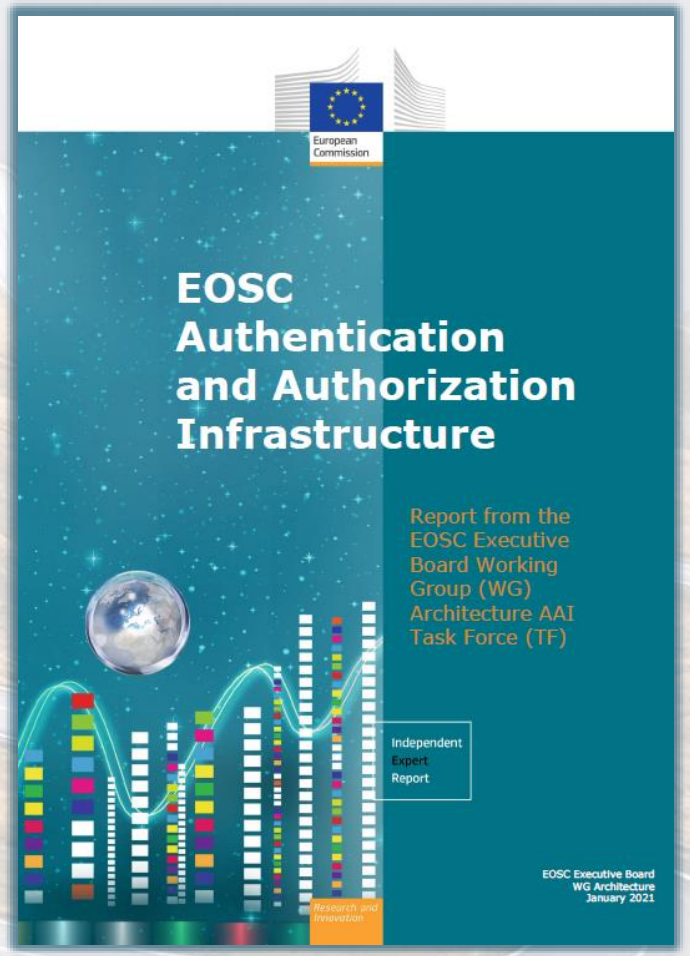
**Entities of all kinds** – EOSC spans from *data sets* to *storage* from *computing* to *publications* & *digital objects*

**Open diverse ecosystem** – user-driven, research and e-Infra services, favouring low entry barrier

***Interoperable* ecosystem** – common frameworks

**An *interdependent* ecosystem** – with composability, collective service design, and a federated approach to AAI

- ***User experience*** *is the only touchstone*
- *All* ***trust flows from communities***
- *There is* ***no centre*** *in a distributed system*



# Translating to security operations and security policy

- clarity on assets and their service management
  with *Core* services are more ‘tightly controlled’ than assets in the *Exchange*
- participants are autonomous, yet subscribe to shared commitment of trust
- security policies follow a baselining approach + good practice guidance
- risk-based on the Hippocratic principle of “*primum non nocere*”
- security incident response is coordinated, with support from the central team
  which for the Core services also has actionable responsibility

# Information Assets in the EOSC

## Subsidiarity

- core service providers are subject to the EOSC Core Agreement, but the operating entities are the primary responsible for their own services
- exchange service providers bring their own (existing) services, and join based on the EOSC *Rules of Participation* and the *On-boarding Agreement*

**Hence the *assets* that the EOSC sees are *services*,**
including the data and digital objects they manage, but
not their hardware, service components, middleware, or people

this provides the touchstone for the ISM policies, following the *EOSChub* model

# Live and let die (in the policy world)

**EOSC ISM Policies that will live**

- Security Operational Baseline
- WISE Baseline AUP

**Policies and processes relegated to service providers and infrastructures**

- top-level security policy: for EOSC, their substance goes into *agreements*
- software vulnerability management: software used in services is matter for SP

**Much more invigorated processes in the EOSC**

- risk assessments, their methods, and their self-assessment and transparency
- multi-stakeholder coordination of incident response

# Evolving the Service Security Policy

## AARC ‘rev 1’ PDK version of “Service Operations” was, purposefully, specific

- 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

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

**Evolved by UK-IRIS addressing many of these concerns**

# EOSC Security Operational Baseline

## 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

## EOSC consultation together with AEGIS, AARC, and GEANT EnCo

- complemented by an ‘FAQ’ with guidance and references, but no new standards: ‘there is enough good stuff out there’
- leverages Sirtfi framework
- connects to the Core Security Team
- part of the EOSC SMS and Core Participation Agreement

## Joint input to the new WISE AARC Service Operational Policy work in SCI

# EOSCSMS – EOSC Security Operational Baseline & FAQ

## 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 Se
   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 administra
   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
   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 se
   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
9. collaborate in a timely fashion with others, including the EOSC Security Team, in the reporting and resolution of security events or incidents rela
   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 retir
    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
    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 doe

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

The EOSC Incident response team can be contacted via abuse AT eosc

### What are 'IT security best practices' in item 7?

On a global scale there are myriad different documents and sources d
well known recommendations that fit your needs. This can depend on
requirements derived from for example certifications like ISO 27000 o
It is important that you take these into consideration, as well as add th
you, especially if there are no written security policies or recommenda

**Generic information security**

1. ISO standardisation, for example ISO 27000 which covers inform
   processes. Closed standard.
2. National standards, offered by for example national public offic
   covering various security aspects. These can also address local l
   individuals.
3. NIST (https://www.nist.gov/cybersecurity) and CISA (https://ww
   example CISA's Cyber Essentials Starter Kit and NIST's cyber sec
4. CIS (https://www.cisecurity.org/cybersecurity-best-practices/), s
5. SANS (https://www.sans.org) provides guidelines and trainings

**Cloud platforms**

1. Cloud security alliance (https://cloudsecurityalliance.org/) provi
2. BSI C5, Cloud Computing Compliance Controls Catalogue (https
   Cloud_Computing-C5.pdf)
3. Several nations provide their standards, which may be targeted

**Software development**

1. OWASP (https://owasp.org/) provides extensive documentation
   ensure that your software has capabilities to defend against co
2. Microsoft SDLC (https://www.microsoft.com/en-us/securityengi

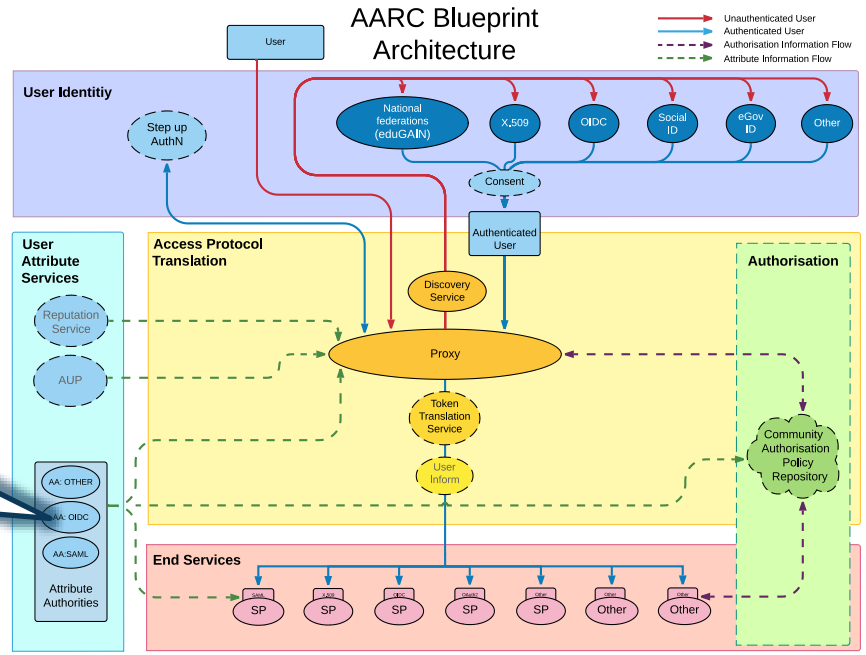
https://wiki.eoscfuture.eu/display/EOSCSMS/EOSC+Security+Operational+Baseline

# Evolving Security and Trust for attribute sources & proxies

## Beyond the baseline:
## supporting interoperable trust for the EOSC Federation

**Community membership management directories and attribute authorities**

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



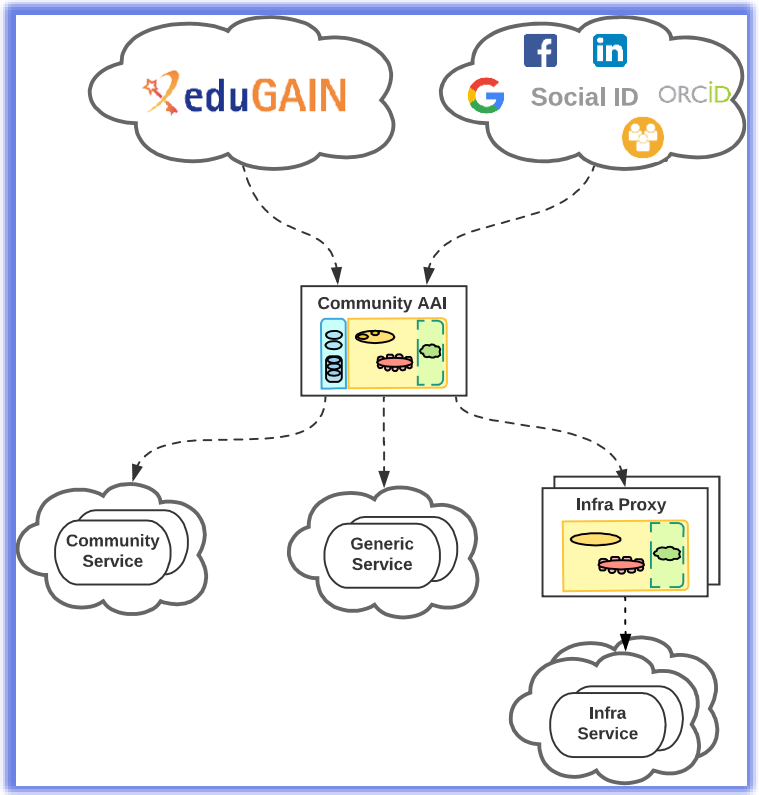
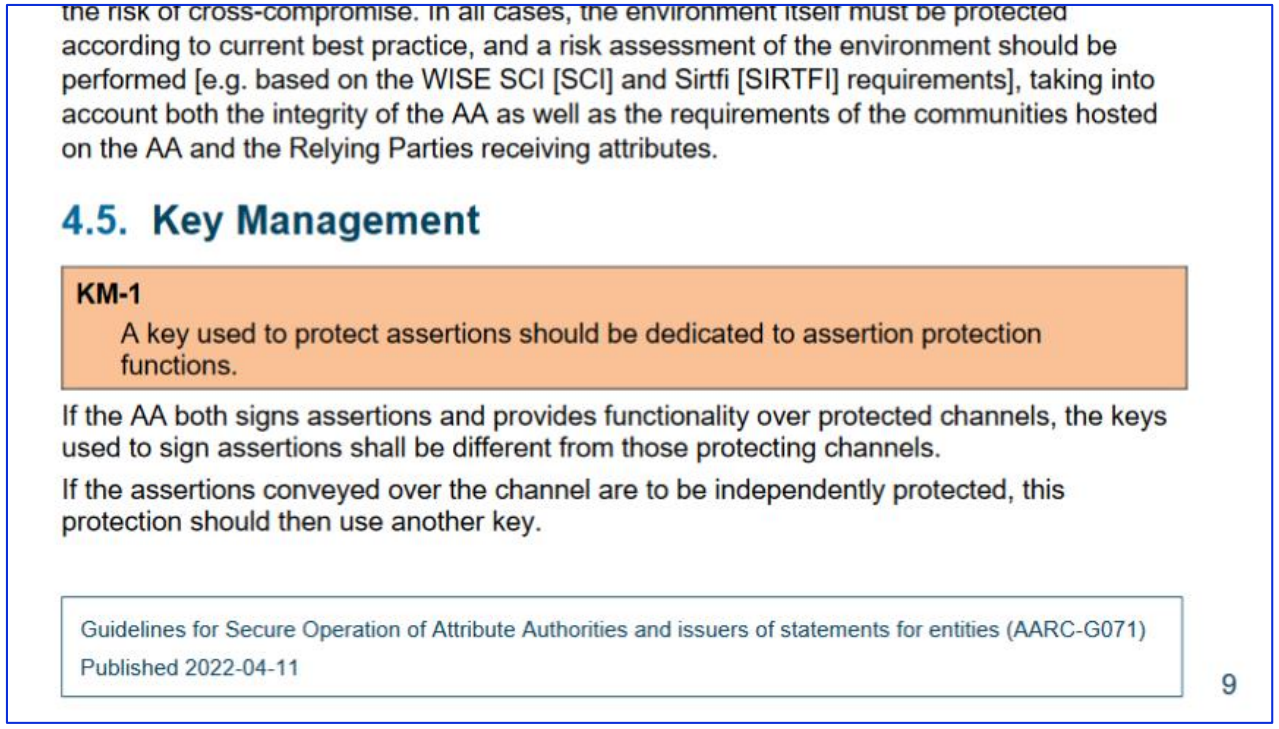




Image source: AARC Community
https://aarc-community.org/architecture/

# Specific guidance and implementation recommendations

Following the IGTF “Annotated Requirements” model, each statement is accompanies with implementation guidance. Technology neutral, i.e. both push and pull* models are in scope



the risk of cross-compromise. In all cases, the environment itself must be protected according to current best practice, and a risk assessment of the environment should be performed [e.g. based on the WISE SCI [SCI] and Sirtfi [SIRTFI] requirements], taking into account both the integrity of the AA as well as the requirements of the communities hosted on the AA and the Relying Parties receiving attributes.

## 4.5. Key Management

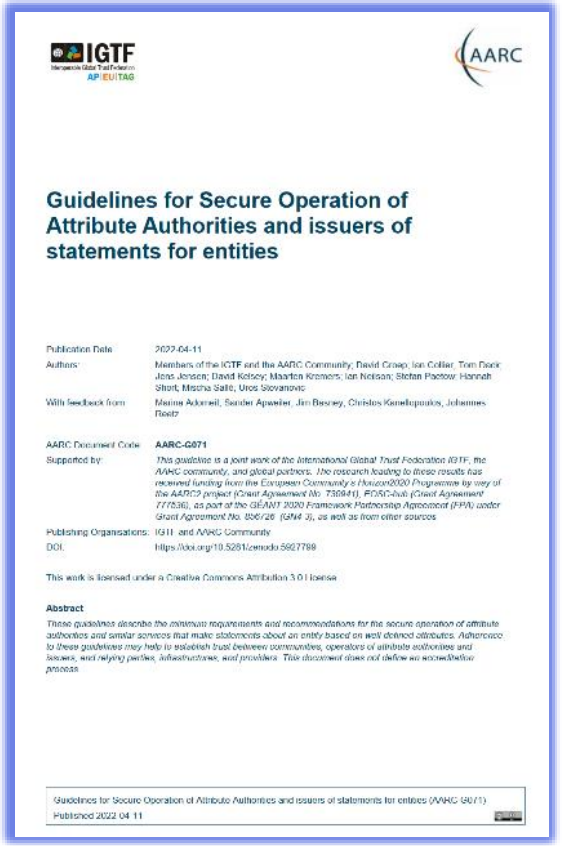
**KM-1**
A key used to protect assertions should be dedicated to assertion protection functions.

If the AA both signs assertions and provides functionality over protected channels, the keys used to sign assertions shall be different from those protecting channels.

If the assertions conveyed over the channel are to be independently protected, this protection should then use another key.

Guidelines for Secure Operation of Attribute Authorities and issuers of statements for entities (AARC-G071)
Published 2022-04-11

9



IGTF AP EU TAG

AARC

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

Publication Date: 2022-04-11

Authors: Members of the IGTF and the AARC Community; David Crooj; Ian Collier; Tom Dack; Jens Jensen; David Kelsey; Maarten Kremers; Ian Neilson; Stefan Paetow; Hannah Short; Mischa Salle; Uros Stevanovic

With feedback from: Maarja Adamell; Sander Apweiler; Jim Basney; Christos Kanellopoulos; Johannes Reetz

AARC Document Code: AARC-G071

Supported by: *This guideline is a joint work of the International Global Trust Federation IGTF, the AARC community, and global partners. The research leading to these results has received funding from the European Community's Horizon2020 Programme by way of the AARC2 project (Grant Agreement No. 730941), FOSC-hub (Grant Agreement 777536), as part of the GÉANT 2020 Framework Partnership Agreement (FPA) under Grant Agreement No. 856726 (GN4-3), as well as from other sources*

Publishing Organisations: IGTF and AARC Community

DOI: https://doi.org/10.5281/zenodo.5927799

This work is licensed under a Creative Commons Attribution 3.0 License

**Abstract**

*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 providers. This document does not define an accreditation process.*

Guidelines for Secure Operation of Attribute Authorities and issuers of statements for entities (AARC-G071)
Published 2022-04-11

aarc-community.org/guidelines/aarc-g071
https://doi.org/10.5281/zenodo.5927799
*see RFC2904 for the model descriptions*



EOSC Future

# Risk assessment

## Scalability and ‘ease of assessment’ by providers driving a new risk model

- usual ‘ISO-style’ risk frameworks need expert assessors to identify risks, appropriate controls, and assign risk ownership
- daunting task, and expertise is scarce

## Use ‘well-known-risks’ driven model, focussing on services, data, liability & trust

- ‘data breach’, ‘systems compromise’, ‘unattended vulnerability’, ‘weak configuration’, ‘DoS’, ‘composite dependencies on external services’
- provide tooling to facility self-assessment: sheet-based approach does not scale
- prepare the ground with a dry-run to generate example assessments
- start with the most critical components in EOSC (such as proxies, web-based tools like a marketplace,

# Is ‘the EOSC’ now ready to respond?

## Distance between operational security and (exchange) services remains large

- *not having face-to-face meetings is a hindrance for ‘conveying the message’*
- *a large and diverse community anyway*

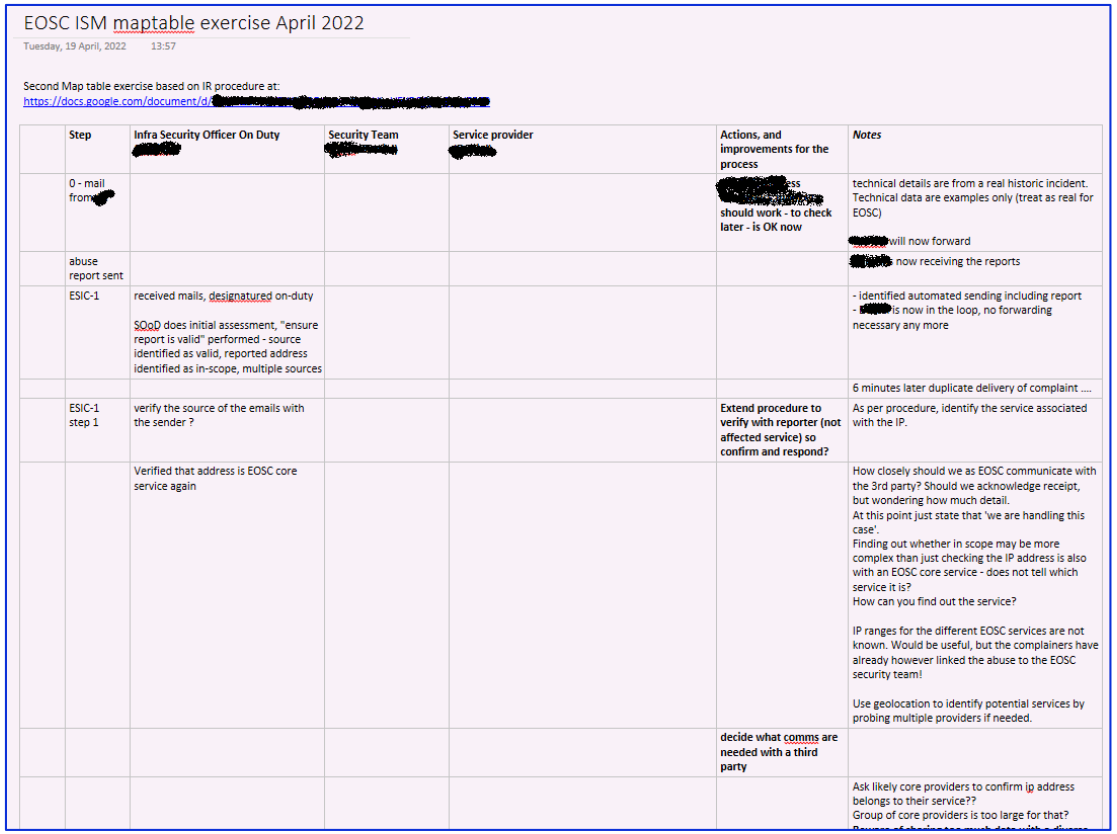
## Core services easier to identify

- security contact are in place
- service management system is known
- on-boarding process being rolled out

**and the security team is in place!**

*see subsequent talk by Pinja!*

## Communicate, exercise … and exercise again!



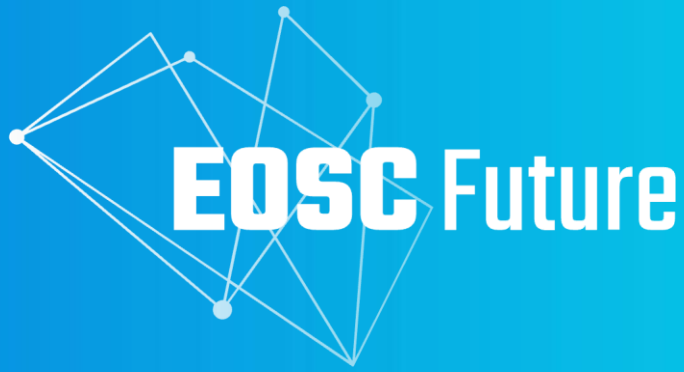
EOSC ISM maptable exercise April 2022

Tuesday, 19 April, 2022 13:57

Second Map table exercise based on IR procedure at:
https://docs.google.com/document/d[redacted]

| | Step | Infra Security Officer On Duty [redacted] | Security Team [redacted] | Service provider [redacted] | Actions, and improvements for the process | Notes |
|---|---|---|---|---|---|---|
| | 0 - mail from[redacted] | | | | [redacted] should work - to check later - is OK now | technical details are from a real historic incident. Technical data are examples only (treat as real for EOSC)<br>[redacted] will now forward |
| | abuse report sent | | | | | [redacted] now receiving the reports |
| | ESIC-1 | received mails, designatured on-duty<br><br>SOoD does initial assessment, "ensure report is valid" performed - source identified as valid, reported address identified as in-scope, multiple sources | | | | - identified automated sending including report - [redacted] is now in the loop, no forwarding necessary any more |
| | | | | | | 6 minutes later duplicate delivery of complaint .... |
| | ESIC-1 step 1 | verify the source of the emails with the sender ? | | | Extend procedure to verify with reporter (not affected service) so confirm and respond? | As per procedure, identify the service associated with the IP. |
| | | Verified that address is EOSC core service again | | | | How closely should we as EOSC communicate with the 3rd party? Should we acknowledge receipt, but wondering how much detail.<br>At this point just state that 'we are handling this case'.<br>Finding out whether in scope may be more complex than just checking the IP address is also with an EOSC core service - does not tell which service it is?<br>How can you find out the service?<br><br>IP ranges for the different EOSC services are not known. Would be useful, but the complainers have already however linked the abuse to the EOSC security team!<br><br>Use geolocation to identify potential services by probing multiple providers if needed. |
| | | | | | decide what comms are needed with a third party | |
| | | | | | | Ask likely core providers to confirm ip address belongs to their service??<br>Group of core providers is too large for that? |

Thanks to the EOSC Future WP7.5 collaborators: Alf Moens, Daniel Kouřil, Baptise Grenier, David Crooks, David Groep, David Kelsey, Ian Neilson, Linda Cornwall, Matt Viljoen, Pinja Koskinen, Ralph Niederberger, Romain Wartel, Sven Gabriel, and Urpo Kaila.




# Securing our EOSC web of FAIR data and services together!

eoscfuture.eu

Nikhef Maastricht University
**David Groep**
**https://www.nikhef.nl/~davidg/presentations/**
**https://orcid.org/0000-0003-1026-6606**

The EOSC Future project is co-funded by the European Union Horizon Programme call INFRAEOSC-03-2020, Grant Agreement number 101017536