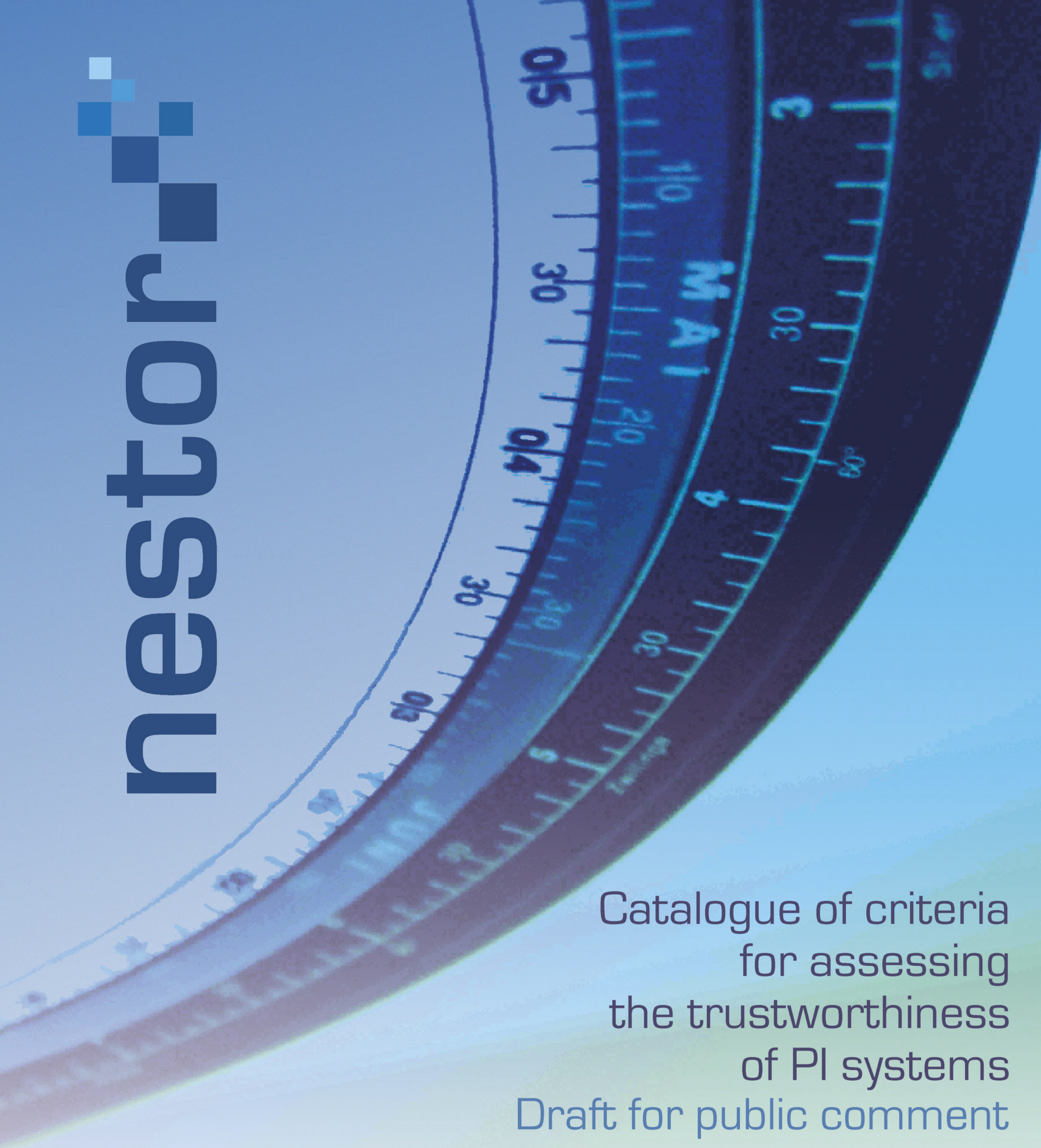

Catalogue of criteria for assessing the trustworthiness of PI systems

Draft for public comment

nestor working group long-term preservation standards

nestor-studies 13

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

nestor

Catalogue of criteria for assessing the trustworthiness of PI systems

Draft for public comment

nestor working group long-term preservation standards

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

nestor-studies 13

published by

nestor - Network of Expertise in Long-Term Storage of Digital Resources

nestor - Kompetenznetzwerk Langzeitarchivierung und
Langzeitverfügbarkeit Digitaler Ressourcen für Deutschland

http://longtermpreservation.de
http://www.langzeitarchivierung.de

Project partners

Bayerische Staatsbibliothek, München
Bundesarchiv
Deutsche Nationalbibliothek (Projektleitung)
FernUniversität in Hagen
Humboldt-Universität zu Berlin - Computer- und Medienservice / Universitätsbibliothek
Institut für Museumsforschung, Berlin
Niedersächsische Staats- und Universitätsbibliothek, Göttingen

nestor working group long-term preservation standards

c/o Niedersächsische Staats und Universitätsbibliothek Göttingen
Jens Ludwig
Papendiek 14
D-37073 Göttingen
Tel.: +49 (0)551-3912121
E-mail:<ludwig@sub.uni-goettingen.de>

URN: urn:nbn:de:0008-20080710227

http://nbn-resolving.de/urn:nbn:de:0008-20080710227

Author

Niklaus Bütikofer, InfoMemory GmbH

Other contributors

Karsten Huth, Bundesarchiv
Katja Hüther, Deutsche Nationalbibliothek
Dr. Christian Keitel, Landesarchiv Baden-Württemberg
Dr. Nikola Korb, Deutsche Nationalbibliothek
Jens Ludwig, Niedersächsische Staats- und Universitätsbibliothek Göttingen
Christa Schöning-Walter, Deutsche Nationalbibliothek
Sabine Schrimpf, Deutsche Nationalbibliothek
Tobias Steinke, Deutsche Nationalbibliothek

Funded by the project Innovation with Norms and Standards (INS) 2008

Catalogue of criteria for
assessing the trustworthiness of PI systems

Release 1.2

Contents:

Introduction

1.1 Purpose

By formulating requirements and criteria relevant for long-term preservation, the present catalogue of criteria for assessing the trustworthiness of persistent identifier systems (PI systems) is intended to help providers and users of persistent identifiers (PIs) keep digital objects identifiable, referenceable and accessible over longer periods and despite unforeseeable changes.

1.2 Context

PI systems exist within a highly dynamic context. There are three main development trends.

(1) A range of different PI systems are available today, all offering the same basic functions. Their main differences lie in the structuring and encoding of the identifiers, in the technology used, in the business model and in the extra services which they increasingly offer as a means of making themselves more attractive to information providers and users.

(2) Potentially, everything which is distinct and nameable can be given a PI (everything from digital documents through to individual metadata elements and procedure calls). This can lead to very large quantities of resolver requests. This is why the scalability of a PI system and the possibility to exclude certain object types which require large resolver capacities is so important.

(3) PI systems themselves are also subject to changes and may incorporate a large number of agents. PI systems, especially the operators of resolver services, are therefore forced to assess the trustworthiness of PIs and data sources and to make this transparent to users.

1.3 Area of application

The present document only addresses the basic PI system functions, and then only the situation in which PIs are published outside a certain institution. The implication is that the objects identified in the PIs can also be accessed by authorised third parties outside a specified institution or after expiry of a specified period.

In preparing the present document, archives and libraries were the main application areas, and long-term preservation and long-term referencing the main application areas. It is therefore likely that other weightings will have to be made for other application areas, and that additional factors will apply.

2 Basic terms

The following key terms are defined and described below for the purposes of terminological clarity and precision. This also represents the conceptual foundation of the catalogue of criteria.[1]

Identifier: A name which is uniquely linked to an object (thing). A name can therefore be said to identify an object if the name is only linked to one object. A name is represented by a string of characters, an object by one or more copies.

Identity: Two or more objects are identical if they share the same significant properties. What constitutes significant properties depends on the purpose, or the context, for/in which identical and non-identical objects are distinguished.[2] For the purposes of content information work, the MS Word and the PDF version of a document are identical, for

[1] The terms and definitions used here are closely related to the ontology devised in the Australian PILIN project: http://resolver.net.au/hdl/102.100.272/RPLZ54PQH

[2] Cf. Norman Paskin, On Making and Identifying a "Copy", D-Lib Magazine 2003, Volume 9 Number 1, DOI: 10.1045/january2003-paskin

example. For the purpose of displaying them on a screen, by contrast, they are not identical, as different software is generally required and different computing processes run.

Name: A name is represented by a string of characters. It belongs to an identifiable name system (context). Within the context of this document a name always consists of the string of the name system together with the string of the name itself. The form of the string must correspond to the rules set by the name system (encoding scheme). Certain resolving procedures may require names which are structured according to a specified encoding scheme.

Object (Thing): An object can be anything which can be talked about, in particular everything which can be distinguished and given an identifier. For example, static or dynamic objects can be identified, as can documents, procedures and aggregated objects or part objects.

The present catalogue of criteria is oriented towards long-term preservation; it is restricted to information objects which are basically in their final form and static. However, long-term preservation today is based on the OAIS reference model which uses the concept of the Archival Information Package (AIP) as the logical unit. As complete packages, AIPs are always dynamic over longer periods, because e.g. they create their own 'preservation history' which is continually supplemented, and because they have to be transferred to new forms periodically in order to be preserved. In their efforts to reconcile preservation of the core work with any necessary changes, all operators of a data source need to establish rules by which they operate.

Persistence: In this catalogue of criteria, persistence means that an identifier remains uniquely and permanently linked to an object. Accordingly, a persistent identifier is only issued once and remains in the relevant resolver system with no time limit. This revolver system serves the corresponding name system and name space and registers if the object in question no longer exists.

Persistent identifier system: A PI system is a mutually referenced combination of

- Definitions
- Policies
- Services and
- Data sources

which are used for the administration and use of persistent identifiers.

Resolver: A resolver is a system which registers and resolves identifiers. When a request is submitted, it returns information on the identifier's links together with the details of the current storage locations of the object (association data, current URL). The resolver is operated as a service. Resolving can be carried out by a number of coordinated operators or by coordinated sub-resolvers in a number of stages.

Data source: A data source is a system for the storage, management and provision of data. The data source is operated as a service. For the purposes of this document, a data source is typically an OAIS[3].

Association data: Association data represents the link between the identifier and the object in a form which can be registered in the resolver and can trigger defined actions when a request is submitted. The association data contains information which is needed to access the identified objects. With regard to the trustworthiness of the PI systems it is irrelevant whether the association data only consists of a URL, complex instructions for the data source's system or of procedural instructions for future data transfer systems, as long as they can effect the link with the object. The resolver system leaves it to the data source how it finds the object allocated to the identifier within its system and makes it accessible.

[3] In accordance with ISO 14721 (2003) Space data and information transfer systems — Open archival information system — Reference model

A single identifier can identify a number of objects and therefore be allocated to a number of different levels of association data. The association data contained in the resolver can trigger different processes:

- For instance, using an http redirect it can send a request for the object to the data source. The data source, for its part, can return the object itself or simply metadata about the object. The data source can also initiate a dialogue with users in which their authorisation is clarified or in which a payment transaction is processed before the object itself is delivered.
- If a number of different objects are registered under a particular identifier, it can initially trigger a selection dialog with the user and, only once a selection has successfully been made, is a request sent to the relevant data source.

Metadata: A resolver must manage a range of metadata in order to be able to maintain its services. In particular it must be able to support data which permits it to check the authorisation of operators of data sources to register identifiers and to check the updating of association data. In the event of multiple association data, it must hold sufficient metadata to permit a selection.

On the other hand, the data source must support the metadata which permits it to update the association data correctly in the resolver system.

Policies: Policies need to be formulated and adhered to, both by the resolver service and the data source, to ensure that the PI system functions as expected. The policies required for reliable operation must be agreed among the participants and be externally transparent.

Agreement: The trustworthiness of a PI system relies both on the resolver service and on the service of the data source. An agreement is therefore required which is transparent for all users and in which both agree to the policies intended to ensure trustworthy operation.

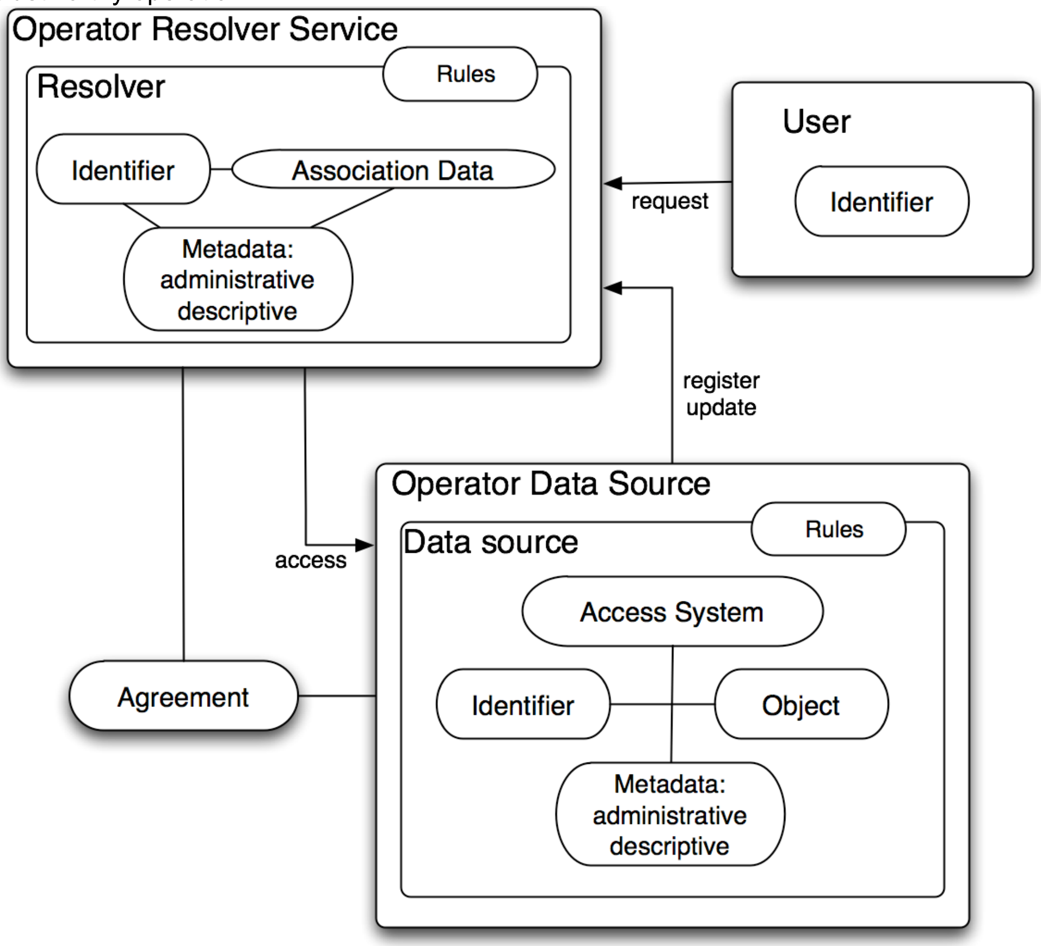

Figure 1: Overview of PI-System

Access system: The data source has an access system which allows it to access the identified object.

Trustworthy: Trustworthiness is the capacity of a system to operate in accordance with its objectives and specifications (i.e. it does exactly what it claims to do)[4]. From the viewpoint of a user, a system is trustworthy if its expectations are fulfilled.

In particular, a PI system is expected to perform its core functions (see below) reliably and these should be available permanently. The same identifiers are also always expected to be linked to the same objects.

A user cannot check the services of a PI system himself. In particular, the user cannot check whether the resolver takes him to the correct object. This is only possible if he has further identifying information (metadata) about the object (e.g. author, title, date,...). Nor can he be sure if the object has been changed; he can only check whether the information he has about the object is still valid.

Core services: The core services of a persistent identifier management system include:

- Regulating the issuing of identifiers: Unique identifiers can be provided by the resolver system. However, the issuing of identifiers can also be delegated through the allocation of a name space to third parties, in particular to data sources.
- Registering: Entering an identifier and the related association data in the resolver and checking whether this has not already been registered.
    a. Identifiers are issued by the resolver system:
    The data source sends its internal object identification and the association data to the resolver. This sends the issued identifier together with the object identification of the data source back to the source.
    b. Identifiers are issued by the data source within a name space allocated to it:
    the data source sends the identifier and the association data together with the authentication information of the data source, thereby permitting its authorisation to issue the identifier to be checked.
- Update: bringing the association data for an identifier up to date.
- Resolving: on request, returning the information from the association data concerning the access to the object identified by the identifier.

Value-added services:

In addition, a PI can also ....

- record information (metadata) about the object to which the identifiers are linked and make this available (e.g. metadata on rights management or on the form and version of the object);
- record and make available associations with other identifiers, the allocated objects of which have a special mutual relationship.

Extra services should not impair the core services.

3 Trustworthiness and persistence challenges

The trustworthy functioning of a PI system may be impaired over time by a series of events and changes.

3.1 Impairment of trustworthiness during the course of operation

The following problems may arise while executing the core services of PI systems besides the common threats facing computing systems:

[4] extended after INS Project 2007, p. 35

During registration of identifiers in the resolver system:

(1) The multiple registration of an identical object under different identifiers by the same or by different data sources can only be recognised and prevented by the resolver system storing and managing additional identifying metadata on the object and by carrying out a corresponding duplicate check for each new registration. Multiple registration is not a problem with regard to the trustworthiness of the PI system if it is clear that it is not possible to infer from different names that the referenced objects are different (see also (13) under 3.2)

(2) Also, multiple registration of non-identical objects under the same name can only be prevented by the resolver system if additional identifying metadata is stored and managed, or if it only permits a single set of association data for each name/identifier.

(3) The association data is not correct and does not permit access to the data source's access system. The resolver system can routinely check whether the association data produces error messages when activated and inform the data sources accordingly if it has a correct address for the relevant data source.

During updating of the association data:

(4) Changes in the data source's system render the association data invalid and the operator of the data source neglects to update the association data in the resolver system in time. [as problem (3)]

(5) New association data for an identifier is registered, but the old invalid data is not deleted. [as problem (3)]

(6) As the result of internal changes, the data source loses the internal link between the object and the identifier or the association data in the resolver system so that it is no longer apparent which association data needs to be updated for which identifier.

(7) Non-authorised persons report misleading association data for certain identifiers to the resolver system.

During resolving:

(8) Assuming that the data in the resolver system is correct (the data sources carry primary responsibility for this), practically the only error sources which can impair the trustworthiness are technical factors or deliberate sabotage. The core service of resolving is, from a technical viewpoint, a relatively simple process which can be protected by applying standard computer system diligence and protection measures.

3.2 Challenges arising from medium and long-term changes

(9) The PI system as a whole, or individual data sources, changes the schema used to form the identifiers.

This is the case e.g. if the identifiers contain significant elements which are changed ("speaking PIs"). The results are:

(1) All citations which use the old identifier become invalid unless the resolver establishes a concordance system which automatically links the old identifiers to the new ones.

(2) All data sources have to adapt the identifiers in their system.

(3) Any additional functions based on a specific structure, e.g. hierarchical, may become obsolete, however the basic functions are not necessarily called into question as a result.

A simple extension to the identifiers is possible if ...

(1) these supplements are applied in a form which permits the supplements to be separated from the previous string of the identifier and if

(2) the resolver system resolves the old identifiers and can redirect the requesting party to the new identifiers.

In the long term it may not be possible to prevent changes being made to identifiers. It is therefore necessary for PI systems to keep a concordance list to facilitate persistent resolving. Concordance lists do not necessarily have to be kept in the resolver system, they can also be generated by the individual data sources. The data source can also maintain the old and the new identifier, each with identical association data, which refer to the same object.

Global changes of identifiers also always carry the inherent risk of errors. These, however, can be more or less excluded with careful preparation and appropriate tests. Such changes must also be made in the data sources, meaning that a global change places great demands on the coordination of all those participating in the system.

(10) The object linked to an identifier is no longer accessible anywhere.

Such cases are unavoidable. Trusted PI systems should be expected to keep a registry of the identifiers and return a qualified response which differs from a technical error message (e.g. "Object no longer available").

(11) The object has been changed. The old version is no longer available. As far as the data source is concerned, the new version is no longer identical to the old one.

(A) The name stays the same.

> Because users of a trustworthy PI system expect that the same identifiers are always linked to identical objects, they have to be made aware of any changes to the object. If the data source has an OAIS-compliant system, such changes are available in the AIP (preservation history). The data source then, however, must then also display these to the user in an appropriate form.
>
> If the old version reappears this can result in multiple instances of non-identical objects under the same identifier. In a trustworthy system this needs to be made transparent to users.

(B) The new version has its own identifier.

> The name of the old version must continue to be resolvable. The association data is replaced by a reference to the name of the new version. The user must be informed that the referenced object is a new version. This can be done by the resolver service or by the data source. The operators of the resolver service and the data source agree appropriate rules.

(12) The object has been changed. The old version remains available.

(A) The object is registered under a second name.

> This case does not represent a problem with regard to trustworthiness. As a supplementary service it would be desirable for users of the resolver service or of the data source to be made aware of the existence of a predecessor or successor version.

(B) The new version is registered in the form of supplementary association data under the same name.

> This case does, however, pose a trustworthiness problem if the user is not made expressly aware of it. This situation must be avoided when new versions are issued, by means of clear rules regarding the issue of PIs.

(13) An object is registered several times under different names.

This case does not create a PI system trustworthiness problem, if those concerned are aware that different names do not refer to different objects.

(14) The technical procedure of the resolver service changes fundamentally.

The technical basis on which the service functions is not important - as long as the changes have no influence on the form of the identifier, as long as the resolver service can execute the expected basic functions, and as long as the resolver service can exchange data with the users and the data sources via the normal standardised channels. The basic functions of the PI system must be independent of any specific technical system.

However, changes to the resolving procedure may indeed involve a change to the identifiers. cf (9).

(15) The PI system is abandoned and the resolver service discontinued.

Given the likelihood that not all systems existing today will survive in the long term, this is a realistic scenario. A trusted PI system must therefore be able to export its core data in an open standard format and have devised a scenario for the successor system.

The following is conceivable:

All objects which were registered in the discontinued system are registered in a new system with a new PI. Depending on the naming procedure of the new system, it may be possible to incorporate the string of characters from the old PI into the new PI (similar to the integration of ISBN numbers in certain PI systems). Otherwise a concordance between the old and new identifiers must be set up, along with a corresponding resolver service.

4 Criteria catalogue

Preliminary remarks:

The criteria below are based on the global requirements of trustworthiness and persistence; persistence is also a prerequisite for trustworthiness in the application area of long-term preservation.

The catalogue is divided into three parts - *Organisational framework*, *Handling objects* and *Infrastructure and safety*. The *Organisational framework* part is general and also contains criteria which have an impact on the infrastructure and handling objects.

Within the criteria catalogue, "public" means accessible to at least all those involved in a PI system, i.e. the operators of resolver services and data sources, and possibly independent organisations, but not necessarily to all users.

4.1 Organisational framework

4.1.1 [Trusteeship] The operators of the resolver services and the data sources in the PI system are key players in the field of application.

The greater the number of key players there are behind a PI system (and which also use it themselves), the greater the spread and the smaller the risk that it will be discontinued for a trivial reason. The names of the institutions involved are publicly known. The operators of the resolver services and the data sources can join together legally to form a trusteeship, and the responsibility can be distributed following different models. It can be cooperative or consist of just one single central institution.

For example: the International DOI Foundation (IDF), with publishing houses and research institutions as members (http://www.doi.org/idf-member-list.html)

4.1.2 [Commitment] The operators of the resolver services commit themselves in a legally binding form, and with long cancellation or withdrawal periods, to maintaining the PI system on a long-term basis.

Even if legal obligations can always be cancelled, they generate trust. Also, long termination or withdrawal periods create time for organising migration to a new system. The core elements of the legal obligations entered into are publicly known.

e.g. the foundation charter of the International DOI Foundation (IDF)

4.1.3 [Operators] The operators of resolver services are legally obliged to adhere to the definitions, basic principles and regulations.

The resolver services can be part of a trustee institution, however they may also be operated as independent organisations, integrated by means of agreements and control mechanisms.

e.g. the URN-NBN resolver service as an organisational unit of the German National Library

4.1.4 [Operators] The resolver service is one of the operator's core tasks.

The operator may perform other core tasks besides the resolver service, but the resolver must have at least the same status as other tasks, i.e. operation should not suffer from other more important core tasks.

If the operator is integrated as a non-independent organisational unit within a larger institution, operation of the PI system must be covered by the tasks allocated to it.

For example: e.g. the URN-NBN resolver service of the German National Library

4.1.5 [Business model] Financing of the resolver service operation is secured on a long-term basis.

The business model and the financing sources are publicly known and there is a constant supply of income. A large proportion of the income within the overall budget is contractually assured or secured via long-standing customer ties. The financial results are publicly known.

The transparency requirements can presumably only be fulfilled by non-profitmaking organisations. It should, however, be possible for the institution to build up reserves. A resolver service should be free of charge for users.

For example: Financing is provided entirely in the form of fixed contributions from the trustee institutions or the operators of the data sources. The trustees are entitled to adjust these contributions if the demands change.

4.1.6 [Rights] The operators of the resolver services possess all the necessary rights to the PI system and the resolver system.

The operators of the resolver services disclose the origin and the legal basis of the main parts of the system. They have unrestricted usage rights in these parts at least.

A trustee organisation has legally protected the string of its name system and the domain of the resolver service all over the world.

4.1.7 [Transparency] The main parts of the system have been published.

The structure of the PI system, the definitions used, data models, rules and technologies are publicly known.

For example: the DOI website (www.doi.org) or the URN-NBN website (www.persistent-identifier.de)

4.1.8 [Neutrality] On no level does the PI system favour linking to objects from certain data sources and it makes multiple availability of objects transparent to the user.

More than one copy of a document exists, e.g. in an archive and in a fee-paying portal. The resolver service informs the user that the object being sought is available at more than one location and permits him to activate both links, one after the other.

For example: The resolver service offers the user a selection of association data on existing copies. The user can then make a free choice.

4.1.9 [Exit strategy] The operators of the resolver services and the data sources have a strategy to ensure ongoing resolution of the issued PIs once resolver operation has been discontinued.

The operators of the resolver services and the data sources have a strategy that can be adopted if operation of a resolver service has to be discontinued. This ensures that the PIs which have been issued are secure.

For example: The operators can stipulate that the PIs can be resolved by other organisations, in particular by the resolver services of other PI systems. It is in possession of declarations of intent from operators of other PI systems who can assume the resolver services if required. It stipulates how the PIs which have already been issued can, if required, be translated into new PIs using a simple application.

It undertakes to hand the URL of the resolver service and any other rights necessary for the further resolution of the PIs to rescue organisations, without making any claims for compensation.

4.1.10 [Data sources] The operators of data sources interested in issuing PIs for their objects make a contractual obligation towards the operators of resolver services to adhere to the basic principles and rules of the PI system.

The content of the agreements and the list of data source operators with which a contract has been concluded are publicly known.

Contracts can be refused or retroactively cancelled if the data sources offer no guarantee to adhere to basis principles and rules.

4.2 Object management

4.2.1 [Scalability] The encoding scheme of the namespace permits any number of name variants.

For example: Names consisting of sequence numbers with no upper limit.

4.2.2 [Uniqueness] The identifier indicates clearly and uniquely to which PI system it belongs.

Uniqueness can only be guaranteed within a name system, accordingly the relevant resolver service must be able to identify and resolve the name system.

For example: The identifier includes the name of the PI system (label of name system)

4.2.3 [Uniqueness] The operators of the resolver services take suitable precautions to prevent multiple issuing of a PI to non-identical objects.

If the issuing of the identifiers is delegated to the operators of sub-resolvers or data sources, this is assigned a clearly delimitable and scalable namespace.

For example: hierarchically extendable subnamespaces such as those used in the URN:NBN scheme

Restriction of authorisation to issue names to those data sources storing the largest number of objects in a specific delimitable field. Only these data sources offer the object via the resolver service. These data sources keep a public register which contains sufficient types of other identifying metadata. This allows other data sources to check whether one of its objects has already had a PI allocated to it.

For example: Restriction of name issuing for "Helvetica" to the Swiss National Library which, according to its brief, must strive to achieve completeness.

The resolver service demands further identifying metadata from the data sources on each object. This metadata should permit a reliable check for duplicates.

The PI issuer takes similar suitable precautions to prevent multiple issuing of a PI to non-identical objects.

4.2.4 [Validity] The resolver service periodically checks the validity of the associated information.

The resolver service regularly activates the association data and checks whether an error message is returned. It provides appropriate feedback to the operators of the data sources.

4.2.5 [Security] The resolving service only permits authorised data sources to register and update PIs.

The data source is authenticated and its authorisation checked before each registration and updating procedure.

For example: Use of digital signatures for data exchange.

4.2.6 [Transparency] The data source sets out its rules for managing its objects and issuing PIs.

The data source's rules define:

- Which objects are to be given PIs and which rules determine their length of storage;
- which changes to the objects necessitate a new version with a new PI;
- which old versions continue to be stored;
- whether PIs of deleted objects will continue to be resolved, triggering qualified feedback to the user (e.g. "Object deleted on 5.10.08, revised version available under PI XY")

The rules can be consulted by all users, allowing them to assess the result of the resolving procedure.

4.2.7 [Transparency] Users receive reliable feedback on the availability and change history.

If an object is not directly accessible the user receives notification from the data source or the resolver service regarding the existence and accessibility of the object.

For example: "No object available for PI XY"; "Objects only accessible for authorised users XY".

If the significant properties of an object have been changed since the PI was issued, the data source provides information on the change history of the objects to a user (especially information which is relevant for the identity of the object)

4.2.8 [Simplicity] The names of PIs have a simple structure.

In certain circumstances it may be necessary to copy a PI manually. Long and complex PIs often cause errors in this case. For this reason, PIs should be short and clearly structured and only consist of ASCII characters.

For example: urn:nbn:ch:bel-9478

4.2.9 [Simplicity] It must be possible for the user to resolve a PI simply and with no hindrances.

The resolver service must be simple to use. The user interface follows recognised standards of usability and should contain no in-built hindrances.

4.3 Infrastructure and Security

4.3.1 [Location independence] Access to the resolver service is possible via distributed public networks.

For example: Access to resolver service via Internet and http protocol services.

4.3.2 [Security] The operator of the resolver service takes suitable and approved measures to ensure computer security.

PI systems use IT systems regarded as trustworthy primarily on account of their regulated operation and the security precautions taken. Recognised standards such as ISO 17799 exist which set out these requirements in detail. There is also a range of audit possibilities suitable for checking that the standards are being adhered to. The operator of the resolving service uses these standards and has their observance checked regularly (audits) by external organisations. The results are published.

4.3.3 [Failsafe solution] The operator maintains a failsafe solution for his resolving service.

The operator of the resolver service indicates how continuous availability is ensured.

For example: Sufficient numbers of mirror servers are available which can cope with all current requests in the event of failure of a resolving server.

4.3.4 [Technology independence] The operator is not dependent upon specific third parties for the use and replacement of system parts.

There are no system components necessary for operation of the resolver service which cannot easily be replaced by other products, the third party usage rights of which can be revoked, and the replacement of which is not certain in the event of a defect.

The operator discloses the origin of the system components.

For example: Use of open source products and of widely available standardised components.

4.3.5 [Migratability] The data necessary for the core services can be exported at any time in openly documented and standardised formats from the system.

Export functions which use openly documented standard formats are necessary to facilitate transfer of the data to other systems.

For example: Export of the resolver entries in an XML format documented by the operator.

4.3.6 [Scalability] The resolver service can be extended as required.

The resolver service has built-in extendability in order to handle the growing quantities of registered PIs and the growing number of requests and to guarantee acceptable response times.