



Report on compliance validation

Main author

Miguel Ferreira (KEEP Solutions, Portugal)

Contributions


Luís Faria (KEEP Solutions, Portugal)

Matthias Hahn (Fachinformationszentrum Karlsruhe, Germany)

Kresimir Duretec (Vienna University of Technology, Austria)

May 2014

This work was partially supported by the SCAPE Project. The SCAPE project is co-funded by the European Union under FP7 ICT-2009.4.1 (Grant Agreement number 270137).

This work is licensed under a CC-BY-SA International License 

References

Ref.	Document	Date	Details and Version
D12.1	Identification of triggers and preservation Watch component architecture, subcomponents and data model	2012-01-27	Final
D14.1	Report on decision factors and their influence on planning	2011-11-30	Final
MS50	White paper: Context and linking for Research Data	2013-09-12	Final
RODA09	RODA: a service-oriented repository to preserve authentic digital objects. http://hdl.handle.net/1822/9408	2009-05-20	Final
CB09	Becker, C., Kulovits, H., Guttenbrunner, M., Strodl, S., Rauber, A., & Hofman, H. (2009). Systematic planning for digital preservation: evaluating potential strategies and building preservation plans. <i>International Journal on Digital Libraries</i> , 10(4), 133–157. doi:10.1007/s00799-009-0057-1	2009	Final
CB12	Becker, C., Duretec, K., Petrov, P., Faria, L., Ferreira, M., & Ramalho, J. C. (2012). Preservation Watch: What to monitor and how. <i>iPres'12</i> . Toronto, Canada.	2012	Final
LF12	Faria, L., Petrov, P., Duretec, K., Becker, C., Ferreira, M., & Ramalho, J. C. (2012). Design and architecture of a novel preservation watch system. <i>ICADL'12</i> (pp. 168–178). Taipei, Taiwan: Springer. doi:10.1007/978-3-642-34752-8_23	2012	Final
RS12	Schmidt, R. (2012). An Architectural Overview of the SCAPE Preservation Platform. <i>iPres'12</i> . Toronto, Canada.	2012	Final
D13.1	Final version of Policy specification model	2013-07-31	Final
D13.2	Catalogue of preservation policy elements	2014-02-28	Final
D20.6	Final best practice guidelines and recommendations For Large-scale long-term repository migration; For Preservation of research data; For Bit preservation	2014	Final

Executive Summary

This whitepaper describes the integrated technologies produced in SCAPE and the results of its assessment against the ISO 16363 – a framework for Audit and Certification of Trustworthy Digital Repositories. The work aims to demonstrate that a preservation ecosystem composed of building blocks as the ones developed in SCAPE is able to comply with most of the system-related requirements of the ISO 16363.

The SCAPE Preservation Environment (SPE) is composed of a repository system, an execution environment, planning & watch services, preservation control policies, and best practice guidelines and reports. From a total of 108 metrics included in the ISO 16363, the SPE fully supports 69 of them. 31 metrics were considered to be “out of scope” as they refer to organisational issues that cannot be solved by technology alone nor can they be analysed outside the framework of a breathing organisation, leaving 2 metrics to be considered “partially supported” and 6 metrics to be considered “not supported”. This gives an overall compliancy level of roughly 90% (if the organisational oriented metrics are not taken into account).

Even though we consider this to be an excellent result, proving and giving guidelines on how it would be possible to have a system compliant with most of the metrics included in ISO 16363, this also enabled us to identify the main weak points of the SCAPE Preservation Environment that should be addressed in the near future. In summary the gaps found were:

- The ability to manage and maintain contracts or deposit agreements through the repository user interfaces;
- Support for tracking intellectual property rights;
- Improve technical documentation, especially on the conversion of Submission Information Packages (SIP) into Archival Information Packages (AIP);
- The ability to aid the repository manager to perform better risk management.

Our goal is to ensure that the SCAPE Preservation Environment fully supports the system-related metrics of the ISO 16363. In order to close the gaps encountered, additional features have been added to the roadmap of the SPE.

Table of Contents

1	Introduction.....	1
1.1	Goals.....	1
1.2	Target audience.....	2
2	The SCAPE Preservation Environment.....	2
2.1	Reference architecture	2
2.2	Reference implementation	4
3	The evaluation framework.....	6
4	Compliance validation.....	7
4.1	Organizational Infrastructure.....	8
4.1.1	Governance & organizational viability.....	8
4.1.2	Organizational structure & staffing	9
4.1.3	Procedural accountability & preservation policy framework.....	10
4.1.4	Financial sustainability.....	11
4.1.5	Contracts, licenses, & liabilities	11
4.2	Digital Object Management	12
4.2.1	Ingest: acquisition of content	12
4.2.2	Ingest: creation of the AIP	13
4.2.3	Preservation planning.....	17
4.2.4	AIP preservation.....	17
4.2.5	Information management.....	18
4.2.6	Access management	18
4.3	Infrastructure and Security Risk Management	19
4.3.1	Technical infrastructure risk management.....	19
4.3.2	Security risk management	21
5	Conclusions.....	21

6	Appendix.....	25
6.1	Screenshot of RODA user action logs.....	25
6.2	Screenshot of RODA’s executed tasks	26
6.3	Screenshot of RODA fixity check.....	27
6.4	Screenshot of RODA ‘Notify access restrict expiration’ plugin.....	28
6.5	Screenshot of policies in Scout	29
6.6	Screenshot of a content profile in Scout.....	30
6.7	Screenshot of an ingest status in RODA.....	31
6.8	Screenshot of the well-formed ingest status in RODA	32
6.9	Screenshot of authorized ingest status in RODA	33
6.10	Screenshot of rejected ingest status in RODA	34
6.11	Screenshot of SIP manual accept form on RODA ingest.....	35
6.12	Screenshot of SIP manual reject on RODA ingest.....	36
6.13	Screenshot of PRONOM format information in Scout.....	37
6.14	Screenshot of PRONOM and MIME IDs inside of PREMIS from RODA.....	38
6.15	Screenshot of fixity event inside preservation tab in RODA.....	39
6.16	Screenshot of Scout source adaptors	40
6.17	Scout notification	41
6.18	Plan details and available action on Plan Management GUI	42
6.19	Repository events in Scout.....	43
6.20	Screenshot of descriptive metadata edit in RODA	44
6.21	Screenshot of object permissions edit in RODA	45
6.22	Screenshot of action alternatives in Plato	46



1 Introduction

Over the last three years, the SCAPE project worked in several directions in order to propose new solutions for digital preservation, as well as improving existing ones. One of the results of this work is the SCAPE preservation environment (SPE). It is a loosely coupled system, which enables extending existing digital repository systems (e.g. RODA) with several components that cover collection profiling (i.e. C3PO), preservation monitoring (i.e. SCOUT) and preservation planning (i.e. Plato). Those components address key functionalities defined in the Open Archival Information System (OAIS) functional model. Existing repository systems lack most of these functionalities or have them implemented them in a very superficial way. As those functionalities are implemented into existing repository systems it is expected that they will improve and further automate the overall digital preservation process.

Establishing trustworthiness of digital repositories is a major concern of the digital preservation community as it makes the threats and risks within a digital repository understandable. There are several approaches developed over recent years on how to address trust in digital repositories. Most notable is Trustworthy Repositories Audit and Certification (TRAC) which has later been promoted to an ISO standard by the International Standards Organization (ISO 16363, released in 2012). The standard comprises of three pillars: organizational infrastructure, digital object management, and infrastructure and security management and for each of these it provides a set of requirements and the expected evidence needed for compliance.

This report presents the compliance validation of the integrated preservation ecosystem that resulted from the SCAPE project according to the specified metrics of the ISO 16363 standard. It presents in short the SCAPE preservation ecosystem and the information flow between the components. It gives a brief overview of the ISO 16363 and the metrics used throughout the assessment process.

The validation is presented in the form of a table in which assessment metrics are backed up with evidence and explanations on how the SCAPE preservation environment is able to meet those requirements.

1.1 Goals

The main goal of this work is to provide an analysis of the SCAPE preservation environment in terms of compliance to the ISO 16363. The report shows how certain requirements of the standard are supported by the preservation ecosystem developed in SCAPE. This should result in a better

understanding of capabilities which can be acquired when such system would be implemented in a certain organization.

1.2 Target audience

This whitepaper aims primarily at the following stakeholders:

- Digital content holders and/or repository owners
- Digital repository vendors and developers
- ISO 16363 auditors
- Digital preservation experts

2 The SCAPE Preservation Environment

This section presents the SCAPE Preservation Environment (SPE), an architecture that includes storage and data management, preservation planning, monitoring and operations (or actions). The SPE allows for long-term preservation of digital information by continuously monitoring internal and external influencers and determining the best actions to undertake in order to preserve the digital materials in custody.

This section also defines the reference architecture of the SPE by describing the components that support each of the underlying preservation activities. It also includes a description of one concrete repository implementation – RODA with SCAPE outcomes – that will be the object of this compliance validation.

2.1 Reference architecture

The **Repository** is an instance of a system which contains the digital content and may include processes such as ingest, access, storage and metadata management. The repository may be as simple as a shared folder with files that represent the content or as complex as information management systems such as DSpace¹, Eprints² and RODA³.

Preservation watch is the process that monitors internal and external influencers and notifies the relevant parties when risks and opportunities for the repository take place. The most noticeable party would be the Preservation manager, i.e. the person whose role is to manage the digital preservation lifecycle and the repository content.

Preservation planning is the process that takes place after a watch notification. It analyses the current situation and helps the Preservation manager to decide what action to take.

¹ <http://www.dspace.org>

² <http://www.eprints.org>

³ <http://www.roda-community.org>

Preservation operations are the processes responsible for changing the contents of the repository according to preservation plans that result from the Planning activity. For example, a recently issued preservation plan might trigger an action that consists of migrating all objects in a given format to a different one in order to save costs in storage or improve its accessibility.

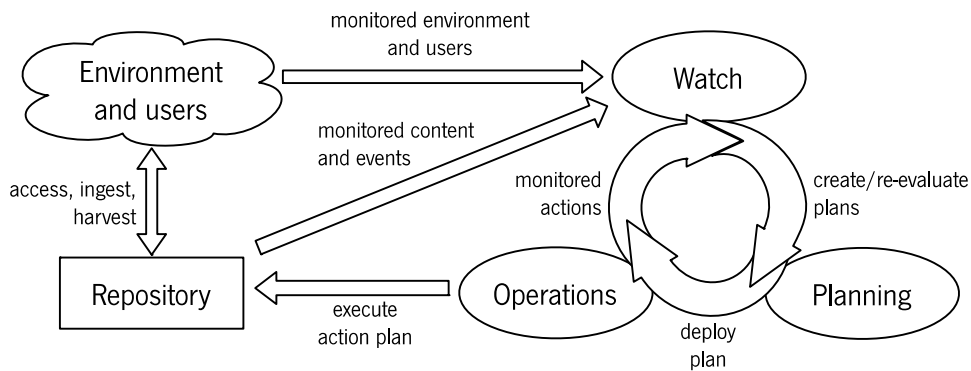


Figure 1 - Digital preservation lifecycle.

Figure 1 illustrates the entire preservation lifecycle of the SPE. One of the main components of the SPE is the Watch component. Its role is to monitor aspects of the world and detect risks and opportunities related to digital content. It monitors the internals of the repository (i.e. content and operations) and the environment around it. It begins with a characterization process that extracts the key characteristics of the digital content held in the repository. Those characteristics are aggregated and fed to the watch component so that the content can be validated against institutional policies to discover non-conformances.

Repository events are the second aspect that is monitored by the watch component. This enables prompt reaction on any event happening in a repository that may trigger a response from the Planning perspective. This can include events such as ingest or access but also anomalies occurring during the execution of preservation plans.

Furthermore, the Watch functional unit validates information about collections against institutional policies (if available in a machine readable format) and notifies the preservation planning process to address the detected violations⁴.

The Planning process carefully examines the risks or opportunities, considering the institution policies, objectives and constraints. It evaluates and compares possible alternatives and produces an action plan that defines which operations should be implemented and which service levels have been agreed on, and documents the reasoning that supports this decision [CB09]. This action plan is implemented in the repository by the Operations component. An action plan can also invoke quality

⁴ See deliverable D13.2 - Catalogue of preservation policy elements for more information.

assurance tools that will measure the outcome of the executed plan to determine if the quality goals are being met. Watch is able to gather information on quality assurance via the repository events and notifies the preservation manager if the quality of the results is below the expected threshold. This may require plans to be re-evaluated.

Also, if certain aspects of the preservation environment change, this may render existing preservation plans invalid. The watch component can also notify the relevant parties that a re-evaluation of existing plans is required. This approach creates a continuous cycle that ensures that content remains aligned with the requirements and goals set for the repository.

2.2 Reference implementation

The reference implementation of the SPE, which will be the subject of evaluation in this report, is comprised by a set of software components that support the processes defined on the previous section. The SPE reference implementation is composed of:

1. **RODA digital repository**⁵ - The digital content in the SPE is managed by RODA, the repository system elected to integrate the various functional components developed in SCAPE. RODA is a state-of-the-art open-source digital repository system designed for digital preservation. It is supported by Fedora Commons and provides simple to use graphical user interfaces for ingest, data management, archival storage, dissemination and administration.
2. **Scout** - The monitoring/watch process is implemented by Scout⁶, a Preservation Watch system supported by a knowledge base that centralizes all necessary information to detect preservation risks and opportunities [CB12, LF12]. It uses plugins to ease the integration of new information sources such as file format registries, tools for characterization, migration and quality assurance, policies and human knowledge. The knowledge base can be easily browsed and triggers can be created to automatically notify parties of new risks and opportunities. Examples of such notification could be: content fails to conform to defined policies, a format became obsolete or new tools which are able to render your content are available.
3. **Plato** - The Planning process is supported by Plato⁷, a well-established tool for systematic preservation planning. It allows for the definition of preservation objectives, criteria and restrictions necessary for decision-making and helps with the evaluation of all action alternatives, arriving to the best possible solution, documenting all the reasoning behind the decisions, and providing traceability, one of the basis for maintaining the authenticity of digital assets [CB09]. The result of preservation planning is an action plan that, besides documenting the decision making process itself, defines the necessary operations to perform on the content.

⁵ <http://www.roda-community.org>

⁶ <https://github.com/openplanets/scout>

⁷ <http://ifs.tuwien.ac.at/dp/plato>

4. **Taverna** - the Operations process is supported by Taverna⁸, a workflow management system widely used, especially in the biology domain. Taverna allows the execution of complex workflows that bring together preservation components like characterization, migration and quality assurance tools. Many common preservation tools were wrapped into a special Taverna workflow, defined as preservation component, and published in the myExperiment site⁹. Research was also done in SCAPE on how to run such complex workflows in large-scale [RS12]. Taverna was chosen as the reference implementation as it is easier to reproduce than the complex systems needed for large-scale execution.

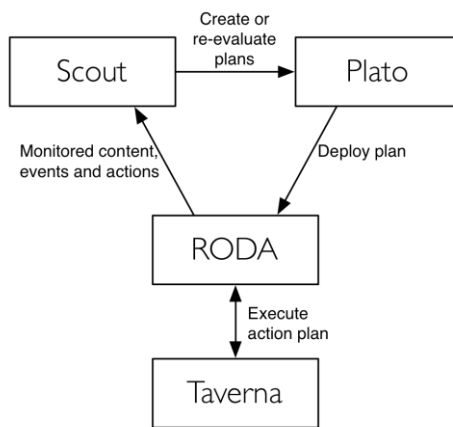


Figure 2 - SPE reference implementation.

Figure 2 illustrates how all of these components function together.

Besides the functional components included in the SCAPE Preservation Environment SCAPE has also produced relevant outputs that should be considered as being part of the SPE, namely:

1. **Policies** - Human-readable top-level preservation policies as well as machine-readable control policies have been produced in SCAPE. These policies are important to fully support automated monitoring activities¹⁰.
2. **Best practice guidelines** – SCAPE produced best practice guidelines on the following aspects of preservation that are relevant in the context of ISO 16363, Data Seal of Approval (DSA) and Nestor (D20.6 - Final best practice guidelines and recommendations¹¹). These are:
 - a. Large-scale long-term repository migration
 - b. Preservation of research data

⁸ <http://www.taverna.org.uk>

⁹ <http://www.myexperiment.org>

¹⁰ D13.1 Final Version of Policy Specification Model and D13.2 Catalogue of preservation policy elements.

¹¹ http://www.scape-project.eu/wp-content/uploads/2014/03/SCAPE_D20.6_KB_V1.0.pdf

c. Bit preservation

3. **SCAPE reports** – SCAPE produced several reports¹² that detail each of the functional components included in the SPE. These reports fully describe the inner workings of these components and may assist adopting organisations in the implementation process.

3 The evaluation framework

In 2003, the Research Library Group (RLG) and the National Archives and Records Administration (NARA) set up a working group to discuss issues related to trust and certification of digital repositories. The goal of that group was to establish a set of criteria that would allow one to assess the ability of a digital repository to store, and provide continuous access to digital materials.

The challenge was to assemble a set of measurable attributes and build sustainable ground that would eventually lead to the certification of digital repositories, these being managed by small institutions or large-scale repositories hosted by national or international wide organizations.

In 2007 a document named Trustworthy Repositories Audit & Certification: Criteria & Checklist was finally published. This document, which later became known as TRAC, brought together a set of requirements considered necessary to establish a climate of trustworthiness around the digital repository. The requirements are loosely grouped into 3 categories:

1. Organizational Infrastructure;
2. Digital Object Management, and
3. Technologies, Technical Infrastructure, & Security.

In mid-2012, TRAC was promoted to an ISO standard. The original document has been refined, reshaped and republished as ISO 16363 - Audit and certification of trustworthy digital repositories.

The ISO 16363 audit and certification standard provides for those who fund or who deposit their valuable resources into the repository the reassurance that their assets will be well preserved for future use. The standard identifies which aspects of the repository are considered to be of trust and warns them about the aspects which are not trustworthy. It also gives them the comfort of knowing that someone else besides the repository owners can actually say that that the repository has (or has not) been doing a good job. The notion of “doing a good job” goes well beyond the simple notion of doing bit preservation. Instead, what the standard aims for is the reassurance is that the digitally encoded information will be accessible and usable into the future, independently of any legal, financial, technical or human constraints.

As TRAC, the ISO 16363 is divided into 3 sections, each of which comprised of considerably large set of requirements. Sections 3 to 5 of the ISO provide the normative metrics against which a digital

¹² <http://www.scape-project.eu/downloads>

repository and the organisation which operates it may be judged. These sections provide metrics grouped as follows:

- Section 3 covers Organizational Infrastructure;
- Section 4 covers Digital Object Management;
- Section 5 covers Infrastructure and Security Risk Management.

Each section of metrics is further divided into one or more subsections.

As it happens in most, if not all, ISO standards, in order to meet a requirement, the repository owner must provide tangible evidence that the repository actually meets the requirement. It is worth mentioning that a considerable number of metrics in the standard are not related to technology. For instance, the first group of metrics is mostly concerned with the risks associated with the organization that owns the repository. For example, it contains metrics related to the financial sustainability, training of the staff members and details on the organizational procedures, which in practice cannot be assessed solely from a technology perspective.

In this work, we used the ISO 16363 - Audit and Certification of Trustworthy Digital Repositories - as an evaluation framework to determine how apt is the SCAPE preservation environment to cope with highly demanding requirements of a trustworthy preservation ecosystem.

4 Compliance validation

ISO standards are part of a suite of standards at the repository, national, and international levels that demonstrate trustworthiness, responsible data management and stewardship. They provide digital repositories of all sizes directions for demonstrating their adherence to quality and consistency, to show respect for data integrity, and a commitment to the long-term preservation of and access to the information entrusted to their care¹³.

In this study we will assess the SCAPE Preservation Environment solely from a technological perspective. This means that metrics that solely focus aspects of the owner organization or hosting infrastructure will not be assessed. We will, however, provide explanations on how the SCAPE Preservation Environment may be able to provide support for those metrics based on the existing functionalities of the technology.

The following sections provide details on the assessment of the SPE according to the requirements of the ISO 16363. For each requirement/metric we provide the level of compliance, and explanations for that assessment. In the cases where compliance has been met, evidence on how the SPE meets the requirement is also provided.

¹³ You may obtain a copy of the Self-Assessment Template for ISO 16363 at <http://www.iso16363.org/assets/Self-AssessmentTemplateforISO16363.xls>.

The considered levels of compliance are as follows:

- **OUT OF SCOPE** – The requirement is not system-related and depends of organisational aspects that are out of the scope of this assessment.
- **NOT SUPPORTED** – The SPE does not meet the requirement.
- **PARTIALLY SUPPORTED** – The SPE does not fully meet the requirement, however, it provides functionality that allows it to partially meet the requirement or to support other non-system-related activities necessary to meet the requirement.
- **FULLY SUPPORTED** – The existing functionality fully meets the requirement.

For the purpose of simplicity and conformity to the terminology used in the standard, from now on the SCAPE preservation environment will also be referred to as the “repository”.

It is also worth mentioning that the metrics described in this document are numbered according to the original numbering of the ISO Standard and not according to the numbering of the sections included in this document. This makes it easier for reader to locate further information about a metric in any additional publication.

4.1 Organizational Infrastructure

4.1.1 Governance & organizational viability

No.	Metric/Requirement	Level of compliance	Explanations and evidence
3.1.1	The repository shall have a mission statement that reflects a commitment to the preservation of, long-term retention of, management of, and access to digital information.	OUT OF SCOPE	This is not a system-related metric, however functionally exists that aids in its implementation. The SPE enables the administrator to set static HTML pages where information such as the mission can be published. Detailed information about policies, risk management and contingency plans can be found on SCAPE deliverables D13.1, D13.2 and D20.6.
3.1.2	The repository shall have a preservation strategic plan that defines the approach the repository will take in the long-term support of its mission	OUT OF SCOPE	This is not a system-related metric, however the SPE documentation includes a policy model that provides guidance on the creation of preservation strategic plans. Detailed information about policies, risk management and contingency plans can be found on SCAPE deliverables D13.1, D13.2 and D20.6.
3.1.2.1	The repository shall have an appropriate, formal succession plan , contingency plans, and/or escrow arrangements in place in case the repository ceases to operate or the governing or funding institution substantially changes its scope.	OUT OF SCOPE	This is not a system-related metric, however the SPE documentation includes guidelines and recommendations on how to perform large-scale repository migrations which provides technical guidance on the creation of succession plans. Detailed information about policies, risk management and contingency plans can be found on SCAPE deliverables D13.1, D13.2 and D20.6.

3.1.2.2	The repository shall monitor its organizational environment to determine when to execute its formal succession plan, contingency plans, and/or escrow arrangements	OUT OF SCOPE	This is not a system-related metric, however functionally exists on the SPE that aids in its implementation. The SPE includes a Watch component that if configured with the right indicators is able to notify users that certain conditions have evolved in ways that may trigger the succession plan. For example, the Watch component may be used to notify the owner of the repository if the ingest process is experiencing constant delays in the SIPs validation step. This may indicate that the repository is lacking the necessary human resources and therefore is unable to pursue its mission. Detailed information about policies, risk management and contingency plans can be found on SCAPE deliverables D13.1, D13.2 and D20.6.
3.1.3	The repository shall have a collection policy or other document that specifies the type of information it will preserve, retain, manage and provide access to.	OUT OF SCOPE	This is not a system-related metric, however the SPE allows the definition of policies that can specify the content set, i.e. a collection of objects that are the focus of the policy. Detailed information about policies, risk management and contingency plans can be found on SCAPE deliverables D13.1, D13.2 and D20.6.

4.1.2 Organizational structure & staffing

No.	Metric/Requirement	Level of compliance	Explanations and evidence
3.2.1	The repository shall have identified and established the duties that it needs to perform and shall have appointed staff with adequate skills and experience to fulfil these duties.	OUT OF SCOPE	This is not a system-related metric.
3.2.1.1	The repository shall have identified and established the duties that it needs to perform.	OUT OF SCOPE	This is not a system-related metric.
3.2.1.2	The repository shall have the appropriate number of staff to support all functions and services.	OUT OF SCOPE	This is not a system-related metric, however functionally exists on the SPE that aids in its implementation. The Watch component can be used to monitor the success of the repository, i.e. if the repository is meeting the objectives defined in its strategic plan. If the objectives are not being met, it could be because there is insufficient number of staff members.
3.2.1.3	The repository shall have in place an active professional development program that provides staff with skills and expertise development opportunities.	OUT OF SCOPE	This is not a system-related metric.

4.1.3 Procedural accountability & preservation policy framework

No.	Metric/Requirement	Level of compliance	Explanations and evidence
3.3.1	The repository shall have defined its designated community and associated knowledge base(s) and shall have these definitions appropriately accessible.	OUT OF SCOPE	This is not a system-related metric, however functionally exists on the SPE that aids in its implementation. The SPE enables the administrator to set static HTML pages where information such as the definition of the designated community can be published.
3.3.2	The repository shall have preservation policies in place to ensure its preservation strategic plan will be met.	FULLY SUPPORTED	The SPE provides documentation and guidance on how to create preservation strategic plans. Preservation control policies can then be formalised to enable monitoring with the Watch component of organizational objectives and repository compliance. Detailed information about control policies can be found on SCAPE deliverables D13.1 and D13.2.
3.3.2.1	The repository shall have mechanisms for review, update, and on-going development of its Preservation Policies as the repository grows and as technology and community practice evolve.	OUT OF SCOPE	This is not a system-related metric, however, the Watch component can be configured to alert the repository owner to review its policies after a defined period of time. Detailed information about policies can be found on SCAPE deliverables D13.1 and D13.2.
3.3.3	The repository shall have a documented history of the changes to its operations, procedures, software, and hardware.	OUT OF SCOPE	This is not a system-related metric.
3.3.4	The repository shall commit to transparency and accountability in all actions supporting the operation and management of the repository that affect the preservation of digital content over time.	FULLY SUPPORTED	The SPE is fully auditable. All actions performed on the SPO either by its human operators or by automated processes are logged for auditing purposes. Transparency can be implemented by publishing reports with statistics, goals accomplishment and other relevant metrics. These reports can be published on the open access pages of the repository. Evidence in appendix 6.1.
3.3.5	The repository shall define, collect, track, and appropriately provide its information integrity measurements .	FULLY SUPPORTED	The SPE automatically verifies the integrity of its data by periodically running a data integrity assessment routine. This routine verifies the checksum of each file in the repository against the checksum stored in the technical metadata. Evidence in appendix 6.3.
3.3.6	The repository shall commit to a regular schedule of self-assessment and external certification .	OUT OF SCOPE	This is not a system-related metric. Detailed information about policies, risk management and contingency plans can be found on SCAPE deliverables D13.1, D13.2 and D20.6

4.1.4 Financial sustainability

No.	Metric/Requirement	Level of compliance	Explanations and evidence
3.4.1	The repository shall have short- and long-term business planning processes in place to sustain the repository over time.	OUT OF SCOPE	This is not a system-related metric.
3.4.2	The repository shall have financial practices and procedures which are transparent, compliant with relevant accounting standards and practices , and audited by third parties in accordance with territorial legal requirements.	OUT OF SCOPE	This is not a system-related metric.
3.4.3	The repository shall have an on-going commitment to analyse and report on risk , benefit, investment, and expenditure (including assets, licenses, and liabilities).	OUT OF SCOPE	This is not a system-related metric.

4.1.5 Contracts, licenses, & liabilities

No.	Metric/Requirement	Level of compliance	Explanations and evidence
3.5.1	The repository shall have and maintain appropriate contracts or deposit agreements for digital materials that it manages, preserves, and/or to which it provides access.	NOT SUPPORTED	Some repository systems present an online license agreement that users must accept before submitting new data to the repository. The SPE assumes that the deposit agreement or contract is established outside of the system. After the producer and the repository agree on the terms of the contract, deposit privileges are granted to the producer. The producer may then submit new material to the repository be ingested.
3.5.1.1	The repository shall have contracts or deposit agreements which specify and transfer all necessary preservation rights , and those rights transferred shall be documented.	NOT SUPPORTED	See metric 3.5.1.
3.5.1.2	The repository shall have specified all appropriate aspects of acquisition, maintenance, access, and withdrawal in written agreements with depositors and other relevant parties.	NOT SUPPORTED	See metric 3.5.1.
3.5.1.3	The repository shall have written policies that indicate when it accepts preservation responsibility for contents of each set of submitted data objects	NOT SUPPORTED	See metric 3.5.1.
3.5.1.4	The repository shall have policies in place to address liability and challenges to ownership/rights.	NOT SUPPORTED	See metric 3.5.1.
3.5.2	The repository shall track and manage intellectual property rights and restrictions on use of repository content as required by deposit agreement, contract, or license.	PARTIALLY SUPPORTED	The SPE includes an action that verifies the permissions of each individual AIP against the access restrictions defined on the descriptive metadata. If the permissions are not set correctly, the repository owner is notified. Evidence in appendix 6.4.

4.2 Digital Object Management

4.2.1 Ingest: acquisition of content

No.	Metric/Requirement	Level of compliance	Explanations and evidence
4.1.1	The repository shall identify the content information and the information properties that the repository will preserve.	FULLY SUPPORTED	The SPE includes a catalogue of preservation control policies enables the repository to formalise, in machine-readable form, the information properties which the repository is committed to preserve. See 4.1.1.1 and 4.1.1.2.
4.1.1.1	The repository shall have a procedure(s) for identifying those Information Properties that it will preserve.	FULLY SUPPORTED	The SPE includes a catalogue of preservation control policies enables the repository to formalise, in machine-readable form, the information properties which the repository is committed to preserve. These control policies can be uploaded to the Watch component so that these can be verified against the contents of the repository. Evidence at appendix 6.5.
4.1.1.2	The repository shall have a record of the Content Information and the Information Properties that it will preserve.	FULLY SUPPORTED	The SPE supports the extraction of information properties from ingested content using characterization tools such as FITS ¹⁴ or Apache Tika ¹⁵ . The outputs of characterization are then aggregated in C3PO ¹⁶ and fed to the Watch component to check its compliance with the control policies. Evidence in appendix 6.6.
4.1.2	The repository shall clearly specify the information that needs to be associated with specific content information at the time of its deposit.	FULLY SUPPORTED	The SPE administrator is capable of specifying the mandatory metadata fields that should be provided by the producer. Additionally, the SIP specification and the SIP validation procedures that take place during ingest are sufficient guarantee that all the necessary information that should be associated with a specific content information is provided at the time of deposit. Evidence in appendix 6.7. Representation information is collected during the creation of the preservation policy. Repository only ingests representations that compliant with the preservation policy.
4.1.3	The repository shall have adequate specifications enabling recognition and parsing of the SIPs.	FULLY SUPPORTED	The specification of the supported SIP structure exists solely in the form of source code. Written documentation is scarce at the moment. Java libraries are provided to support developers in the creation of SIP files. Additional technical documentation should be created in order to fully support this metric. Evidence at appendix 6.8.
4.1.4	The repository shall have mechanisms to appropriately verify the depositor of all materials.	FULLY SUPPORTED	Individual depositors are granted user-specific credentials to use the system and specific permissions to deposit on a given collection. Evidence in appendix 6.9.

¹⁴ <https://code.google.com/p/fits/>

¹⁵ <http://tika.apache.org>

¹⁶ <http://ifs.tuwien.ac.at/imp/c3po>, <https://github.com/peshkira/c3po>

4.1.5	The repository shall have an ingest process which verifies each SIP for completeness and correctness.	FULLY SUPPORTED	<p>The SPE validates each individual SIP according to well documented ingest workflow. This workflow entails the following activities:</p> <ol style="list-style-type: none"> 1. Unpacking 2. Virus check 3. Envelope and metadata validation 4. Depositor authorization 5. Format normalisation (optional) 6. Format identification and property extraction 7. Human inspection 8. SIP transformation into AIP <p>This ingest workflow is specific to RODA, one of the components of the SPE. Variations of this may exist in different preservation environments. Evidence in appendix 6.7.</p>
4.1.6	The repository shall obtain sufficient control over the digital objects to preserve them.	FULLY SUPPORTED	The SPE has full control over the digital objects after these are ingested. The repository does not support external assets to be part of the collections. The legal control is assured by the deposit agreement previously established with the producer. Evidence at [RODA09].
4.1.7	The repository shall provide the producer/depositor with appropriate responses at agreed points during the ingest processes .	FULLY SUPPORTED	The depositor can inspect the status of the ingest process by logging into the system and accessing the ingest graphical user interfaces. For each individual SIP the SPE exposes the step of the ingest workflow on which the SIP is currently at and also provides detailed information on the outcome of each step. Evidence in appendix 6.7.
4.1.8	The repository shall have contemporaneous records of actions and administration processes that are relevant to content acquisition.	FULLY SUPPORTED	A complete ingest report is available on the SPE which records all ingest actions and their outcome for every processed SIP. Evidence in appendix 6.7.

4.2.2 Ingest: creation of the AIP

No.	Metric/Requirement	Level of compliance	Explanations and evidence
4.2.1	The repository shall have for each AIP or class of AIPs preserved by the repository an associated definition that is adequate for parsing the AIP and fit for long-term preservation needs.	FULLY SUPPORTED	Documentation exists that specifies how the AIPs are structured and how individual files are related to each other. [RODA09]
4.2.1.1	The repository shall be able to identify which definition applies to which AIP .	FULLY SUPPORTED	The AIP specification refers to all AIPs in the repository. There is only one AIP format.

4.2.1.2	The repository shall have a definition of each AIP that is adequate for long term preservation , enabling the identification and parsing of all the required components within that AIP.	FULLY SUPPORTED	Documentation exists that specifies how each individual component of the AIP is related to each other and how these can be retrieved without resorting to the system itself, i.e. just by looking at the file system. Evidence include documentation on how to rebuild Fedora Commons ¹⁷ and documentation on how Fedora Commons objects relate to each other in RODA [RODA09].
4.2.2	The repository shall have a description of how AIPs are constructed from SIPs .	NOT SUPPORTED	Apart from the RODA source code itself, which can be inspected, documentation on how SIPs are transformed in AIPs is yet to be written.
4.2.3.1	The repository shall follow documented procedures if a SIP is not incorporated into an AIP or discarded and shall indicate why the SIP was not incorporated or discarded .	FULLY SUPPORTED	The SPE fully documents the reason why SIPs have been rejected. This information is kept by the system. Evidence at appendix 6.10.
4.2.4	The repository shall have and use a convention that generates persistent, unique identifiers for all AIPs	FULLY SUPPORTED	The SPE implements the Handle System ¹⁸ and assigns a Persistent Identifier to each AIP.
4.2.4.1	The repository shall uniquely identify each AIP within the repository .	FULLY SUPPORTED	Each AIP has both an internal unique identifier and a persistent identifier. Evidence is the same as in 4.2.4.
4.2.4.1.1	The repository shall have unique identifiers .	FULLY SUPPORTED	Each AIP has both an internal unique identifier and a Persistent Identifier that is also unique. Evidence is the same as in 4.2.4.
4.2.4.1.2	The repository shall assign and maintain persistent identifiers of the AIP and its components so as to be unique within the context of the repository.	FULLY SUPPORTED	Each individual component of the AIP has a unique internal identifier. The AIP as a whole also has a Persistent Identifier based on the Handle System.
4.2.4.1.3	Documentation shall describe any processes used for changes to such identifiers .	FULLY SUPPORTED	It is not possible to manually change those identifiers. They are generated and managed by the repository system.
4.2.4.1.4	The repository shall be able to provide a complete list of all such identifiers and do spot checks for duplications.	FULLY SUPPORTED	The repository supports SOAP and REST APIs that can be used to obtain a list of all metadata records in the repository, which also includes the identifiers.
4.2.4.1.5	The system of identifiers shall be adequate to fit the repository's current and foreseeable future requirements such as numbers of objects.	FULLY SUPPORTED	There is no design limitation to the number of IDs supported by the Handle system or the Fedora Commons repository on which the SPE is based. See section 1.2 about the scalability of the Handle system at http://www.handle.net/tech_manual/Handle_Technical_Manual.pdf . Also, see the theoretical maximum number of objects in Fedora ¹⁹ .

¹⁷ <https://wiki.duraspace.org/display/FEDORA34/Command-Line+Utilities>

¹⁸ <http://www.handle.net>

¹⁹ Based on <http://fedora-commons.org/documentation/2.2.4/Fedora%20Identifiers.html>, the PID can be a maximum of 64 characters, is automatically increment from 1 upwards, which removing the 5 chars needed for the "roda" namespace and ":" separator, give 1×10^{59} objects, which is 8 times more than the number of atoms in the sun.

4.2.4.2	The repository shall have a system of reliable linking/resolution services in order to find the uniquely identified object , regardless of its physical location.	FULLY SUPPORTED	The SPE implements the Handle System and assigns a Persistent Identifier to each AIP. The Handle system provides identifiers that are independent of the physical location of the assets.
4.2.5.1	The repository shall have tools or methods to identify the file type of all submitted Data Objects.	FULLY SUPPORTED	The SPE performs file format identification using FITS during the ingest process. FITS includes file format identification tools such as Droid ²⁰ , FIDO ²¹ , Unix file, Apache Tika and others. Evidence in appendix 6.14.
4.2.5.2	The repository shall have tools or methods to determine what Representation Information is necessary to make each Data Object understandable to the Designated Community.	FULLY SUPPORTED	All files ingested into the repository are identified using Droid. A PRONOM's Persistent Unique Identifier is produced and kept in the preservation metadata for each file. The PUID enables the repository to obtain the Representation Information from the PRONOM ²² registry Web site. Evidence in appendix 6.14 and the PRONOM page for PDF 1.3, see ²³ .
4.2.5.3	The repository shall have access to the requisite Representation Information .	FULLY SUPPORTED	All files ingested into the repository are identified using Droid. A PUID is produced and kept in the preservation metadata for each file. The PUID enables the repository to obtain the Representation Information from the PRONOM registry Web site. Evidence is the same as in 4.2.5.2.
4.2.5.4	The repository shall have tools or methods to ensure that the requisite Representation Information is persistently associated with the relevant Data Objects .	FULLY SUPPORTED	The SPE relies on the PRONOM registry for Representation Information. The risk of losing access to relevant Representation Information is mitigated by preserving local replicas of the PRONOM registry. Scout fetches information from the PRONOM registry, evidence at appendix 6.13.
4.2.6	The repository shall have documented processes for acquiring preservation description information (PDI) for its associated content information and acquire PDI in accordance with the documented processes.	FULLY SUPPORTED	PREMIS preservation metadata is generated during ingest for each representation and individual file. The preservation metadata is an integral part of the AIP and can be inspected on the UI by all users that have access to the representation. Evidence at appendix 6.14.
4.2.6.1	The repository shall have documented processes for acquiring PDI .	FULLY SUPPORTED	The acquisition of PDI is specified in source code ²⁴ and the SIP description. [RODA09]

²⁰ <http://sourceforge.net/projects/droid/>

²¹ <https://github.com/openplanets/fido>

²² <http://apps.nationalarchives.gov.uk/PRONOM/>

²³ <http://apps.nationalarchives.gov.uk/PRONOM/Format/proFormatSearch.aspx?status=detailReport&id=616>

²⁴ <https://github.com/keeps/roda>

4.2.6.2	The repository shall execute its documented processes for acquiring PDI .	FULLY SUPPORTED	PREMIS preservation metadata is generated during ingest for each representation and individual file. The preservation metadata is an integral part of the AIP and can be inspected on the UI by all users that have access to the representation. Evidence is the same as in 4.2.5.2.
4.2.6.3	The repository shall ensure that the PDI is persistently associated with the relevant Content Information .	FULLY SUPPORTED	PDI in the form of PREMIS is an integral part of the AIP. Although it can be inspected individually, it cannot be separated from the AIP. Evidence is the same as in 4.2.5.2.
4.2.7	The repository shall ensure that the content information of the AIPs is understandable for their designated community at the time of creation of the AIP.	FULLY SUPPORTED	The final step of the ingest procedure is a manual/semantic validation. In this step, a human user is expected to validate the correctness and usefulness of the descriptive metadata and also validate that the AIP is rendered properly. This acts as a proxy for the designated community. The outcome of this step is recorded in the system and related to the SIP. After ingest, user feedback is used to determine if a given content is not readily understandable. Evidence is in appendix 6.11.
4.2.7.1	Repository shall have a documented process for testing understandability for their Designated Communities of the Content Information of the AIPs at their creation.	FULLY SUPPORTED	The final step of the ingest procedure is a manual/semantic validation. In this step, a human user is expected to validate the correctness and usefulness of the descriptive metadata and also validate that the AIP is rendered properly. The outcome of this step is recorded in the system and related to the SIP. Evidence is in appendix 6.11.
4.2.7.2	The repository shall execute the testing process for each class of Content Information of the AIPs.	FULLY SUPPORTED	The testing process is executed for each AIP ingested. Evidence is the same as in 4.2.7.1.
4.2.7.3	The repository shall bring the Content Information of the AIP up to the required level of understandability if it fails the understandability testing.	FULLY SUPPORTED	If the Content Information fails render properly the SIPs are rejected. The producers are notified and a new SIP is expected to be deposited. Evidence in appendix 6.12.
4.2.8	The repository shall verify each AIP for completeness and correctness at the point it is created.	FULLY SUPPORTED	The final step of the ingest procedure is a manual/semantic validation. In this step, a human user is expected to validate the correctness and usefulness of the descriptive metadata and also validate that the AIP is rendered properly. The outcome of this step is recorded in the system and related to the SIP. Evidence is in appendix 6.11.
4.2.9	The repository shall provide an independent mechanism for verifying the integrity of the repository collection/content.	FULLY SUPPORTED	The SPE automatically verifies the integrity of its data by periodically running a data integrity assessment routine. This routine verifies the checksum of each file in the repository against the checksum stored in the technical metadata. The administrator can setup a specific verification routine by using the scheduler mechanism offered by the system. The set of objects of collection to analyse can be configured on the task itself. Evidence is at appendix 6.15.

4.2.10	The repository shall have contemporaneous records of actions and administration processes that are relevant to AIP creation.	FULLY SUPPORTED	All actions performed by humans or automatic processes are logged by the SPE for auditing purposes. The log can be consulted and queried on the user interface by the administrator of the repository. Evidence at appendix 6.1 and 6.2.
--------	---	-----------------	--

4.2.3 Preservation planning

No.	Metric/Requirement	Level of compliance	Explanations and evidence
4.3.1	The repository shall have documented preservation strategies relevant to its holdings.	FULLY SUPPORTED	Preservation plans created by Plato document all preservation strategies relevant to its holdings. Evidence in appendix 6.22.
4.3.2	The repository shall have mechanisms in place for monitoring its preservation environment.	FULLY SUPPORTED	Scout monitors the environment by allowing external information sources to be monitored. Evidence in appendix 6.16.
4.3.2.1	The repository shall have mechanisms in place for monitoring and notification when Representation Information is inadequate for the Designated Community to understand the data holdings.	FULLY SUPPORTED	Scout allows cross-referencing the content with monitored information on internal and external influencers, create triggers that can indicate inadequacies between the representations and the designated community, and send notification to the users when non-conformances are detected. Evidence in appendix 6.17.
4.3.3	The repository shall have mechanisms to change its preservation plans as a result of its monitoring activities.	FULLY SUPPORTED	The plan management GUI enables a plan to be updated. The reason for updating the plan should be inside of the plan itself, as inputted in Plato. Evidence is in appendix 6.18.
4.3.3.1	The repository shall have mechanisms for creating, identifying or gathering any extra Representation Information required.	FULLY SUPPORTED	The SPE characterizes all content and provides a collection profile by using C3PO, which is monitored by Scout. This identifies and gathers any extra representation information required. Plato can then be used to select the best action to create any new required representation information. Evidence in appendix 6.6.
4.3.4	The repository shall provide evidence of the effectiveness of its preservation activities .	FULLY SUPPORTED	The SPE includes quality assurance processes within the preservation activities. The output of the quality assurance processes is captured by Scout in order to provide evidence of its effectiveness. Evidence in appendix 6.19.

4.2.4 AIP preservation

No.	Metric/Requirement	Level of compliance	Explanations and evidence
4.4.1	The repository shall have specifications for how the AIPs are stored down to the bit level.	FULLY SUPPORTED	AIPs are stored in the file system according to the specifications of Fedora Commons. Evidence at Fedora Digital Object Model documentation ²⁵ .

²⁵ <http://fedora-commons.org/documentation/2.2.4/Fedora%20Digital%20Object%20Model.html>

4.4.1.1	The repository shall preserve the Content Information of AIP's.	FULLY SUPPORTED	The content of the AIPs is preserved within the AIPs. Specifications exist on how these AIPs are stored, see 4.4.1.
4.4.1.2	The repository shall actively monitor the integrity of AIPs .	FULLY SUPPORTED	The SPE automatically verifies the integrity of its data by periodically running a data integrity assessment routine. This routine verifies the checksum of each file in the repository against the checksum stored in the technical metadata, which indirectly check the data model as it needs to go through all parts of the AIP to reach the files and the technical metadata. Evidence in appendix 6.15.
4.4.2	The repository shall have contemporaneous records of actions and administration processes that are relevant to storage and preservation of the AIPs.	FULLY SUPPORTED	All actions performed by humans or automatic processes are logged by the SPE for auditing purposes. The log can be consulted and queried on the UI by the administrator of the repository. Evidence in appendices 6.1 and 6.2.
4.4.2.1	The repository shall have procedures for all actions taken on AIPs.	OUT OF SCOPE	This requirement is about written documentation. This documentation varies from one institution to another.
4.4.2.2	The repository shall be able to demonstrate that any actions taken on AIPs were compliant with the specification of those actions	FULLY SUPPORTED	All actions performed to AIPs can be inspected by looking at the system log where all the actions are recorded or by inspecting the preservation metadata associated to an AIP. The latter records any events that have been performed on a specific AIP. Evidence in appendices 6.1, 6.2 and 6.3.

4.2.5 Information management

No.	Metric/Requirement	Level of compliance	Explanations and evidence
4.5.1	The repository shall specify minimum information requirements to enable the designated community to discover and identify material of interest.	FULLY SUPPORTED	The SPE allows the administrator to set the mandatory descriptive metadata fields. SIPs that don't not comply with the definition are rejected during ingest. Evidence in appendix 6.20.
4.5.2	The repository shall capture or create minimum descriptive information and ensure that it is associated with the AIP.	FULLY SUPPORTED	The SPE has support for descriptive metadata in Encoded Archival Description (EAD) and NSESS formats. Evidence at appendix 6.20.
4.5.3	The repository shall maintain bi-directional linkage between each AIP and its descriptive information .	FULLY SUPPORTED	The descriptive metadata is part of the AIP and is constantly linked to it as it can be observed on the RODA data model. [RODA09]
4.5.3.1	The repository shall maintain the associations between its AIPs and their descriptive information over time.	FULLY SUPPORTED	The descriptive information is always associated with the AIP representations, even when new representations are created by migration actions defined by normalization rules or preservation plans. See evidence on the RODA data model in [RODA09].

4.2.6 Access management

No.	Metric/Requirement	Level of compliance	Explanations and evidence
4.6.1	The repository shall comply with access policies .	FULLY SUPPORTED	The SPE has fine-grained permissions at the user and group levels. It also supports CAS authentication for a centralised user management. A full range of access policies can be implemented. Evidence in appendix 6.21.

4.6.1.1	The repository shall log and review all access management failures and anomalies.	FULLY SUPPORTED	All authentication operations are logged by the system and can easily be inspected by the system administrators. Evidence in appendix 6.1.
4.6.2	The repository shall follow policies and procedures that enable the dissemination of digital objects that are traceable to the originals , with evidence supporting their authenticity.	FULLY SUPPORTED	All representations in the SPE are accompanied by preservation metadata. In that metadata, all the information about the events that involve a given representation is kept for later reference (e.g. format migrations, checksum verifications, etc.). Inspecting the PREMIS metadata it is possible to trace the object back to the SIP file that has been originally ingested into the repository. Evidence in appendix 6.15 and [RODA09]. Detailed information about policies can be found on SCAPE deliverables D13.1 and D13.2.
4.6.2.1	The repository shall record and act upon problem reports about errors in data or responses from users.	FULLY SUPPORTED	The repository notifies the system administrators when certain events occur. For example, in the event of a system failure, the monitoring system will warn the people in charge. Feedback channels are also in place that enable users to report any issues found in the data or in the repository.

4.3 Infrastructure and Security Risk Management

4.3.1 Technical infrastructure risk management

No.	Metric/Requirement	Level of compliance	Explanations and evidence
5.1.1	The repository shall identify and manage the risks to its preservation operations and goals associated with system infrastructure .	PARTIAL SUPPORTED	Some of the sub-requirements are out of scope as they refer to hardware technologies, organizational or funding issues. See the sub-requirements below for more details.
5.1.1.1	The repository shall employ technology watches or other technology monitoring notification systems.	FULLY SUPPORTED	The SPE uses Scout to for preservation watch, which notifies the user when non-conformities are found. Evidence at appendix 6.16 and 6.17.
5.1.1.1.1	The repository shall have hardware technologies appropriate to the services it provides to its designated communities.	OUT OF SCOPE	Hardware technologies are outside the scope of this evaluation which focuses on the SPE software package.
5.1.1.1.2	The repository shall have procedures in place to monitor and receive notifications when hardware technology changes are needed .	FULLY SUPPORTED	Hardware technologies can also be monitored by Scout, by developing adaptors for sources of information on the specific hardware technology to be monitored, or by allowing manual input of such information into Scout knowledge base.
5.1.1.1.3	The repository shall have procedures in place to evaluate when changes are needed to current hardware .	FULLY SUPPORTED	The SPE allows to monitor current hardware resource consumption using RODA's integration with Munin ²⁶ , a networked resource monitoring tool that can help analyze resource trends . This system enables evaluation of the current hardware to check if is it properly scaled to the usage requirements. Plato can also be used to decide what is the best alternative for hardware change.

²⁶ <http://munin-monitoring.org>

5.1.1.1.4	The repository shall have procedures, commitment and funding to replace hardware when evaluation indicates the need to do so.	OUT OF SCOPE	This is not a system-related metric as it relates to organisational and funding domains.
5.1.1.1.5	The repository shall have software technologies appropriate to the services it provides to its designated communities.	FULLY SUPPORTED	The SPE depends solely on state-of-the-art open technologies that are under permanent development and supported by thousands of developers worldwide. A roadmap exists for the development of the RODA repository system itself.
5.1.1.1.6	The repository shall have procedures in place to monitor and receive notifications when software changes are needed.	FULLY SUPPORTED	The SPE can monitor software and send notification via Scout. Plato can be used to evaluate what is the best alternative and if change is indeed needed.
5.1.1.1.7	The repository shall have procedures in place to evaluate when changes are needed to current software.	FULLY SUPPORTED	The SPE can monitor current software and send notification via Scout by manual creation of a software inventory. Plato can be used to evaluate what is the best alternative and if change is indeed needed.
5.1.1.1.8	The repository shall have procedures, commitment and funding to replace software when evaluation indicates the need to do so.	OUT OF SCOPE	This is not a system-related metric as it relates to organisational and funding domains.
5.1.1.2	The repository shall have adequate hardware and software support for backup functionality sufficient for preserving the repository content and tracking repository functions.	FULLY SUPPORTED	By backing up all files in storage, all information can be recovered, see requirement 4.2.1.2.
5.1.1.3	The repository shall have effective mechanisms to detect bit corruption or loss.	FULLY SUPPORTED	The SPE automatically verifies the integrity of its data by periodically running a data integrity assessment routine. This routine verifies the checksum of each file in the repository against the checksum stored in the technical metadata. Evidence at appendix 6.3.
5.1.1.3.1	The repository shall record and report to its administration all incidents of data corruption or loss, and steps shall be taken to repair/replace corrupt or lost data.	OUT OF SCOPE	The SPE however is capable of notifying administrators by email when errors occur in the system. The recording of incidents is made on a platform that is independent of the repository (i.e. a ticketing system).
5.1.1.4	The repository shall have a process to record and react to the availability of new security updates based on a risk-benefit assessment.	OUT OF SCOPE	This requirement is related to the availability of written procedures. Nonetheless, modern operating systems generally notify and record any actions taken to improve security via updates.
5.1.1.5	The repository shall have defined processes for storage media and/or hardware change (e.g., refreshing, migration).	OUT OF SCOPE	This is not a system-related metric.
5.1.1.6	The repository shall have identified and documented critical processes that affect its ability to comply with its mandatory responsibilities.	OUT OF SCOPE	This is not a system-related metric.
5.1.1.6.1	The repository shall have a documented change management process that identifies changes to critical processes that potentially affect the repository's ability to comply with its mandatory responsibilities.	OUT OF SCOPE	This is not a system-related metric.

5.1.1.6.2	The repository shall have a process for testing and evaluating the effect of changes to the repository's critical processes.	OUT OF SCOPE	This is not a system-related metric.
5.1.2	The repository shall manage the number and location of copies of all digital objects.	FULLY SUPPORTED	The SPE does not support more than one master copy of the digital object. Other copies are made by the backup system which should manage the location by itself. This is then considered to be indirectly supported by common backup systems.
5.1.2.1	The repository shall have mechanisms in place to ensure any/multiple copies of digital objects are synchronized .	FULLY SUPPORTED	See requirement 5.1.2.

4.3.2 Security risk management

No.	Metric/Requirement	Level of compliance	Explanations and evidence
5.2.1	The repository shall maintain a systematic analysis of security risk factors associated with data, systems, personnel, and physical plant.	OUT OF SCOPE	This is not a system-related metric. The implementation of ISO 27001 greatly helps in being compliant with this requirement.
5.2.2	The repository shall have implemented controls to adequately address each of the defined security risks .	OUT OF SCOPE	This is not a system-related metric. The implementation of ISO 27001 greatly helps in being compliant with this requirement.
5.2.3	The repository staff shall have delineated roles, responsibilities, and authorizations related to implementing changes within the system .	OUT OF SCOPE	This is not a system-related metric, however, the SPE has built in support for fine-grained permissions, roles, groups and user management. Any authorization policy can easily be implemented with existing functionality. The implementation of ISO 27001 greatly helps in being compliant with this requirement.
5.2.4	The repository shall have suitable written disaster preparedness and recovery plan(s) , including at least one off-site backup of all preserved information together with an offsite copy of the recovery plan(s).	OUT OF SCOPE	This is not a system-related metric. The implementation of ISO 27001 greatly helps in being compliant with this requirement.

5 Conclusions

In this work, the ISO 16363 Audit and Certification of Trustworthy Digital Repositories has been used to determine the trustworthiness of the SCAPE preservation environment, a combination of SCAPE outcomes that provides a full life-cycle preservation support to digital preservation activities. The SCAPE Preservation Environment has been assessed solely from a technological perspective. Nevertheless, responses have been given for the metrics that focus primarily on the organizational and infrastructural aspects of repository.

The requirements included in the ISO 16363 are divided into three main sections: 1) Organizational Infrastructure, 2) Digital Object Management and 3) Infrastructure and Security Management. Table 1 summarises the results of the assessment work described in this report.

Table 1 - Assessment results.

Metric/Requirement	FULLY SUPPORTED	PARTIALLY SUPPORTED	NOT SUPPORTED	OUT OF SCOPE
Organizational Infrastructure	3	1	5	16
Governance & organizational viability	-	-	-	5
Organizational structure & staffing	-	-	-	4
Procedural accountability & preservation policy framework	3	-	-	4
Financial sustainability	-	-	-	3
Contracts, licenses, & liabilities	-	1	5	-
Digital Object Management	56	0	1	1
Ingest: acquisition of content	10	-	-	-
Ingest: creation of the AIP	27	-	1	-
Preservation planning	6	-	-	-
AIP preservation	5	-	-	1
Information management	4	-	-	-
Access management	4	-	-	-
Infrastructure and Security Risk Management	10	1	0	13
Technical infrastructure risk management	10	1	-	9
Security risk management	-	-	-	4
Totals	69	2	6	31

The Organizational Infrastructure requirement is subdivided into five subsections:

1. Governance & organizational viability
2. Organizational structure & staffing
3. Procedural accountability & preservation policy framework
4. Financial sustainability
5. Contracts, licenses & liabilities.

Mostly all metrics in this section are “out of scope” for the SPE except for three metrics, which are “fully supported”, one metric that is “partially supported” and 5 metrics that were considered “not supported”. The fully supported metrics deal with preservation policies, transparency and accountability of all actions and integrity verifications. Not supported metrics have to do with the ability of the repository to manage contracts established with producers. This could very well be considered to be out of scope, but since there are some repository systems (e.g. DSpace) that provide support for acknowledging deposit agreements, we opt to mark this set of requirements as “not supported”. The out of scope metrics are focused on organisational issues, such as management of human resources and existence of written procedures and governance.

All the “out of scope” metrics are related to policies and procedures. These metrics are supported by the SCAPE deliverables D13.1 and D13.2 - Catalogue of preservation policy element. These deliverables describe a framework consisting of three levels of policy making going from a high level abstract view of preservation within an organization - the Guidance Policy - to more defined descriptions of policy intent - the Preservation Procedure Policies - through to concrete applicable statements which can support automated workflow - the Control Policies. This set of documents

serve as good reference point for any institution willing to adopt good practices in preservation policy making.

The section dealing with Digital Object Management is divided into the following subsections:

1. Ingest: acquisition of content,
2. Ingest: creation of the AIP
3. Preservation Planning
4. AIP preservation
5. Information Management
6. Access Management.

The SPE fully supports all metrics in this section except for one: the need for a description of how AIPs are constructed from SIPs. Here, the SCAPE Preservation Environment only provides information on a source code level. Additional documentation must be written in order to cope with this requirement. There was also one metric that was considered to be out of scope: the repository shall have procedures for all actions taken on AIPs. We interpreted this as being a procedural/documentation issue and evaluated it as being “out of scope”.

The results of the third and last section are about Infrastructure and Security Risk Management. It is subdivided onto:

1. Technical Infrastructure Risk Management
2. Security Risk Management

The latter is entirely out of scope for SPE but the former metrics are partially fulfilled (10 out of 20 metrics are fully supported). The development of SCOUT, a software application designed to watch the repositories actions like ingest etc., is a key player here. SCOUT extends a preservation repository with monitoring capabilities with respect to technology and software changes. In this section, 9 of the metrics were considered out of scope as they have mostly to do with the existence of written procedures for managing several aspects of the infrastructure.

In summary, the SCAPE Preservation Environment, which is composed of a repository system, an execution environment, planning & watch services, preservation control policies, and best practice guidelines and reports, is able to meet almost all metrics in the Digital Object Management section and covers a good part of the metrics in the Infrastructure and Security Risk Management of ISO 16363.

Only metrics that deal with organizational or hosting infrastructure are not supported or are out of scope of the SCAPE Preservation Environment. These would need to be addressed by those adopting the SPE but are organisationally specific and out of the remit of the technical support of the SPE although addressed within the Policy work and Best Practices resources.

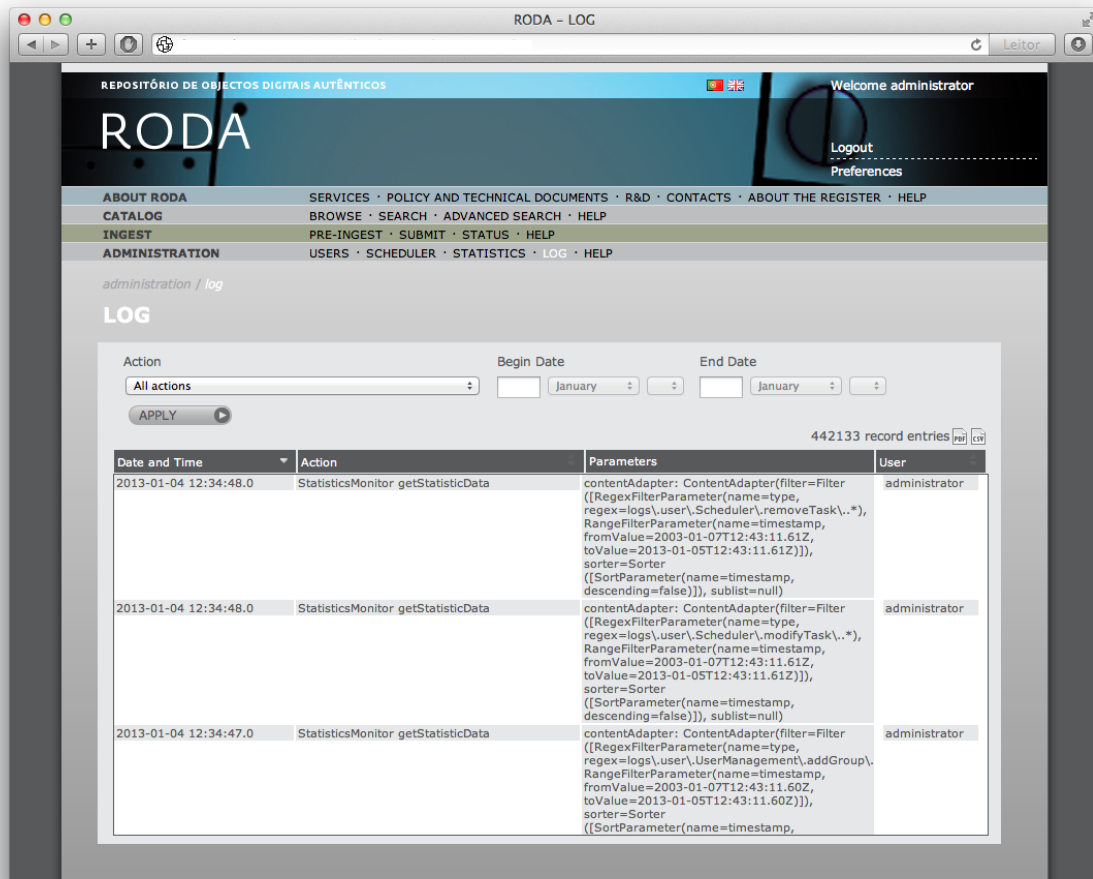
This assessment enabled the technical coordination team to include items on the SPE roadmap that will enable the preservation environment and its individual components to comply with the metrics where it was considered to be lacking full support. In summary these include the following aspects:



- The ability to manage and maintain contracts or deposit agreements through the repository user interfaces;
- Support for tracking intellectual property rights;
- Improve technical documentation, especially on the conversion of SIPs into AIPs;
- The ability to aid the repository manager to perform better risk management.

6 Appendix

6.1 Screenshot of RODA user action logs



RODA - LOG

REPOSITÓRIO DE OBJECTOS DIGITAIS AUTÊNTICOS

Welcome administrator

Logout
Preferences

ABOUT RODA SERVICES · POLICY AND TECHNICAL DOCUMENTS · R&D · CONTACTS · ABOUT THE REGISTER · HELP

CATALOG BROWSE · SEARCH · ADVANCED SEARCH · HELP

INGEST PRE-INGEST · SUBMIT · STATUS · HELP

ADMINISTRATION USERS · SCHEDULER · STATISTICS · LOG · HELP

administration / log

LOG

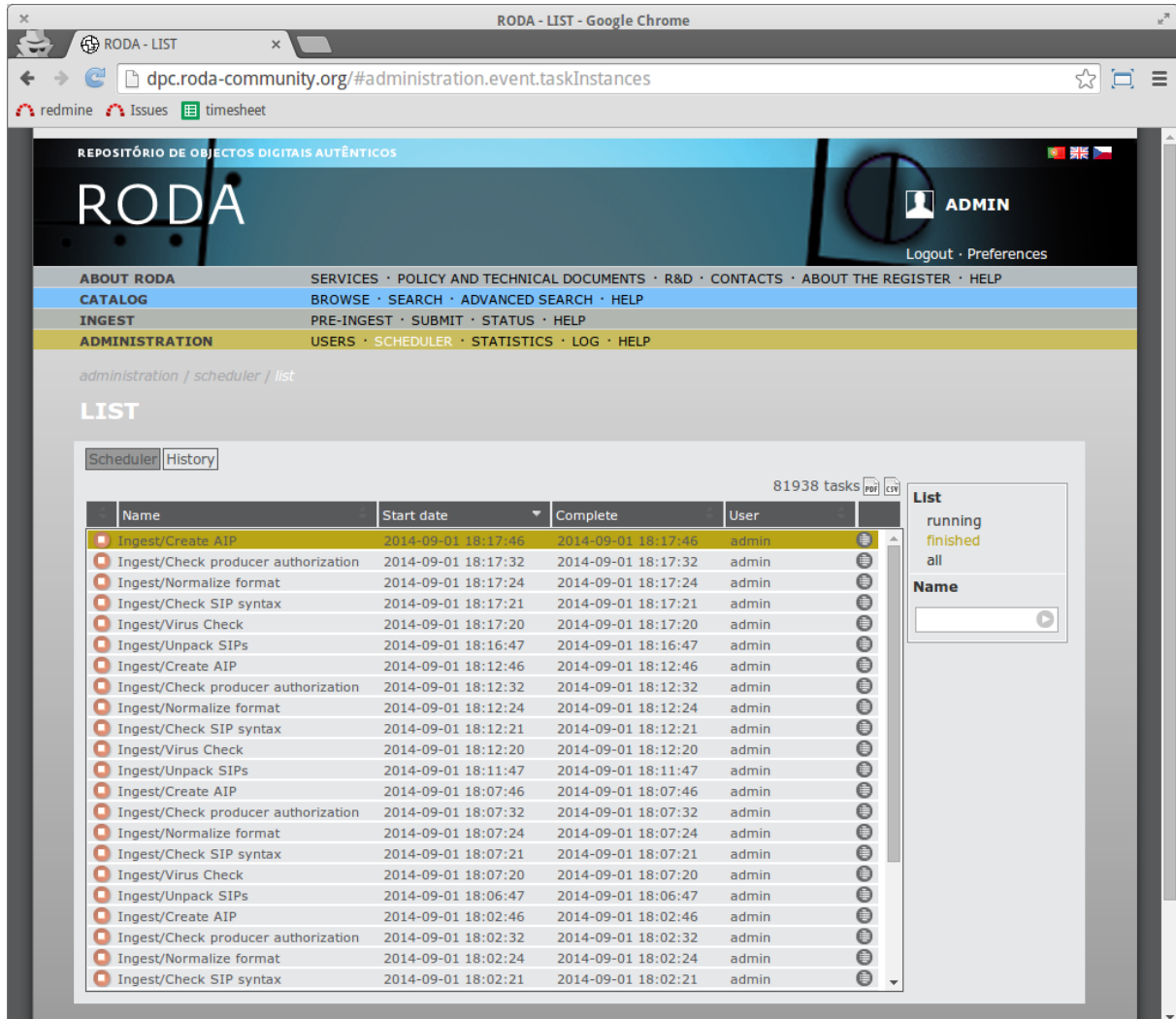
Action: All actions Begin Date: January End Date: January

APPLY

442133 record entries

Date and Time	Action	Parameters	User
2013-01-04 12:34:48.0	StatisticsMonitor getStatisticData	contentAdapter: ContentAdapter(filter=Filter ((RegexFilterParameter(name=type, regex=logs\.user\.Scheduler\.removeTask\..*)), RangeFilterParameter(name=timestamp, fromValue=2003-01-07T12:43:11.61Z, toValue=2013-01-05T12:43:11.61Z))), sorter=Sorter ((SortParameter(name=timestamp, descending=false))), sublist=null)	administrator
2013-01-04 12:34:48.0	StatisticsMonitor getStatisticData	contentAdapter: ContentAdapter(filter=Filter ((RegexFilterParameter(name=type, regex=logs\.user\.Scheduler\.modifyTask\..*)), RangeFilterParameter(name=timestamp, fromValue=2003-01-07T12:43:11.61Z, toValue=2013-01-05T12:43:11.61Z))), sorter=Sorter ((SortParameter(name=timestamp, descending=false))), sublist=null)	administrator
2013-01-04 12:34:47.0	StatisticsMonitor getStatisticData	contentAdapter: ContentAdapter(filter=Filter ((RegexFilterParameter(name=type, regex=logs\.user\.UserManagement\.addGroup\..*)), RangeFilterParameter(name=timestamp, fromValue=2003-01-07T12:43:11.60Z, toValue=2013-01-05T12:43:11.60Z))), sorter=Sorter ((SortParameter(name=timestamp,	administrator

6.2 Screenshot of RODA's executed tasks



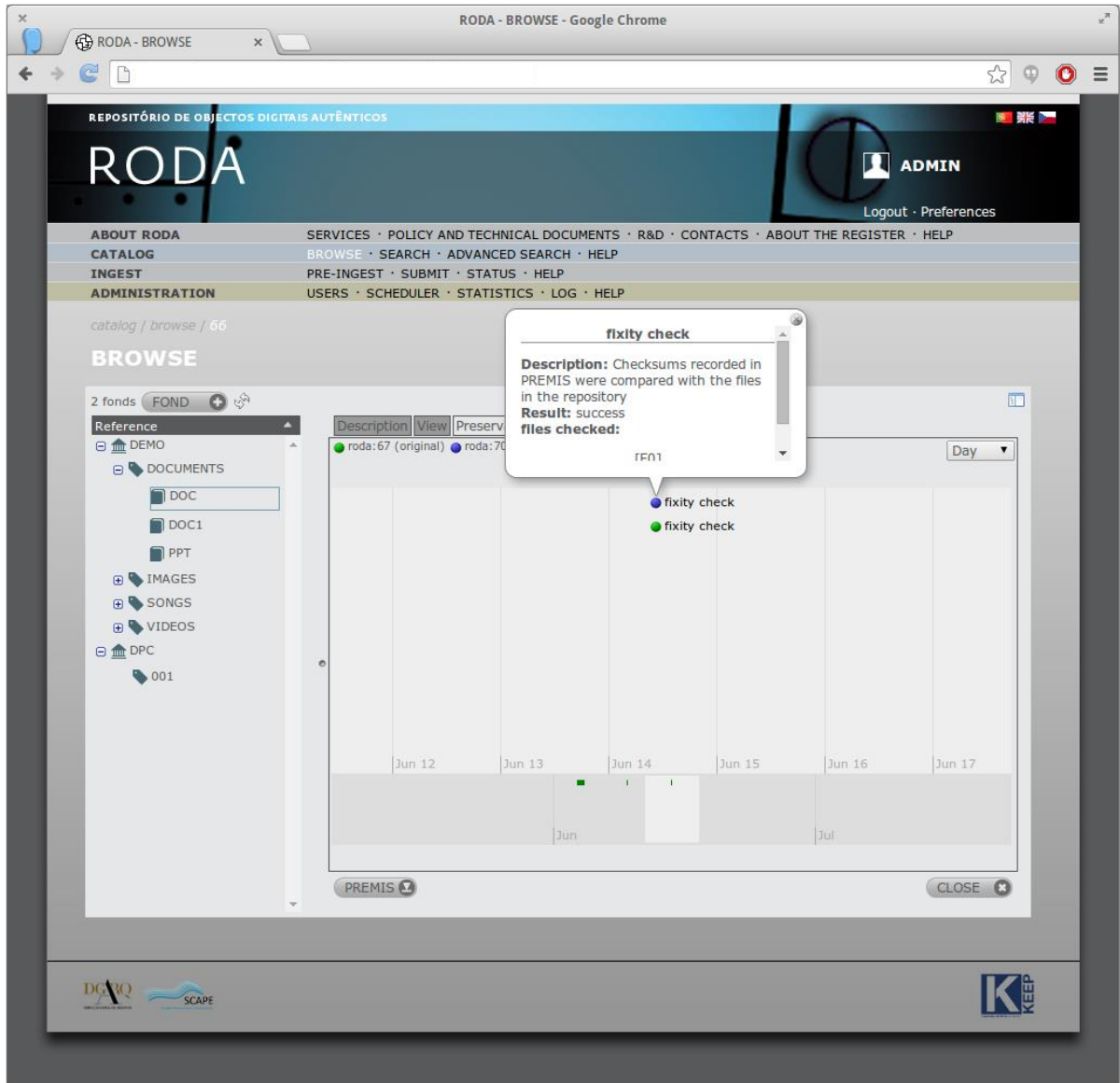
The screenshot shows the RODA administration interface in a Google Chrome browser. The page title is "RODA - LIST" and the URL is "dpc.roda-community.org/#administration.event.taskInstances". The interface includes a navigation menu with categories like ABOUT RODA, CATALOG, INGEST, and ADMINISTRATION. The current view is "administration / scheduler / list".

The main content area displays a "LIST" of tasks. There are two tabs: "Scheduler" and "History". The "Scheduler" tab is active, showing a table of 81938 tasks. The table has columns for Name, Start date, Complete, and User. The tasks are listed in descending order of start date, with the most recent task at the top.

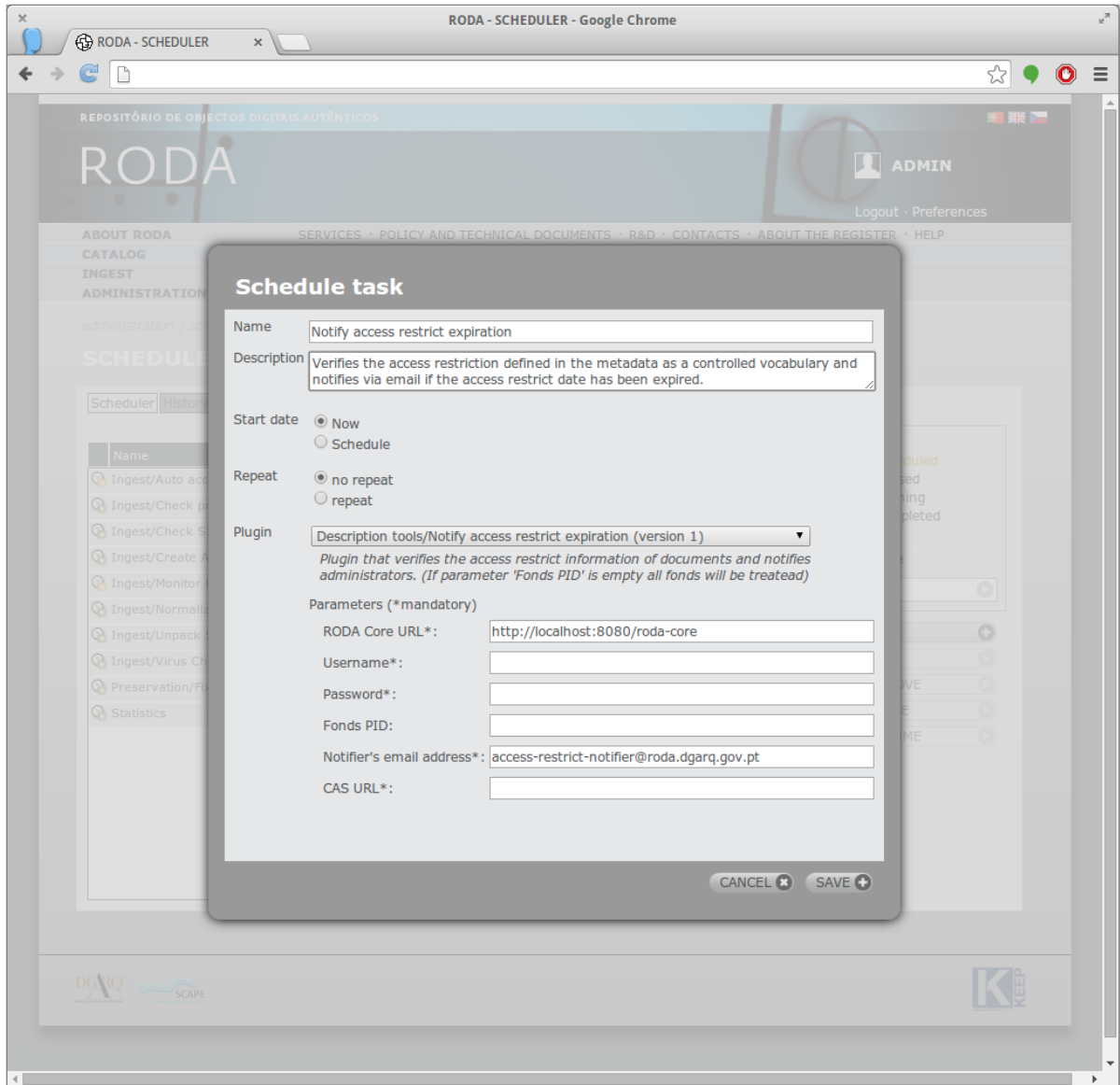
Name	Start date	Complete	User
Ingest/Create AIP	2014-09-01 18:17:46	2014-09-01 18:17:46	admin
Ingest/Check producer authorization	2014-09-01 18:17:32	2014-09-01 18:17:32	admin
Ingest/Normalize format	2014-09-01 18:17:24	2014-09-01 18:17:24	admin
Ingest/Check SIP syntax	2014-09-01 18:17:21	2014-09-01 18:17:21	admin
Ingest/Virus Check	2014-09-01 18:17:20	2014-09-01 18:17:20	admin
Ingest/Unpack SIPs	2014-09-01 18:16:47	2014-09-01 18:16:47	admin
Ingest/Create AIP	2014-09-01 18:12:46	2014-09-01 18:12:46	admin
Ingest/Check producer authorization	2014-09-01 18:12:32	2014-09-01 18:12:32	admin
Ingest/Normalize format	2014-09-01 18:12:24	2014-09-01 18:12:24	admin
Ingest/Check SIP syntax	2014-09-01 18:12:21	2014-09-01 18:12:21	admin
Ingest/Virus Check	2014-09-01 18:12:20	2014-09-01 18:12:20	admin
Ingest/Unpack SIPs	2014-09-01 18:11:47	2014-09-01 18:11:47	admin
Ingest/Create AIP	2014-09-01 18:07:46	2014-09-01 18:07:46	admin
Ingest/Check producer authorization	2014-09-01 18:07:32	2014-09-01 18:07:32	admin
Ingest/Normalize format	2014-09-01 18:07:24	2014-09-01 18:07:24	admin
Ingest/Check SIP syntax	2014-09-01 18:07:21	2014-09-01 18:07:21	admin
Ingest/Virus Check	2014-09-01 18:07:20	2014-09-01 18:07:20	admin
Ingest/Unpack SIPs	2014-09-01 18:06:47	2014-09-01 18:06:47	admin
Ingest/Create AIP	2014-09-01 18:02:46	2014-09-01 18:02:46	admin
Ingest/Check producer authorization	2014-09-01 18:02:32	2014-09-01 18:02:32	admin
Ingest/Normalize format	2014-09-01 18:02:24	2014-09-01 18:02:24	admin
Ingest/Check SIP syntax	2014-09-01 18:02:21	2014-09-01 18:02:21	admin

On the right side of the task list, there is a "List" control panel with a dropdown menu showing "running", "finished", and "all". Below the dropdown is a search input field labeled "Name".

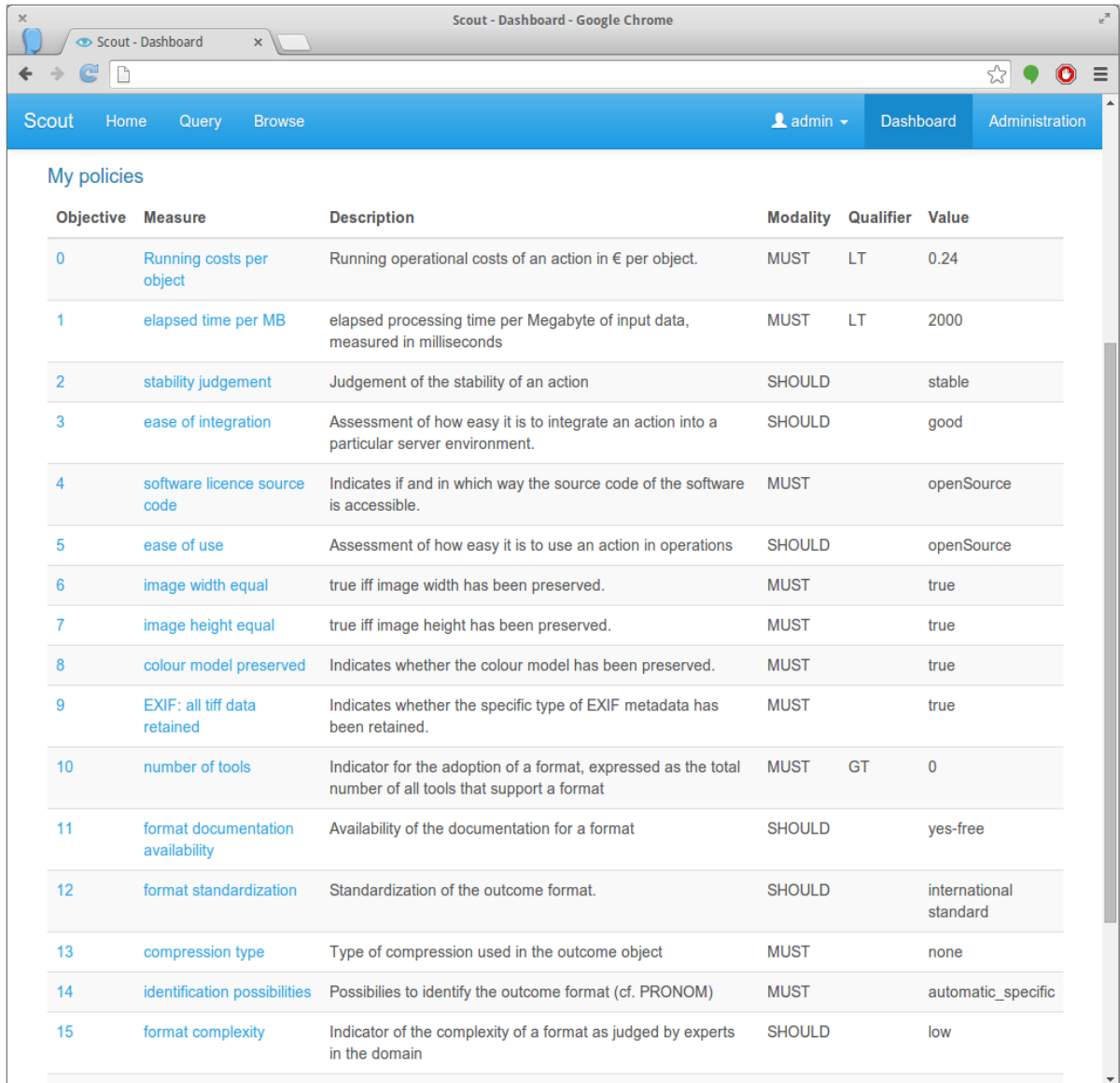
6.3 Screenshot of RODA fixity check



6.4 Screenshot of RODA 'Notify access restrict expiration' plugin



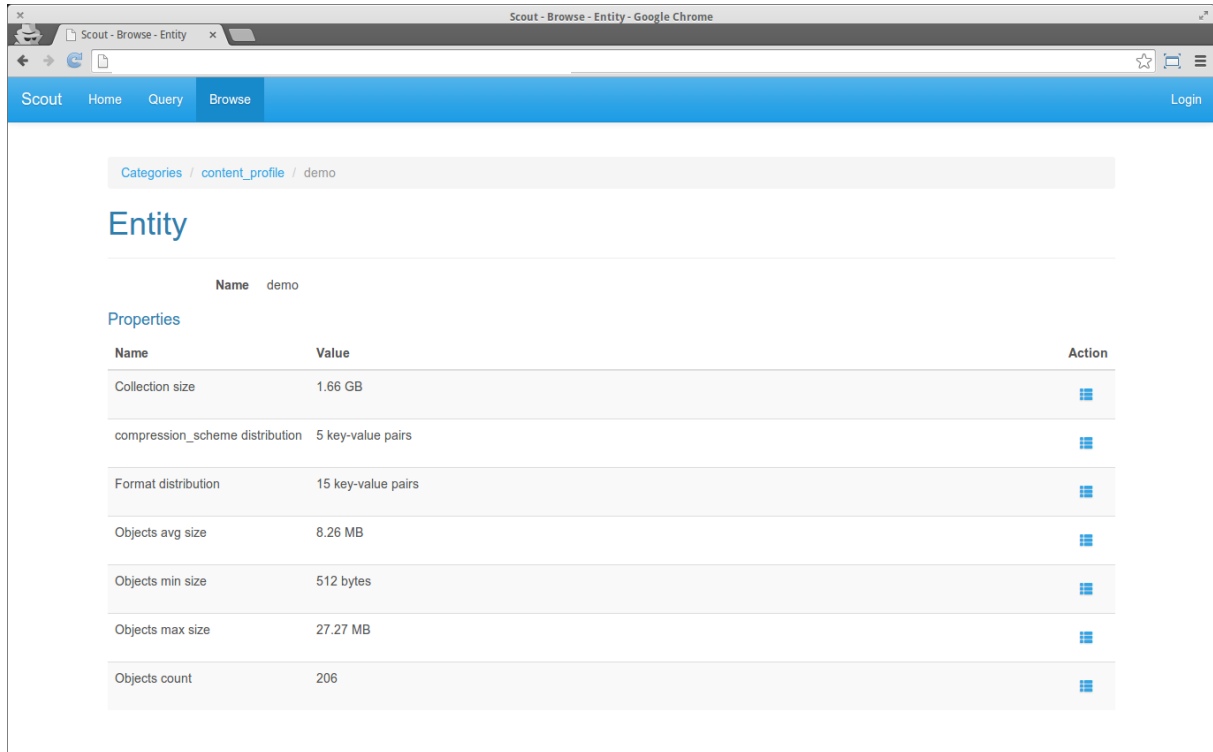
6.5 Screenshot of policies in Scout










The screenshot shows a web browser window titled "Scout - Dashboard - Google Chrome". The page displays a navigation menu with "Scout", "Home", "Query", and "Browse". The user is logged in as "admin" and is viewing the "Dashboard" section. The main content area is titled "My policies" and contains a table with 16 rows of policy data.

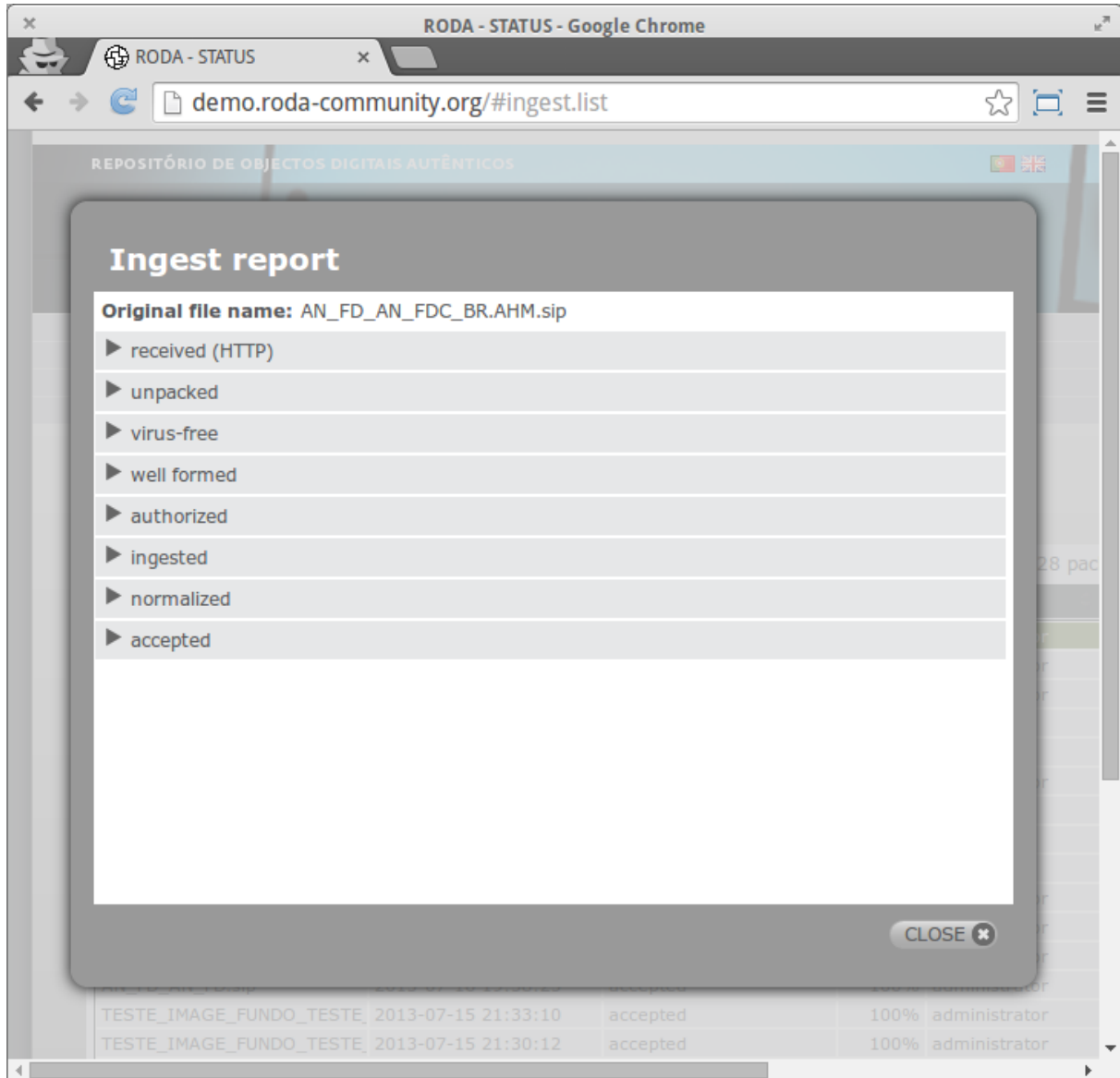
Objective	Measure	Description	Modality	Qualifier	Value
0	Running costs per object	Running operational costs of an action in € per object.	MUST	LT	0.24
1	elapsed time per MB	elapsed processing time per Megabyte of input data, measured in milliseconds	MUST	LT	2000
2	stability judgement	Judgement of the stability of an action	SHOULD		stable
3	ease of integration	Assessment of how easy it is to integrate an action into a particular server environment.	SHOULD		good
4	software licence source code	Indicates if and in which way the source code of the software is accessible.	MUST		openSource
5	ease of use	Assessment of how easy it is to use an action in operations	SHOULD		openSource
6	image width equal	true iff image width has been preserved.	MUST		true
7	image height equal	true iff image height has been preserved.	MUST		true
8	colour model preserved	Indicates whether the colour model has been preserved.	MUST		true
9	EXIF: all tiff data retained	Indicates whether the specific type of EXIF metadata has been retained.	MUST		true
10	number of tools	Indicator for the adoption of a format, expressed as the total number of all tools that support a format	MUST	GT	0
11	format documentation availability	Availability of the documentation for a format	SHOULD		yes-free
12	format standardization	Standardization of the outcome format.	SHOULD		international standard
13	compression type	Type of compression used in the outcome object	MUST		none
14	identification possibilities	Possibilities to identify the outcome format (cf. PRONOM)	MUST		automatic_specific
15	format complexity	Indicator of the complexity of a format as judged by experts in the domain	SHOULD		low

6.6 Screenshot of a content profile in Scout

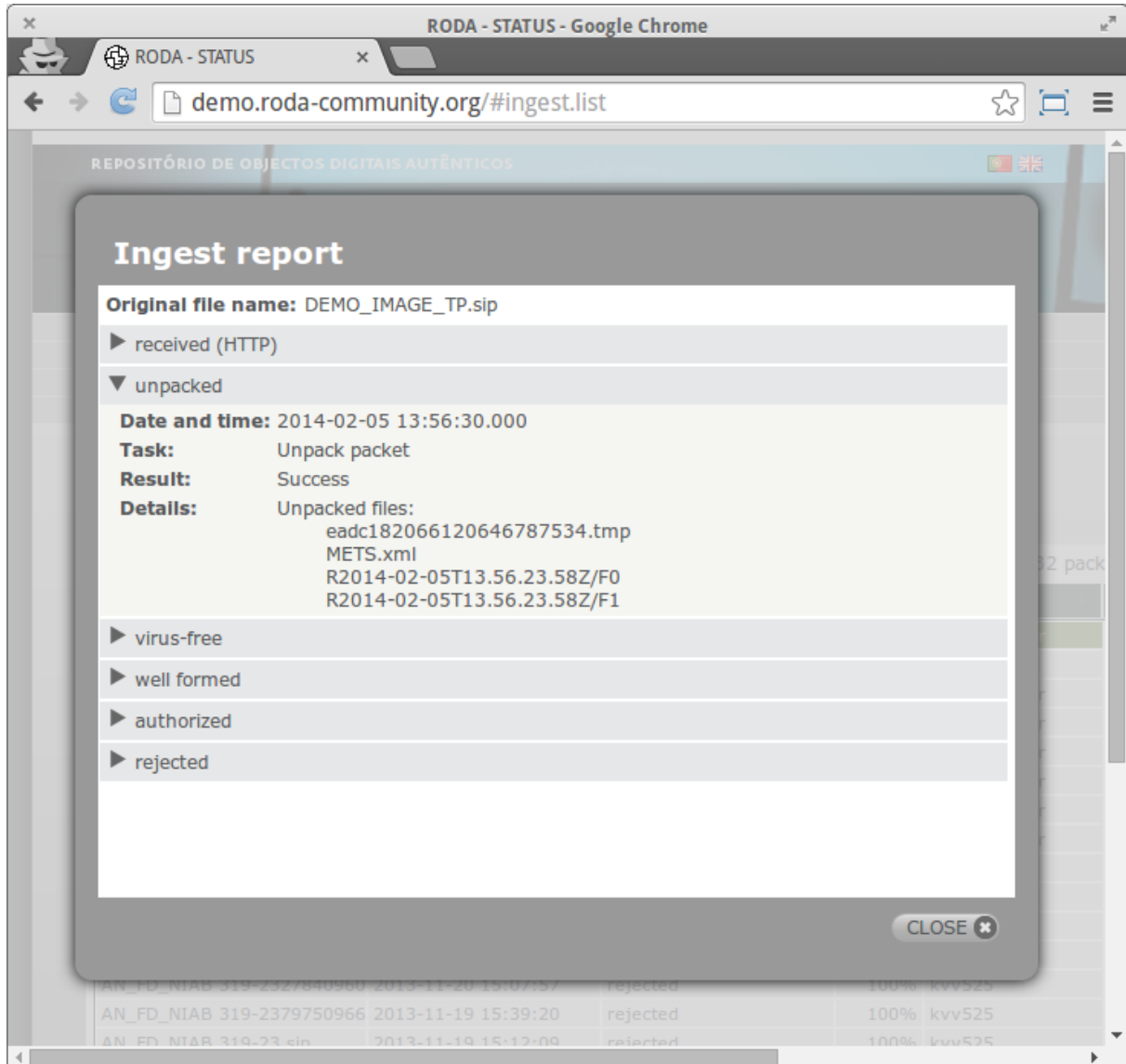
A screenshot of a web browser displaying the Scout interface. The browser's address bar shows "Scout - Browse - Entity - Google Chrome". The page has a blue navigation bar with "Scout", "Home", "Query", and "Browse" tabs, and a "Login" link on the right. Below the navigation bar is a breadcrumb trail: "Categories / content_profile / demo". The main heading is "Entity". Underneath, it says "Name demo". A section titled "Properties" contains a table with the following data:

Name	Value	Action
Collection size	1.66 GB	
compression_scheme distribution	5 key-value pairs	
Format distribution	15 key-value pairs	
Objects avg size	8.26 MB	
Objects min size	512 bytes	
Objects max size	27.27 MB	
Objects count	206	

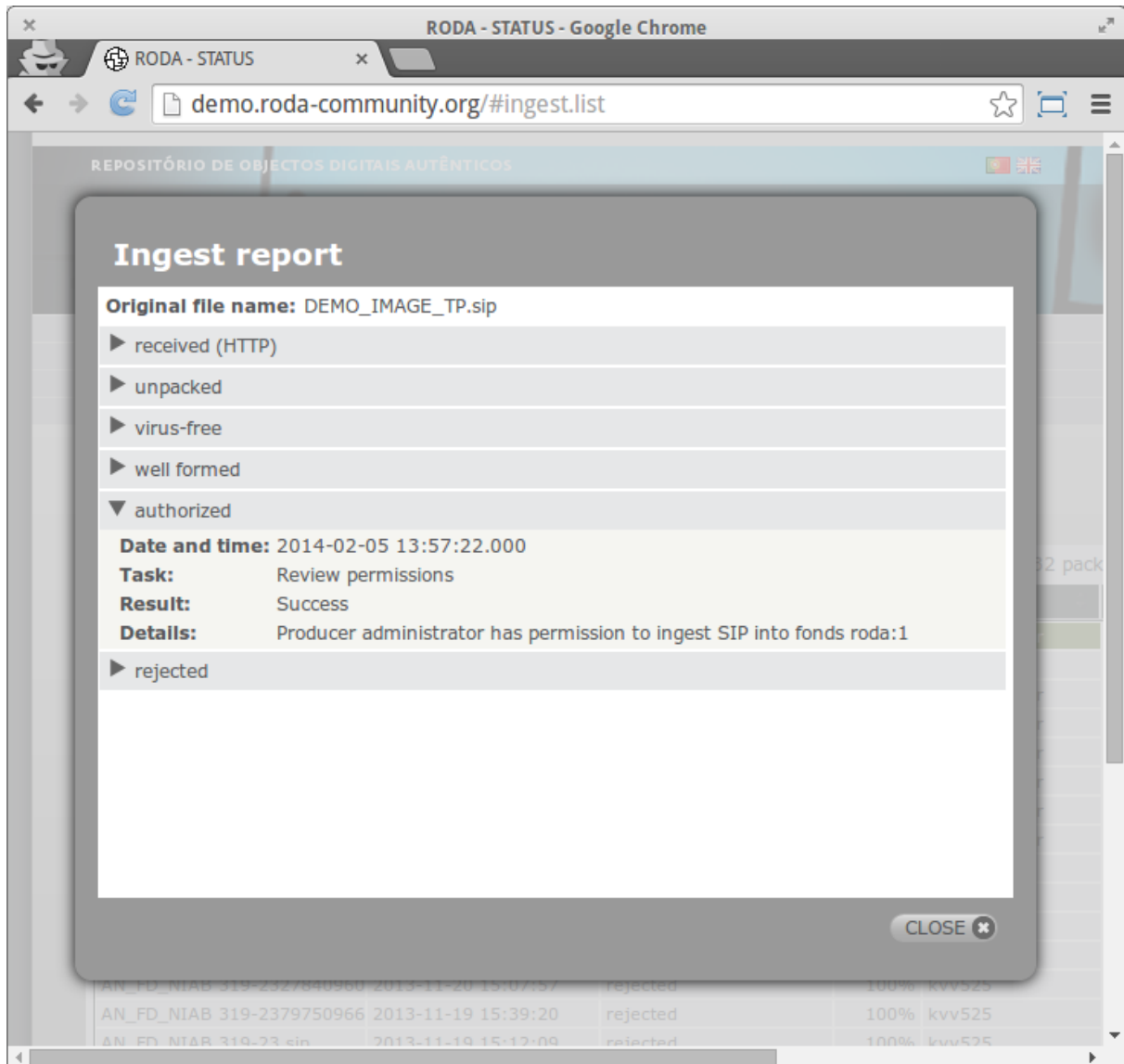
6.7 Screenshot of an ingest status in RODA



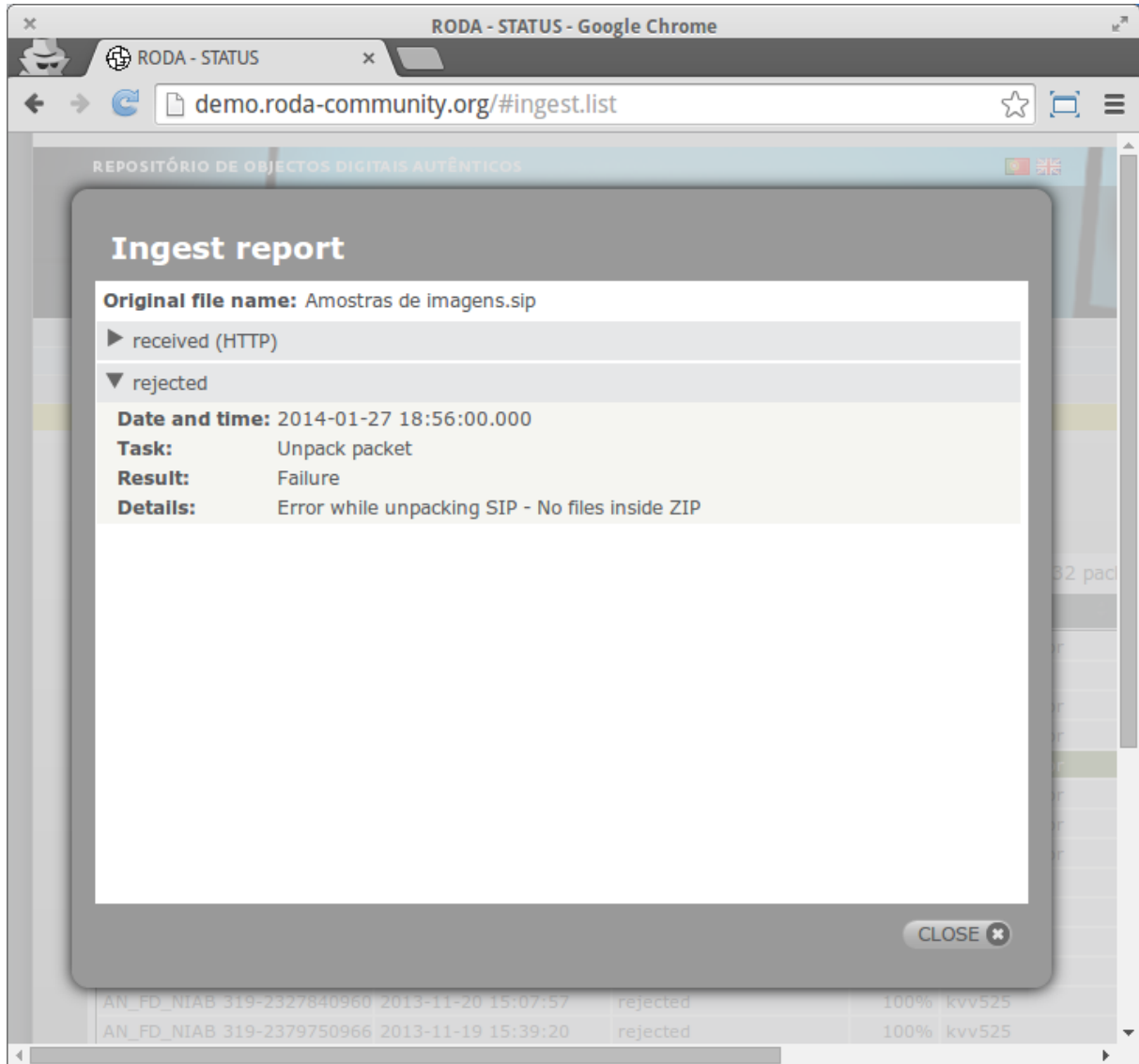
6.8 Screenshot of the well-formed ingest status in RODA



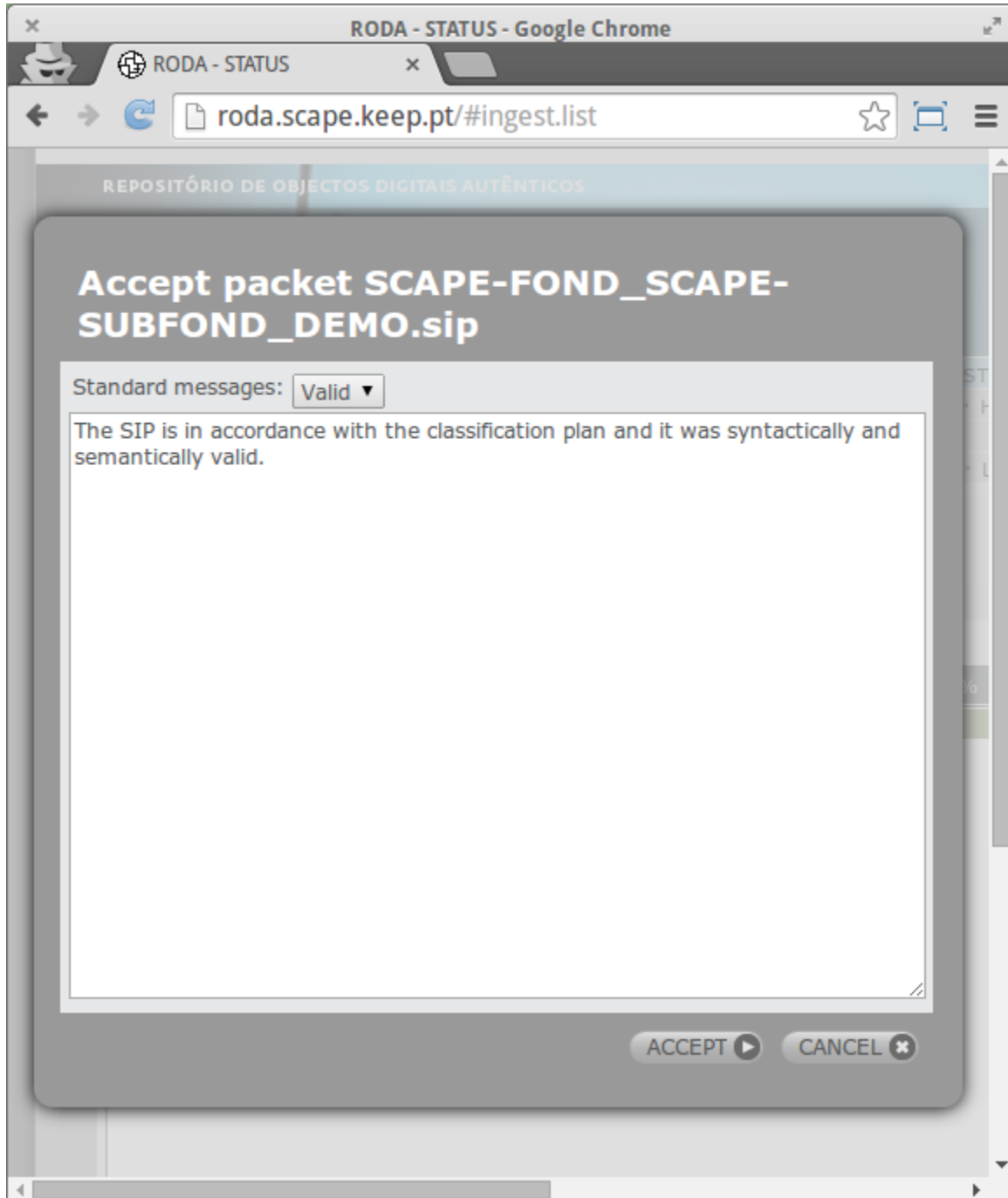
6.9 Screenshot of authorized ingest status in RODA



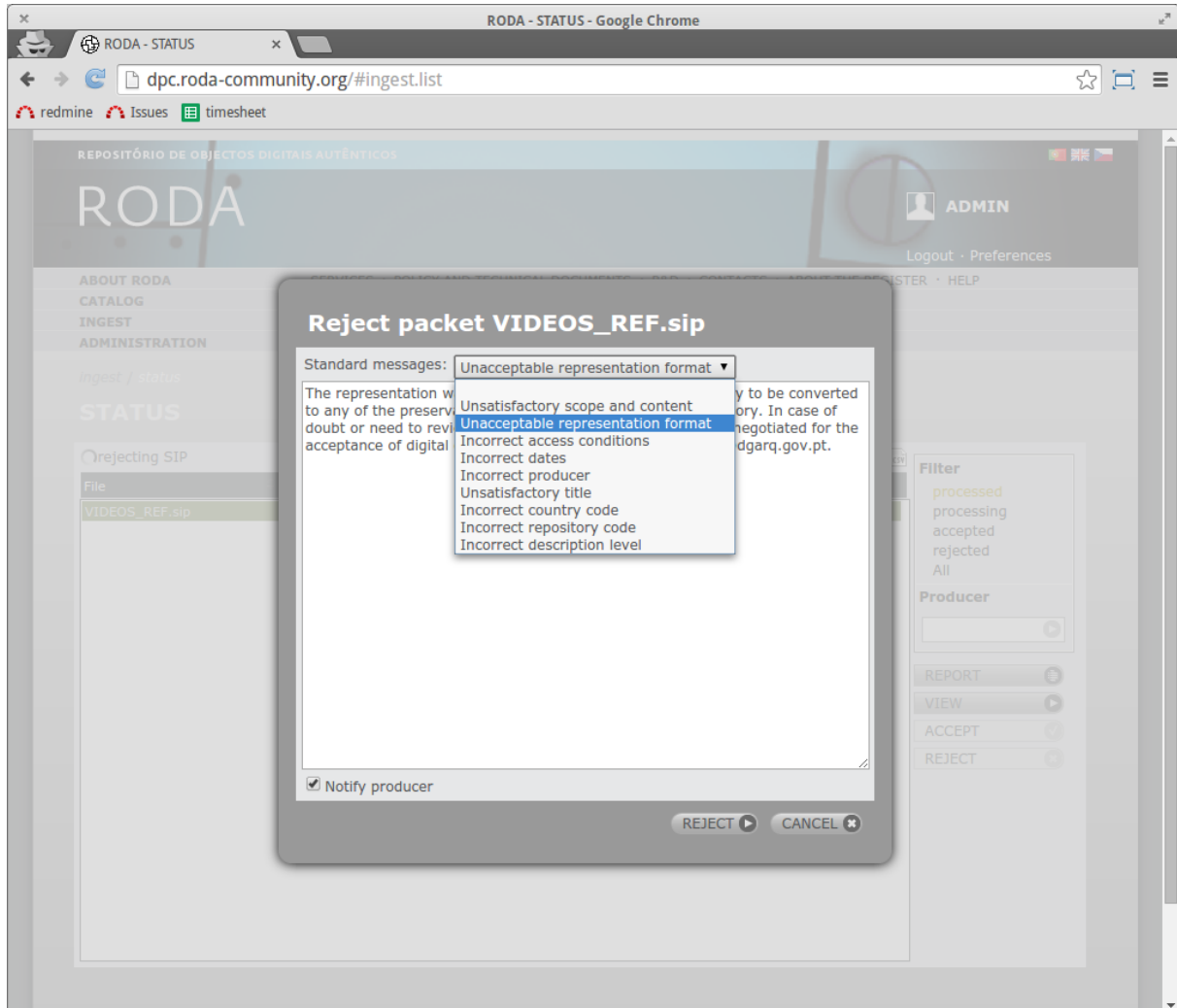
6.10 Screenshot of rejected ingest status in RODA



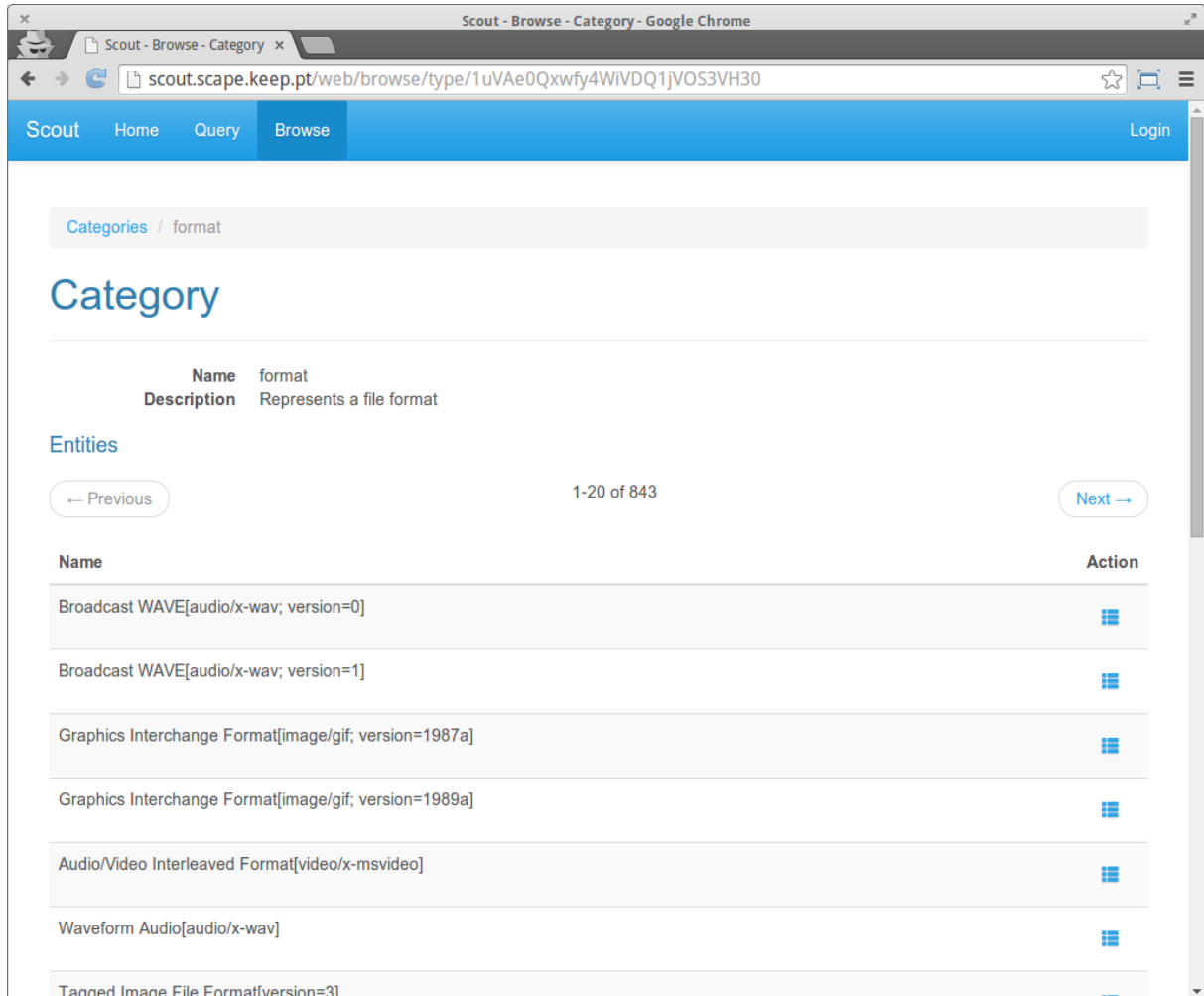
6.11 Screenshot of SIP manual accept form on RODA ingest



6.12 Screenshot of SIP manual reject on RODA ingest



6.13 Screenshot of PRONOM format information in Scout










The screenshot shows a web browser window with the URL `scout.scape.keep.pt/web/browse/type/1uVAe0Qxwfy4WIVDQ1jVOS3VH30`. The page title is "Scout - Browse - Category". The navigation menu includes "Scout", "Home", "Query", "Browse", and "Login".

The breadcrumb trail is "Categories / format". The main heading is "Category".

The category details are:

- Name:** format
- Description:** Represents a file format

The "Entities" section shows a list of 843 items, with "1-20 of 843" displayed. The list includes:

Name	Action
Broadcast WAVE[audio/x-wav; version=0]	
Broadcast WAVE[audio/x-wav; version=1]	
Graphics Interchange Format[image/gif; version=1987a]	
Graphics Interchange Format[image/gif; version=1989a]	
Audio/Video Interleaved Format[video/x-msvideo]	
Waveform Audio[audio/x-wav]	
Tagged Image File Format[version=3]	

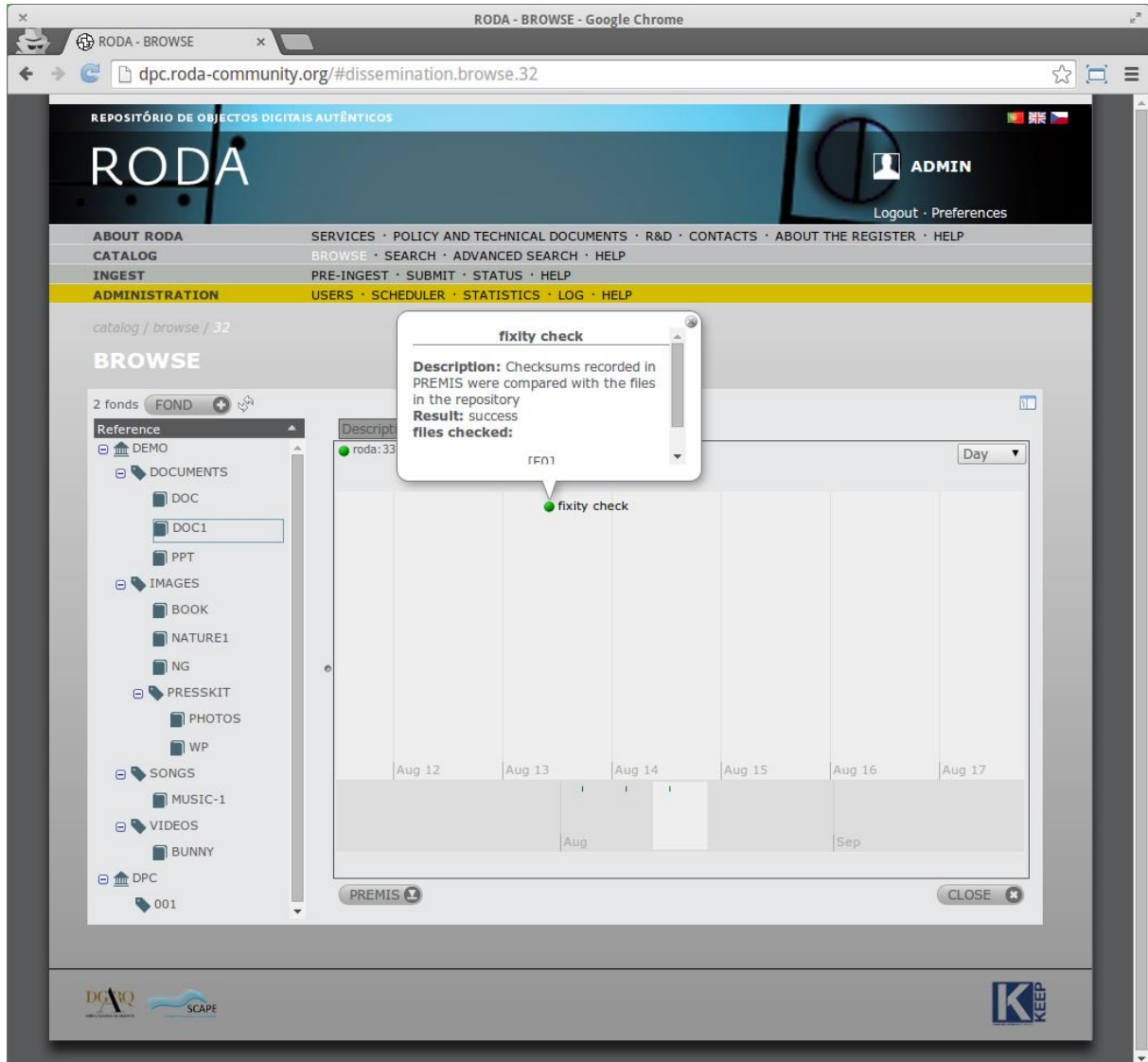
6.14 Screenshot of PRONOM and MIME IDs inside of PREMIS from RODA

```

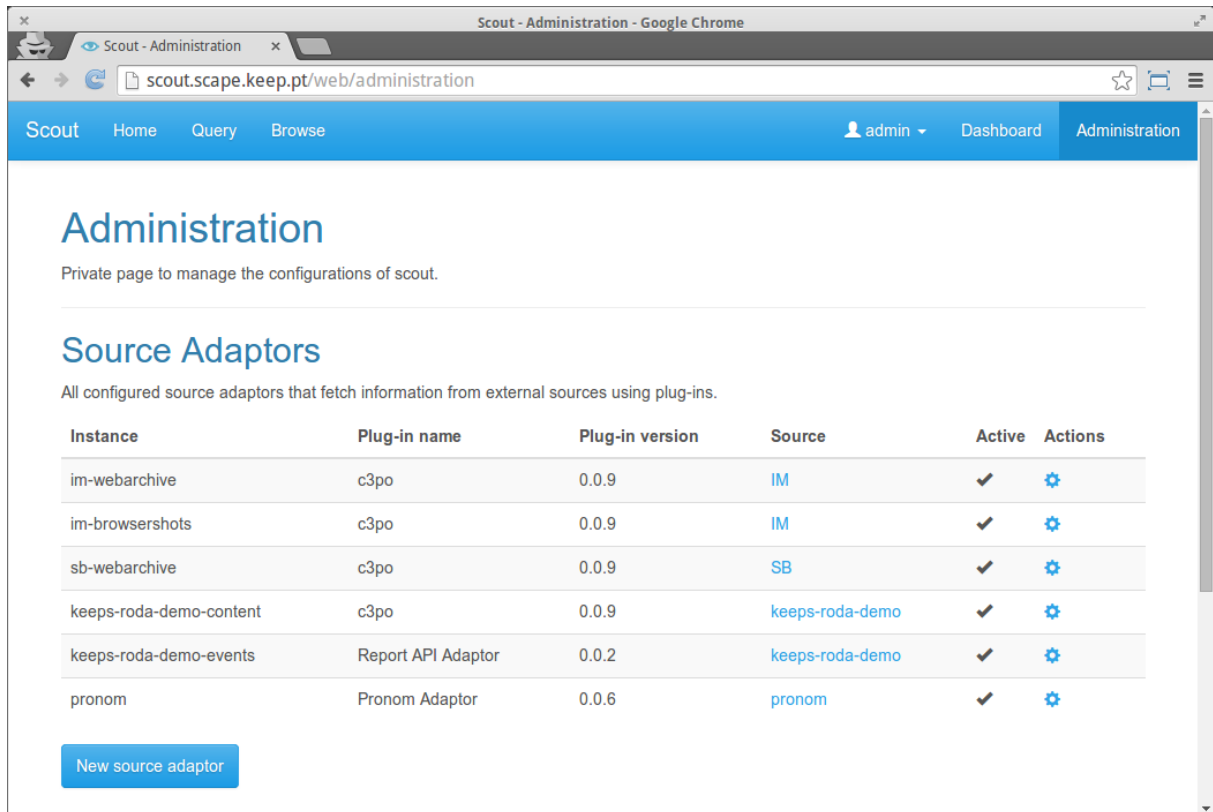
x F0.premis.xml (-/.cache/fr-TwhtcQ/representation_roda_34) - Scratch
+ x F0.premis.xml
31 <identification>
32 <identity format="Acrobat PDF 1.3 - Portable Document Format" mimetype="application/pdf" toolname="FI
TS" toolversion="0.8">
33 <tool toolname="fido" toolversion="v1.3.1"/>
34 <tool toolname="Droid" toolversion="6.1.3"/>
35 <tool toolname="Jhove" toolversion="1.5"/>
36 <tool toolname="NLNZ Metadata Extractor" toolversion="3.4GA"/>
37 <tool toolname="Tika" toolversion="1.3"/>
38 <tool toolname="file utility" toolversion="5.09"/>
39 <tool toolname="Exiftool" toolversion="9.13"/>
40 <tool toolname="ffident" toolversion="0.2"/>
41 <version toolname="Droid" toolversion="6.1.3" status="CONFLICT">1.3</version>
42 <version toolname="Jhove" toolversion="1.5" status="CONFLICT">1.4</version>
43 <externalIdentifier toolname="fido" toolversion="v1.3.1" type="puid">fmt/17</externalIdentifier>
44 </identity>
45 </identification>
46 <fileinfo>
47 <size toolname="Jhove" toolversion="1.5">4104124</size>
48 <creatingApplicationName toolname="NLNZ Metadata Extractor" toolversion="3.4GA">Mac OS X 10.7.5 Quart
z PDFContext/Word</creatingApplicationName>
49 <lastmodified toolname="Tika" toolversion="1.3" status="CONFLICT">2013-10-04T11:08:06Z</lastmodified>
50 <lastmodified toolname="Exiftool" toolversion="9.13" status="CONFLICT">2014:06:03 12:12:16+01:00</las
tmodified>
51 <created toolname="Exiftool" toolversion="9.13" status="SINGLE_RESULT">2013:10:04 11:08:06Z</created>
52 <filepath toolname="OIS File Information" toolversion="0.2" status="SINGLE_RESULT">/opt/roda/tomcat/a
pache-tomcat-6.0.39/temp/rFile6701923615129312496temp</filepath>
53 <filename toolname="OIS File Information" toolversion="0.2" status="SINGLE_RESULT">rFile6701923615129
312496temp</filename>

```

6.15 Screenshot of fixity event inside preservation tab in RODA



6.16 Screenshot of Scout source adaptors



The screenshot shows the Scout Administration interface in a Google Chrome browser. The page title is "Administration" and the subtitle is "Private page to manage the configurations of scout." Below this, there is a section for "Source Adaptors" with the description "All configured source adaptors that fetch information from external sources using plug-ins." A table lists the configured adaptors, and a "New source adaptor" button is visible at the bottom left.

Instance	Plug-in name	Plug-in version	Source	Active	Actions
im-webarchive	c3po	0.0.9	IM	✓	⚙️
im-browsershots	c3po	0.0.9	IM	✓	⚙️
sb-webarchive	c3po	0.0.9	SB	✓	⚙️
keeps-roda-demo-content	c3po	0.0.9	keeps-roda-demo	✓	⚙️
keeps-roda-demo-events	Report API Adaptor	0.0.2	keeps-roda-demo	✓	⚙️
pronom	Pronom Adaptor	0.0.6	pronom	✓	⚙️

New source adaptor

6.17 Scout notification

Scout notification - scape.pw@gmail.com - Gmail - Google Chrome
https://mail.google.com/mail/u/0/?ui=2&view=bt&ver=1&search=inbox&th=140e4c0d4be3f...

Inbox x

Scout <noreply@scout.scape.keep.pt>
to me

03/09/2013 ☆

One of your requests has been triggered.

SCOUT

Preservation Watch System

What is SCOUT?
SCOUT is a preservation watch system that monitors the whole world to warn you of preservation risks or opportunities.

Why did I received this email?
A trigger was created to warn you when something important happened. Your email was defined as a notification that this important event has occurred.

There is a notification for you!

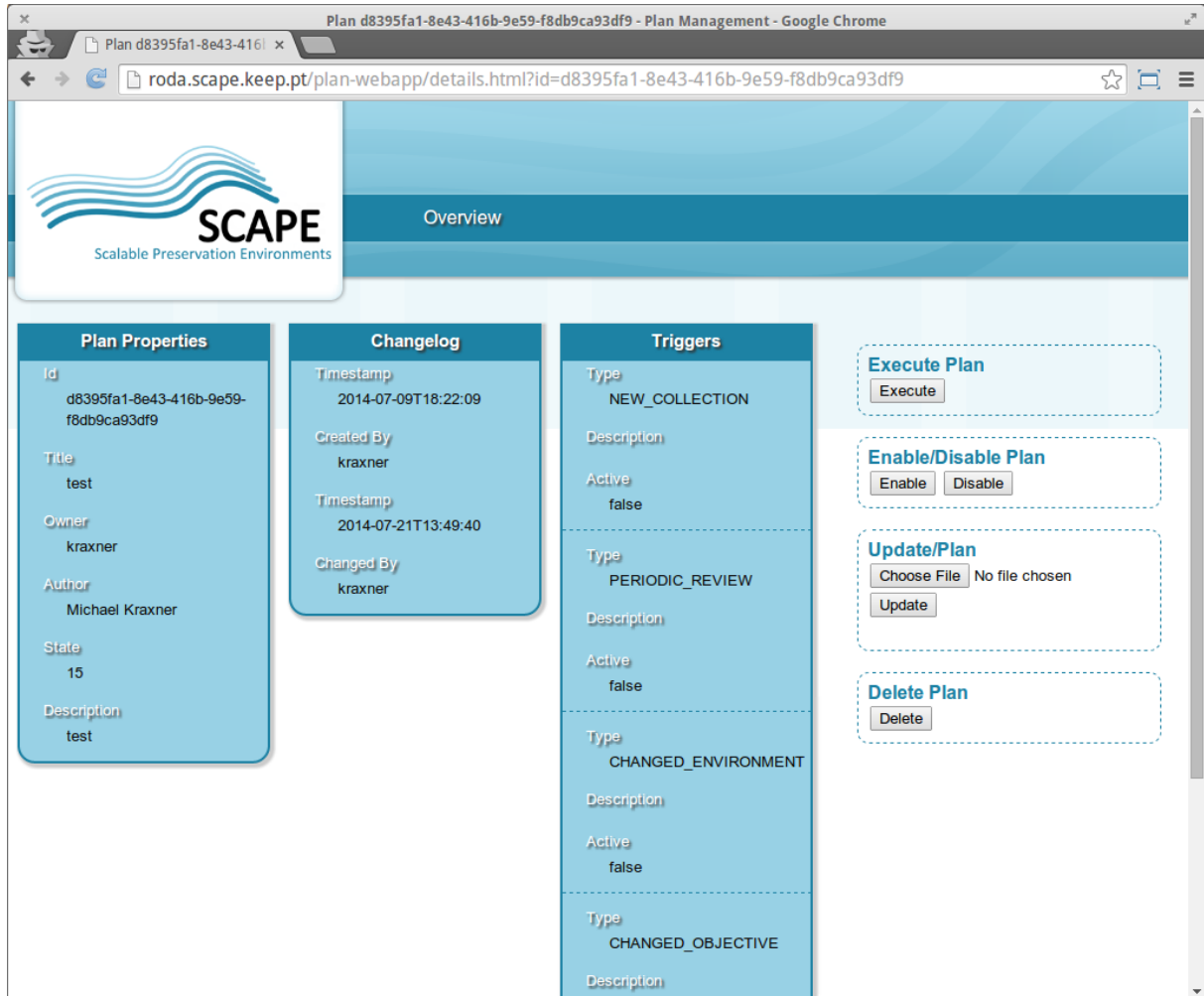
Request: Check collection policy conformance

Question
Question assessed on this trigger.
SPARQL: ?s watch:entity ?collection ; watch:property ?compressionSchemeDist ; watch:stringDictionaryValue ?value . ?compressionSchemeDist watch:id "ci-KDNE_rjmuRKxjIhnqeHpYgnw"^^xsd:string . ?value ?l ?dictionaryItem . {?dictionaryItem watch:key ?compressionType1 . ?policy1 a cp:FormatObjective ; cp:measure measure:117 ; cp:value "none"^^xsd:string . FILTER regex(?compressionType1, "^(Unknown|Uncompressed)") } UNION {?dictionaryItem watch:key ?compressionType2 . ?policy2 a cp:FormatObjective ; cp:measure measure:117 ; cp:value "lossless"^^xsd:string . FILTER regex(?compressionType2, "^(Conflicted|JPEG)") }
Target: PROPERTY_VALUE

This software is copyrighted by the SCAPE Project Consortium. The SCAPE project is co-funded by the European Union under FP7 ICT-2009.4.1 (Grant Agreement number 270137).

This is an open-source project available at [GitHub](#)

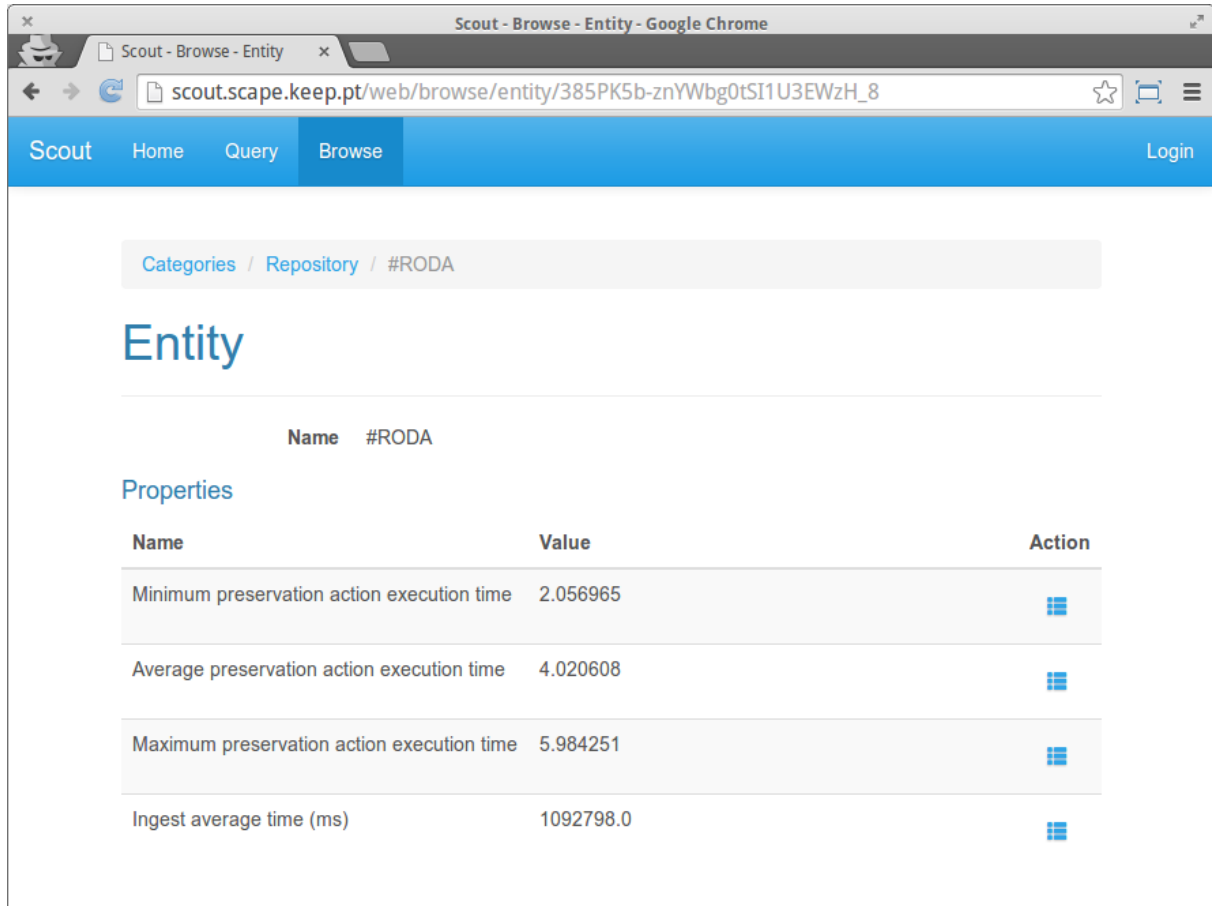
6.18 Plan details and available action on Plan Management GUI



The screenshot displays the SCAPE Plan Management GUI in a Google Chrome browser window. The page title is "Plan d8395fa1-8e43-416b-9e59-f8db9ca93df9 - Plan Management - Google Chrome". The URL is "roda.scape.keep.pt/plan-webapp/details.html?id=d8395fa1-8e43-416b-9e59-f8db9ca93df9". The page features the SCAPE logo and the text "Scalable Preservation Environments". The main content area is titled "Overview" and is divided into several sections:

- Plan Properties:**
 - Id:** d8395fa1-8e43-416b-9e59-f8db9ca93df9
 - Title:** test
 - Owner:** kraxner
 - Author:** Michael Kraxner
 - State:** 15
 - Description:** test
- Changelog:**
 - Timestamp:** 2014-07-09T18:22:09
 - Created By:** kraxner
 - Timestamp:** 2014-07-21T13:49:40
 - Changed By:** kraxner
- Triggers:**
 - Type:** NEW_COLLECTION
 - Description:**
 - Active:** false
 - Type:** PERIODIC_REVIEW
 - Description:**
 - Active:** false
 - Type:** CHANGED_ENVIRONMENT
 - Description:**
 - Active:** false
 - Type:** CHANGED_OBJECTIVE
 - Description:**
- Actions:**
 - Execute Plan:** Execute
 - Enable/Disable Plan:** Enable, Disable
 - Update/Plan:** Choose File (No file chosen), Update
 - Delete Plan:** Delete

6.19 Repository events in Scout



Scout - Browse - Entity - Google Chrome

scout.scape.keep.pt/web/browse/entity/385PK5b-znYWbg0tSI1U3EWzH_8





Scout Home Query Browse Login

Categories / Repository / #RODA

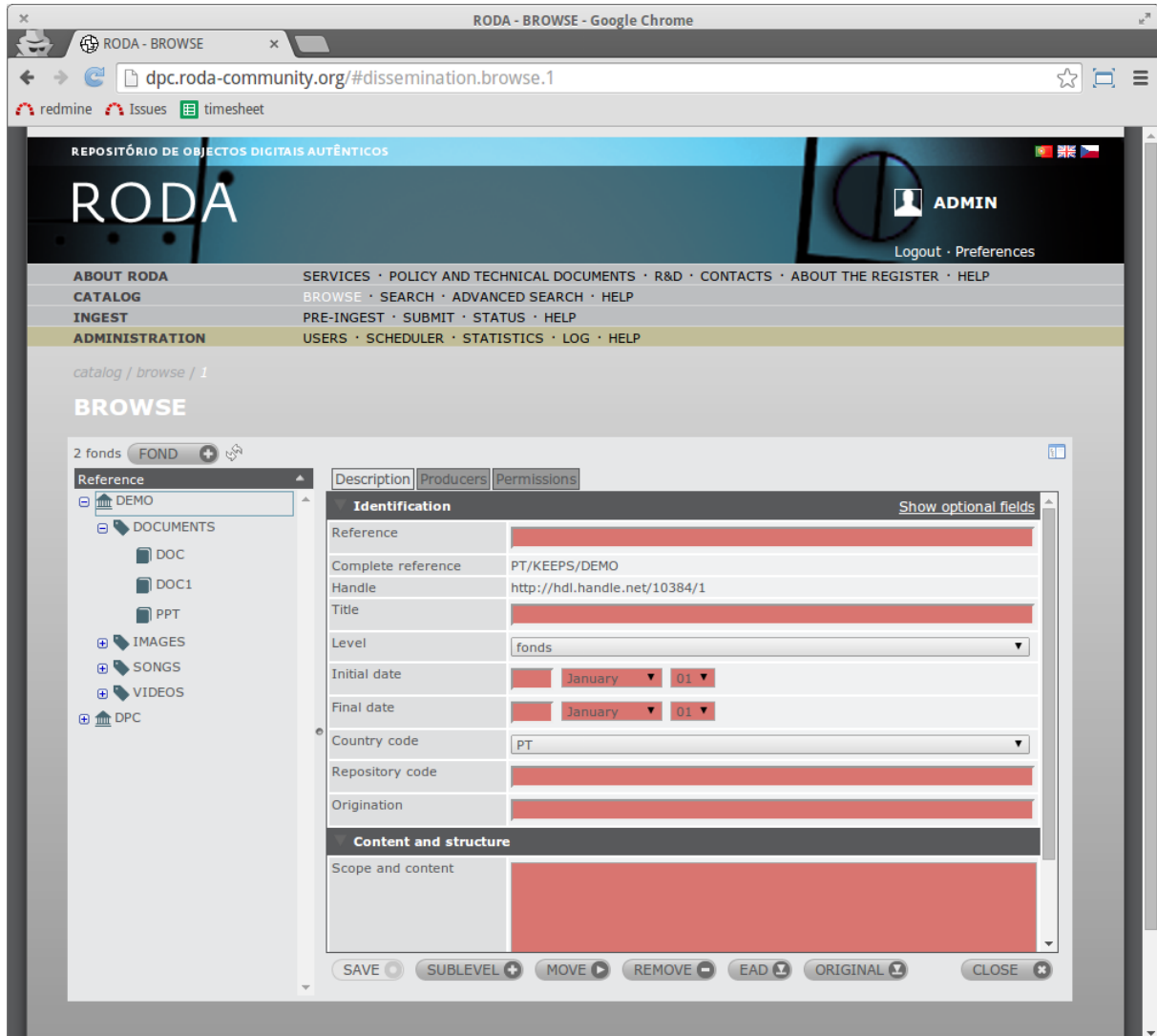
Entity

Name #RODA

Properties

Name	Value	Action
Minimum preservation action execution time	2.056965	
Average preservation action execution time	4.020608	
Maximum preservation action execution time	5.984251	
Ingest average time (ms)	1092798.0	

6.20 Screenshot of descriptive metadata edit in RODA



The screenshot shows a web browser window titled "RODA - BROWSE - Google Chrome" with the URL `dpc.roda-community.org/#dissemination.browse.1`. The page header includes the RODA logo and navigation links for ADMIN, Logout, and Preferences. A main navigation bar lists categories like ABOUT RODA, SERVICES, POLICY AND TECHNICAL DOCUMENTS, R&D, CONTACTS, ABOUT THE REGISTER, and HELP. Below this, there are sections for CATALOG, BROWSE, SEARCH, ADVANCED SEARCH, HELP, INGEST, PRE-INGEST, SUBMIT, STATUS, HELP, and ADMINISTRATION, USERS, SCHEDULER, STATISTICS, LOG, HELP.

The main content area is titled "BROWSE" and shows "2 fonds" under the "FOND" category. A left sidebar lists various document types: DOCUMENTS (DOC, DOC1, PPT), IMAGES, SONGS, VIDEOS, and DPC. The main editing area is divided into tabs: "Description", "Producers", and "Permissions". The "Description" tab is active, showing a form for editing metadata. The form is organized into sections: "Identification" and "Content and structure".

Identification Section:

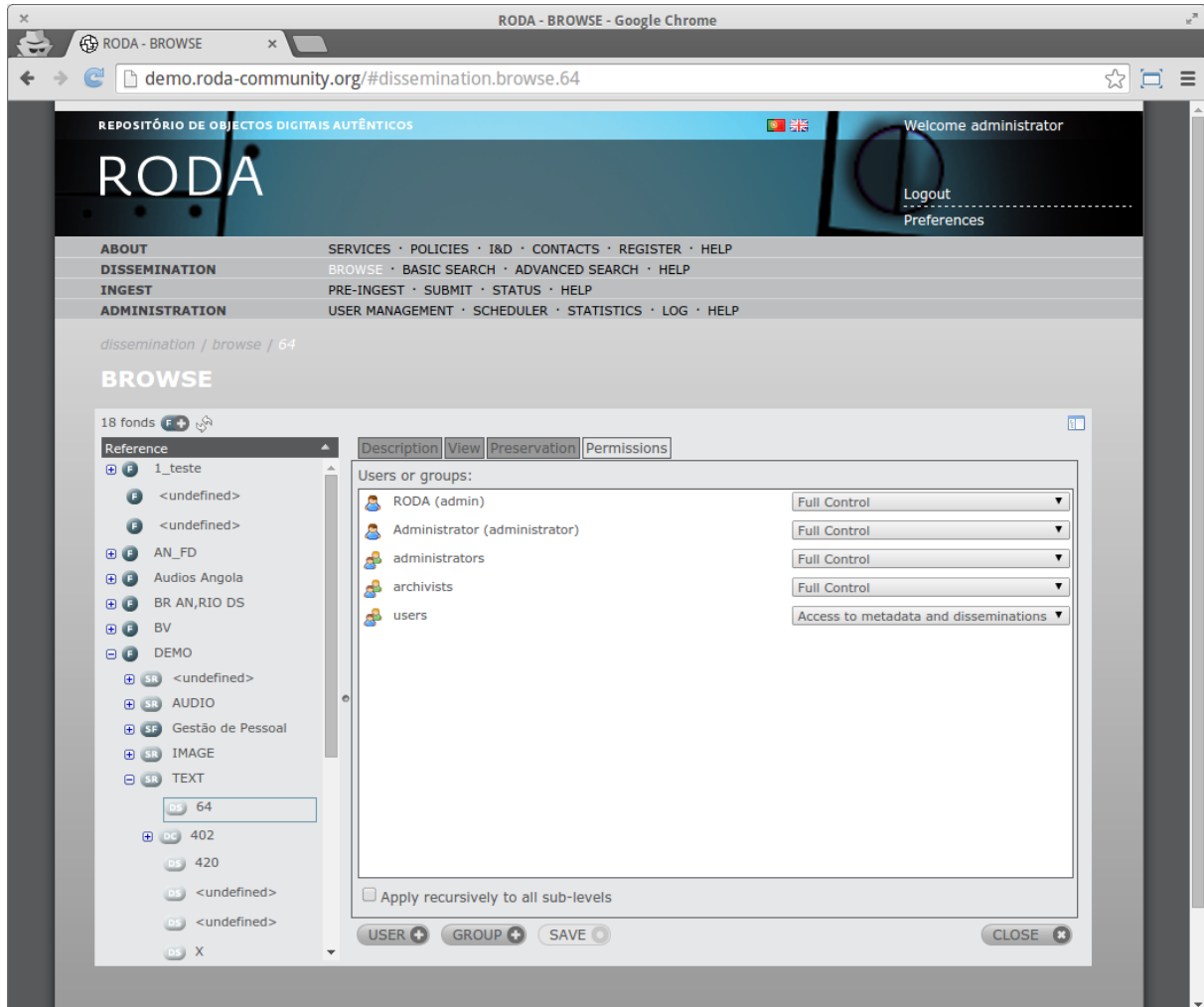
- Reference: [Redacted]
- Complete reference: PT/KEEPS/DEMO
- Handle: `http://hdl.handle.net/10384/1`
- Title: [Redacted]
- Level: fonds
- Initial date: January D1
- Final date: January D1
- Country code: PT
- Repository code: [Redacted]
- Origination: [Redacted]

Content and structure Section:

- Scope and content: [Redacted]

At the bottom of the form, there are several action buttons: SAVE, SUBLEVEL (+), MOVE (right arrow), REMOVE (-), EAD (down arrow), ORIGINAL (down arrow), and CLOSE (star icon).

6.21 Screenshot of object permissions edit in RODA



The screenshot shows the RODA web interface in Google Chrome. The browser address bar shows the URL: `demo.roda-community.org/#dissemination.browse.64`. The page header includes the RODA logo and navigation links for ABOUT, DISSEMINATION, INGEST, and ADMINISTRATION. A "Welcome administrator" message is visible in the top right corner.

The main content area is titled "BROWSE" and displays a list of 18 digital object sets (funds). The selected fund is "64". A modal window titled "Permissions" is open, showing the "Permissions" tab. The modal displays a table of users or groups and their assigned permissions:

Users or groups:	Permissions
RODA (admin)	Full Control
Administrator (administrator)	Full Control
administrators	Full Control
archivists	Full Control
users	Access to metadata and disseminations

At the bottom of the modal, there is a checkbox for "Apply recursively to all sub-levels" and buttons for "USER +", "GROUP +", "SAVE", and "CLOSE".

6.22 Screenshot of action alternatives in Plato



Plan Define Requirements Evaluate Alternatives Analyse Results Build Preservation Plan [scape.pw](#)


Define the alternatives to consider for the plan

[Add alternative](#)
[Descriptive Information](#)

Different preservation strategies, using for example migrations tools or emulators, are selected. A detailed description of each preservation alternative is provided. [more](#)


<p>ImageMagick to tiff</p> <p>SCAPE Migration Component using service at: http://www.myexperiment.org/workflows/4062/download/converts_any_imagemagick_supported_image_format_to_tiff_131242.t2flow?version=1</p>	-
<p>imagemagick convert - to tiff</p> <p>Converts tiff to tiff using imagemagick convert with the provided compression using service at: http://www.myexperiment.org/workflows/4064/download/imagemagick_convert_-_tiff2tiff_-_compression_168727.t2flow?version=1</p>	-

[\[+\] Add alternatives](#)




Custom

Add custom alternative




Show Services



MiniMEE

Show Services



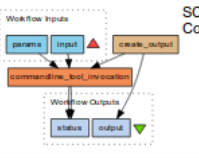
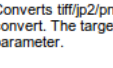
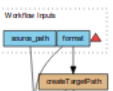
MiniREEF

Show Services

Sample 00000056.jp2.jpg has the following format: **JPEG File Interchange Format, version 1.01.**

image/jpeg ~ Dependency Installation Filter

« « « 1 2 » » »

<p>+</p>  <p>Workflow Inputs: <code>parameters</code>, <code>input</code>, <code>create_output</code></p> <p>Workflow Outputs: <code>status</code>, <code>output</code></p> <p>Commandline: <code>convert</code></p>	<p>Converts any ImageMagick supported image format to TIFF (v1)</p> <p>SCAPE Migration Component</p> <pre>image/jp2 ~> image/tiff image/png ~> image/tiff image/jpeg ~> image/tiff image/vnd.microsoft.icon ~> image/tiff image/gif ~> image/tiff image/bmp ~> image/tiff</pre> <p>http://purl.org/DP/components#TargetObject http://purl.org/DP/components#Status</p> <p>#Ubuntu imagemagick [8] #Debian imagemagick [8]</p> <p>Open on myExperiment #MigrationAction component, scape, test, migration Kraxner by-sa ☆☆☆☆</p>
<p>+</p>  <p>Workflow Inputs: <code>source_path</code>, <code>format</code></p> <p>Workflow Outputs: <code>createTargetPath</code></p>	<p>Converts tiff/jp2/png/jpeg images using graphicsmagick convert. The target format can be selected with the format parameter.</p> <pre>image/tiff ~> image/jp2 image/jpeg ~> image/jp2 image/png ~> image/jpeg image/jpeg ~> image/png image/jp2 ~> image/png image/jp2 ~> image/jp2 image/jpeg ~> image/jpeg image/tiff ~> image/png image/png ~> image/png image/tiff ~> image/tiff image/jpeg ~> image/tiff image/png ~> image/tiff image/png ~> image/jp2 image/jp2 ~> image/jpeg image/jp2 ~> image/tiff image/tiff ~> image/jpeg</pre> <p>http://purl.org/DP/components#Status http://purl.org/DP/components#TargetObject</p> <p>#Debian graphicsmagick 1.3.16 [8]</p> <p>Open on myExperiment #MigrationAction component Markus Plangg by-nd ☆☆☆☆</p>
<p>+</p>  <p>Workflow Inputs: <code>source_path</code>, <code>format</code></p> <p>Workflow Outputs: <code>createTargetPath</code></p>	<p>Converts tiff/jp2/png/jpeg images using imagemagick convert. The target format can be selected with the format parameter.</p> <pre>image/jp2 ~> image/jp2 image/tiff ~> image/tiff image/tiff ~> image/jp2 image/png ~> image/tiff image/jp2 ~> image/jpeg</pre> <p>http://purl.org/DP/components#Status http://purl.org/DP/components#TargetObject</p> <p>#Debian imagemagick 5 [8]</p>