AARC Authentication and Authorisation for Research and Collaboration

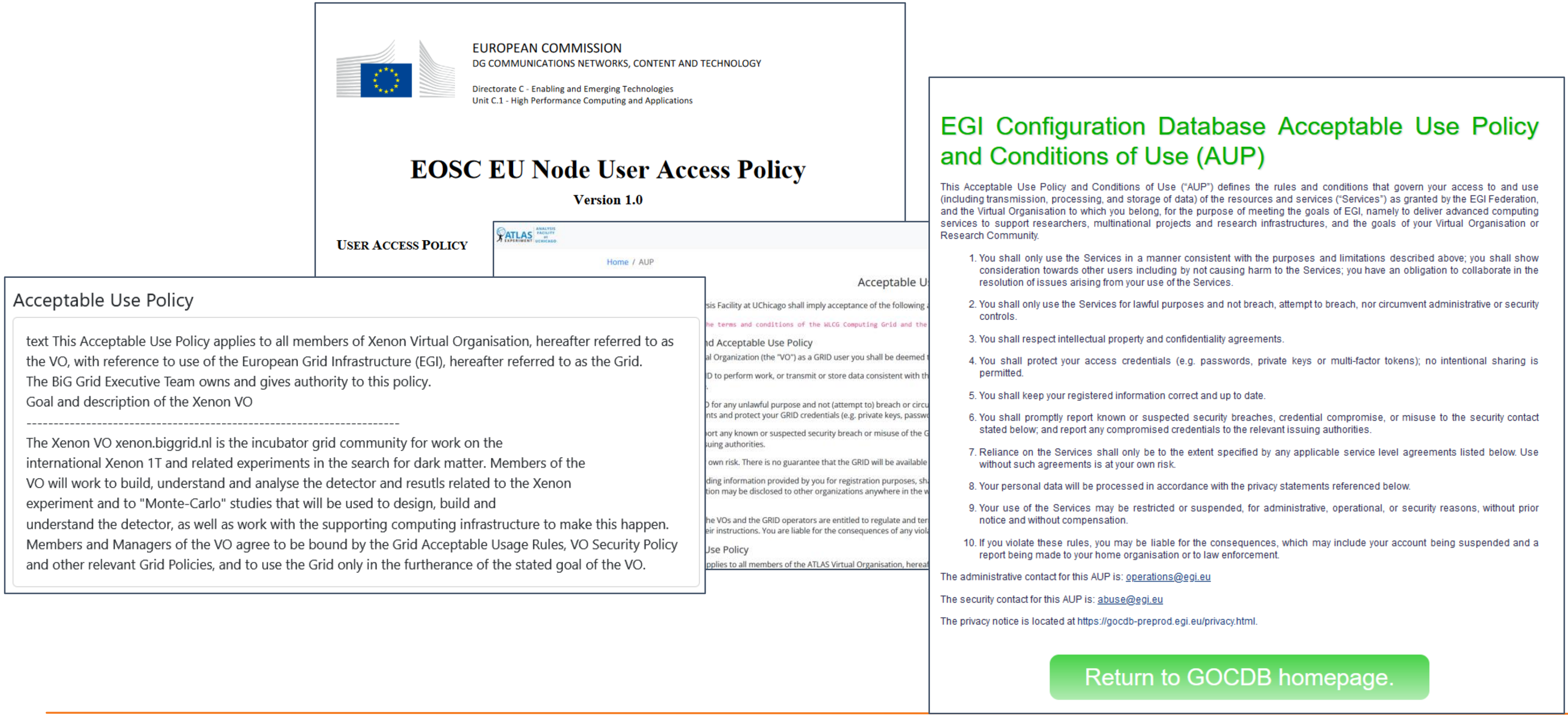
More resources with fewer clicks!

Notice management by AARC BPA proxies

David Groep
AARC Policy WG
Nikhef and Maastricht University

AEGIS meeting 2025-01-13
January 2025

How many of these?



EUROPEAN COMMISSION
DG COMMUNICATIONS NETWORKS, CONTENT AND TECHNOLOGY
Directorate C - Enabling and Emerging Technologies
Unit C.1 - High Performance Computing and Applications

EOSC EU Node User Access Policy

Version 1.0

User Access Policy

ATLAS EXPERIMENT
ANALYSIS FACILITY at UCHICAGO
Home / AUP

Acceptable U

sis Facility at UChicago shall imply acceptance of the following

he terms and conditions of the WLCG Computing Grid and the

d Acceptable Use Policy

al Organization (the "VO") as a GRID user you shall be deemed

D to perform work, or transmit or store data consistent with th

D for any unlawful purpose and not (attempt to) breach or circu
nts and protect your GRID credentials (e.g. private keys, passw

ort any known or suspected security breach or misuse of the G
uing authorities.

own risk. There is no guarantee that the GRID will be available

ding information provided by you for registration purposes, sh
tion may be disclosed to other organizations anywhere in the w

he VOs and the GRID operators are entitled to regulate and ter
eir instructions. You are liable for the consequences of any viol

Use Policy

pplies to all members of the ATLAS Virtual Organisation, hereaf

Acceptable Use Policy

text This Acceptable Use Policy applies to all members of Xenon Virtual Organisation, hereafter referred to as the VO, with reference to use of the European Grid Infrastructure (EGI), hereafter referred to as the Grid.
The BiG Grid Executive Team owns and gives authority to this policy.
Goal and description of the Xenon VO

The Xenon VO xenon.biggrid.nl is the incubator grid community for work on the
international Xenon 1T and related experiments in the search for dark matter. Members of the
VO will work to build, understand and analyse the detector and resutls related to the Xenon
experiment and to "Monte-Carlo" studies that will be used to design, build and
understand the detector, as well as work with the supporting computing infrastructure to make this happen.
Members and Managers of the VO agree to be bound by the Grid Acceptable Usage Rules, VO Security Policy
and other relevant Grid Policies, and to use the Grid only in the furtherance of the stated goal of the VO.

EGI Configuration Database Acceptable Use Policy and Conditions of Use (AUP)

This Acceptable Use Policy and Conditions of Use ("AUP") defines the rules and conditions that govern your access to and use (including transmission, processing, and storage of data) of the resources and services ("Services") as granted by the EGI Federation, and the Virtual Organisation to which you belong, for the purpose of meeting the goals of EGI, namely to deliver advanced computing services to support researchers, multinational projects and research infrastructures, and the goals of your Virtual Organisation or Research Community.

1. You shall only use the Services in a manner consistent with the purposes and limitations described above; you shall show consideration towards other users including by not causing harm to the Services; you have an obligation to collaborate in the resolution of issues arising from your use of the Services.
2. You shall only use the Services for lawful purposes and not breach, attempt to breach, nor circumvent administrative or security controls.
3. You shall respect intellectual property and confidentiality agreements.
4. You shall protect your access credentials (e.g. passwords, private keys or multi-factor tokens); no intentional sharing is permitted.
5. You shall keep your registered information correct and up to date.
6. You shall promptly report known or suspected security breaches, credential compromise, or misuse to the security contact stated below; and report any compromised credentials to the relevant issuing authorities.
7. Reliance on the Services shall only be to the extent specified by any applicable service level agreements listed below. Use without such agreements is at your own risk.
8. Your personal data will be processed in accordance with the privacy statements referenced below.
9. Your use of the Services may be restricted or suspended, for administrative, operational, or security reasons, without prior notice and without compensation.
10. If you violate these rules, you may be liable for the consequences, which may include your account being suspended and a report being made to your home organisation or to law enforcement.

The administrative contact for this AUP is: operations@egi.eu

The security contact for this AUP is: abuse@egi.eu

The privacy notice is located at https://gocdb-preprod.egi.eu/privacy.html.

WISE Baseline AUP

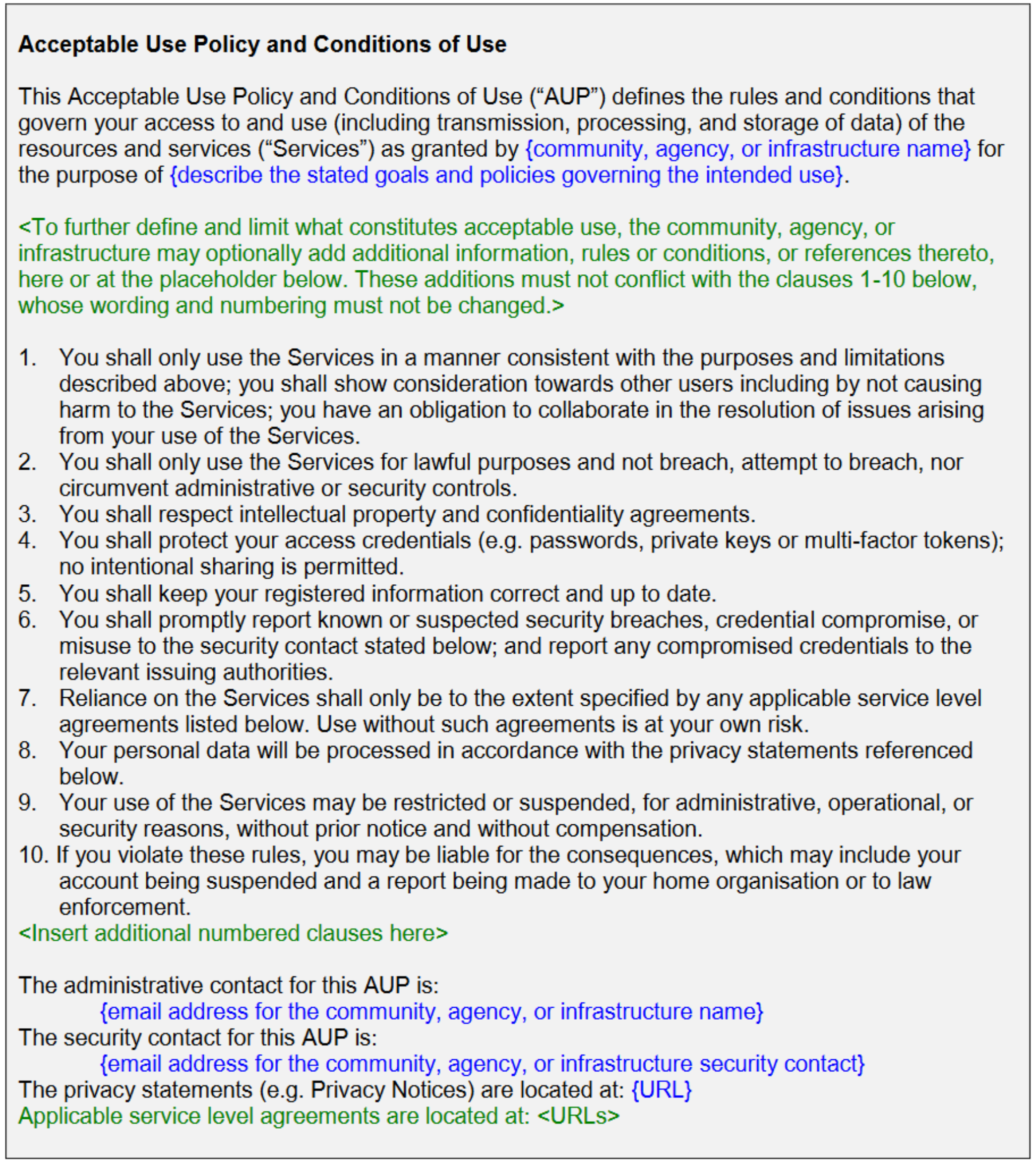
Template for a common and cascading AUP and T&C notice

by intent focusses primarily on *acceptable use*

- do not dwell on unintended use
- guarantee and service levels are T&Cs, not acceptable use interoperability

Placeholder model for

- *scope of the AUP* (purpose binding) – mirrored in Service Security operational baseline
- 10 commandments
- placeholder for additional T&Cs
- privacy notice references and authority



Acceptable Use Policy and Conditions of Use

This Acceptable Use Policy and Conditions of Use (“AUP”) defines the rules and conditions that govern your access to and use (including transmission, processing, and storage of data) of the resources and services (“Services”) as granted by {community, agency, or infrastructure name} for the purpose of {describe the stated goals and policies governing the intended use}.

<To further define and limit what constitutes acceptable use, the community, agency, or infrastructure may optionally add additional information, rules or conditions, or references thereto, here or at the placeholder below. These additions must not conflict with the clauses 1-10 below, whose wording and numbering must not be changed.>

1. You shall only use the Services in a manner consistent with the purposes and limitations described above; you shall show consideration towards other users including by not causing harm to the Services; you have an obligation to collaborate in the resolution of issues arising from your use of the Services.
2. You shall only use the Services for lawful purposes and not breach, attempt to breach, nor circumvent administrative or security controls.
3. You shall respect intellectual property and confidentiality agreements.
4. You shall protect your access credentials (e.g. passwords, private keys or multi-factor tokens); no intentional sharing is permitted.
5. You shall keep your registered information correct and up to date.
6. You shall promptly report known or suspected security breaches, credential compromise, or misuse to the security contact stated below; and report any compromised credentials to the relevant issuing authorities.
7. Reliance on the Services shall only be to the extent specified by any applicable service level agreements listed below. Use without such agreements is at your own risk.
8. Your personal data will be processed in accordance with the privacy statements referenced below.
9. Your use of the Services may be restricted or suspended, for administrative, operational, or security reasons, without prior notice and without compensation.
10. If you violate these rules, you may be liable for the consequences, which may include your account being suspended and a report being made to your home organisation or to law enforcement.

<Insert additional numbered clauses here>

The administrative contact for this AUP is:
{email address for the community, agency, or infrastructure name}
The security contact for this AUP is:
{email address for the community, agency, or infrastructure security contact}
The privacy statements (e.g. Privacy Notices) are located at: {URL}
Applicable service level agreements are located at: <URLs>

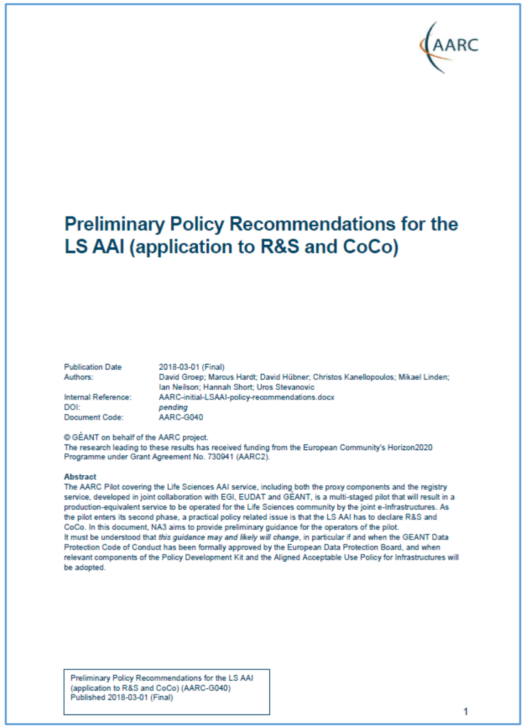
Proxies have more challenges as well: AUPs, T&Cs, Privacy notices, …

For large ‘multi-tenant’ proxies

- some subset users in some communities use a set of services – how to present their Terms and Conditions and their privacy policies, so that users
  - only see the T&Cs and notices for services they will access
  - this does not to need to be manually configured for each community
  - is automatically updated when services join

For community and dedicated proxies

- when new (sensitive) services join, who needs to see the new T&Cs?
- can we communicate existing acceptance of T&Cs to downstream services?



AARC

Preliminary Policy Recommendations for the LS AAI (application to R&S and CoCo)

Publication Date	2018-03-01 (Final)
Authors:	David Groep; Marcus Hardt; David Hübner; Christos Kanellopoulos; Mikael Linden; Ian Neilson; Hannah Short; Uros Stevanovic
Internal Reference:	AARC-initial-LSAAI-policy-recommendations.docx
DOI:	*pending*
Document Code:	AARC-G040

© GÉANT on behalf of the AARC project.
The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

Abstract
The AARC Pilot covering the Life Sciences AAI service, including both the proxy components and the registry service, developed in joint collaboration with EGI, EUDAT and GÉANT, is a multi-staged pilot that will result in a production-equivalent service to be operated for the Life Sciences community by the joint e-Infrastructures. As the pilot enters its second phase, a practical policy related issue is that the LS AAI has to declare R&S and CoCo. In this document, NA3 aims to provide preliminary guidance for the operators of the pilot.
It must be understood that *this guidance may and likely will change*, in particular if and when the GEANT Data Protection Code of Conduct has been formally approved by the European Data Protection Board, and when relevant components of the Policy Development Kit and the Aligned Acceptable Use Policy for Infrastructures will be adopted.

Preliminary Policy Recommendations for the LS AAI
(application to R&S and CoCo) (AARC-G040)
Published 2018-03-01 (Final)

1

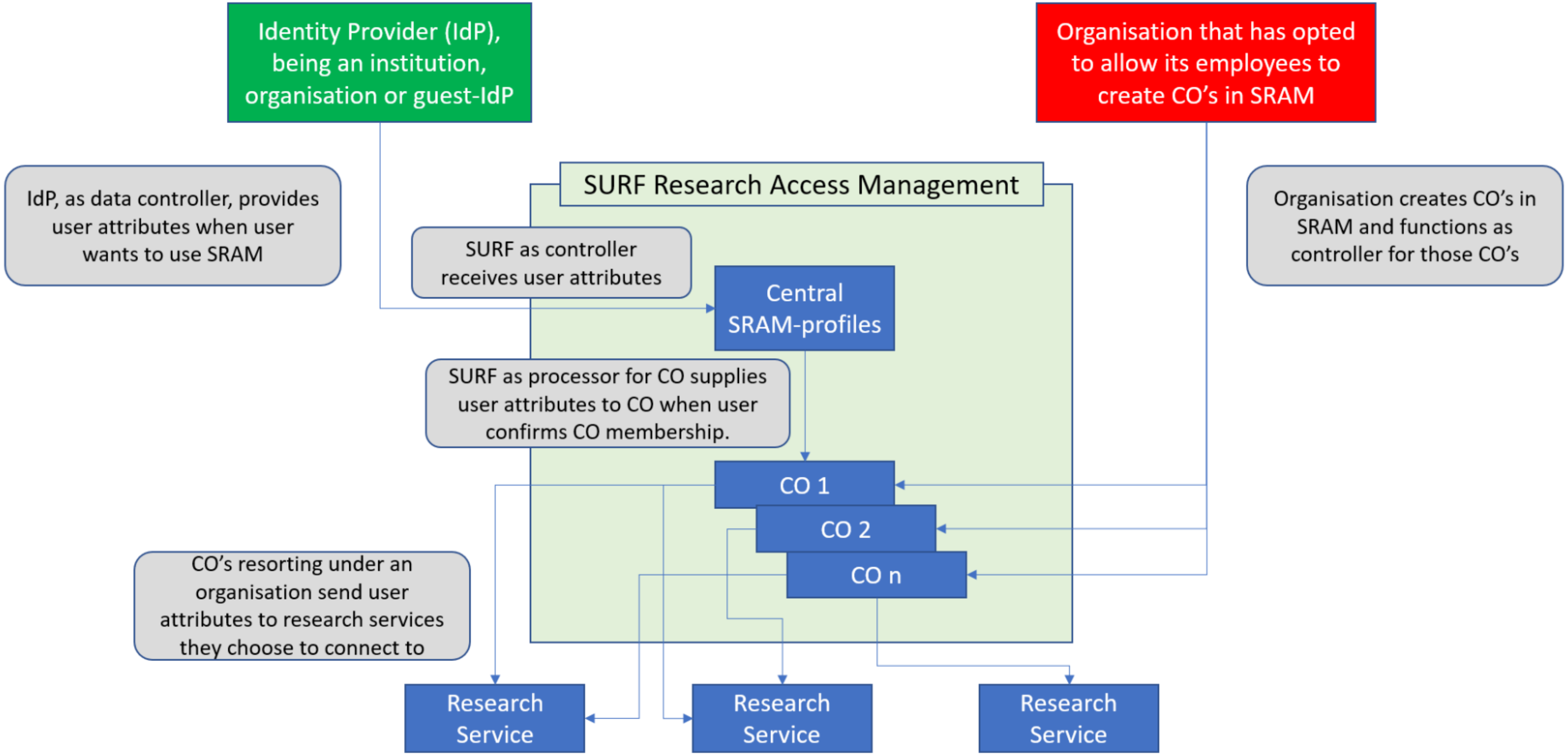
beyond AARC-G040

Limits to the I044 and G040 model

The introduction of multi-community and multi-tenancy proxies has changed that premise in two ways:

- the proxy does not equate the community, with multiple communities being hosted on the same proxy instance, or individuals registering first with the proxy in a generic mode (without specifying the community) and subsequently registering with one or more communities; and
- the proxy and the controller (as meant in the EEA GDPR) of access personal data (elaborated below) are not the same entity, and the role of the proxy operator may change over time even for the same user (as the user takes on different roles duing the registration life cycle in the proxy).

SURF SRAM multi-tenancy proxy and GDPR role assignments



Identity Provider (IdP), being an institution, organisation or guest-IdP

Organisation that has opted to allow its employees to create CO's in SRAM

IdP, as data controller, provides user attributes when user wants to use SRAM

SURF Research Access Management

SURF as controller receives user attributes

Organisation creates CO's in SRAM and functions as controller for those CO's

SURF as processor for CO supplies user attributes to CO when user confirms CO membership.

CO's resorting under an organisation send user attributes to research services they choose to connect to

Constraints on the notice management, depending on connected services?

Offline access and non-interactive (brokered) workflows

Activities that occur or continue to execute without user presence may require specific notices to be presented to the user to prevent abuse and unintended consequences. This in particular applies to OIDC flows that use the *offline_access* scope for requesting refresh tokens, as defined in the OpenID Connect Core specification section 11 (https://openid.net/specs/openid-connect-core-1_0.html#OfflineAccess).

In these cases, the OP (including a proxy) either MUST or SHOULD have explicitly received or have consent for offline access, depending on the application type as stated in the OIDC Core specification. To ensure the user does not need to be presented with an interstitial consent page, this request for explicit consent MUST be presented as part of the initial set of notices if the user workflow(s) are, or likely are, requiring offline access.

The service provider or proxy requiring offline access that is capable of presenting notice meta-data should signal this requirement in that way, and any service or proxy may (in lieu of or in addition) signal this by out-of-band mechanisms (e.g. in explicit agreements) for *single common notice* and *cascading notice* points in upstream proxies.

AARC G083 Notice Management by Proxies

Four presentation models. In order of preference

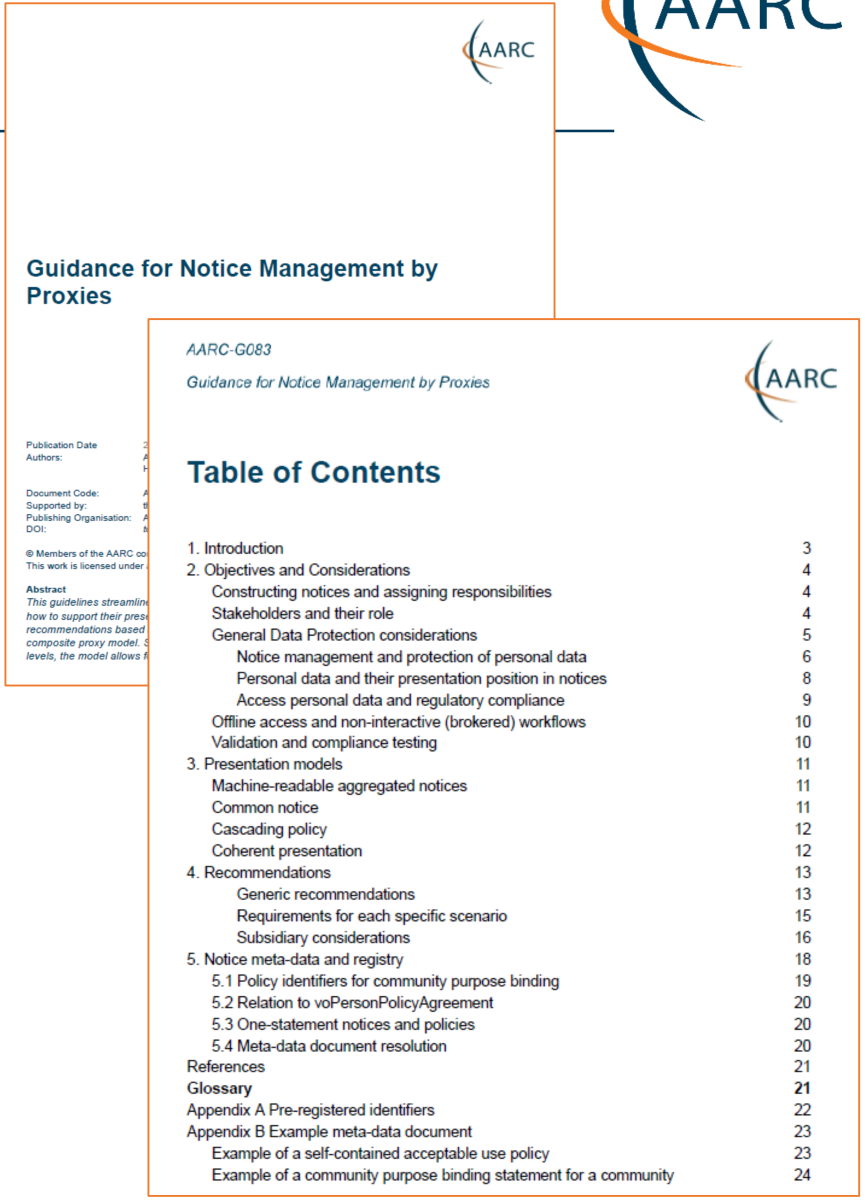
1. machine-readable aggregated notice
2. common notice (single common **authority domain**)
3. cascading notices (**assume responsibility** for underlings)
4. coherent presentation: you show what you need (but not more)

Generic recommendations

- use the WISE Baseline AUP composition model, record what and when user confirmed acceptance, and be able to confirm this downstream

plus a **machine-actionable model** to construct notices based on a hierarchy of proxies

- sufficient to build you a comprehensive WISE Baseline AUP
- and a set of privacy notices (for those GDPR encumbered)
- plus a namespace inspired by RFC6711's LoA registry



Guidance for Notice Management by Proxies

Publication Date
Authors:

Document Code:
Supported by:
Publishing Organisation:
DOI:

© Members of the AARC co
This work is licensed under

Abstract
This guidelines streamline
how to support their prese
recommendations based
composite proxy model. S
levels, the model allows f

AARC-G083
Guidance for Notice Management by Proxies

Table of Contents

https://aarc-community.org/guidelines/aarc-g083/

Recommendations – generic and per presentation model

- use of the WISE Baseline AUP is RECOMMENDED
- the notice presentation component MUST record, collect and retain time-stamped information related to notice presentation
- a notice presentation component that records logs about notice presentations SHOULD collect and retain necessary user contact information
- a service provider or proxy that is intentionally connected up-stream to an AARC BPA proxy MUST inform all accepted and acknowledged upstream proxy operators

But how to prevent duplicate presentation of ‘already confirmed’ notices?

- List of machine-readable **policies MUST be the same for all users of the service** and there SHOULD be one location to retrieve policy notice information per proxy, service/data provider (we *know* this is a limitation, but will catch 80+% of the use cases)
- When sending claims or attribute assertions towards downstream connected services and proxies, the proxy MUST include identifiers of all the policies to which the user has agreed, using the assigned policy identifiers and **send that via the *voPersonPolicyAgreement*** AVA or *vo_person_policy_agreeement* claim (multivalued)
- When a service or proxy keeps persistent state about a user, and as part of a transaction receives a *voPersonPolicyAgreement* identifier from a trusted party, it SHOULD associate this information with the user state, and MUST NOT present notices that are (according to that receiving service provider or proxy) materially equivalent to notices that the user has already received.

Can we construct all of the WISE Baseline AUP at the proxy?

Four elements are needed:

- the *purpose binding* for everything the user is going to experience
- the 10 commandments (or materially equivalent)
- aggregate of the terms and conditions for the proxy and the services behind it to which the user will (or may!) have access
  including limits on personal data processing for *data held within the service or data provider*
- list of privacy notices for connected services (‘two clicks away’)

plus the source(s) of authority for this combined notice

Mechanisms

- ‘meta-data’ for notice information at a well known endpoint
- voPersonPolicyAgreement signalling downstream on a per-user bases
- aggregation rules for included and augmenting notices
- notice types in line with the WISE Baseline AUP (purpose, acceptable-use, conditions, sla, privacy)
  where privacy notices are those for ‘access personal data’ as meant in REFEDS CoCo v2

and:

- include state information on validity, acceptance period, refresh period, and version
- multi jurisdiction (EEA and others) and multi-language are needed

Automatically constructing notices? Will that work? We can at least try!

```
{
  "id": "urn:doi:10.60953/68611c23-ccc7-4199-96fe-74a
  "aut": "https://www.nikhef.nl/",
  "aut_name": "Nikhef",
  "valid_from": 1649023200,
  "ttl": 604800,
  "contacts": [
    "helldesk@nikhef.nl",
    "information-security@nikhef.nl"
  ],
  "security_contacts": [
    "abuse@nikhef.nl"
  ],
  "privacy_contacts": [
    "privacy@nikhef.nl"
  ],
  "policy_class": "acceptable-use",
  "notice_refresh_period": 34214400,
  "includes_policy_uris": [
    "https://documents.egi.eu/document/2623"
  ],
  "policy_uri": "https://www.nikhef.nl/aup/",
  "description#nl_NL": "Deze Gebruiksvoorwaarden betr
netwerk en computers bij Nikhef. Iedere gebruiker van
wordt geacht op hoogte te zijn van deze voorwaarden e
  "description": "This Acceptable Use Policy governs
networking and computer services; all users of these services are expected to
understand and comply to these rules."
}
```

```
{
  "id": "https://operations-portal.egi.eu/vo/view/voname/xenon.biggrid.nl",
  "aut": "https://xenonexperiment.org/",
  "aut_name": "Xenon-nT collaboration",
  "valid_from": 1311890400,
  "ttl": 31557600,
  "contacts": [
    "grid.support@nikhef.nl",
  ],
  "security_contacts": [
    "vo-xenon-admins@biggrid.nl"
  ],
  "policy_class": "purpose",
  "augments_policy_uris": [
    "https://wise-community.org/wise-baseline-aup/v1/"
  ],
  "policy_uri": "https://operations-
portal.egi.eu/vo/view/voname/xenon.biggrid.nl",
  "description": "detector construction and experiment analysis for the search
of dark matter using Xenon detectors"
}
```

Identifying notices for composition

Identifiers registered under this guideline require to:

- Be in the form of a URI,
- Be assigned a name, being a string uniquely and unambiguously identifying the notice for use in human presentation, and in protocols where URIs are not appropriate, and
- Include a resolvable http or https informational URL pointing to a JSON document containing additional structured information.

And

- it SHALL NOT be used for identity assurance levels: we have RFC6711 for that
- but it *does* establish a registry for notices (and a resolver) akin to the IANA one for LoA's

and, no, there is no formal schema yet, just the textual description and the examples

and we know that voPersonPolicyAgreement needs a small update (URL->URI)

Submitted to you, but welcoming feedback

https://aarc-community.org/guidelines/aarc-g083/

Welcome your feedback (and implementation)
on applicability,
on the four representation types *and*
on the meta-data json document format/schema

Thank you

Any Questions?

davidg@nikhef.nl

AARC

https://aarc-community.org

The work leading to these results has received funding from the European Union and other sources.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them. Grant Agreement No. 101131237 (AARC TREE).

- **id (required, single-value):** string containing the URI of the identifier for the policy
- **aut (recommended, single-value):** URI identifying the authority governing this policy. It is recommended to use identifiers assigned by a recognised naming agency (such as a LEI-based URN) or long-term stable URL to the main web presence of an organisation. For privacy notices as meant in the EU GDPR (policy_class: “privacy#eu”), this SHOULD identify the data controller.
- **aut_name (required, single-value):** plain-text human-readable and disambiguating name of the authority (used in the WISE Baseline AUP preamble)
- **valid_from (recommended, single-value):** time from which this policy is in effect. This is expressed as Seconds Since the Epoch. When present, this value MUST increment whenever there is a minor change to the policy referring to this informational document. Note that major material changes SHOULD be assigned a new policy URI (id). Minor and major are defined discretionarily by the authority for the policy.
- **ttl (optional, single-value):** the time period after which this document SHOULD be retrieved again by consumers. This is expressed in seconds. In absence of this key, the document SHOULD NOT be retrieved more often than once a day; should be cached.

- **contacts (required, multi-value),**
  security_contacts (recommended, multi-value),
  privacy_contacts (recommended, multi-value): JSON arrays with one or more strings representing contact persons at the Entity. These MAY contain names, e-mail addresses, descriptions, phone numbers, etc. (incorporated from OpenID Federation 1.0) (used in the WISE Baseline AUP postscript)

- **policy_class (required, single-value):**
  string from the limitative enumeration: ‘purpose’, ‘acceptable-use’, ‘conditions’, ’sla’, ’privacy’.

  The value ‘privacy’ MAY be qualified with a jurisdiction (e.g. ‘privacy#eu’). Jurisdictions SHALL use IANA ccTLD identifiers where possible. The jurisdiction value “eea” MAY be used to indicate the European Economic Area (e.g. “privacy#eea” will indicate a privacy policy in accordance with Regulation (EU) 2016/679 ‘GDPR’). Assigned subdomain names under the .int TLD MAY be used to indicate international organisations holding their own jurisdiction (e.g. “privacy#cern.int” will indicate a policy in accordance with CERN’s OC11).

  The policy_class ‘privacy’ applies to privacy policies governing service access data only (i.e. data used *for enabling access*, as meant in the REFEDS Data Protection Code of Conduct). Policies regarding privacy of the data processed in the service or in services connected to the proxy MUST be expressed in a ‘conditions’ policy_class.

- **notice_refresh_period (optional, single-value):** number of seconds after which this same notice has to be presented again to the same user, regardless of any earlier acceptance. Used to trigger periodic re-acceptance of e.g. acceptable use policies.
- **includes_policy_uris (optional, multi-value):** JSON array of policy URIs that are included in this policy and therefore implicitly fulfilled. Those policy URIs SHOULD be listed in the registry (which is machine-readable, but machine-readable only) . This list MAY include also policies that are superseded by this policy, if the material content of deprecated policies is fully subsumed in this policy.
- **augments_policy_uris (optional, multi-value):** JSON array of policy URIs that are augmented by this policy, e.g. the WISE Baseline AUP itself. A presenting application MAY merge the presentation of this policy and any policies this policy augments.
- **policy_uri (recommended, single-value):** URL of the documentation of conditions and policies in human-readable form (incorporated from OpenID Federation 1.0)
- **description (recommended):** shortest plain-text human-readable description of the policy to be used for presentation in composite notices (used in the WISE Baseline AUP preamble)

All human-readable keys (aut_name, description) MAY be postfixed with a hash-sign followed by a locale code in RFC 4646 format (example: aut_name#nl_NL: “nationaal instituut”).

5.4 Meta-data document resolution

- The resolution mechanism for meta-data JSON documents SHOULD be left to the AARC Architecture working group. The resolution set MAY be of the form of a HTTP GET request for a document at *https://nr.aarc-community.org/resolv/v1/<URL-encoded-URI>*. This URL MUST result in a 301 “Moved Permamently” response, and include a HTTP response “Location” header indicating the URL of the JSON meta-data document.

For the prior example …

- It might potentially then be retrievable from https://nr.aarc-community.org/resolv/v1/https%3A%2F%2Foperations-portal.egi.eu%2Fvo%2Fview%2Fvoname%2Fxenon.biggrid.nl
- Following AARC-G069, the identifier could have been auto-completed, once a namespace has been defined for BiG Grid communities. In that case, the identifier would have been “urn:geant:nikhef.nl:projects:biggrid:group:xenon”, with associated resolver URL https://nr.aarc-community.org/resolv/v1/urn%3Ageant%3Anikhef.nl%3Aprojects%3Abiggrid%3Agroup%3Axenon