FAIR-IMPACT
Expanding FAIR solutions across EOSC

Project Title	Expanding FAIR solutions across EOSC
Project Acronym	FAIR-IMPACT
Grant Agreement No.	101057344
Start Date of Project	2022-06-01
Duration of Project	36 months
Project Website	www.fair-impact.eu

Deliverable D3.3 - Guidelines for creating a user tailored EOSC Compliant PID Policy

Work Package	**WP 3, Persistent Identifiers**
Lead Author (Org)	**René van Horik (DANS-KNAW)** **Wim Hugo (DANS-KNAW)**
Contributing Author(s) (Org)	**Joy Davidson (DCC)** **Josefine Nordling (CSC)** **Liisa Marjamaa-Mankinen (CSC)** **Lassi Lager (CSC)** **Gabriela Mejias (DataCite)** **Elizabeth Newbold (STFC)**
Due Date	**2024-05-31**
Date	**2024-05-30**
Version	**V1.0 - DRAFT NOT YET APPROVED BY THE EUROPEAN COMMISSION**

Dissemination Level	
X	PU: Public
	PP: Restricted to other programme participants (including the Commission)
	RE: Restricted to a group specified by the consortium (including the Commission)
	CO: Confidential, only for members of the consortium (including the Commission)

Funded by the European Union

Versioning and contribution history

Version	Date	Author	Notes
0.1	2024.01.17	Wim Hugo	Inception, outline, content description
0.2	2024.03.14	Wim Hugo	Added guidelines discussed and annotated at the EOSC Winter School, Jan/Feb 2024
0.3	2024.04.10	René van Horik	Restructure of report
0.4	2024.04.29	René van Horik	Concept version of deliverable
0.5	2024.05.03	René van Horik Wim Hugo	Version for review with task members, Joy Davidson, Josefine Nordling, Liisa Marjamaa-Mankinen, Lassi Lager, Gabriela Mejias, Elizabeth Newbold
0.9	2024.05.03	René van Horik Wim Hugo	Version for internal review
1.0	2024.05.31	René van Horik	Version for community consultation following internal review by Olivier Rouchon, Esteban Gonzalez, Vasso Kalaitzi

Disclaimer

FAIR-IMPACT has received funding from the European Commission's Horizon Europe funding programme for research and innovation programme under the Grant Agreement no. 101057344. The content of this document does not represent the opinion of the European Commission, and the European Commission is not responsible for any use that might be made of such content.

TERMINOLOGY

Terminology/Acronym	Description
CAT	Compliance Assessment Toolkit, a service being developed in the FAIRCORE4EOSC project to assist with EOSC PID Policy compliance assessment
Compliance Assessment	The process of determining to what extent a service, object, organisation, or capabilities comply with a set of criteria, based on reproducible tests
PID Authority	A controller responsible for maintaining the rules for defining the integrity of PIDs within a PID Scheme. These rules may include setting standards for lexical formats, algorithms, and protocols to ensure global uniqueness, together with setting quality of service conditions to enforce compliance to the rules.
EOSC PID Policy	The policy being developed by the EOSC PID Policy and Implementation Task Force to ensure a minimum standard of performance for the PID ecosystem in EOSC
PID Ecosystem	The collection of standards, services, actors, and roles that enable a specific PID Stack to provide a service, together with the specific end users of the PID Stack
PID Landscape	The supply of and demand for PID Services and the rules that govern the exchange
PID Manager	PID Managers have responsibilities to maintain the integrity of the relationship between entities and their PIDs, in conformance to a PID Scheme defined by a PID Authority
PID Scheme	A set of rules and standards defining the nature of a PID. This would include a set of lexical formatting rules for PIDs within a namespace. It could also define for example: associated PID Type; definition of associated metadata; quality assurance conditions; usage rights, terms and conditions, and algorithmic methods for generating PID names and enforcing PID properties.
PID Stack	The collection of services and actors, supported by standardisation, resolution mechanisms, and namespace management that results in a branded or unique PID Service to PID Managers

Table of Contents

Funded by the European Union

List of Figures

List of Tables

Executive Summary

FAIR-IMPACT aims to support the implementation phase of the European Open Science Cloud (EOSC) by helping Research Performing Organisations (RPOs), such as Higher Education Institutes, repositories and data and metadata service providers, and national initiatives to adopt FAIR-enabling practices, tools and services.

Persistent Identifiers (PIDs) are an essential component of the FAIR principles. In 2020 a Persistent Identifier (PID) policy for the European Open Science Cloud[1] was published that aims to be of interest for all EOSC stakeholders. The policy "defines a set of expectations about what PIDs will be used to support a functioning environment of FAIR research." The EOSC PID policy is one of the foundations of the activities under FAIR-IMPACT Task 3.3 entitled "EOSC PID policy alignment and support" and of which this report is the formal deliverable. The main target group of the activities in Task 3.3 are PID Managers, who have the responsibility to maintain the integrity of the relationship between entities and their PIDs. PID Managers may include a provider of a data repository, a data catalogue, or a research workflow system.

The main topic of this report concerns the formulation of guidelines for PID Managers regarding the creation of a "user tailored EOSC compliant PID policy." Central to the work of T3.3 are the following questions. How can we determine the quality of the EOSC PID policy and - in collaboration with all stakeholders - how can we implement a user tailored PID policy? In other words, what principles, roles and criteria can we distinguish when it comes to the use of PIDs in the EOSC. To answer this question, we need to thoroughly and systematically analyse the PID landscape (of which PID Managers are a part). For this, we are working closely with the FAIRCORE4EOSC project in which a Compliance Assessment Toolkit (CAT) is being developed.[2] The CAT will support PID Managers and others with services to encode, record, and query compliance with the policy. The EOSC PID policy is, as a case study, analysed with the CAT. This requires mapping the PID landscape, that is the supply of and demand for PID Services and the rules that govern the exchange. The EOSC PID Policy and Implementation Task Force which, among other things, is working on an update of the EOSC PID policy, by processing recommendations and best practices provided by the CAT method.

By distinguishing between the different actors in the PID ecosystem and formulating which criteria these actors should meet (as well as providing evidence that these criteria have or have not been met), T3.3 contributes to improving the EOSC PID policy and alignment of PID infrastructures with EOSC policy and architecture. Workshops and webinars have been

[1] European Commission, Directorate-General for Research and Innovation, Hellström, M., Heughebaert, A., Kotarski, R. et al., A Persistent Identifier (PID) policy for the European Open Science Cloud (EOSC), Publications Office, 2020, https://data.europa.eu/doi/10.2777/926037

[2] See: https://faircore4eosc.eu/eosc-core-components/compliance-assessment-toolkit-cat [Cited 21 april 2024]

organised to align the work with stakeholders (such as the EOSC PID Policy and Implementation Task Force as well as other EOSC projects).[3]

The activities in this task facilitated the discussion to elaborate the formulation and assessment of PID policies in a standard and comprehensive manner. In total 16 guidelines for formulating PID policies are compiled and presented in chapter 4. On this basis, targeted support can be provided for the formulation of EOSC compliant PID policies as provided by the FAIR-IMPACT project. This is a task in the FAIR-IMPACT PID work package T3.4 that follows the completion of the work in T3.3.

[3] For information on the workshops see: “Milestone 3.6. 3 PID Policy Alignment Workshops and Feedback Report”. 10.5281/zenodo.11371085

Funded by the European Union

1 Introduction and Context

The objective of WP3 “Persistent Identifiers” of the FAIR-IMPACT project is to “work with PID Service providers and infrastructures to meet user needs, align with EOSC policy and maximise uptake”. The WP consists of four tasks. T3.1 “Setting up a coordination mechanism for EOSC PID Service providers” works towards a shared long-term vision for PID Service providers on PID usage in EOSC. T3.2 “integration of PID practices into FAIR data management” works on use cases focusing on user needs and reproducible research. Examples are PIDs in managing workflows and PIDs for sensitive data. The main objective of T3.3 “EOSC PID policy alignment and support” is to provide support for defining PID policies in line with the EOSC PID policy. The last task of this WP, T3.4 “PID implementation”, is mainly aimed at practical support for creating EOSC compliant PID policies. This report is related to T3.3 of WP3 and is the first deliverable of the work package. Table 1 provides an overview of the tasks of WP3.

Task	Title	Main goal / activities
T3.1	Setting up a coordination mechanism for EOSC PID Service providers	• Assessment of PIDs for different objects (including “emerging” PIDs) • Aligning requirements for onboarding PID providers into EOSC • Development of long-term vision for PID Service providers
T3.2	Integration of PID practices into FAIR data management	• Collection of PID requirements for sensitive, dynamic, sensor, and workflow data • Providing user guidelines for EOSC PID implementation in FAIR data management
T3.3	EOSC PID policy alignment and support	• Identification of different EOSC actors and mapping of existing PID policies in use • Analysis of the compliance (using CAT) of existing policies with the EOSC PID policy • providing guidelines for formulating PID policies (in compliance with the EOSC PID Policy)
T3.4	PID implementation	• Offering practical implementation support for creating EOSC compliant PID policies • Assessing PID compliance of different repositories and services

Table 1 - Overview of Task in Work package 3 “Persistent Identifiers”

The main goal of T3.3 is to provide support for establishing PID policies in accordance with the EOSC PID policy. To achieve this goal, as listed in Table 1, three types of activities were conducted.

The first activity, identification of different EOSC actors and mapping of existing PID policies in use, aims to describe the "PID Landscape", that "refers to a loosely coupled collection of services, end users, and governance mechanisms that impact either users, services, or both - in essence, the supply of and demand for PID Services and the rules that govern the exchange."[4] The PID Landscape and its related concepts are covered in Chapter 2, "The PID Landscape".

The second activity in this task concerns the compliance of existing PID policies with the EOSC PID policy. To achieve this goal, two conditions must be met. First, a compliance assessment method must be available and second, there must be an EOSC PID policy that can be analysed. Compliance assessment concerns the process of determining to what extent a service, object, organisation, or capabilities comply with a set of criteria based on reproducible tests.[5] The FAIRCORE4EOSC project develops the Compliance Assessment Toolkit (CAT) that is used in this activity. Concerning the second condition, the availability of an EOSC PID policy the following can be noted. In 2020 "A Persistent Identifier (PID) policy for the European Open Science Cloud"[6] was published. In 2021 the EOSC Association installed task forces to address key areas of the implementation of the EOSC and the EOSC PID Policy and Implementation Task Force (PID TF) was one of them. Among other things the PID TF "will provide different kinds of recommendations on PIDs management and will set up criteria and certification of PIDs."[7] Communication between T3.3 and the PID TF is essential to achieve the goals of T3.3 and also has taken place. The EOSC PID policy was analysed with the CAT conceptual model and the results were discussed with the EOSC Task Force and this will be reported in Chapter 3 "Compliance Assessment of PID policies". It should be noted that the results of the EOSC PID policy evaluation by the CAT are not endorsed by the EOSC Association and that a strategic reorganisation of task forces is underway which means that the PID TF is no longer active. So it has to be seen to what extent the results of the compliance assessment will be taken into consideration by the EOSC in the future.[8]

The third activity in T3.3, and main focus of this deliverable, concerns the formulation of guidelines for PID policies, in line with the assessed EOSC PID policy, targeting a specific actor in the PID landscape (as presented in chapter 2), namely the PID Manager. In chapter 3

[4] See: Hugo, W., Van de Sompel, H., & Hakala, J. (2024). The PID Landscape - a Technical View (0.8.0 Draft). https://doi.org/10.5281/zenodo.11108203. The report was compiled in a joint effort between FAIRCORE4EOSC WP2 and FAIR-IMPACT Task 3.3. The document serves as a knowledge base for this report, and is a source of data and contextual information about the provision and application of PIDs.
[5] Hugo, W., Steinhoff, W., Turner, D., Buys, M., & Zamani, T. (2023). D2.1 Compliance Assessment Specification. Zenodo. https://doi.org/10.5281/zenodo.10067253 p 2.
[6] European Commission, Directorate-General for Research and Innovation, Hellström, M., Heughebaert, A., Kotarski, R. et al., A Persistent Identifier (PID) policy for the European Open Science Cloud (EOSC), Publications Office, 2020, https://data.europa.eu/doi/10.2777/926037
[7] https://eosc.eu/advisory-groups/pid-policy-implementation/ [Cited 20 april 2024]
[8] Further communication on this issue occurred during the EOSC Winter School 2024 (Thessaloniki, 29 January - 1 February 2024) where projects and members of the PID TF identified efforts, challenges and opportunities for future collaboration on PIDs. See:
https://eosc.eu/news/2024/05/report-on-the-eosc-winter-school-2024-is-released/ [Cited 23 may 2024]

Funded by the European Union

analyses of the 2020 EOSC PID policy (using the CAT) are presented. General criteria, guidelines and best practices that can be extracted from this analysis are presented in Chapter 4 "Guidelines for formulating PID policies for PID Managers". The ambition of these guidelines is that they provide a solid foundation for further quality assessment of all actors in the PID landscape.

Funded by
the European Union

2 The PID Landscape

PIDs are identifiers that can be assigned to any type of object (physical or digital). They are mostly being assigned to persons, organisations, and research outputs. Their purposes (besides persistent identification) are to improve research management and information retrieval.[9]

A way to map out all the uses and dependencies of PIDs is to formulate a "PID Landscape" and within T3.3 an information model that represents the PID Landscape is defined and provided in Figure 1. The PID Landscape contains the supply of and demand for PID Services and the rules that govern the exchange. The information model is derived iteratively by gathering information about the landscape, and noting the main nodes, and the relations. A comprehensive review of literature and web-based resources is used to determine the characteristics of supply and demand of persistent identifiers.[10] The information model can be further expanded and modified in the future.

The aim of the PID Landscape information model is to cater for a wide range of stakeholders, such as PID Service providers, PID users and PID authorities (These are the "Actors and Roles" in Figure 1). For now we will cover the information model with the main target group this report in mind: PID Managers. PID Managers have, as one of their main responsibilities, to maintain the integrity of the relationship between entities and their PIDs, in conformance to a PID scheme defined by a PID authority. A PID Manager will typically subscribe to PID Services to offer functionality to PID owners within the PID Managers' services. One example is a service provider which uses PID Services as part of its own service delivery. PID Managers may include a provider of a data repository, a data catalogue, or a research workflow system.[11]

[9] de Castro, P., Herb, U., Rothfritz, L., & Schöpfel, J. (2023). Building the plane as we fly it: the promise of Persistent Identifiers. Zenodo. https://doi.org/10.5281/zenodo.7258286 p 9. The relevance of PIDs to support the FAIR principles are covered extensively in this publication.

[10] See: Hugo, W., Van de Sompel, H., & Hakala, J. (2024). The PID Landscape - a Technical View (0.8.0 Draft). https://doi.org/10.5281/zenodo.11108203.

[11] Hugo, W., Steinhoff, W., Turner, D., Buys, M., & Zamani, T. (2023). D2.1 Compliance Assessment Specification. Zenodo. https://doi.org/10.5281/zenodo.10067253 p 29.

Funded by the European Union

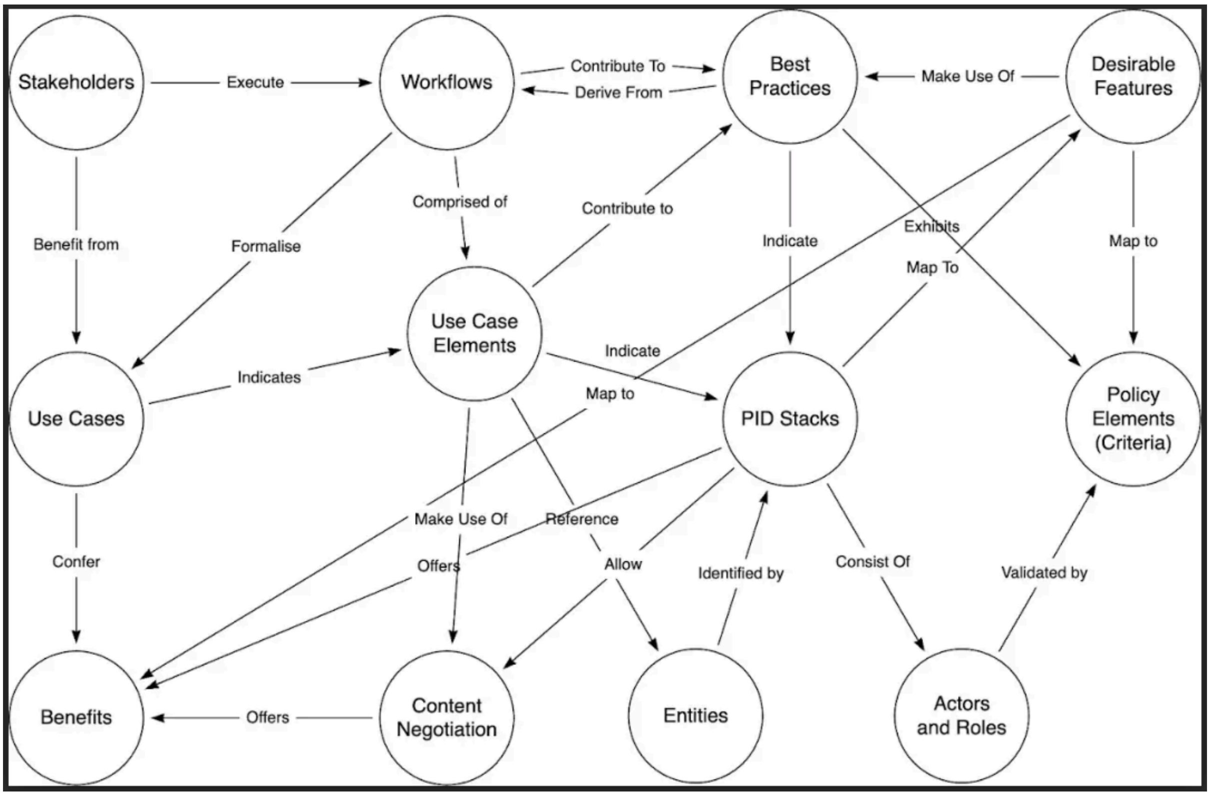


Figure 1 - Information model for the PID landscape[12]

With the role as PID Manager in mind, a journey through the PID landscape as shown in Figure 1 can be made by visiting the most interesting places in the landscape. This journey is described below.

- The PID Manager, as **Stakeholder**, benefits from implementation of a number of **Use Cases** (see section 2.3), but these use cases are generally not well structured or standardised, and are described arbitrarily in terms of structure and granularity. It is possible to extract common **Use Case Elements**, and these can be included into more structured and well-defined (possibly machine-actionable) **Workflows**[13].

- PID Managers can execute one or more Workflows in practice to obtain the **Benefits** of **PID Stacks** (see section 2.2), the collection of services and actors, supported by standardisation, resolution mechanisms, and namespace management that results in a branded or unique PID Service to PID Managers. An example of a PID Stack is a DOI (as a PID) that identifies an object in the Zenodo repository (as PID Manager). This DOI is provided by Datacite as a registration agency. A DOI is a specific

[12] The model will change as new information is obtained that may not fit the model. The authoritative version can be found here [Cited 23 april 2024]

[13] Comprehensive attention for PIDs in workflows can be found in: Brown, J., Jones, P., Meadows, A., & Murphy, F. (2022, September 16). PID-optimised workflows: A vision of a more efficient future. Zenodo. https://doi.org/10.5281/zenodo.7085489

Funded by the European Union

implementation of the Handle identifier, consisting of a prefix and a suffix, whereas the DOI has a specific prefix and is a dedicated implementation of a Handle. Datacite in turn is supported by the International DOI Foundation that governs the DOI system. The DONA foundation, another component of this PID Stack, has the responsibility for the overall administration of the "Global Handle Registry". The components described above together form a PID Stack. Much more PID Stacks can be distinguished in the PID Landscape.

- The PID Stacks are used to *persistently and unambiguously identify* **Entities**. Some PID Stacks may offer additional **Content Negotiation**[14] that provides more **Benefits** beyond persistent identification and resolution, and these include exposure of metadata, linking to additional information, version histories, and distinguishing links to the object, its context, etc. A more detailed treatment of the concept of PID Stack follows later in this chapter.

- The Workflows are ideally based on **Best Practices**, in turn defined and refined by a review of the most commonly adopted workflows, **use case elements**, and PID Stacks in the community. The Best Practices also ensure that **Desirable Features** of PID Stacks are fully utilised.

- PID Stacks are implemented (operationalised) by a combination of **Actors and Roles** in the PID Ecosystem (covered further on in this chapter). The PID **Policy Elements** developed for EOSC should ensure that the most important Desirable Features of PID Stacks are guaranteed to the Stakeholders by assigning compliance criteria to Actors. This aspect links Compliance Assessment for the EOSC PID Policy and is covered in the next chapter.

2.1 PID Ecosystem

The **PID Landscape** refers to a loosely coupled collection of services, end users, and governance mechanisms that impact either users, services, or both - in essence, the supply of and demand for PID Services and the rules that govern the exchange. It also includes a variety of stakeholders that rely on these services. The **PID Ecosystem** refers more specifically to the collection of standards, services, actors, and roles required to ensure that PIDs are unique and remain resolvable over time. The PID Landscape information model forms the knowledge base that describes the PID Ecosystem.

The current state of the PID Ecosystem model is discussed below and shown in Figure 2, based on a review of several PID Services. The EOSC PID policy provides a good starting point for the characterisation of the actors and roles involved in the PID Ecosystem.

[14] Content negotiation allows a user to request a particular representation of a web resource. DOI resolvers use content negotiation to provide different representations of metadata associated with DOIs. See: https://citation.crosscite.org/docs.html#sec-3 [Cited 25 april 2024]

Funded by
the European Union

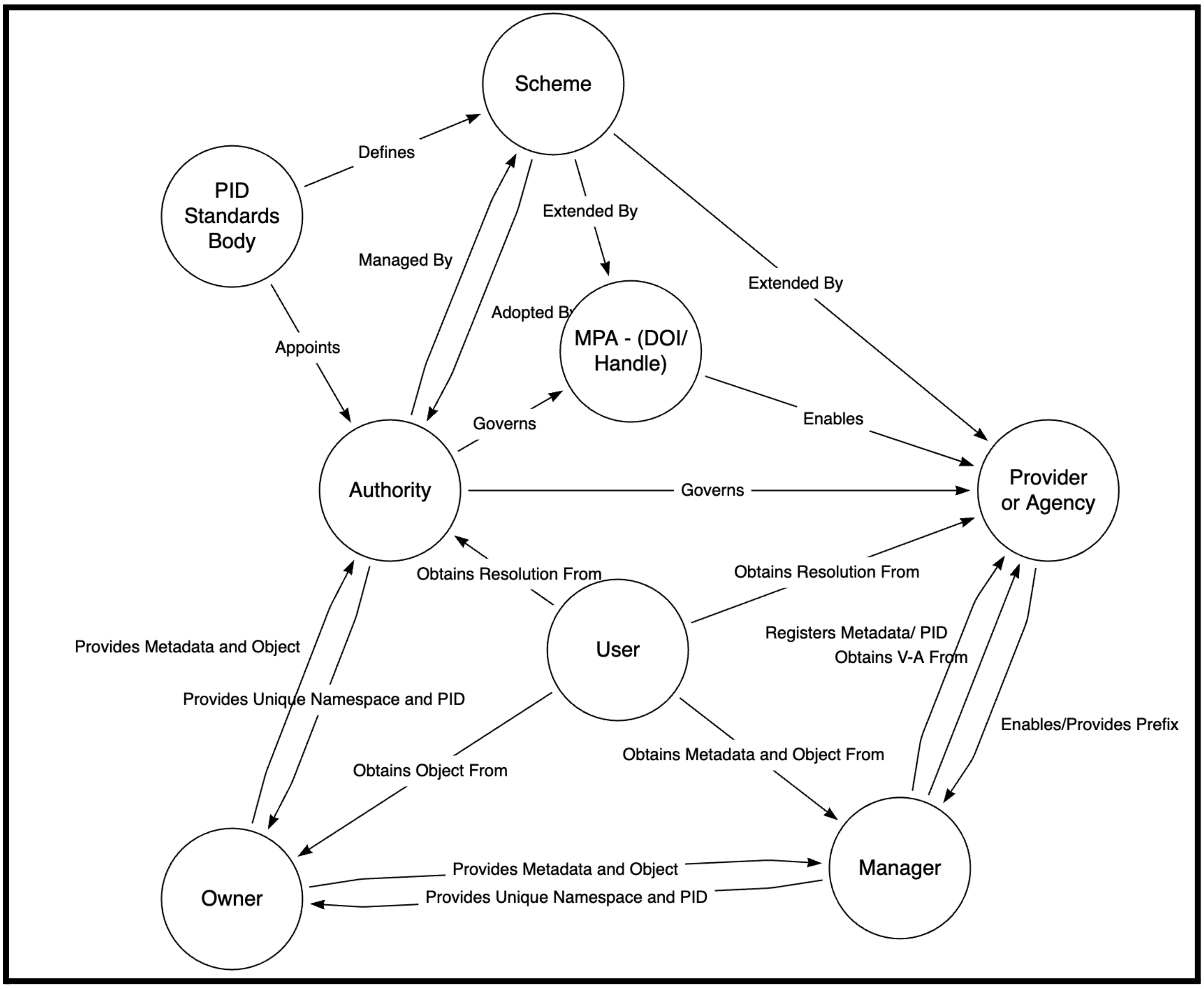


Figure 2 - Actors and Roles in the PID Ecosystem

Whereas in the PID Landscape (see Figure 1) the PID Manager is one of the stakeholders, in the PID Ecosystem the PID Manager (and other stakeholders) are explicitly mentioned as "Actors".[15] Now follows a brief description of the components of the PID Ecosystem.

1. A published PID **Scheme**[16] is governed and maintained by an **Authority**[17], and is often linked to or based on one or more published **Standards**. In some cases, the **Authority** is appointed by the **Standards Body** to manage the **Scheme.** In other cases, an **Authority** may adopt a **Scheme** published by a **Standards Body**.

[15] A description of all Actors and Roles of the PID Ecosystem can be found in: Hugo, W., Steinhoff, W., Turner, D., Buys, M., & Zamani, T. (2023). D2.1 Compliance Assessment Specification. Zenodo. https://doi.org/10.5281/zenodo.10067253 p 28-29.
The role and function of the main Actors in the PID Ecosystem are covered in a document in which vehicle licence plates are used as an analogy for PIDs. See: "Actors in the PID ecosystem.pdf" that is part of the Zenodo record: van Horik, R., Nordling, J., van Lieshout, N., Marjamaa-Mankinen, L., Lager, L., Hugo, W., & Davidson, J. (2024). Workshop: Defining Criteria for Assessing PID Policies and Services. Zenodo. https://doi.org/10.5281/zenodo.10791006
[16] Scheme is the template /structure of a specific PID, eg. ORCID for researchers: a 16-digit number that is compatible with the ISO Standard 27729
[17] For instance, the DONA Foundation is the Authority for the Handle identifier

Funded by the European Union

2. An **Authority** serves as the repository of unique identifiers, and handles primary resolution duties together with basic kernel metadata. Some **Authorities** provide PID registration, editing, and resolution services directly to the **Owners**[18] and **Users** of the identifiers.

3. In some cases, the **Authority** directly enables a **Provider**[19] to act as local resolution provider, and to optionally extend the kernel metadata schema. Many PID Stacks, however, introduce an additional layer of resolution and/ or uniqueness management between **Providers** and the **Authority** (**Multi-Provider Agencies or MPA**s). Such MPAs may also extend metadata kernel information defined in the **Scheme**.

4. **Providers (**frequently called 'Services'**)** enable **Managers**[20] to register PIDs on behalf of **Owners**, and often receive value-added services from the **Provider**. More often than not, **Managers** are repositories of physical and digital materials, or registries of concepts, and several other terms may be used to describe them - e.g. 'Allocating Agents'.

5. The **Provider** maintains the relation between the referenced entity, the identifier, and the detailed kernel metadata for that object or concept where applicable - usually on behalf of the **Owner** of the object or concept.

6. When **Users** (humans or machines) encounter a PID, resolution is handled by the **Provider** in most cases, but if a PID was issued directly by an **Authority**, resolution is handled by the **Authority**.

7. Resolution directs the user either directly to the entity (object) or to its proxy, which is often a (metadata) landing page maintained by the **Manager** on behalf of the **Owner**. In such cases, it is possible to obtain the entity either directly from the **Owner**, or from the **Manager**. This process may not be machine-actionable and may involve manual permission, retrieval, and sharing.

2.2 PID Stack

PID Stacks have been referred to a number of times in this report. What follows is a definition of this concept using some examples and published information about the structure of PID Services. PID Stacks are interdependent arrays of actors and roles that serve the end user community (Owners and Users). Several actors and roles in the ecosystem contribute to more than one PID Stack, and they map onto the model defined in Figure 2 in various ways.

[18] For instance the researcher that registers an ORCID ID is the owner of this PID
[19] For instance DataCite is the service provider for the DOI identifier
[20] Managers, the main target group of this report, are for instance data repositories, data catalogues or search workflow systems

Funded by the European Union

Table 2 lists some of the most prominent PID Stacks. The list is extracted from the PID Knowledge Base, developed in support of FAIRCORE4EOSC CAT with input and assistance from FAIR-IMPACT.[21]

Scheme	Authority	MPA[22]	Provider (Registration Agencies)	Manager (Examples)
Handle System	DONA Foundation	International DOI Foundation	CrossRef DOI	
Handle System	DONA Foundation	International DOI Foundation	DataCite DOI	DANS, Zenodo
Handle System	DONA Foundation	ePIC Consortium	GRANT, CLARIN, …	GRNET
Handle System	DONA Foundation	ROR, CDL, Crossref, DataCite	CDL, Crossref, DataCite	N/A
Handle System	DONA Foundation	IGSN, DataCite	IGSN Members	IGSN Members
Handle System	DONA Foundation			
ISNI	ISNI-IA	ISNI-AA	e.g. British Library	
ISNI	ISNI-IA			
ISNI	ORCID	N/A	ORCID	NWO
N2T	ARK Alliance	N/A	CDL	Individual Owners
URN	URN:NBN	N/A	URN:NBN:NL	Individual Owners
URN	URN:NBN	N/A	URN:NBN:FI	Individual Owners
URN	URN:ISBN	N/A	National Libraries	National Libraries

Table 2 - Examples of PID Stacks

2.3 Use Cases

A starting point for understanding the needs of the user community is a review of the workflows and use cases that are commonly associated with PID use, and the typical benefits that the user community expects from such use. Assessment of the current state of the community was derived from literature review, including analysis of National PID Policies that were included by the relevant RDA Working Group[23] in its survey, as well as publications on the role of PIDs in research workflows. In all, 163 publications and websites were reviewed, and led to the identification of 39 unique use cases and the typical benefits expected from them. The use cases share 27 common elements or steps (for example the unambiguous identification of a researcher, project, or research output). Figure 3 shows the most common elements, with examples of the unique use cases that were identified. Some elements are related (e.g. 'Identification of Researchers' is related to 'Identification of Authors', but not functionally equivalent - the motivation for use is different.

[21] A more detailed coverage of PID Stacks can be found in: Hugo, W., Van de Sompel, H., & Hakala, J. (2024). The PID Landscape - a Technical View (0.8.0 Draft). https://doi.org/10.5281/zenodo.11108203.

[22] Multi-Primary Administrator (MPA) is an organisation that is authorised and credited by the authority (e.g. the DONA foundation) to operate identifier services (such as the GHR, the Global Handle Registry).

[23] Simons, N., Brown, C., Bangert, D., Sadler, S. (2023). Pathways to National PID Strategies - Guide and Checklist to facilitate uptake and alignment, RDA Output, 10.15497/rda00091

Funded by the European Union

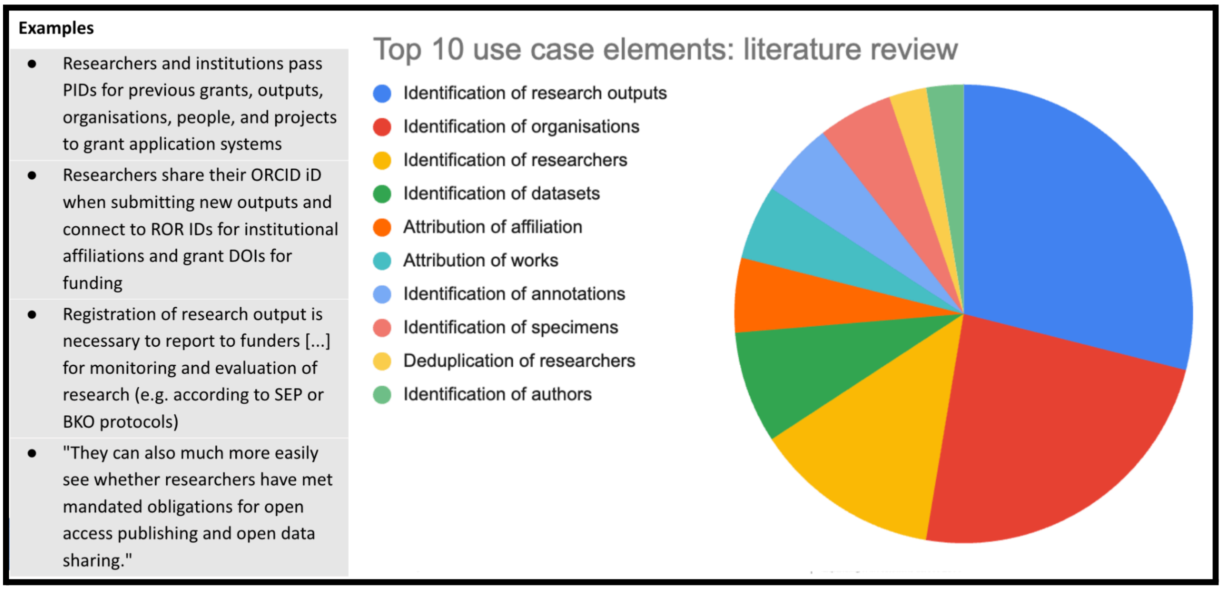


Figure 3 - Share of use cases that include a specific element

Implementation of PIDs in these use cases are expected to yield benefits, and these were identified and categorised as part of the literature review. Figure 4 indicates the typical and most common benefits that are expected from implementation of PIDs in the use cases associated with research workflows.

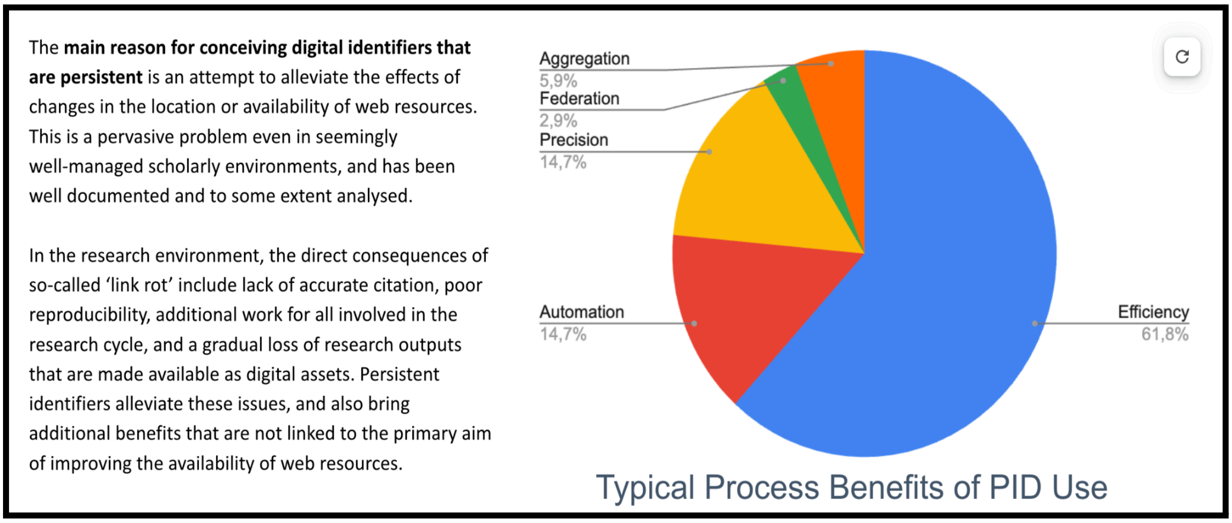


Figure 4 - Main Benefits Expected from PID Implementation

Percentage: share of use cases that identify a specific benefit

These benefits largely fall into the following five main categories[24]:

1. **Efficiency**: the most commonly identified benefit, it is aimed at reducing the administrative, collation, and verification burden placed on researchers, funders,

[24] Hugo, W., Van de Sompel, H., & Hakala, J. (2024). The PID Landscape - a Technical View (0.8.0 Draft). Zenodo. https://doi.org/10.5281/zenodo.11108203

research managers, infrastructure providers, and research performing organisations during the course of many workflows that they engage in.

2. **Precision**: Persistent identifiers assist with more precise citation and attribution, more accurate metadata about co-authors, affiliations, and funding, improved tracing of data sources for scientific results with suitable granularity, improved reporting and assessment, and increased interoperability of data.

3. **Automation**: As both scientific, service, and administrative workflows become increasingly automated, identifiers will play an increasingly important role to allow such automation to be executed with a minimum of error. It is a direct objective of FAIR to improve machine actionability through the use of persistent identifiers.

4. **Federation**: Federation of services of various types become simpler using persistent identifiers - including linked open data-based contextualisation of resources.

5. **Aggregation**: At the various scales, aggregating information about entities and the relationships between them enables strategic analysis, benchmarking, monitoring, and evaluation. The emergence of PID Graphs and Scientific Knowledge Graphs will depend increasingly on precise referencing via persistent identifiers.

The workflows in which the use cases are embedded were also categorised, and aligned with published definitions of such workflows.[25] Figure 5 summarises the scope of workflows that were identified, ranging from those purely focused on research administration, through research life cycle workflows (grant applications, research execution, publication and dissemination, and discovery and reuse), to those focused in the research process itself ('scientific workflows'). By including PIDs in the use cases within these workflows, the record of research activity is improved.

[25] Amongst others: Brown, Josh, Jones, Phill, Meadows, Alice, & Murphy, Fiona. (2022, September 16). PID-optimised workflows: A vision of a more efficient future. Zenodo. https://doi.org/10.5281/zenodo.7085489

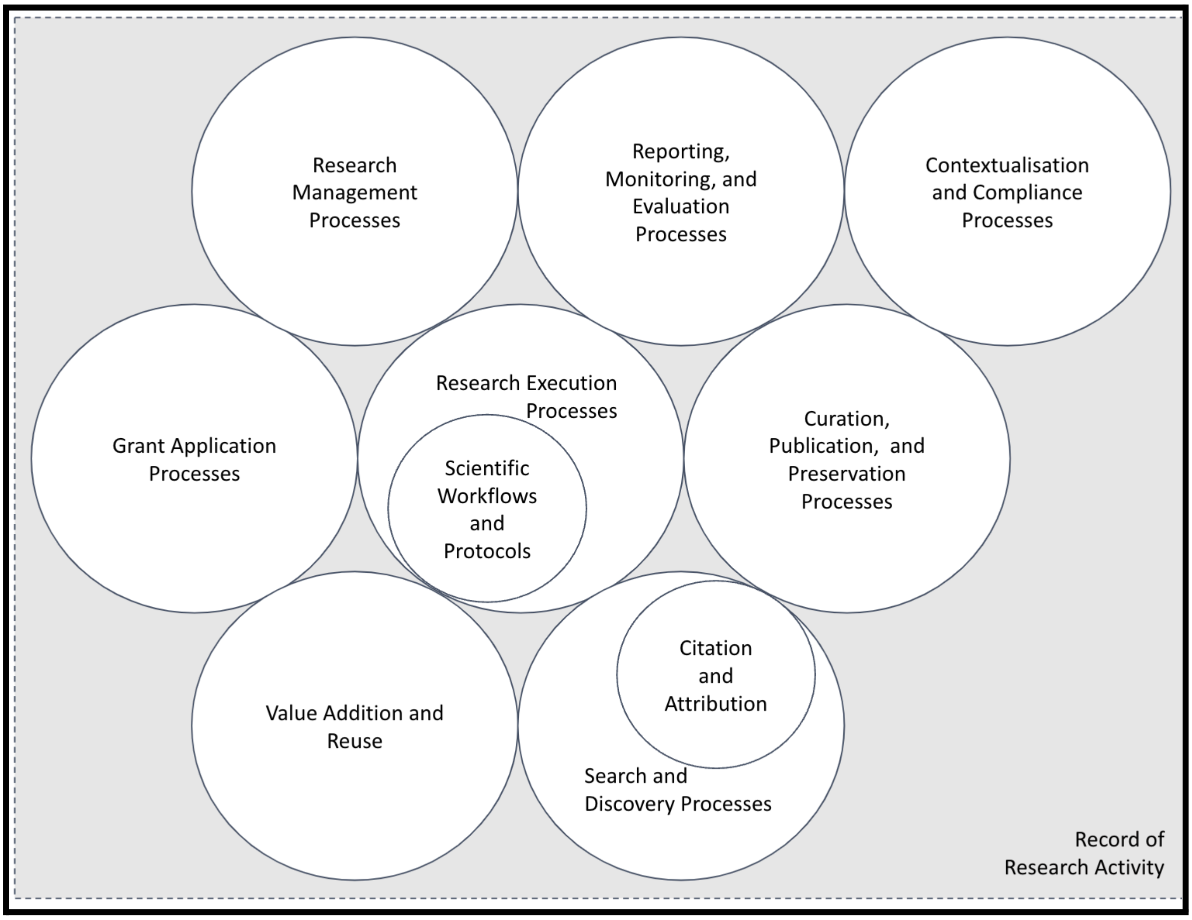


Figure 5 - Workflows identified as main groupings of use cases, covering the research life cycle and its support/ management processes

Characterisation of the use cases and its main elements is important for understanding the demand for PID services, and is foundational to matching user needs with appropriate services. A synthesis of use case elements mapped to the entity being referenced (concepts, or physical/ digital objects) was constructed, and this serves as a basis for identification of appropriate PID services for each use case element.[26]

By introducing and discussing the PID Landscape, the PID Ecosystem, the concept of PID Stacks, and providing Use Cases, this chapter covers the first aim of T3.3, the identification of different EOSC actors and mapping of existing PID policies in use.

[26] Interactive mapping between use case elements and entities: https://atlas.mindmup.com/scientilla/f_43_4_2_use_cases/index.html

Funded by the European Union

3 Compliance Assessment of PID Policies

In this chapter the second aim of T3.3 is addressed, the analysis of the compliance of existing policies with the EOSC PID policy. Input of the FAIRCORE4EOSC Project plays a prominent role in operationalising this goal. In general terms the following process is applied. The EOSC PID policy published in 2020 is assessed by using the CAT method. Next, the "case study analysis" assessment of the EOSC PID policy, carried out by the FAIRCORE4EOSC and FAIR IMPACT project is presented. The results are available as "public draft".[27] The outcomes of this case study were discussed with the EOSC PID TF and initial feedback was received.[28] As explained in the introduction of this report, this process was not finalised so the outcomes of the EOSC PID policy compliance could not be endorsed by the EOSC Association.

3.1 Compliance assessment method

PID policies are required as the basis to build a PID infrastructure. Here it is important that the quality of a PID policy be determined as objectively as possible and that there be consensus on what criteria apply to the characteristics of PIDs. A model and method for this, the CAT, is developed by the FAIRCORE4EOSC project. This method is being evaluated and supported by the FAIR-IMPACT project.

The Compliance Assessment Toolkit (CAT) intends to support the EOSC PID policy. The specifications are based on a Conceptual Model for Compliance Assessment. The conceptual model identifies a number of entities and concepts, categorised in four main groups: Motivations, Implementation, Realisation and Elaboration.[29] The conceptual model (covering these four main groups) for compliance assessment is presented in Figure 6. Relevant to note for this report is that the components of the conceptual model have a relationship to either the FAIRCORE4EOSC project, or the FAIR-IMPACT project or for both FAIRCORE4EOSC and the EOSC PID Task Force. This is expressed by the background colours in Figure 6. The methodological basis of compliance assessment lies with the FAIRCORE4EOSC project, which is also building an online compliance assessment service, the CAT.

Relevant for this report is that FAIR-IMPACT is tasked with addressing "Best Practices" and "Recommendations", both of which build on "Criteria" provided by FAIRCORE4EOSC. The model also shows that the "Criteria" are an elaboration of "Principles and Objectives". The model also states that these "Best Practices" and "Recommendations" contribute to "Guidance", the main topic of this report (and focusing on a specific actor: the PID Manager).

[27] Case Study Analysis: EOSC PID Policy. Public Draft. LINK TO THE "PUBLIC DRAFT" DOCUMENT
[28] On November 7th 2023 a meeting was held with representatives of the FAIR-IMPACT project, the FAIRCORE4EOSC project and members of the EOSC PID Policy and Alignment Taskforce". The aim of the meeting was to introduce the CAT and to discuss the case-study assessment of the EOSC PID policy. The Taskforce was open to process the outcomes of the case-study analysis, but due to the reorganisation of the task forces by the EOSC Association this process could not be completed.
[29] Hugo, W., Steinhoff, W., Turner, D., Buys, M., & Zamani, T. (2023). D2.1 Compliance Assessment Specification. Zenodo. https://doi.org/10.5281/zenodo.10067253 p 15.

Funded by
the European Union

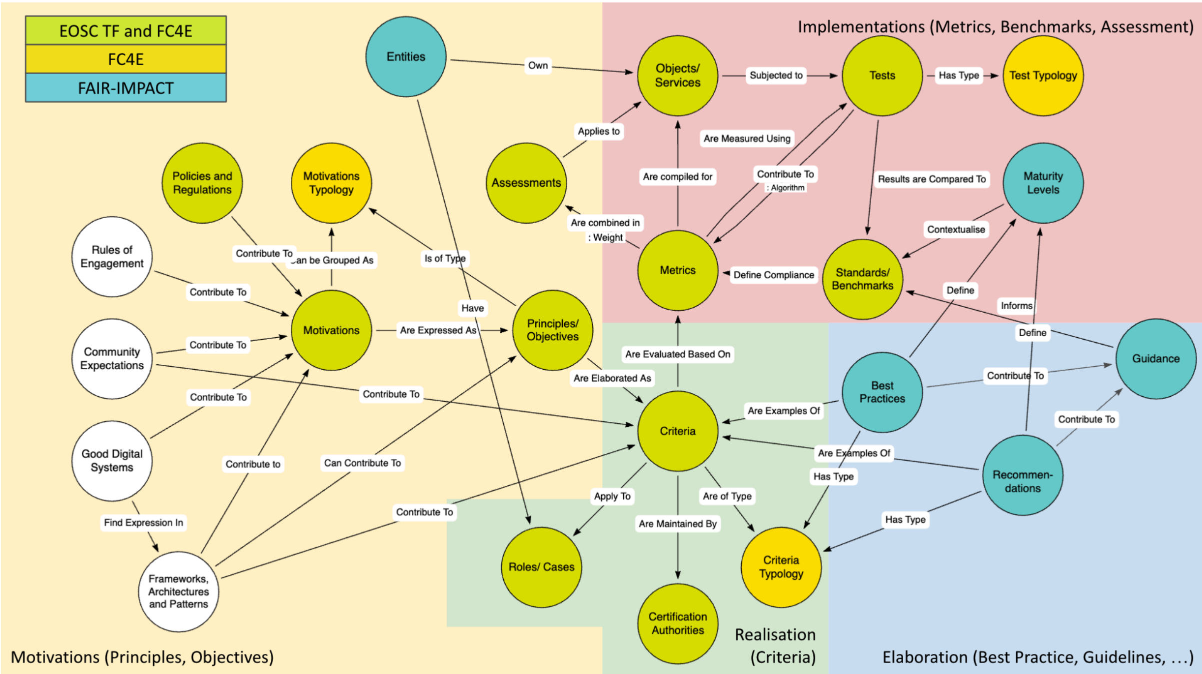


Figure 6 - Conceptual Model for Compliance Assessment[30]

3.2 Case study analysis: EOSC PID Policy assessment for PID Managers

Applying the compliance assessment of Figure 6 to EOSC's PID policy published in 2020 results in the following. Ten “Principles and Objectives” are distinguished, that are elaborated into 35 “Criteria”. These criteria are applied to 5 actors (ref. Figure 2): Scheme, Authority, Service, Manager, and Owner of which the (PID) Manager as the target group for this report is the most relevant.[31] The full case study analysis of the PID policy based on the compliance model is published and a summary is given below.[32]

Of the list of 10 “Principles and Objectives” the first 4 are presented in Table 3. The text of the EOSC PID policy is analysed and the statement “PID application depends on unambiguous ownership, proper maintenance, and unambiguous identification of the entity being referenced” is classified under the term “Application”. How this principle can be translated into “Criteria”, is illustrated in Table 4. The description of the principles can be converted into 4 criteria in which the Actor is mentioned, e.g. criteria 5 (C5) states that the “PID Manager MUST provide the functionality required to maintain PID attributes.”

[30] Compliance Toolkit. Landscape Assessment (Draft) F.43.5.1 Compliance Toolkit - Landscape Assessment p 14. [Cited 24 April 2024].
[31] Besides the 10 “Principles and Objectives” and 35 “Criteria also 35 "Tests" and "Guidance Principles” to assess the compliance of the PID policy are formulated.
[32] Hugo, W., Steinhoff, W., Turner, D., Buys, M., & Zamani, T. (2023). D2.1 Compliance Assessment Specification. Zenodo. https://doi.org/10.5281/zenodo.10067253. The case study analysis of the EOSC PID Policy can be found on p 58-78. This case study analysis contains an overview of all “Principles and Objectives” and “Criteria” that are applied to the 5 Actors.

Funded by the European Union

#	Principle or Objective	Description
P1	Application	PID application depends on unambiguous ownership, proper maintenance, and unambiguous identification of the entity being referenced.
P2	Secure	PID Services for EOSC need to address (a wide variety of) applications (including those) that require secure mechanisms built into the PID Infrastructure.
P3	Ecosystem	An ecosystem of PID Infrastructures is needed to support the wide variety of scientific applications and offers sufficient flexibility (service providers, scheme, attribute set) and capacity.
P4	Levels of Granularity	The PID ecosystem ideally supports multiple levels of granularity and encourages/ fosters links between them.
Pn	…	…

Table 3 - Principles and Objectives extracted from the EOSC PID Policy

#	Principle or Objective	Suggested Label	Description / Explanation	Benchmark[33]
C1	Application	Minimum Operations	Service providers **SHOULD** provide a common Application Programming Interface to interact with PIDs, supporting a minimum set of operations (create, resolve and modify PID and PID Kernel Information)	=0 ⟶ 0 =1 ⟶ 1
C2	Secure	Sensitive Metadata	Sensitive kernel metadata **MAY** require access control and/or encryption of the Kernel Information.	<5 ⟶ 0 =5 ⟶ 1
C3	Application	Ownership	PID ownership **MUST** be visible to other actors in the ecosystem.	=0 ⟶ 0 =1 ⟶ 1
C4	Application	Maintenance	The PID owner **SHOULD** maintain PID attributes.	=0 ⟶ 0 =1 ⟶ 1
C5	Application	Update Functionality	The PID Manager **MUST** provide the functionality required to maintain PID attributes.	=0 ⟶ 0 =1 ⟶ 1
Cn	…	…	…	…

Table 4 - Criteria and Benchmarks of the EOSC PID policy

[33] The Benchmark indicates whether the Criterium either must be met ("0" = No, "1" = yes, or a level of compliance is allowed, e.g. at "C2" where 5 levels of security are distinguished. The tests connected to the criteria are covered in: Hugo, W., Steinhoff, W., Turner, D., Buys, M., & Zamani, T. (2023). D2.1 Compliance Assessment Specification. Zenodo. https://doi.org/10.5281/zenodo.10067253. Table 5. p 63.

Funded by the European Union

The next step in the compliance assessment of the EOSC PID Policy concerns the mapping of the criteria to Actors. With other words: Which criteria are applicable for which Actor? Since the PID Manager is the target audience of this report, the criteria belonging to this actor will be explored in more detail.

Twelve of the 35 criteria (of which C5 of Table 4 is one of them) can be mapped to PID Managers. All 12 criteria are stated in Table 5.[34]

#	Criterion	Description	Imperative
C5	Update Functionality	The PID Manager **MUS**T provide the functionality required to maintain PID attributes. (Also mapped to the Actor: Service)	MUST
C6	Ownership Transfer	The PID Manager **SHOULD** provide policies and contractual arrangements for transfer of ownership should the owner no longer be able to assume responsibilities in compliance with the policy.	SHOULD
C7	Resolution Integrity	The PID Manager **MUST** maintain the integrity of the relationship between entities and their PIDs, in conformance to a PID Scheme defined by a PID Authority.	MUST
C11	Versioning - Procedure	PID Services and PID Managers **SHOULD** have clear versioning policies. (Also mapped to the Actor: Service)	SHOULD
C14	Resolution Authenticity	PID Manager **MUST** ensure that the entity remains linked to the PID. In case that the entity being identified is deleted or ceases to exist, tombstone information needs to be included in the PID attribute set.	MUST
C16	Digital Representation	Physical and conceptual entities **MUST** be represented via a digital representation (e.g. landing page, metadata, attribute set, database index) to have a presence in the digital landscape.	MUST
C19	Accurate Entity Metadata	The PID Service **MUS**T maintain entity metadata as accurately as possible in collaboration with the PID Owner. This copy is the authoritative version.	MUST
C22	No End User Cost	The basic services of PID registration and resolution **SHALL** have no cost to end users.	SHALL
C28	Certification	PID Authorities and Services **MUST** agree to be certified with a mutually agreed frequency in respect of policy compliance. (Also mapped to the Actors: Scheme, Authority, Service, Owner)	MUST
C29	Agreed Responsibilities	PID Services **SHOULD** agree with PID Managers the responsibilities for Kernel Information maintenance, preferably via contract (Also mapped to the Actor: Service)	SHOULD

[34] The table with the Criteria mapped to all 5 Actors (Scheme, Authority, Service, Manager, Owner) can be found in: Hugo, W., Steinhoff, W., Turner, D., Buys, M., & Zamani, T. (2023). D2.1 Compliance Assessment Specification. Zenodo. https://doi.org/10.5281/zenodo.10067253 p 62-63.

Funded by the European Union

C34	Persistence Median	PID Services **SHOULD** aim for a persistence median that is acceptable to and aligns with community and dependency expectations. (Also mapped to the Actors: Scheme, Authority, Service)	SHOULD
C35	Resolution Percentage	PID Service **SHOULD** resolve at least p percent of PIDs in a randomised sample, where p is determined by community and dependency expectations. (Also mapped to the Actors: Scheme, Authority, Service)	SHOULD

Table 5 - Applicability of Criteria to PID Managers

Of the 12 criteria in Table 5, six are attributed to the PID Manager alone. The remaining 6 criteria are also relevant to other Actors, with the Actor "Service" playing a role in all of them.

The last phase in the process to formulate the role of the Actor PID Manager in the PID Ecosystem is to make a distinction between the mandatory criteria (SHALL/MUST), the desirable criteria (SHOULD) and optional criteria (MAY) of the PID policy. Table 6 contains the proposed assessment for the PID Manager.

Aspect	**Explanatory note**	**Relevant Criteria (ref. Table 5)**
Go/No Go	If the criterion is not met, the PID Manager does not comply with the EOSC PID policy	C5+C7+C14+C16+C19+C22
Ranking	The extend to which the PID Manager meets the criterion determines the quality of the PID policy compliance	C6+C11+C28+C29+C34+C35

Table 6 - PID policy criterion assessment for PID Managers

In this chapter relevant criteria to assess the compliance of a PID policy (for PID Managers) are presented, the next step concerns the formulation of guidelines for PID policies. This is covered in the next chapter.

4 Guidelines for formulating PID policies for PID Managers

This chapter covers the third objective of T3.3, providing guidelines for formulating PID policies aimed at PID Managers. The PID Landscape (Figure 1) is the foundation for this and the PID Ecosystem (Figure 2) is the model to describe Actors such as PID Managers, their Roles and relations. The Compliance Assessment Model (Figure 3) provides a way to assess requirements and criteria for guidance for Actors to define a PID policy. Based on this, guidelines can be formulated for EOSC compliant PID policy tailored for PID Managers.

4.1 Information sources of the guidelines

The main source for the guidelines are the outcomes of the compliance assessment of the EOSC PID policy. Other sources of best practice are a review of national and institutional PID policies, outputs and recommendations of the Research Data Alliance (RDA), review of PID Stack documentation and published use of PIDs in workflows and specific use cases. The outcomes of this survey of features, characteristics and attributes is visualised in a mind map[35] with the title "PID Essential Elements".[36]

The work on 'PID Essential Elements' aims to create a categorised inventory of the elements, attributes, and features of PID Stacks, using an approach similar to the GORC International Model.[37] Essential Elements are high-level categories that group the collections of features and attributes applicable to both the provision of and demand for PID services. For each of the essential elements, there may be any number of subcategories, and these in turn may have subcategories. Each of these nodes can have distinguishing features (for example mechanisms to deal with versioning) that differ for individual PID Stacks, and associated attributes (e.g. availability statistics, number of PIDs allocated, and so on). Below, table 7 covers the main elements of PID Stacks and some of its important features.

Element	**Category**	**Subcategory**	**Typical Features and Attributes**
Functionality	Persistence	Commitment	Formal commitments made by the PID Stack in respect of future availability of the service
		Duration	Features and attributes that confirm the stated and actual persistence of the identifier
		Components	The working parts of the persistence mechanism - roles of the identifier, actors, and object owner
	Uniqueness	Identifier	Whether the identifier Scheme is standardised or not, how uniqueness is guaranteed, and the scope of

[35] See: https://en.wikipedia.org/wiki/Mind_map [Cited 30 april 2024]
[36] The online version of the mind map "PID Essential Elements" can be found at: https://atlas.mindmup.com/scientilla/f43_4_1_pid_essential_elements/index.html [Cited 30 april 2024]
[37] Woodford, C., Treloar, A., Leggott, M., Payne, K., Jones, S., Lopez Albacete, J., Madalli, D., Genova, F., Dharmawardena, K., Chibhira, N., Åkerström, W. N., Macneil, R., Nurnberger, A., Pfeiffenberger, H., Tanifuji, M., Zhang, Q., Jones, N., Sesink, L., Wood-Charlson, E., & RDA GORC International Model WG. (2023). The Global Open Research Commons International Model, Version 1 (1.0). Zenodo. https://doi.org/10.15497/RDA00099

Funded by
the European Union

			uniqueness
	Resolvability	Actionable - Machines	Once resolved, is one or more of the resolution targets machine actionable? Are content negotiation and/ or ‘multiple resolution’ supported?
		Actionable - Humans	Are one or more resolution targets human readable?
		Performance	Do targets remain available and resolvable? Is the resolution mechanism efficient and interoperable?
	Content Variability	Versioning	Description of the versioning strategies and features supported by the PID Stack, and typical versioning policy considerations
		Versioning Triggers	A description of the cases that may trigger versioning actions
	PID Schema	Mutability	How and where in the associated schema are changes allowed over time?
		Identifier Metadata	The type of metadata captured with the identifier in the authority registry
		Kernel Metadata	Standards applicable to kernel metadata, and its main features and attributes
		Custom Metadata	Allowance is made for profiles of the kernel metadata or managers are free to create or adopt domain and format specific schema.
	Scalability	Service Scalability	Attributes of the PID Stack or service in respect of scalability
		Extensibility	Attributes in respect of extensibility of the service - new actors, amendments to kernel metadata schema, and similar features.
	Independence	Protocol Independence	Some services are limited to HTTP, while some are not.
		Platform Independence	Some services, especially of the code supporting the service is open source, can be deployed on any platform
		Technical Independence	Aspects such as encoding support and ASCII case folding are examples
Service Topology	Centralised		All features are provided at a single point by a centralised service.
	Decentralised	Hierarchy	A tree of interdependent actors, possibly with cascading resolution and administration

			responsibilities
		Network or Federation	An interconnected set of equivalent nodes that all provide similar services
		Independent	Nodes provide similar services independently of one another, and some features guarantee uniqueness without information exchange between them.
Cost	End User Costs		Are end user costs (Owners and Users) free? If not, how is payment arranged?
	Service Cost Recovery		Source of funding for services: pay-per-use, sponsored, membership or subscription fees, and hybrid arrangements of these options
	Business Type	Community Service	A service is provided free on behalf of the community with in-kind contributions and no obvious source of funding
		Project	The main source of funding is a project with a finite lifetime
		Non-Profit	A non-profit association with a means of income generation provides the service, based on cost recovery models described above
		For-Profit	Characteristics of commercial companies offering services
Performance	Governance (Social Sustainability)	Coverage	Do the services apply worldwide, regionally, nationally, or only in a specific domain, project, or initiative?
		Stakeholder Engagement	How are stakeholders engaged in service governance? Options include working groups, board participation, and steering group or periodic review contributions.
		Membership Rules	Is anyone allowed to become a member, or is participation restricted in any way?
		Transparency	Features or attributes that promote transparency.
		Single Focus	The service is focused on the PID Stack, and is not involved in other services that are not related.
	Financial Sustainability	Funding for Operations	Funding for operations are derived from sustainable income and not from grants or projects.
		Contingency	Arrangement that allow continued operations in times of income pressure
		Surplus	Mechanisms to invest in R&D, renewal, and improvements are available via grants, income surpluses, or similar.

		Consistency	Income is mission-consistent, and not spent on services or initiatives that do not support the mission.
	Technical Sustainability		Technical infrastructure (code, and data) related to core services are open source, accessible, and do not involve external rights or patents.
	Value Addition	Services	Services and features are available to add value to the basic features expected of PID services - for example citation metrics, APIs, resolution checking, etc.
		Guidance	Aspects of community and end user support via published guidance, best practices, and recommended use.
	Service Levels	Administrative Capacity	Human and system resources available to the PID Stack in support of its services
		Information Integrity	The measures and provisions that are taken to safeguard information integrity and security
		Certification	Formal certification in respect of conformance with community or industry norms and expectations
		Defined Responsibilities	A legal and agreement framework exists to define the roles and responsibilities of the actors in the PID Stack
Mitigation	Link Rot		Mechanism or features are available to combat link rot, for example via spot checks and engagement with PID owners and managers to correct issues
	Versioning		Features of the PID Stack assist with versioning (for example by having well-defined relations to other versions in kernel metadata)
	Content Drift		Content drift is addressed in cases where it is not desirable or intended through guidance and versioning policies. Recommendations could be implemented (for example ‘Link Decoration’ to mitigate content drift.
	Accuracy		Features or mechanism are in place to ensure accuracy, for example via checksums or check digits
Definition	Scheme		Scheme attributes and features are available - for example standards compliance, resolution and registry APIs, pattern definition, and namespace services
	Authority	Institution	Features and attributes of the institution that serves as Authority - identifier, description, mission, business location, and other contextualising information is available.
		Resolver	A resolution service, and potentially a namespace registry is made available to any user

Funded by the European Union

Table 7 - Main elements of PID Stacks as basis for guidelines for PID Managers

4.2 16 Guidelines applicable to PID Managers

This section contains a list of 16 guidelines for creating a EOSC compliant PID policy for PID Managers.[38] This is the main objective of this report. The guidelines are aimed as guidance both to formulate a PID policy and to evaluate an existing PID policy. The Compliance Assessment Toolkit enables PID managers (and other Actors) to assess a PID policy and inspire them to improve them. The guidelines are accompanied by a brief description.

Guideline 1. "Select a PID Stack that is globally unique and persistently resolvable"

Select a PID Stack with persistence, uniqueness, and resolution characteristics appropriate to the use case. For this the acronym GUPRI can be used: the PID must be Globally Unique, Persistent with a Resolvable Identifier.

Guideline 2. "Manage Persistence"

Guaranteeing persistence requires effort - usually from the registry (Authority) and from the Manager. Managers must develop policies and procedures to guarantee maintenance of the correct link between the identifier and the resolution target, and make sure the responsibilities are well defined in their agreements or contracts with the PID owner. The two main manifestations of lack of persistence are "link rot"(the weblink does not resolve to a resource) and "content drift" (the original link does not refer to the resource it was initially connected to).

Guideline 3. "Manage Versions"

Managers must have a clear policy on version management. The provisions of the policy depend on the purpose of referencing resources by the persistent identifier. The semantics of versioning principles may be aligned with good practice as used in the versioning of software and adapted as follows.[39] Given a version number the "major", "minor" and "patch" increments are:

-"Major" version when you make changes that do not support reproducibility

-"Minor" version when you add content in a reproducibility-compatible manner

-"Patch" version when you make backward compatible improvements

Guideline 4. "Involve Stakeholders"

[38] The first version of the Guidelines were presented and discussed at the EOSC Winter School. See: https://eosc.eu/oa1-pids-persistent-identifiers/ [Cited 28 may 2024]
[39] See "Semantic Versioning" at: https://semver.org/ [Cited 3 may 2024]

Managers SHOULD make time and resources available to participate in governance structures of PID Stacks that they use. Typical activities in this respect are participation in governance through a board or oversight committee and the development of kernel, domain and custom metadata schema.

Guideline 5. “Conform to a PID Stack checklist”

Managers SHOULD confirm the degree to which PID Stacks (providers/ agencies, authorities) support or conform to a number of important considerations. Some of these will be guaranteed by EOSC PID Policy Compliance and/ or alignment with the Principles of Open Scholarly Infrastructures (POSI).[40] The main items of the checklist are “Certification and Compliance”, “Continuity”, “Sustainability”, “Responsibilities”, and “Value-added services”.

Guideline 6. “Select an appropriate scale”

Managers MUST consider the scale at which PIDs will be used - this can range from 100s (for research outputs) to hundreds of millions (for graph-like nodes and relations with versioning and authenticity). Two interrelated considerations are: scalability of the service, and the cost. Also future migration and annual growth should be considered.

Guideline 7. “Select appropriate identifier schema and structure”

Managers SHOULD consider the type of identifier and determine its stability (preferably a published and managed standard), as well as its implications for migration and its scope. Also consider human readability of the standard.

Guideline 8. “Consider resolution options”

Managers SHOULD consider the type of resolution mechanism offered to users and owners when selecting a service and creating their own infrastructure. Impacts on usability for humans and machines, and on interoperability. Examples of approaches for resolution options are “via HTTP wrappers”, “via a Web page”, “via API”, “via support for compact identifiers” and “via a MetaResolver Service”.

Guideline 9. “Maintain resolution integrity”

Managers MUST maintain the link between the identifier and its resolution mechanism, and the object or concept being referenced. In most cases, Managers offer custom metadata for the object or concept that is authoritative, and this MUST be maintained. Tombstones MUST be offered in cases where objects or concepts are no longer available, based on rational cases.

The link between the identifier and its resolution mechanism, and the object or concept being referenced is usually maintained as a direct web reference to the Digital Object, a Landing Page that usually provides human- and machine readable custom metadata, and in cases where an object or concept is no longer available, a Tombstone Page (‘Targets’).

[40] See: https://openscholarlyinfrastructure.org/ [Cited 29 april 2024]

Funded by the European Union

Physical objects and concepts must also have landing pages. A landing page can (optionally) point to the object for access, and a tombstone page can optionally point to or be similar to the metadata landing page. There are only a few reasons why a PID target is deleted - such as fraud or withdrawal or expiry of publication permissions for legal reasons - and hence Managers must make a strong commitment towards maintenance of the link.

Guideline 10. “Manage Metadata”

Managers SHOULD manage metadata in alignment with community and disciplinary standards, and MUST maintain an authoritative version of the metadata - either as kernel or custom metadata - in collaboration with the owner (depositor). There must always be at least one authoritative version of metadata, and there are different candidates for this depending on the PID Stack in use.

Guideline 11. “Consider implementation of Machine-Actionable Extensions”

Managers SHOULD consider implementation of content negotiation and machine-actionable links to improve the usability of the resource across the research enterprise (‘mediations’). Some recently developed approaches that are potentially useful for this are stated in table 8.

Approach	Description	Application
Content Negotiation	This is typically used to modify the response format of the web-based resource, and can be part of a header request or sometimes as a parameter or child node of the URI.	Example: instead of a human-readable metadata page (HTML) one could request a machine-readable one (e.g. XML or JSON).
Inflection and Multiple Resolution	Adding standard processors to a URI to request a different type of resource or format	Inflection implemented by ARK. Provides access to detailed metadata and to policy/ commitments. Multiple Resolution is offered amongst others by the Handle System
Signposting	A mechanism for redirecting machines to other resources in a named relation with the target, using the header. Can be summarised in a single linkset relation.	For example redirecting to author pages, project pages, query APIs, supplementary materials, linked publications, etc.
RO-Crate	Provides a mechanism for describing the research context of the object for reproducibility improvement.	Can be included in the Signposting linkset for convenience.
Affordances	Allows repository-level added services to be described and defined.	For example directling to query APIs or harvesting endpoints that apply to all resources

Table 8 - Approaches to implement machine-actionable extensions

Funded by the European Union

Guideline 12. "Monitor Resolution Integrity"

Managers SHOULD consider implementation of mechanisms (procedures) to verify the integrity of the resolution of the PID. Integrity verification includes two elements: link rot and content drift, and the latter is partly dependent on versioning strategy. Sampling larger collections periodically, with a small error margin and high certainty, is an option.

Guideline 13. "Take sensitive metadata into consideration"

Managers SHOULD consider implementation of practices to deal with sensitive metadata in cases where it is required.

Guideline 14. "Consider periodic resolvability sampling"

Managers that curate a large number of PID-referenced resources MAY consider random sampling to verify resolvability. Detailed guidance indicates sampling sizes required for specific error margins and certainty.

Guideline 15. "Develop and implement sustainability and continuity mechanisms"

Managers MUST develop and implement mechanisms to ensure continued access should their services need to wind down or change, and preferably have access to sustainable funding. If applicable, certification as a trustworthy repository (e.g based on the CoreTrustSeal[41]) ensures that adequate measures are in place. In this respect also the TRUST principles[42] are relevant.

Guideline 16. "Adopt a level for maturity and availability of Services"

Managers SHOULD adopt the EU Technology Readiness Level classification[43] for services and web resources. Infrastructure and maintenance SHOULD aim for a level of availability that is acceptable to end users.

[41] See: https://www.coretrustseal.org/ [Cited 29 april 2024]
[42] See: Lin, D., Crabtree, J., Dillo, I. *et al.* The TRUST Principles for digital repositories. *Sci Data* 7, 144 (2020). https://doi.org/10.1038/s41597-020-0486-7
[43] Technology Readiness Levels: See: https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf [Cited 29 april 2024)

5. Conclusion and next steps

This report places PIDs for research entities in a broad context and provides guidance on establishing a PID policy for PID managers. It first introduces the PID Landscape in which different Actors and Roles play a role. The PID Stack is intended to provide a collection of services and actors supported by resolution mechanisms and namespaces that result in a proprietary, unique PID service aimed at PID managers. This clarifies, for example, that a DOI is based on the Handle identifier schema related to a number of other organisations and standards. Second, it introduces a method to measure the quality of PID policies: the Compliance Assessment method. This method is used to analyse EOSC PID policies. Based on the outcomes of this analysis, combined with other sources of information, a total of 16 guidelines are formulated. These guidelines will assist PID Managers in increasing the quality of their PID policies and making them EOSC compliant.

We now move from theory to practice. In task 3.4 ("PID Implementation") of the FAIR Impact project, which follows after the completion of this report, practical implementation support is provided for the creation of EOSC compliant PID policies. Assessing the compliance of repositories and services is part of this process. The methods and guidelines presented in this report are a prominent foundation for the activities carried out in the support action.

Funded by
the European Union

Annexure: Detailed Guidelines

The guidelines produced in this document represent a snapshot of ongoing work in FAIR-IMPACT, in collaboration with FAIRCORE4EOSC, to create guidance and best practices for the FAIRCORE4EOSC Compliance Assessment Toolkit (CAT). The CAT will be operational by mid-2025, but beta versions are already available to end users and guidance to these users is being updated from time to time.

The guidance is based on an assessment of the technical aspects of the PID Landscape[44], which examines the features, capabilities, and characteristics of PID services, and compares these to the expectations of the user community. The assessment is informed by the criteria and objectives of the EOSC PID Policy.

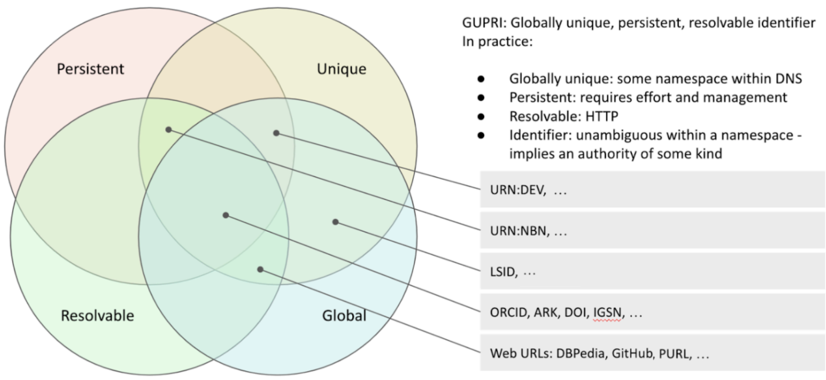
We present a more detailed view of each of the guidelines here.

A.1 Guideline 1

C7 C14 C34 C35

Guideline 1: GUPRI
Select a PID Stack with persistence, uniqueness, and resolution characteristics appropriate to the use case. For this the acronym GUPRI can be used: the PID must be Globally Unique, Persistent with a Resolvable Identifier.

The FAIR-IMPACT Knowledge Base (under construction) will provide guidance in this respect and link to the Compliance Assessment Toolkit.



Not all PID services exhibit the same characteristics of global uniqueness and resolvability. As an example, URN:NBN, used to uniquely identify National Library collection items, are only unique within each country's implementation, and there is no global resolver for URN:NBNs.

Persistence is also highly variable, but not all use cases require 'indefinite' persistence.

It is important to understand your expectations in respect of uniqueness, persistence, and resolvability when selecting an appropriate PID Service[45].

A.2 Guideline 2

[44] Hugo, W., Van de Sompel, H., & Hakala, J. (2024). The PID Landscape - a Technical View (0.8.0 Draft). https://doi.org/10.5281/zenodo.11108203
[45] The CAT will include selection guidance in the near future.

C5 C34

Guideline 2: Managing Persistence
Guaranteeing persistence requires effort - usually from the registry (**Authority**) and from the **Manager**. Managers MUST develop policies and procedures to guarantee maintenance of the correct link between the identifier and the resolution target, and make sure the responsibilities are well defined.

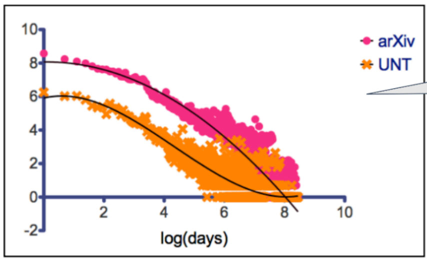


Figure 5. log() of publication/archive date difference vs log() of count of such URLs

One would expect to improve on this using well-managed persistent identifiers. Lack of persistence has two main components: ***failure to resolve*** and ***content drift.***

Guaranteeing persistence requires effort - usually from the registry (Authority) and from the Manager. Managers must develop policies and procedures to guarantee maintenance of the correct link between the identifier and the resolution target, and make sure the responsibilities are well defined in their agreements or contracts with the PID owner. The two main manifestations of lack of persistence are “link rot”(the weblink does not resolve to a resource) and “content drift” (the original link does not refer to the resource it was initially connected to).

There are now multiple recorded and published assessments[46,47] of persistence and resolvability that highlights the potential problems if proper management is not in place.

A.3 Guideline 3

Versioning semantics MAY be aligned with good practice in respect of software versioning [171], adapted as follows:

Given a version number MAJOR.MINOR.PATCH, increment the:

- MAJOR version when you make changes that do not support reproducibility;
- MINOR version when you add content in a reproducibility-compatible manner
- PATCH version when you make backward compatible improvements

The versioning policy and strategy depends on the use case, as indicated below.

[46] Sanderson, R., Phillips, M., van de Sompel, H. Analysing the Persistence of Referenced Web Resources with Memento, Open Repositories 2011 Conference, 2011 https://arxiv.org/abs/1105.3459v1

[47] Eve, M. (2024) 'Digital Scholarly Journals Are Poorly Preserved: A Study of 7 Million Articles', Journal of Librarianship and Scholarly Communication. 12(1) doi: 10.31274/jlsc.16288

Funded by the European Union

C5 C11

Guideline 3: Managing Versions
Managers MUST have a clear policy on version management, and the provisions of the policy depends on the purpose of referencing resources by the persistent identifier.

User expectations in respect of content variance is not a single concept, although there is often a perception that the resource referenced by a PID should 'remain unchanged forever'. There are several generic scenarios. The table summarises the typical best practice appropriate for a number of scenarios.

Main Objective	Recommended practice
Stable Citation/ Reference	Metadata and non-critical data enhancements lead to minor versions with the same PID and provenance
Reproducibility and Authenticity	Data amendments that change the checksum of the referenced object leads to a new PID with provenance links to the previous version
Content Evolution and Manifestations	All previous versions must be available, and there is a choice 1. Same PID, resolving to the latest version but with previous versions easily available (e.g. Zenodo) 2. Each 'manifestation' has a unique identifier with version links to other manifestations.
Dynamic Content Growth	Community recommendations from RDA, and published formally, represents good practice

A.4 Guideline 4

C21 C31

Guideline 4: Stakeholder Involvement
Managers SHOULD make time and resources available to participate in governance structures of PID Stacks that they use. Typical activities in this respect are participation in governance through a board or oversight committee and the development of kernel, domain and custom metadata schema.

This is especially applicable in the following contexts:

- Managers that are also European Research Infrastructures and/ or

e-Infrastructures
- National or multinational domain repositories

Typical activities

- Participation in governance through a board or oversight committee
- Development of kernel, domain and custom metadata schema

A.5 Guideline 5

C21 C31

Guideline 5: PID Stack Checklist
Managers SHOULD confirm the degree to which PID Stacks (providers/ agencies, authorities) support or conform to a number of important considerations. Some of these will be guaranteed by EOSC PID Policy Compliance and/ or alignment with POSI.

Aspect	Recommended practice
Certification and Compliance	EOSC PID Policy, POSI, ISO 27001
Continuity	Publication of a continuity plan, and/ or a 'living will'.
Sustainability	Financial, technical and social sustainability aspects to be taken into account.
Responsibilities	Responsibilities of actors in the ecosystem are well defined and preferably captured in formal agreements
Value-added services	CItation metrics, guidance and best practices, APIs, …

1. Providers and services that demonstrate elements of their capabilities via external certification are more likely to have proper procedures, management, continuity planning, and governance in place.
2. Continuity and sustainability are obviously critical aspects of PID provision.
3. Less mature or emerging PIDs often lack soft infrastructure, even though they may have other important or useful features. These may include proper documentation, support, guidance, value-added services, or well-defined procedures, contractual arrangements and obligations.

A.6 Guideline 6

Funded by the European Union

C22

Guideline 6: Select Appropriate Scale
Managers MUST consider the scale at which PIDs will be used - this can range from 100s (for research outputs) to hundreds of millions (for graph-like nodes and relations with versioning and authenticity). Two interrelated considerations: scalability of the service, and the cost. Also consider future migration and annual growth.

<table>
<tr><th>Scale</th><th>As a Manager</th><th>As an Owner</th></tr>
<tr><td>Less than 1,000</td><td colspan="2">Almost any infrastructure or service will do, provided other criteria are met. Migration can be manual if required.</td></tr>
<tr><td>1,000-10,000</td><td>Consider registration with a provider, which may involve fixed and variable costs. Cost is not likely to be a deciding factor.</td><td rowspan="2">Consider Managers that are registered with a stable provider and offer a migration possibility.</td></tr>
<tr><td>10,000-100,000</td><td rowspan="2">As above, costs may start being significant and determine choice of provider. Migration readiness becomes a major consideration.</td></tr>
<tr><td>100,000-1,000,000</td><td>Larger collections may result in a cost from Managers, depending on service. If so, consider becoming a Manager.</td></tr>
<tr><td>1,000,000-10,000,000</td><td>Consider becoming a Provider in an established stack.</td><td>Consider becoming a Manager.</td></tr>
<tr><td>10,000,000 and more</td><td colspan="2">Consider own infrastructure and mirroring/ federation for performance and availability.</td></tr>
</table>

An important consideration for those applications where a very large number of PIDs are in scope to establish an independent PID infrastructure. Some PID stacks and services allow this to be done by replicating software and registries (e.g. Handle and ARK).

A.7 Guideline 7

C6

Guideline 7: Select Appropriate Identifier Schema and Structure
Managers SHOULD consider the type of identifier and determine its stability (preferably a published and managed standard), as well as its implications for migration and its scope. Also consider ***human readability*** - important in some use cases!

The type of namespace that is most appropriate is determined by four considerations:

1. How is uniqueness guaranteed? Only some namespace schemata guarantee global uniqueness of the identifier string.

Funded by
the European Union

2. How do you expect resolution to work? Some PID services are globally resolvable, but others require knowledge of distributed or federated resolution endpoints.
3. Do you expect to migrate the PIDs to a different manager at some point? If so, identifiers based on namespaces that allow prefixes and suffixes may be more appropriate.
4. Must the identifiers be human readable? If this is the case, for example for sample labels, many namespace types will not be suitable.

Approach	**Uniqueness**	**Usage and Resolution**	**Migration**
A single namespace for all identifiers (directly globally unique)	Globally unique	Simple to use and resolve	Difficult to migrate to a new manager and/ or owner
A root namespace (prefix) with sub-namespaces for Providers		Simple to use, resolution requires additional registry information	Difficult to migrate to a new manager and/ or owner but provider might assist
A root namespace (prefix) with sub-namespaces for Managers (suffixes)		More complex resolution infrastructure	Simple to migrate managers, but not owners
A root namespace (prefix) with sub-namespaces for Owners (suffixes)		Complex to manage	Simple to migrate managers and owners
Multiple unique namespaces without a specific structure	Not guaranteed to be globally unique	Very complex to manage	Migration is simple.
No namespace in use (usually implied in internal systems)		Not suitable as external PIDs	Migration is controlled locally.

A.8 Guideline 8

Guideline 8: Consider Resolution Options C7 C14
Managers SHOULD consider the type of resolution mechanism offered to users and owners when selecting a service and creating their own infrastructure. Impacts on usability for humans and machines, and on interoperability.

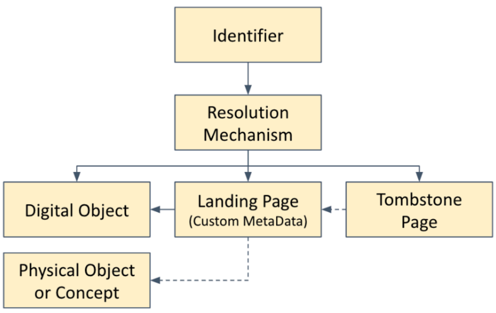
Not all PID services offer the same portfolio of resolution mechanisms. Machine actionability is improved if the service offers resolution via an API or an HTTP pattern (e.g. DOIs, ORCID, and so on). In some cases, it may be adequate to support only resolution via a web page (i.e. human users), but these are increasingly rare.

Approach	Machine Usability	Human Usability
Via HTTP Wrappers or Prefixes for the Identifier	Yes, but patterns must be machine discoverable from a registry.	Yes, but additional information is required with some technical capability to create URLs.
Via a Web Page	Not usable.	Yes, human-directed infrastructure.
Via API	Yes, but a registry of APIs and patterns is likely required for multiple PID stacks.	Not easy to use without some technical knowledge.
Supports Compact Identifiers	Some implementations require compact identifiers to be handled by the resolution mechanism. If not, it requires an implementation layer locally to resolve compact identifiers, or third-party services (such as e.g. a metaresolver).	
Via a MetaResolver Service	Yes, if an API is offered.	Yes, if a UI is offered.

A.9 Guideline 9

Guideline 9: Resolution Integrity C5 C7 C14 C16

Managers MUST maintain the link between the identifier and its resolution mechanism, and the object or concept being referenced. In most cases, Managers offer custom metadata for the object or concept that is ***authoritative***, and this MUST be maintained. Tombstones MUST be offered in cases where objects or concepts are no longer available, based on rational cases - see below.



Once registered with a Provider, PIDs cannot be deleted. For development and test purposes, provisional PIDs can be offered.

The link between the identifier and its resolution mechanism, and the object or concept being referenced is usually maintained as a direct web reference to the Digital Object, a Landing Page that usually provides human- and machine readable custom metadata, and in cases where an object or concept is no longer available, a Tombstone Page (‘Targets’).

Physical objects and concepts must also have landing pages. A landing page can (optionally) point to the object for access, and a tombstone page can optionally point to or be similar to the metadata landing page.

There are only a few reasons why a PID target is deleted - such as fraud or withdrawal or expiry of publication permissions for legal reasons - and hence Managers must make a strong commitment towards maintenance of the link.

A.10 Guideline 10

Guideline 10: Metadata Management C4 C5 C11 C19
Managers SHOULD manage metadata in alignment with community and disciplinary standards, and MUST maintain an authoritative version of the metadata - either as kernel or custom metadata - in collaboration with the owner (depositor).

PID Stack	**Authority**	**MPA**	**Provider**	**Manager**	**Owner**
Metadata Scope	*Identifier and Kernel Metadata*			*Custom (Resource) Metadata*	
Handle System	Handle Metadata	N/A	N/A	N/A	Optional
DataCite DOI	Handle Metadata	IDF Metadata	DataCite	Manager	Optional
IGSN DOI	Handle Metadata	IDF Metadata	IGSN	Manager	Optional
ARK	ARK Metadata	N/A	Optional		Optional
URN:NBN	N/A	N/A	Optional	Optional	Optional
ORCID	ORCID Metadata	N/A	N/A	Optional	N/A
ePIC	Handle Metadata	ePIC Metadata	Optional	N/A	Optional

Shaded: grey: resource (custom) metadata authoritative copy, blue: identifier and kernel metadata authoritative copy

Advice - Kernel metadata: used for citations and inventories of collections. Custom metadata: good for findability, interoperability, and re-use.

One should select PID services and stacks that offer the requisite control over metadata management, and if it is important to work within an agreed community metadata schema, only some options are available to allow for that. The examples above highlight some differences between PID services and stacks, and where authoritative metadata under control of the Manager can be found.

A.11 Guideline 11

Guideline 11: Machine-Actionable Extensions C20 C22 C24
Managers SHOULD consider implementation of content negotiation and machine-actionable links to improve the usability of the resource across the research enterprise ('mediations').

Approach	**Description**	**Application**
Content Negotiation	This is typically used to modify the response format of the web-based resource, and can be part of a header request or sometimes as a parameter or child node of the URI.	Example: instead of a human-readable metadata page (HTML) one could request a machine-readable one (e.g. XML or JSON).
Inflection and Multiple Resolution	Adding standard processors to a URI to request a different type of resource or format	Inflection implemented by ARK. Provides access to detailed metadata and to policy/ commitments. MR by Handle System
Signposting	A mechanism for redirecting machines to other resources in a named relation with the target, using the header. Can be summarised in a single linkset relation.	For example redirecting to author pages, project pages, query APIs, supplementary materials, linked publications, etc.
RO-Crate	Provides a mechanism for describing the research context of the object for reproducibility improvement.	Can be included in the Signposting linkset for convenience.
Affordances	Allows repository-level added services to be described and defined.	For example directling to query APIs or harvesting endpoints that apply to all resources.

Content negotiation and inflection represent one approach class, where the URI used to resolve a PID is modified to add user-determined refinements and options to the resolution result (more human-friendly).

The other approaches are aimed at provision of a standardised linkset whereby machines can discover more options.

A.12 Guideline 12

Guideline 12: (Monitoring) Resolution Integrity C20 C22 C24
Managers SHOULD consider implementation of mechanisms (procedures) to verify the integrity of resolution - for large collections this could be based on sampling. Integrity verification includes two elements: ***link rot*** and ***content drift***, and the latter is partly dependent on versioning strategy.

Versioning Approach	**Link Rot**	**Content Drift**
Stable Citation	A sample of PIDs must resolve to the expected digital object or landing page. This can be achieved by comparing objects that do not resolve as expected to - for example - Memento snapshots of the object going back in time.	Any changes to a digital object that invalidates a citation needs to be versioned - e.g. corrections to a text or dataset. Improvements to metadata or supplementary materials need not be versioned or can be a minor version of the same PID.
Reproducibility		An entire digital object has to remain essentially unchanged: checksum-level similarity is required.
Content Evolution (Minor versions)		Ensure that a PID landing page provides links to previous and newer versions.
Authenticity (Major versions)		Ensure that each version has a unique PID, and that the landing page for each is linked to the next/ previous ones in the series.
Dynamic Content Growth		Several strategies can be followed, with a PID for the dynamic dataset, and linking PIDs for citable sub-sets of data used by researchers. Costly and difficult to maintain.

A.13 Guideline 13

Guideline 13 Sensitive Metadata C2
Managers SHOULD consider implementation of practices to deal with sensitive metadata in cases where it is required.

Bear in mind that sensitive metadata usually cannot be indexed, and as a result does not add value to search and discovery, but only to reuse. The exception may occur when it is possible to grant access to an entire catalogue or collection.

Funded by
the European Union

For typical long-tail repositories, this means obtaining permission from thousands of owners (or even more) - not practically feasible.

Approach	Kernel Metadata	Custom Metadata
Avoid Sensitive Metadata	Not Applicable	Owners are asked not to include sensitive metadata when describing an object or concept.
Compartmentalise Sensitive Metadata	Not Applicable	Sensitive metadata is submitted as an encrypted or protected file, and is not indexed. Access is granted on request by the Owner or Curator.
Explicit Support	Metadata can be marked as sensitive and encrypted, and access is granted on request.	Sensitive metadata can be accommodated as a separate metadata category with limited access, and possibly encrypted.
		Metadata can be marked as sensitive and encrypted, and access is granted on request.

A.14 Guideline 14

C20 C22 C24

Guideline 14: (Monitoring) Resolution Integrity - Sampling Size
Managers that curate a large number of PID-referenced resources MAY consider random sampling to verify resolvability. The tables below indicate sampling sizes required for specific error margins and certainty.

If a Manager would consider sampling resolution integrity from time to time, the sample size is determined by the number of PID instances and the desired confidence level. Some examples are provided below:

Statistically significant sample sizes[48] (2% error margin)

Population (number of PIDs)	Certainty (Confidence)		
	90%	**95%**	**99%**
100,000	1663	2345	3980

[48] https://www.qualtrics.com/blog/calculating-sample-size/

Funded by the European Union

1,000,000	1689	2396	4128
10,000,000	1691	2401	4143
100,000,000	1691	2401	4144
1,000,000,000	1691	2401	4145
Unlimited/ Unknown	1691	2401	4145

A.15 Guideline 15

Guideline 15: Sustainability and Continuity C2 C28
Managers MUST develop and implement mechanisms to ensure continued access should their services need to wind down or change, and preferably have access to sustainable funding. If applicable, certification as a trustworthy repository ensures that adequate measures are in place.

Sustainability Aspect	Description
Technical	Data must be open, accessible, and adequately mirrored and backed up. Software used for metadata and PID management should preferably be open source.
Financial	Managers should have a sustainable business model.
Social and Governance	A continuity plan that makes provision for transfer of custom metadata, digital objects, and associated supplementary materials to a suitable custodian environment should be a strong consideration.

Continuity options vary, and depend on the nature of the digital objects.

- Open digital content, with simple content types, can typically just be exported as static web resources that require little further curation.
- If the digital objects are large or complex and need specialised technology to be maintained, the continuity options also become more complex.
- If some of the digital objects and metadata are sensitive, active management of access requests will be required.

Options for certification are limited to dataset managers (Repositories) via CoreTrustSeal[49],

[49] https://www.coretrustseal.org/

Funded by the European Union

nestor seal[50], or ISO 16363[51].

CoreTrustSeal guidance[52] provides good additional best practice.

A.16 Guideline 16

BP16: Maturity and Availability of Services C1 C23 C24 C25
Managers SHOULD adopt the EU Technology Readiness Level classification for services and web resources. Infrastructure and maintenance SHOULD aim for a level of availability that is acceptable to end users.

Readiness Level[53]	**Description and Applicability**
TRL9	*System proven in an operational environment* . All main services (creating and updating PID metadata, resolution targets) must be at this level.
TRL8	*System complete and qualified.* Demonstration systems and full beta releases. Applicable for releases of value-added, non-critical services.
TRL7	*Prototype demonstration in operational environment.* Alpha releases. Releases of value-added, non-critical services, but not advised.
TRL6	*Demonstrated in a relevant environment.* Experiments and labs. Applicable to all services with appropriate disclaimers.
Lower Levels	Not applicable.

Availability expected of Managers depend on their context, and can vary from commercial-level expectations of near-permanent availability and associated agreements, to the typical research consensus (no guarantees of service after hours, and the services are free).

Irrespective of the context, service levels should be published explicitly, even for free services.

[50] https://www.langzeitarchivierung.de/Webs/nestor/EN/Zertifizierung/nestor_Siegel/siegel.html
[51] http://www.iso16363.org/
[52] https://www.coretrustseal.org/wp-content/uploads/2019/11/2019-10-CoreTrustSeal-Extended-Guidance-v2_0.pdf
[53] https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf

Availability is expressed in a standard notation[54] that can be considered.

[54] https://en.wikipedia.org/wiki/High_availability

Funded by
the European Union