Technical Guide

Core Identifier Framework Matrix

The Distributed Management Task Force, Inc

Technical Guide

Core Identifier Framework Matrix

ISBN: 1-931624-73-9

Document Number: G071

Published by The Open Group, April 2007.

Comments relating to the material contained in this document may be submitted to:

The Open Group
Thames Tower
37-45 Station Road
Reading
Berkshire, RG1 1LX
United Kingdom

or by electronic mail to:

ogspecs@opengroup.org

Contents

Preface

The Open Group

The Open Group is a vendor-neutral and technology-neutral consortium, whose vision of Boundaryless Information Flow™ will enable access to integrated information within and between enterprises based on open standards and global interoperability. The Open Group works with customers, suppliers, consortia, and other standards bodies. Its role is to capture, understand, and address current and emerging requirements, establish policies, and share best practices; to facilitate interoperability, develop consensus, and evolve and integrate specifications and Open Source technologies; to offer a comprehensive set of services to enhance the operational efficiency of consortia; and to operate the industry's premier certification service, including UNIX® certification.

Further information on The Open Group is available at www.opengroup.org.

The Open Group has over 15 years' experience in developing and operating certification programs and has extensive experience developing and facilitating industry adoption of test suites used to validate conformance to an open standard or specification.

More information is available at www.opengroup.org/certification.

The Open Group publishes a wide range of technical documentation, the main part of which is focused on development of Technical and Product Standards and Guides, but which also includes white papers, technical studies, branding and testing documentation, and business titles. Full details and a catalog are available at www.opengroup.org/bookstore.

As with all *live* documents, Technical Standards and Specifications require revision to align with new developments and associated international standards. To distinguish between revised specifications which are fully backwards-compatible and those which are not:

- A new *Version* indicates there is no change to the definitive information contained in the previous publication of that title, but additions/extensions are included. As such, it *replaces* the previous publication.
- A new *Issue* indicates there is substantive change to the definitive information contained in the previous publication of that title, and there may also be additions/extensions. As such, both previous and new documents are maintained as current publications.

Readers should note that updates – in the form of Corrigenda – may apply to any publication. This information is published at www.opengroup.org/corrigenda.

The Network Applications Consortium

The Network Applications Consortium (NAC) is a consortium of IT end-user organizations representing combined revenues of over $800 billion, more than 55,000 network servers, and more than 1 million workstations. 55% of NAC members are Fortune 500 companies – members

include large, complex, distributed end-user organizations in healthcare, insurance, education, automotive, financial services, government, technology, and aerospace.

Since its founding in 1990, NAC has emerged as a premier group of information technologists dedicated to promoting technology integration, interoperability, and member and vendor collaboration. NAC's collaborative process – involving members, alliance partners, and vendors – is designed to improve members' ability to deliver agile IT infrastructure in support of business objectives.

Information about the NAC can be found at www.netapps.org.

This Document

This document is the Core Identifier Framework Matrix. It provides a reference point for identifier classifications, and provides a basis for the selection of an identifier form for a global standard common core identifier.

This document was developed by the Core Identifier Work Group, a joint initiative of the Distributed Management Task Force (DMTF), the Network Applications Consortium (NAC), and The Open Group. It was approved by these sponsoring consortia. It is intended to be a living document, and change to it can be expected. Any such change is the joint responsibility of the sponsoring consortia members, and must be formally approved by each of them.

Trademarks

Acknowledgements

The Open Group gratefully acknowledges the contribution of the following people in the development of this Technical Guide:

- Paul Agbabian, Symantec
- Pamela Campagna, Network Applications Consortium (NAC)
- Merl Ferguson, Progress Energy
- Chris Harding, The Open Group
- Don Hirst, ABN AMRO
- Jim Hosmer, Lockheed Martin
- Ed MacIver, CGI Group Inc.
- Richard Paine, Boeing
- Drummond Reed, Cordance
- Marty Schleiff, Boeing

Referenced Documents

There are many documents referenced in the Core Identifier Framework Matrix. In most cases, the document is only referenced in one section, and details of how to find it are given in that section. Those documents are not listed here. The following documents are referenced in more than one section of the Matrix, or in other parts of this Technical Guide:

[ASCII] The American Standard Code for Information Interchange, standardized as ISO/IEC 646 (available from www.iso.org).

[CIDSCEN] Business Scenario, December 2006, Identifiers in the Enterprise (K061), published by The Open Group (available from www.opengroup.org/bookstore/catalog/k061.htm).

[FRAMEWORK] Core Identifiers – Standards Framework Document (available from www.opengroup.org/projects/coreid/uploads/40/12817/Core_Identifier_ Framework_Document_v1.pdf).

[IDMWP] White Paper, March 2004, Identity Management (W041), published by The Open Group (available from www.opengroup.org/bookstore/catalog/w041.htm).

[IETF RFC 4122] IETF RFC 4122: A Universally Unique IDentifier (UUID) URN Namespace, P. Leach, M. Mealling, & R. Salz, July 2005 (available from www.ietf.org/rfc/rfc4122.txt).

[UNICODE] An extension of ASCII defined by the Unicode Consortium to accommodate multiple character sets. The current version is the Unicode Standard, Version 5.0, Fifth Edition, The Unicode Consortium, Addison-Wesley Professional, Oct. 27, 2006, ISBN 0-321-48091-0. The original version was extended and developed into ISO/IEC 10646: Information Technology – Universal Multiple-Octet Coded Character Set (UCS) (available from www.iso.org).

1 Introduction

1.1 Objective

This document was produced by the Core Identifier Work Group, a joint initiative of the Distributed Management Task Force (DMTF), the Network Applications Consortium (NAC), and The Open Group.

The Core Identifier Work Group was formed following the publication by The Open Group of its White Paper on Identity Management [IDMWP], which states that: "There is a compelling need for a set of standards for specifying and exchanging a core identifier."

Organizations need to manage the identities of several classes of people, including their members or employees, employees of their business partners, and their customers. These identities are stored in and managed by software programs. Often, mission-critical components rely on the identities for their operation.

Organizations also need to manage the identities of "non-human" entities such as software, items of equipment, services (system, network, and storage), and virtualizations of these entities.

Unfortunately, there are many different ways of defining identifiers. The differences are due partly to different practices in different organizations and departments, and partly to the adoption of different formats by product manufacturers.

This means that a large organization has to cope with many different representations of identifiers. If the systems that use these identifiers are to interoperate, then the organization must provide mappings between the identifiers. Special products or custom software may be needed to implement these mappings. The whole process of managing identifiers becomes unnecessarily cumbersome and complex.

A common, standard way of classifying and representing identities would significantly improve operational efficiency, and would help organizations to comply with identity and privacy legislation. Joint work by industry bodies and consortia is needed to achieve this aim.

The Core Identifier Work Group was formed to pursue this work. Its mission is to set the stage for widespread usage of a common, standard way of representing identities of people and things. It does this by stating and explaining requirements, and by working with standards bodies and product vendors to ensure that a framework for identifier taxonomies is agreed, that instances of standards for identifier syntax and semantics are defined and approved, and that these standards are reflected in and used by other relevant standards, and are widely implemented in products that are successful in the marketplace.

The vision of the Core Identifier Work Group is twofold. First, that a framework exists that allows for the grouping of related concepts of identity into useful categories. Second, that, for a number of widely implemented categories, a common format and structure for the representation

of identifiers is specified in standards and adopted by makers of IT systems. This standardization provides a reduction in complexity, leading to increased usage, and improved interoperability and reliability with reduced costs.

The Core Identifier Work Group has addressed key issues described in the Identity Management White Paper [IDMWP]. The present document is one of the Work Group's primary work products, and a significant step towards achieving the group's objectives. Other work products include a Business Scenario [CIDSCEN] and a Framework Description [FRAMEWORK]. They precede this document, and provide additional background and context for the results presented here. That said, this is a stand-alone document that can be read without reference to the preceding documents.

The classification presented in this document is the result of the Work Group's analysis using the requirements and models identified in the Framework Description [FRAMEWORK]. It has a number of objectives:

1. To delineate standards and specifications that relate to identifiers.
2. To provide a glossary of terms related to identifiers.
3. To identify standards and specifications that relate to core identifiers.
4. To identify distinctions between identifiers, particularly related to core and common core identifiers.
5. To provide links to the relevant standards and specifications, responsible parties, and support organizations.
6. To highlight any overlaps and gaps identified in fulfilment of the agreed requirements.
7. To guide analysis concerning specification of common core identifiers.
8. To define development objectives for further standardization, as necessary; e.g., by recommending priority for further action.

The Core Identifier Work Group anticipates that publication of this document will clarify the existence and relationships among standards and specifications related to identifiers and identity, and lead to further work to standardize common core identifiers. This document does not recommend a particular common core identifier form, but it identifies candidates for core and common core identifiers, and makes it clear that further standardization activities are needed and useful. It also identifies the requirements that any such proposed standards must fulfil.

The Core Identifier Work Group also intends that the Core Identifier Framework Matrix presented in this document will guide development of software services that use the characteristics of the named standards and specifications to enable automated mapping of trust relationships from one set of identifiers to another set of identifiers, particularly when the subject identifiers are specified as "core" or "common core" identifiers. The mappings must meet established requirements for security, timeliness, integrity, non-repudiation, and inter-system operation. This is a stringent set of requirements, and the resulting software services are expected to take time and care to create, test, and place into use. Still, that is the challenge that drives this effort, because the present complexity and difficulty (not to say inability) for systems to automatically exchange identifiers is no longer acceptable.

1.2 Overview

There are technical problems relating to the use and management in enterprises of identifiers for people and things that have significant business implications. The Identifiers in the Enterprise Business Scenario [CIDSCEN] describes these problems and their implications, and proposes a solution with three components: a documentary framework for enterprise identifiers, a common identifier form to which existing identifiers can be mapped algorithmically, and a global standard common core identifier for each person or thing that an enterprise needs to identify.

This document provides a reference point for identifier classifications. It lists and classifies known *de jure* and *de facto* standards and specifications that are related to identifiers. As such, it forms a crucial part of the documentary framework for enterprise identifiers.

The Business Scenario puts forward the Extensible Resource Identifier (XRI) as an appropriate standard for the common identifier form, and recommends its adoption for this purpose. This document assumes the use of XRI as the common identifier form. It gives, for each identifier, a linkage to a canonical XRI representation, where such a representation is defined.

This document provides a basis for the selection of an identifier form for the global standard common core identifier. It suggests appropriate forms, but does not recommend a particular choice. The forms that are appropriate are certain specific forms of XRI, and identifiers consisting of pairs of Universal Unique Identifiers (UUIDs).

The choice between these forms should be made as a result of further study. The analysis in this document was made largely by customer organizations. Vendors of products that will use the common core identifier form must participate in the work on selecting a common core identifier for the results of that work to be valid. It should include pilot implementations, and liaison between the consortia sponsoring the Core Identifier Work Group and appropriate standards bodies.

1.3 Conformance

This Technical Guide has no conformance requirements.

2 The Role of the Matrix

The Business Scenario [CIDSCEN] sets out requirements for three things:

1. A documentary framework for existing identifier forms that will help enterprises to manage their complexity and to reduce that complexity over time.

2. A common identifier form to which existing identifiers can be mapped mechanically that will enable standardization of system components and interface mechanisms, simplifying the enterprise IT architecture.

3. A global standard common core identifier for each person or thing that an enterprise needs to identify that will:

    a. Simplify identifier mappings within the enterprise by enabling all other identifiers to be mapped to the core identifier (a "2n problem") rather than being mapped to each other (an "n^2 problem")

    b. Provide a persistent identifier for security principals that enables responsibility for actions to be established clearly across the enterprise, and as long after the time of the actions as necessary

    c. Enable sharing of identifiers across an organization's internal and external boundaries

The Core Identifier Framework Matrix presented in this document forms an important part of the documentary framework. It lists important existing identifier forms used by enterprises, and shows their characteristics and attributes.

The Matrix assumes use of the Extensible Resource Identifier (XRI) as the common identifier form. For each identifier listed in the Matrix there is a reference to a canonical XRI representation, where such a representation is defined.

The Matrix also indicates, for each identifier, whether it could serve as core identifier or common core identifier. Several identifiers are indicated as potentially qualifying as common core identifiers, but no conclusion is put forward as to which should be selected as the global standard common core identifier form; this is left for further study.

3 Requirements

The Business Scenario [CIDSCEN] sets out the following requirements for the Documentary Framework, the Common Identifier Form, Core Identifiers, and Common Core Identifiers.

3.1 Documentary Framework

The documentary framework must:

1. Comprehend all important existing identifier forms used by enterprises
2. Allow for the definition of new forms
3. Explain identifier characteristics and attributes
4. Include the common identifier form and core identifiers
5. Be an authoritative reference
6. Be easy to read and understand

3.2 Common Identifier Form

The common identifier form must:

1. Allow an entity to have multiple identifiers
2. Be able to be handled by computer programs that do not require direct participation of people in the processes (except possibly in exceptional circumstances)
3. Map algorithmically (not including table lookups, and in conformance with agreed standards) to existing syntaxes for identifiers in use within enterprises, such as:
    a. User-friendly identifiers
    b. Short-form identifiers that can be conveyed verbally
    c. Long-form identifiers that are guaranteed unique
    d. Systemic identifiers
    e. Identifiers that support specific requirements; e.g., HIP identifiers for Secure Mobile Architecture (SMA)
4. Allow for new identifiers that support innovative built-in functionalities

5. Enable some attributes of the identified entity to be determined by inspection of the identifier, where appropriate, but also allow for opaque identifiers to protect privacy and confidentiality[1]

6. Comprehend identifiers with different characteristics, and enable some characteristics of the identifier to be determined by inspection of it where appropriate, including:

    a. The authority responsible for issuing the identifier

    b. The process by which the identifier can be resolved to discover further information about its subject and its issuing authority

    c. Whether the identifier is static (e.g., to support personalization), or dynamic (e.g., to avoid profiling)

    d. Whether the identifier is permanent or re-assignable (e.g., for finite or dynamic namespaces)

7. Have a standard process for resolution to discover further information about its subject and its issuing authority, noting that:

    a. Determination of the issuing organization cannot be guaranteed (for example, it may have been issued by a company that has gone out of business and no longer exists).

    b. It must be possible to control the amount of information about the subject that can be discovered.

8. Be portable (capable of being issued by one organization and used by others) based on cross-organization standards

9. Be independent of how the subject is accessed (for example, the identifier for a file should not depend on whether the file is accessed via a file manager or via the web)

3.3 Core and Common Core Identifiers

Core identifiers must:

1. Be portable – able to be issued by one organization and used by others – based on cross-organization standards

2. Have a clear, unambiguous name form

3. Convey no meaning other than that they identify someone or something – there should be no need to parse names

4. Impose no constraints on directory namespace

5. Be easily generated without reliance on complex interactions with some central authority

6. Not be tied to any language or cultural environment[2]

[1] The Business Scenario only refers to privacy, but confidentiality is important also. Privacy is generally related to an individual, whereas confidentially is related to a business context.

7. Be flexible enough to accommodate different business models
8. Be able to be integrated into single sign-on systems where security and privacy of the identifier information is critical
9. Allow for the fact that an individual is usually represented by some authority that holds sway over him; e.g., his credit card company, his government, etc.
10. Be compatible with federated identity standards
11. Be applicable to things as well as to people – anything that needs to be subject to access control policy, not just a person, can be a security principal
12. Be applicable to groups as well as to individuals
13. Allow for anonymity – there is a need for "friendly handles" that can be used to refer to people in transactions without revealing their real identities – anonymity can be a requirement in some cases
14. Provide for processing efficiency (e.g., fixed-length identifiers are more efficient in some situations)

Common core identifiers must, in addition:

15. Be persistent over time
16. Uniquely distinguish an entity within a global scope
17. Uniquely distinguish the issuing authority, which is within the same scope
18. Be capable of representation in common identifier form syntax
19. Be assured of interoperability among domains or systems, according to agreed standards and related policy

The definition of common core identifiers should leverage existing technology where feasible.[3]

[2] A human or computer language is meant, here.
[3] The Business Scenario also states that fixed length would be a desirable characteristic.

4 The Framework Matrix

Material in the Core Identifier Framework Matrix is arranged in tabular form, as follows.

Each tabular entry describes an existing, identified standard or specification related to identifiers. At the time of publication (early 2007), there were 28 items described in the Framework Matrix. As others are identified and approved, they can be included in this list, through application to one of the sponsoring consortium members.

The tabular entries are divided into types and topics. The types of data are description, characteristics, and analysis. The topics relate to the identified standards and specifications. These types and topics are explained in Table 1:

Type	Topic Name	Description
Description	Classification Number	Ordinal number, used only to provide a tag and count for the items in the table. Where standards or classifications are related – i.e., by scheme or namespace – the subordinate standards are indicated by decimal numbering, below the decimal point. For example, the IRI standard is 14, and the IRI Scheme "hdl" (handle) standard is 14.1 in the Framework Matrix table.
	Identifier/ Standard Name	Common/short name of identifier or standard.
	Platform	Operating system scope for identifier.
	Identifier/ Standard Description	Full name/description of identifier or standard.
	Reference	Text reference to full description of identifier.
	URL	Hypertext link to full description of identifier.
	Responsible Organization/Contact	Name and contact information of organization responsible for identifier.
	Related Standard(s)	Names/links to any related standards.
Characteristics	XRI Representation	Expression of canonical XRI representation of identifier if such representation is defined (if not defined, an example of a proposed XRI representation is given).
	Formats of Identifier	How identifier is formatted, such as number string, dotted decimal, alpha string, alphanumeric string, capitalization rules, etc.
	Type of Identifier	Type description of identifier, such as digit string, alpha string, alphanumeric string, binary number, etc.

Type	Topic Name	Description
	Related Identifier(s)/ Type(s) of Identifier(s)	Names of any related identifier(s)/type(s) of identifiers.
	Uniqueness	Whether identifier is unique (yes/no), with scope limitations, if any.
	Persistence Characteristics	Whether identifier is persistent, with scope limitations if any.
	Usage Scope	How identifier is/can be used, with scope specification.
	Mapping/Equivalence Checking	Approach for mapping/equivalence checking among identifiers; e.g., through encoding in XRI.
	How Generated	How identifier is generated.
	How Recognized	How identifier is recognized.
Analysis	Context for Core	Context in which the identifier is a core identifier.
	Core/Non-core/ Common Core	Identifier status: Core/Non-core/Common Core.
	Rationale	Why identifier is Core/Non-core/Common Core.

Table 1: Classification Types and Topics

In the Core Identifier Framework Matrix, the following values are used with the following meaning:

N/A (Not Applicable) The identified concept or topic does not apply in this instance.

None There is no identified topic or concept which applies in this instance.

Not specified The applicability of the identified topic or concept is not specified in this instance.

The initial material used to fill in the Framework Matrix is taken from earlier published documents from The Open Group [IDMWP] and the Core Identifier Work Group [CIDSCEN].

4.1 Operating System User Name

Description	
Classification Number	1
Identifier/Standard Name	Operating System User Name
Platform	General
Identifier/Standard Description	Operating system-dependent. Identifier as specified by Operating System rules.
Reference	System Vendor
URL	Per System Vendor
Responsible Organization/Contact	System Vendor
Related Standard(s)	None
Characteristics	
XRI Representation, meeting Common Core ID Requirements	Example of OS user name using syntax indicating/claiming persistence: `xri://!!1000!1234.a1b2/!userid`
Formats of Identifier (Canonical/Other)	Unstructured alphanumeric string
Type of Identifier	Type per system
Related Identifier(s)/ Type(s) of Identifier(s)	None
Uniqueness	Within system
Persistence Characteristics	Limited. When used as external reference, must be managed to persistence.
Usage Scope	Within system
Mapping/Equivalence Checking (Canonical)	Exact match, leading zeros irrelevant.
How Generated	System-specific
How Recognized	System-specific
Analysis	
Context for Core	Within system
Core/Non-core/Common Core	Core only, within system.
Rationale	Core since unique identifier within system. Not common core due to complete lack of standards compliance. Possible to use as common core with XRI adornment.

4.2 Email Address

Description	
Classification Number	2
Identifier/Standard Name	Email Address
Platform	General
Identifier/Standard Description	`mailbox-name@domain_name` An `addr-spec` is a specific Internet identifier that contains a locally interpreted string followed by the at-sign character ("`@`", ASCII value 64) followed by an Internet domain. The locally interpreted string is either a quoted-string or a dot-atom.
Reference	IETF RFC 2822: Internet Message Format, P. Resnick, April 2001. Replaces IETF RFC 822: Standard for the Format of ARPA Internet Text Messages, D. Crocker, August 1982 (www.ietf.org/rfc/rfc822.txt).
URL	www.ietf.org/rfc/rfc2822.txt
Responsible Organization/Contact	IETF Secretariat c/o Corporation for National Research Initiatives 1895 Preston White Drive, Suite 100 Reston, VA 20191-5434, USA Tel: +1 703 620 8990 Fax: +1 703 620 9071 Email: ietf-info@ietf.org
Related Standard(s)	DNS (domain specification)
Characteristics	
XRI Representation, meeting Common Core ID Requirements	Example of email address using syntax indicating/claiming persistence: `xri://!!1000!1234.a1b2/!(mailto:mailbox@domain)`
Formats of Identifier (Canonical/Other)	Per IETF RFC 822, IETF RFC 2822
Type of Identifier	Character string
Related Identifier(s)/ Type(s) of Identifier(s)	None
Uniqueness	Unique at any point in time, re-use may occur, allowing different principals to have the same identifier at different times, and principals often have multiple e-mail addresses at the same time, representing different authorities.
Persistence Characteristics	Limited
Usage Scope	Global

Mapping/Equivalence Checking (Canonical)	Case ignores string match to check equivalence between identifiers.
How Generated	Local generation, not standardized beyond issuing organization, except for format.
How Recognized	By email system
Analysis	
Context for Core	Email system usage.
Core/Non-core/Common Core	Core only, within email domain.
Rationale	Not common core due to limited domain, non-compliance with requirements, and lack of stability, particularly with regards to DNS portion of the email address. Possible to use as common core with XRI adornment.

4.3 X.500 Distinguished Name

Description	
Classification Number	3
Identifier/Standard Name	X.500 Distinguished Name
Platform	General
Identifier/Standard Description	X.500 X.500 is an ISO and ITU standard that defines how global directories should be structured. X.500 directories are hierarchical with different levels for each category of information, such as country, state, and city.
Reference	ITU X.500 Series of Recommendations
URL	www.itu.int/ITU-T/publications/recs.html
Responsible Organization/Contact	ITU Place des Nations CH-1211 Geneva 20 Switzerland Tel: +41 22 730 51 11 Fax: +41 22 730 65 00
Related Standard(s)	IS 9594 Parts 1 through 10
Characteristics	
XRI Representation, meeting Common Core ID Requirements	Note: A canonical representation of an X.500 Distinguished Name using syntax indicating/claiming persistence has not yet been defined. Following is an example of what such a representation might look like: `xri://!!1000!1234.a1b2/!($dn* o:University%20of%20Michigan*c:US* cn:Babs%20Jensen)` Note: A colon is used as the DN assertion delimiter in this example as = is an XRI reserved character.
Formats of Identifier (Canonical/Other)	Sequence of assertions in the form "`type=value`"; organized in a hierarchical tree format.
Type of Identifier	Abstract data structure with multiple possible encodings.
Related Identifier(s)/ Type(s) of Identifier(s)	No known alternatives or related competing definitions.
Uniqueness	Algorithmically unique within the context of the tree's root (designed to be global, uniqueness limited by the practice of not registering names).

Persistence Characteristics	Distinguished name is subject to instability caused by arbitrary relocation of objects in the directory or by arbitrary renaming of any branch in the DN hierarchy.
Usage Scope	Within any system that recognizes X.500 style naming (includes LDAP).
Mapping/Equivalence Checking (Canonical)	Per X.500 equivalence rules
How Generated	Authority at each level of the tree ensures uniqueness of names created at that level.
How Recognized	Depends on encoding scheme – standards exist which permit the use of BER, DER, and string-based encoding.
Analysis	
Context for Core	General Usage
Core/Non-core/Common Core	Non-core
Rationale	Not sufficiently stable; actually used to identify a location within a naming tree, rather than the object itself. Possible to use as common core with XRI adornment.

4.4 Domain Component Name

Description	
Classification Number	4
Identifier/Standard Name	Domain Component Name
Platform	General
Identifier/Standard Description	DC-Name IETF RFC 2247 defines a subset of the possible distinguished name structures for use in representing names allocated in the Internet Domain Name System. It is possible to algorithmically transform any Internet domain name into a distinguished name, and to convert these distinguished names back into the original domain names.
Reference	IETF RFC 2247: Using Domains in LDAP/X.500 Distinguished Names, S. Kille, M. Wahl, A. Grimstad, R. Huber, & S. Sataluri, January 1998.
URL	www.ietf.org/rfc/rfc2247.txt
Responsible Organization/Contact	IETF Secretariat c/o Corporation for National Research Initiatives 1895 Preston White Drive, Suite 100 Reston, VA 20191-5434, USA Tel: +1 703 620 8990 Fax: +1 703 620 9071 Email: ietf-info@ietf.org
Related Standard(s)	X.500 and IS 9594
Characteristics	
XRI Representation, meeting Common Core ID Requirements	Note: A canonical representation of an X.500 Domain Component Distinguished Name using syntax indicating/claiming persistence has not yet been defined. Following is an example of what such a representation might look like: `xri://!!1000!1234.a1b2/!($dn*dc:cs,dc:ucl,dc:ac,dc:uk)` Note: Colon is used as the DN assertion delimiter in this example as = is an XRI reserved character.
Formats of Identifier (Canonical/Other)	Fully compatible with X.500 DN; specifies the "`domainComponent`" attribute type and rules for associating the value field with DNS domain components.
Type of Identifier	Abstract data structure with multiple possible encodings.

Related Identifier(s)/ Type(s) of Identifier(s)	DNS domain names, Fully Qualified Domain Name
Uniqueness	Same as above; intended to map onto exactly one DNS domain name.
Persistence Characteristics	DCN is subject to same persistence issues as X.500 DN.
Usage Scope	Within any system that recognizes X.500 style naming (includes LDAP).
Mapping/Equivalence Checking (Canonical)	Maps to DNS domain names.
How Generated	DNS name is registered; corresponding DN is algorithmically mapped.
How Recognized	Depends on encoding scheme – standards exist which permit the use of BER, DER, and string-based encoding.
Analysis	
Context for Core	General Usage
Core/Non-core/Common Core	Non-core
Rationale	Not sufficiently stable; actually used to identify a location within a naming tree, rather than the object itself. Possible to use as common core with XRI adornment.

4.5 SPKI/SDSI Name

Description	
Classification Number	5
Identifier/Standard Name	SPKI/SDSI Name
Platform	General
Identifier/Standard Description	Simple PKI/Simple Distributed Security Infrastructure Name
Reference	IETF Working Group/MIT Cryptography and Information Security Group Research Project
URL	Not available. (This item was not considered in detail due to apparent lack of activity.)
Responsible Organization/Contact	N/A
Related Standard(s)	N/A
Characteristics	
XRI Representation, meeting Common Core ID Requirements	N/A
Formats of Identifier (Canonical/Other)	N/A
Type of Identifier	N/A
Related Identifier(s)/ Type(s) of Identifier(s)	N/A
Uniqueness	N/A
Persistence Characteristics	N/A
Usage Scope	N/A
Mapping/Equivalence Checking (Canonical)	N/A
How Generated	N/A
How Recognized	N/A
Analysis	N/A
Context for Core	Deprecated
Core/Non-core/Common Core	Deprecated
Rationale	Deprecated from further consideration due to lack of IETF activity.

4.6 DCE Name

Description	
Classification Number	6
Identifier/Standard Name	DCE Name
Platform	General
Identifier/Standard Description	Distributed Computing Environment Name DCE names are hierarchical names consisting of a series of components delimited by the "/" character.
Reference	The Open Group Distributed Computing Environment (DCE)
URL	www.opengroup.org/dce
Responsible Organization/Contact	The Open Group 44 Montgomery St., Suite 960 San Francisco CA 94104-4704, USA Tel: +1 415 374 8280 Fax: +1 415 374 8293
Related Standard(s)	None
Characteristics	
XRI Representation, meeting Common Core ID Requirements	No recommended form is available; at present there is no strong incentive to specify this format.

Formats of Identifier (Canonical/Other)	In Global Directory (used as a directory to DCE cells) X.500 naming is used; however, representation is reversed and with slashes; e.g.,:
	`/.../c=us/o=organization/ou=orgUnit`
	The three dots indicate the global root, and DCE names that begin as such are called "global names". DCE can also use BIND as a directory to DCE cells, so DNS-style naming is also supported; e.g.:
	`/.../orgUnit.organization.com)`
	In Cell Directory, each entry has a UUID, although it may also have other identifiers. An identifier within the scope of a local cell begins with dot colon – dot colon is a shorter way to express "`/.../<local cell name>`" when a more fully qualified identifier is not required (e.g.,. `/.:/user`). Even within a local scope, hierarchical naming is supported, with levels delimited by slashes (e.g., `/.:/dept/user`). When fully qualified, the dot colon is replaced by the cell's name – such an identifier could appear as:
	`/.../c=us/o=organization/ou=orgUnit/dept/user`
	or perhaps:
	`/.../orgUnit.organization.com/dept/user`

Type of Identifier	Identifiers of DCE cells (similar to Windows domains), and identifiers of principles within cells.
Related Identifier(s)/ Type(s) of Identifier(s)	X.500, DNS, UUID
Uniqueness	When fully qualified with the cell name, the identifiers are globally unique.
Persistence Characteristics	Various identifiers can be used in a cell. UUIDs tend to be persistent; however, research did not reveal any statement that an identifier within a cell must never be re-assigned.
Usage Scope	DCE has shrinking relevance.
Mapping/Equivalence Checking (Canonical)	Generally, use case-ignore string compare. However, DNs in the Global Directory may be compared following the detailed DN matching rules in the standard.
How Generated	Identifiers within a cell may be established according to the practices used within the cell.
How Recognized	Recognized by the Global Directory Agent (GDA) capability inherent in DCE-capable systems.
Analysis	
Context for Core	General Usage

Core/Non-core/Common Core	Core, but not Common Core
Rationale	1. Must be capable of representation in the framework: Yes 2. Must be suitable for digital representation: Yes 3. Must be suitable for dereferencing to industry standards: Unspecified 4. Must be sparing of resource usage: Yes 5. Must be capable of both partial and full qualification to allow for different usage constraints: Yes Core – meets requirements for core identifiers for general use. Not Common Core due to lack of compliance with syntax requirements (5, 6, 7).

4.7 HIT

Description	
Classification Number	7
Identifier/Standard Name	HIT
Platform	General
Identifier/Standard Description	Host Identity Tag
Reference	IETF Host Identity Protocol (HIP) Working Group
URL	www.ietf.org/html.charters/hip-charter.html
Responsible Organization/Contact	IETF Secretariat c/o NeuStar, Inc. Corporate Headquarters 46000 Center Oak Plaza Sterling, VA 20166, USA Tel: +1 571 434 3500 Fax: +1 571 434 3535
Related Standard(s)	DNS (domain specification), RSA public key algorithm (rfc3110), DSA algorithm
Characteristics	
XRI Representation, meeting Common Core ID Requirements	Example of HIT using syntax indicating/claiming persistence: `xri://!!1000!1234.a1b2/!($hit*a76f4e9c083de7a23b3deac46b98f7c3)`
Formats of Identifier (Canonical/Other)	Type-1 identifier: Prefix (8 bits); Fixed prefix TBD. All other values reserved. — 0x40 – SHA-1 hash algorithm. All other values reserved. — Hash (120 bits) – Lower-order bits of the hash (as specified by the hash algorithm) of the public key. Type-2 identifier: Host Assigning Authority Field (HAA), and only the last 64 bits come from a SHA-1 hash of the Host Identity.
Type of Identifier	Binary number
Related Identifier(s)/ Type(s) of Identifier(s)	Public key
Uniqueness	Unique in space and time (statistically)
Persistence Characteristics	Indefinite
Usage Scope	Global
Mapping/Equivalence Checking (Canonical)	Binary number comparison

How Generated	See Appendix D at www.ietf.org/internet-drafts/draft-ietf-hip-base-03.txt for description of generation of Host Identity Tags.
How Recognized	System-specific
Analysis	
Context for Core	General Usage Any application or context that understands this type of identifier; e.g., IP Networks.
Core/Non-core/Common Core	Core, but not Common Core.
Rationale	1. Must be capable of representation in the framework: Yes 2. Must be suitable for digital representation: Yes 3. Must be suitable for dereferencing to industry standards: Yes 4. Must be sparing of resource usage: Yes 5. Must be capable of both partial and full qualification to allow for different usage constraints: Yes Core – meets requirement for core identifiers for general use. Not Common Core due to lack of compliance with requirements.

4.8 Universal Identifier

Description	
Classification Number	8
Identifier/Standard Name	Universal Identifier
Platform	General
Identifier/Standard Description	Structure for the Identification of Organizations and Organization Parts, International Standards Organization ISO/IEC 6523. ISO/IEC 6523 establishes a method to uniformly identify an identification code system to use under one namespace, even under different systems.
Reference	ISO/IEC 6523-1:1998 ISO/IEC 6523-2:1998
URL	www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=25773 www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=25774
Responsible Organization/Contact	ISO Registration Authority c/o British Standards Institution 389 Chiswick High Road London W4 4AL, United Kingdom Tel: +44 20 89 96 74 12 Fax: +44 20 89 96 74 48 Email: telecoms@bsi-global.com
Related Standard(s)	None
Characteristics	
XRI Representation, meeting Common Core ID Requirements	No recommended form is available; at present there is no strong incentive to specify this format.
Formats of Identifier (Canonical/Other)	Character String
Type of Identifier	Organizational identifiers only.
Related Identifier(s)/ Type(s) of Identifier(s)	None
Uniqueness	Unique in space and time, when registered.
Persistence Characteristics	Indefinite
Usage Scope	Global
Mapping/Equivalence Checking (Canonical)	Case ignore string match to check equivalence between identifiers.
How Generated	Follow generation rules per standard.
How Recognized	Follow parsing rules per standard.

Analysis

Context for Core	General usage
Core/Non-core/Common Core	Non-core
Rationale	Organization/parts of organizations only. Insufficient granularity for use as core identifier.

4.9 IUID

Description	
Classification Number	9
Identifier/Standard Name	IUID
Platform	General
Identifier/Standard Description	Item Unique Identification USA Department of Defense IUID is a system of marking items delivered to the Department of Defense with unique item identifiers that have machine-readable data elements to distinguish an item from all other like and unlike items.
Reference	The Basics: UID 101 (November 2004)
URL	www.acq.osd.mil/dpap/UID/guides.htm www.acq.osd.mil/dpap/Docs/uid/UID%20101.pdf
Responsible Organization/Contact	USD (AT&L), DPAP, SPEC ASST 3E1044 3060 Defense Pentagon Washington , DC 20301-3060, USA Tel: +1 703 848 7314 Email: info@uniqueid.org
Related Standard(s)	DoD Guide to Uniquely Identifying Items, Version 1.5
Characteristics	
XRI Representation, meeting Common Core ID Requirements	To be defined according to Military Standard 130L
Formats of Identifier (Canonical/Other)	UID of items is accomplished by marking each qualifying item with a permanent two-dimensional data matrix.
Type of Identifier	Unique identification is a set of data for assets that is globally unique and unambiguous, ensures data integrity and data quality throughout life, and supports multi-faceted business applications and users. The technology used to mark an item is 2D Data Matrix ECC 200 Symbol.
Related Identifier(s)/ Type(s) of Identifier(s)	The specification references a wide variety of identifiers and related standards.
Uniqueness	Within US DoD scope.
Persistence Characteristics	Lifetime of marked item.
Usage Scope	Within US DoD scope.
Mapping/Equivalence Checking (Canonical)	N/A

How Generated	Per US DoD specification
How Recognized	Requires 2D Scanner and related software.
Analysis	
Context for Core	Physical markings for parts.
Core/Non-core/Common Core	Non-core
Rationale	Identifiers for physical items only. Insufficient generality for core identifier.

4.10 RFID

Description	
Classification Number	10
Identifier/Standard Name	RFID
Platform	General
Identifier/Standard Description	Radio Frequency Identification Radio Frequency Identification (RFID) is a technology that has existed for decades. It is an automatic identification method, relying on storing and remotely retrieving data using devices called RFID tags or transponders. At a simple level, it is a technology that involves tags that emit radio signals and devices called readers that pick up the signal.
Reference	Radio Frequency IDentification (RFID)
URL	www.epcglobalinc.org
Responsible Organization/Contact	EPCglobal US Princeton Pike Corporate Center 1009 Lenox Drive, Suite 202 Lawrenceville, NJ 08648, USA Tel: +1 609 620 4549 Fax: +1 609 620 0255 President: Mike Meranda EPCglobal Contact: John Seaner Email: EPCInfo@EPCglobalUS.org www.EPCglobalUS.org
Related Standard(s)	Electronic Product Code (EPC): The EPC is a globally unique serial number that identifies an item in the supply chain. This allows enquiries to be made about a single instance of an item, wherever it is within the supply chain. The ID System: The ID System consists of EPC tags and EPC readers. EPC tags are RFID devices that consist of a microchip and an antenna attached to a substrate. The EPC is stored on this tag, which is applied to cases, pallets, and/or items. EPC tags communicate their EPCs to EPC readers using RFID. EPC readers communicate with EPC tags via radio waves and deliver information to local business information systems using EPC middleware.
Characteristics	
XRI Representation, meeting Common Core ID Requirements	Inappropriate
Formats of Identifier (Canonical/Other)	Inappropriate

Type of Identifier	Inappropriate
Related Identifier(s)/ Type(s) of Identifier(s)	Inappropriate
Uniqueness	Inappropriate
Persistence Characteristics	Inappropriate
Usage Scope	Inappropriate
Mapping/Equivalence Checking (Canonical)	Inappropriate
How Generated	Inappropriate
How Recognized	Inappropriate
Analysis	
Context for Core	Not appropriate for inclusion, as RFID is a transmission mechanism, not an identifier standard.
Core/Non-core/Common Core	Non-core
Rationale	Inappropriate

4.11 URI

Description	
Classification Number	11
Identifier/Standard Name	URI
Platform	General
Identifier/Standard Description	A Uniform Resource Identifier (URI) is a compact sequence of characters that identifies an abstract or physical resource. This specification defines the generic URI syntax and a process for resolving URI references that might be in relative form, along with guidelines and security considerations for the use of URIs on the Internet. The URI syntax defines a grammar that is a superset of all valid URIs, allowing an implementation to parse the common components of a URI reference without knowing the scheme-specific requirements of every possible identifier.
Reference	IETF RFC 3986: Uniform Resource Identifier (URI): Generic Syntax, T. Berners-Lee, R. Fielding, & L. Masinter, January 2005.
URL	www.ietf.org/rfc/rfc3986.txt
Responsible Organization/Contact	IETF Secretariat c/o Corporation for National Research Initiatives 1895 Preston White Drive, Suite 100 Reston, VA 20191-5434, USA Tel: +1 703 620 8990 Fax: +1 703 620 9071 Email: ietf-info@ietf.org
Related Standard(s)	Internationalized Resource Identifier
Characteristics	
XRI Representation, meeting Common Core ID Requirements	Any resource identified with a URI may be represented using XRI cross-reference syntax. Following is an example of a persistent XRI that incorporates an HTTP URI: `xri://!!1000!1234.a1b2/!(http://example.com/example/resource)`
Formats of Identifier (Canonical/Other)	A Uniform Resource Identifier (URI) is defined in IETF RFC 3986 as a sequence of characters chosen from a limited subset of the repertoire of US-ASCII [ASCII] characters.
Type of Identifier	US-ASCII Character String
Related Identifier(s)/ Type(s) of Identifier(s)	XRI, IRI, all related specifications.

Uniqueness	Within registration scope.
Persistence Characteristics	Unlimited, depends on DNS systems. URI is a location-dependent naming convention and its persistence is dependent on the complete stability of the entire path specification to the object, including DNS hierarchy and folder hierarchy.
Usage Scope	General
Mapping/Equivalence Checking (Canonical)	Case ignore string match to check equivalence between identifiers.
How Generated	Per RFC specification
How Recognized	Per RFC specification
Analysis	
Context for Core	General usage
Core/Non-core/Common Core	Core, Common Core, but being replaced with IRIs.
Rationale	Meets requirements for core identifiers. Certain schemes meet requirements for common core, as specified in the IRI section below.

4.12 XRI

Description	
Classification Number	12
Identifier/Standard Name	XRI
Platform	General
Identifier/Standard Description	An Extensible Resource Identifier (XRI) is a scheme and resolution protocol for abstract identifiers compatible with the IETF Uniform Resource Identifier (URI) and Internationalized Resource Identifier (IRI) specifications. The purpose of XRI is to provide a universal format for abstract, structured identifiers that are domain, location, application, and transport-independent, so they can be shared across any number of domains, directories, and interaction protocols.
Reference	Specifications produced by the OASIS XRI Technical Committee
URL	www.oasis-open.org/committees/xri
Responsible Organization/Contact	OASIS Post Office Box 455 Billerica, MA 01821, USA Tel: +1 978 667 5115 Fax: +1 978 667 5114 Email: info@oasis-open.org
Related Standard(s)	IETF RFC 2396, IETF RFC 1737
Characteristics	
XRI Representation, meeting Common Core ID Requirements	All absolute XRIs that consist entirely of persistent subsegments (which begin with a `!` symbol) meet the Common Core ID requirements. For example: `Xri://!!1000!1234!a1b2/!14!7`
Formats of Identifier (Canonical/Other)	The XRI scheme is a superset of the URI scheme defined by IETF RFC 3986 and the IRI (Internationalized Resource Identifier) scheme defined by IETF RFC 3987. For resources that need to be persistently identified and linked, the XRI scheme also incorporates syntax meeting the functional requirements for URNs (Uniform Resource Names) as described in IETF RFC 1737. Lastly, the XRI resolution protocol defines both generic and trusted means of resolving XRIs using http(s) to retrieve XML documents describing the target resource.
Type of Identifier	XRI Character String based on IRI format (IETF RFC 3987).

Related Identifier(s)/ Type(s) of Identifier(s)	IRI, URI
Uniqueness	Uniqueness as defined in XRI string.
Persistence Characteristics	Persistence as defined in XRI string (XRI syntax has a specific delimiter character (!) reserved for persistent identifiers at all levels).
Usage Scope	General
Mapping/Equivalence Checking (Canonical)	As described in XRI standard.
How Generated	Follow generation rules per standard.
How Recognized	Follow parsing rules per standard.
Analysis	
Context for Core	General Usage
Core/Non-core/Common Core	Core, Common Core
Rationale	For standard constructions which claim common core status, meets all requirements for common core. Recommended.

4.13 URN

Description

Classification Number	13
Identifier/Standard Name	URN (Uniform Resource Name)
Platform	General
Identifier/Standard Description	Uniform Resource Names (URNs) are resource identifiers with the specific requirements for enabling location-independent identification of a resource, as well as longevity of reference.
Reference	IETF RFC 2141: URN Syntax, R. Moats, May 1997. IETF RFC 3305: Uniform Resource Identifiers (URIs), URLs, and Uniform Resource Names (URNs): Clarifications and Recommendations, M. Mealling, & R. Denenberg, August 2002. IETF RFC 3406: Uniform Resource Names (URN) Namespace Definition Mechanisms, L. Daigle, D.W. van Gulik, R. Iannella, P. Faltstrom, October 2002.
URL	www.ietf.org/rfc/rfc2141.txt www.ietf.org/rfc/rfc3305.txt www.ietf.org/rfc/rfc3406.txt
Responsible Organization/Contact	IETF Secretariat c/o Corporation for National Research Initiatives 1895 Preston White Drive, Suite 100 Reston, VA 20191-5434, USA Tel: +1 703 620 8990 Fax: +1 703 620 9071 Email: ietf-info@ietf.org
Related Standard(s)	Internationalized Resource Identifier, Uniform Resource Identifier

Characteristics

XRI Representation, meeting Common Core ID Requirements	Any resource identified with a URN may be represented using XRI cross-reference syntax since a URN is itself a URI scheme. Following is an example of a persistent XRI that incorporates a URN: `xri://!!1000!1234.a1b2/!(urn:isbn:0-395-36341-1)`

Formats of Identifier (Canonical/Other)	The term Uniform Resource Name (URN) has been used historically to refer to both URIs under the "urn" scheme defined in IETF RFC 2141, which are required to remain globally unique and persistent even when the resource ceases to exist or becomes unavailable, and to any other URI with the properties of a name. This is in contrast to the term Uniform Resource Locator (URL) which refers to the subset of URIs that, in addition to identifying a resource, provides a means of locating the resource by describing its primary access mechanism (e.g., its network "location"). Note that the term URL is being deprecated, and should be referred to as HTTP URI. The W3C has since clarified that a URI can be further classified as a locator, a name, or both. An individual URI scheme does not have to be classified as being just one of "name" or "locator". Instances of URIs from any given scheme may have the characteristics of names or locators or both, often depending on the persistence and care in the assignment of identifiers by the naming authority, rather than on any quality of the scheme. The W3C recommends that future specifications and related documentation should use the general term "URI" rather than the more restrictive terms "URL" and "URN".
Type of Identifier	US-ASCII Character String
Related Identifier(s)/ Type(s) of Identifier(s)	URI, XRI, IRI, all related specifications.
Uniqueness	Within registration scope.
Persistence Characteristics	Unlimited (as defined in IETF RFC 2141).
Usage Scope	General
Mapping/Equivalence Checking (Canonical)	Case ignore string match to check equivalence between identifiers.
How Generated	Per RFC specification
How Recognized	Per RFC specification
Analysis	
Context for Core	General usage
Core/Non-core/Common Core	Core, Common Core
Rationale	Meets requirements for core and common core identifiers.

4.13.1 Universal Unique Identifier (UUID)/Globally Unique Identifier (GUID)

Description	
Classification Number	13.1
Identifier/Standard Name	URN Namespace: Universal Unique Identifier (UUID)/ Globally Unique Identifier (GUID)
Platform	General
Identifier/Standard Description	IETF RFC 4122 is arguably the most current and complete reference to the several variations in UUID-GUID. It defines a Uniform Resource Name namespace for UUIDs (Universally Unique IDentifier), also known as GUIDs (Globally Unique IDentifier). A UUID is 128 bits long, and requires no central registration process.
Reference	IETF RFC 4122: A Universally Unique IDentifier (UUID) URN Namespace, P. Leach, M. Mealling, & R. Salz, July 2005.
URL	www.ietf.org/rfc/rfc4122.txt
Responsible Organization/Contact	IETF Secretariat c/o Corporation for National Research Initiatives 1895 Preston White Drive, Suite 100 Reston, VA 20191-5434, USA Tel: +1 703 620 8990 Fax: +1 703 620 9071 Email: ietf-info@ietf.org
Related Standard(s)	ISO/IEC 11578:1996
Characteristics	
XRI Representation, meeting Common Core ID Requirements	Example of UUID using syntax indicating/claiming persistence: `xri://!!1000!1234.a1b2/!($uuid*6ba7b810-9dad-11d1-80b4-00c04fd430c8)`
Formats of Identifier (Canonical/Other)	128-bit value
Type of Identifier	Binary number
Related Identifier(s)/ Type(s) of Identifier(s)	No known alternatives or related competing definitions.
Uniqueness	Unique in space and time (statistically)
Persistence Characteristics	Valid through CY 3400.
Usage Scope	General
Mapping/Equivalence Checking (Canonical)	Per UUID specification IETF RFC 4122. Straight comparison of binary (128-bit) quantity.
How Generated	Standard algorithm which provides high probability of uniqueness.

How Recognized	Based on context and length comparison. Depends on agreed format and visual representation, per standards. Not able to ascertain by inspection alone unless it follows a specified scheme (e.g., IETF RFC 4122).
Analysis	
Context for Core	General Usage
Core/Non-core/Common Core	Core, but not Common Core.
Rationale	Core since unique and stable across time. Not common core due to non-compliance with related requirements. Possible to use as common core with XRI adornment.

4.13.2 UUID Pair

Description	
Classification Number	13.2
Identifier/Standard Name	URN Namespace: UUID Pair
Platform	General
Identifier/Standard Description	The idea of using pairs of UUIDs as common core identifiers has been proposed within The Open Group, but has not been standardized. [IETF RFC 4122] defines a URN namespace for a single UUID (not a pair).
Reference	N/A
URL	N/A
Responsible Organization/Contact	The Open Group 44 Montgomery St., Suite 960 San Francisco CA 94104-4704, USA Tel: +1 415 374 8280 Fax: +1 415 374 8293
Related Standard(s)	ISO/IEC 11578:1996 IETF RFC 4122
Characteristics	
XRI Representation, meeting Common Core ID Requirements	A canonical XRI representation of a UUID Pair has not yet been defined. Following is an example of such a form using syntax indicating/claiming persistence: `xri://!($uuidpair*6ba7b810-9dad-11d1-80b4-00c04fd430c8*5af6a709-8cfc-00c0-79a3-99b93ec329b7)`
Formats of Identifier (Canonical/Other)	2 x 128-bit values, separated by a defined delimiter
Type of Identifier	Binary number (UUID) pair, where the first UUID represents a source of authority for a subject, which is represented by the second UUID.
Related Identifier(s) Type(s) of Identifier(s)	No known alternatives or related competing definitions.
Uniqueness	Unique in space and time (statistically)
Persistence Characteristics	No UUID collisions through CY 3400 using the time-based format.
Usage Scope	General
Mapping/Equivalence Checking (Canonical)	Per UUID specification IETF RFC 4122. Straight comparison of binary (128-bit) quantity.

How Generated	Several standard algorithms which each provide high probability of uniqueness but varying degrees of privacy protection. CCID assumes (recommends) use of Time-Random Number approach.
How Recognized	Based on context and length comparison. Depends on agreed format and visual representation, per standards. Not able to ascertain by inspection alone. Could be recognized by a URI scheme or XRI $ type if either one is defined.

Analysis

Context for Core	General Usage
Core/Non-core/Common Core	Core, Common Core
Rationale	Core since unique and stable across time. Common core due to compliance with all requirements.

4.14 IRI

Description

Classification Number	14
Identifier/Standard Name	IRI
Platform	General
Identifier/Standard Description	Internationalized Resource Identifier IETF RFC 3987 defines a new protocol element, the Internationalized Resource Identifier (IRI), as a complement to the Uniform Resource Identifier (URI). An IRI is a sequence of characters from the Universal Character Set [UNICODE]. A mapping from IRIs to URIs is defined, which means that IRIs can be used instead of URIs, where appropriate, to identify resources.
Reference	IETF RFC 3987: Internationalized Resource Identifiers (IRIs), M. Duerst, & M. Suignard, January 2005. This document defines a new protocol element, the Internationalized Resource Identifier (IRI), as a complement to the Uniform Resource Identifier (URI).
URL	www.ietf.org/rfc/rfc3987.txt
Responsible Organization/Contact	IETF Secretariat c/o Corporation for National Research Initiatives 1895 Preston White Drive, Suite 100 Reston, VA 20191-5434, USA Tel: +1 703 620 8990 Fax: +1 703 620 9071 Email: ietf-info@ietf.org
Related Standard(s)	Uniform Resource Identifier, Uniform Resource Locator

Characteristics

XRI Representation, meeting Common Core ID Requirements	Any resource identified with an IRI may be represented using XRI cross-reference syntax. Following is an example of a persistent XRI that incorporates an HTTP IRI: `xri://!!1000!1234.a1b2/!(http://example.com/example/résumé)`

Formats of Identifier (Canonical/Other)	A Uniform Resource Identifier (URI) is defined in IETF RFC 3986 as a sequence of characters chosen from a limited subset of the repertoire of US-ASCII [ASCII] characters. IETF RFC 3987 defines a new protocol element called Internationalized Resource Identifier (IRI) by extending the syntax of URIs to a much wider repertoire of characters. It also defines "internationalized" versions corresponding to other constructs from IETF RFC3986, such as URI references.
Type of Identifier	Generalized/Internationalized Character String
Related Identifier(s)/ Type(s) of Identifier(s)	URI, XRI, all related specifications.
Uniqueness	Within registration scope.
Persistence Characteristics	Unlimited, depends on DNS systems.
Usage Scope	General
Mapping/Equivalence Checking (Canonical)	Case ignore string match to check equivalence between identifiers.
How Generated	Per RFC specification
How Recognized	Per RFC specification
Analysis	
Context for Core	General usage.
Core/Non-core/Common Core	Some schemes/namespaces meet requirements for core. Only specific schemes/namespaces, named below, meet all requirements for Common Core.
Rationale	Meets requirements for core identifiers. Some schemes/namespaces meet requirements for common core; see following elements.

4.14.1 Handle

Description	
Classification Number	14.1
Identifier/Standard Name	IRI Scheme: *hdl* (handle)
Platform	General
Identifier/Standard Description	The Handle System provides a confederated name service that allows any existing local namespace to join the global handle namespace by obtaining a unique Handle System naming authority. Local names and their value-binding(s) remain intact after joining the Handle System. Any handle request to the local namespace may be processed by a service interface speaking the Handle System protocol. Combined with the unique naming authority, any local name is guaranteed unique under the global handle namespace. The Handle System is a comprehensive system for assigning, managing, and resolving persistent identifiers, known as "handles", for digital objects and other resources on the Internet. Handles can be used as Uniform Resource Names (URNs).
Reference	The Handle System Introduction
URL	www.handle.net/introduction.html
Responsible Organization/Contact	Corporation for National Research Initiatives 1895 Preston White Drive Reston, Virginia 20191, USA Tel: +1 703 620 8990 Fax: +1 703 620 0913 Email: info@cnri.reston.va.us
Related Standard(s)	IRI
Characteristics	
XRI Representation, meeting Common Core ID Requirements	Although a canonical XRI representation of a Handle has not yet been defined, any resource identified using the *hdl* URI scheme may be represented using XRI cross-reference syntax. Following is an example of a persistent XRI that incorporates an *hdl* URI: `xri://!!1000!1234.a1b2/!(hdl:10.1045/april2006-paskin)`

Formats of Identifier (Canonical/Other)	Handles may consist of any printable characters from the Universal Character Set (UCS-2) of ISO/IEC 10646, which is the exact character set defined by Unicode v3.0 [UNICODE]. The UCS-2 character set encompasses most characters used in every major language written today. To allow compatibility with most of the existing systems and to prevent ambiguity among different encodings, the Handle System protocol mandates UTF-8 to be the only encoding used for handles.
Type of Identifier	UTF-8 Character String
Related Identifier(s)/ Type(s) of Identifier(s)	URI, XRI, IRI, all related specifications.
Uniqueness	Globally unique identifiers.
Persistence Characteristics	Unlimited, depends on Handle systems.
Usage Scope	General
Mapping/Equivalence Checking (Canonical)	Case ignore string match to check equivalence between identifiers.
How Generated	Per Handle System specification
How Recognized	Per Handle System specification
Analysis	
Context for Core	General usage
Core/Non-core/Common Core	Core, Common Core
Rationale	Meets all requirements for common core. Limited scope, not recommended.

4.14.2 Digital Object Identifier

Description	
Classification Number	14.2
Identifier/Standard Name	IRI Scheme: *doi* (digital object identifier)
Platform	General
Identifier/Standard Description	Digital Object Identifier The Digital Object Identifier (DOI) is a system which provides a mechanism to interoperably identify and exchange intellectual property in the digital environment. Based on the Handle System (see previous entry), DOI provides an extensible framework for managing intellectual content based on proven standards of digital object architecture and intellectual property management. It is an open system based on non-proprietary standards.
Reference	The DOI Handbook This Handbook is intended as a definitive reference to the DOI for the non-technical reader; a central point of reference for more complex technical content, through the appendices; and a means of providing updated information.
URL	www.doi.org/handbook_2000/intro.html
Responsible Organization/Contact	The International DOI Foundation
Related Standard(s)	IRI
Characteristics	
XRI Representation, meeting Common Core ID Requirements	Although a canonical XRI representation of a DOI has not yet been defined, any resource identified using the *doi* URI scheme may be represented using XRI cross-reference syntax. Following is an example of a persistent XRI that incorporates a DOI URI: `xri://!!1000!1234.a1b2/!(doi:10.1045/april2006-paskin)`

Formats of Identifier (Canonical/Other)	A DOI is an “opaque string” or “dumb number” – nothing at all can or should be inferred from the number in respect of its use in the DOI system. The DOI has two components, known as the prefix and the suffix. These are separated by a forward slash. The two components together form the DOI: 10.1000/123456. In this example, the prefix is “10.1000” and the suffix is “123456”. All DOIs start with “10”. This distinguishes a DOI from any other implementation of the Handle System. The next element of the prefix is the number (string) that is assigned to an organization that wishes to register DOIs. Following the prefix (separated by a forward slash) is a unique suffix (unique to a given prefix) to identify the entity. The combination of a prefix for the Registrant and unique suffix provided by the Registrant avoids any necessity for the centralized allocation of DOI numbers. The DOI suffix can be any alphanumeric string that the Registrant chooses.
Type of Identifier	Generalized/Internationalized Character String
Related Identifier(s)/ Type(s) of Identifier(s)	The DOI is structured as an IRI-HDL (Handle) namespace.
Uniqueness	Globally unique identifiers.
Persistence Characteristics	Unlimited, depends on Handle Systems.
Usage Scope	General
Mapping/Equivalence Checking (Canonical)	Case ignore string match to check equivalence between identifiers.
How Generated	Per Handle System specification and DOI Handbook
How Recognized	Per Handle System specification and DOI Handbook
Analysis	
Context for Core	General usage.
Core/Non-core/Common Core	Core, Common Core
Rationale	Meets all requirements for common core. Limited scope, not recommended.

4.14.3 Archive Resource Key

Description	
Classification Number	14.3
Identifier/Standard Name	IRI Scheme: *ark* (archive resource key)
Platform	General
Identifier/Standard Description	Archive Resource Key The Archival Resource Key (ARK) identifier is a naming scheme for persistent access to digital objects (including images, texts, data sets, and finding aids), currently being tested and implemented by the California Digital Library (CDL) for collections that it manages. The ARK naming scheme is designed to facilitate the high-quality and persistent identification of information objects. A founding principle of the ARK is that persistence is purely a matter of service and is neither inherent in an object nor conferred on it by a particular naming syntax. The best that an identifier can do is to lead users to the services that support persistence.
Reference	California Digital Library ARK is a proposal at this time, and has only limited usage.
URL	www.cdlib.org/inside/diglib/ark www.cdlib.org/inside/diglib/ark/arkspec.pdf
Responsible Organization/Contact	California Digital Library Office of the President University of California 415 20th Street, 4th Floor Oakland, CA 94612-2901, USA Tel: +1 510 987 0555, +1 510 987 0425 Fax: +1 510 893 5212 Email: cdl@www.cdlib.org
Related Standard(s)	IRI
Characteristics	
XRI Representation, meeting Common Core ID Requirements	Although a canonical XRI representation of an ARK has not yet been defined, any resource identified using the *ark* URI scheme may be represented using XRI cross-reference syntax. Following is an example of a persistent XRI that incorporates an ark URI: `xri://!!1000!1234.a1b2/!(ark:/12025/654xz321/s3/f8.05v.tiff)`

Formats of Identifier (Canonical/Other)	The term ARK itself refers both to the scheme and to any single identifier that conforms to it. An ARK has five components:
	`[http://NMAH/]`
	`ark:/NAAN/Name[Qualifier]`
	— An optional and mutable Name Mapping Authority Hostport
	— The "*ark*:" label
	— The Name Assigning Authority Number (NAAN)
	— The assigned Name
	— An optional and possibly mutable Qualifier supported by the NMA
	The NAAN and Name together form the immutable persistent identifier for the object. An ARK is a special kind of URL that connects users to three things: the named object, its metadata, and the provider's promise about its persistence.

Type of Identifier	An ARK is represented by a sequence of characters (a string) that contains the label "*ark*:", optionally preceded by the beginning part of a URL.
Related Identifier(s)/ Type(s) of Identifier(s)	URI, XRI, IRI, all related specifications.
Uniqueness	Within registration scope.
Persistence Characteristics	Based on service provider, essentially unlimited.
Usage Scope	General
Mapping/Equivalence Checking (Canonical)	Case ignore string match to check equivalence between identifiers.
How Generated	Per RFC draft specification
How Recognized	Per RFC draft specification
Analysis	
Context for Core	General usage.
Core/Non-core/Common Core	Core, Common Core
Rationale	Meets all requirements for common core. Limited scope, not recommended.

4.14.4 Persistent Uniform Resource Locator

Description	
Classification Number	14.4
Identifier/Standard Name	IRI Scheme: *purl http* (persistent uniform resource locator)
Platform	General
Identifier/Standard Description	OCLC Persistent URL The persistence requirement of URN schemes is not a technological issue so much as an outcome of the social structures that evolve to meet a common community need. OCLC's origin is deeply rooted in precisely this shared commitment to providing reliable, long-term access to information. Standardization is necessarily slow and deliberate. Putting all the pieces in place will require consensus in the IETF, developments in the community of web browser implementers, and deployment of new code by the community of network system managers who administer the Domain Name System (DNS) for the Internet. The concerns and problems of the library community may not be fully appreciated or adequately addressed by these groups in a timely manner. Libraries can and should provide leadership in the solution of these problems.
Reference	OCLC website PURL: Persistent Uniform Resource Locators
URL	purl.oclc.org/docs/new_purl_summary.html www.purl.org
Responsible Organization/Contact	OCLC Online Computer Library Center, Inc. 6565 Frantz Road Dublin, Ohio 43017-3395, USA Tel: +1 614 764 6000 Tel (toll-free): +1 800 848 5878 (USA & Canada only) Fax: +1 614 764 6096 Email: oclc@oclc.org
Related Standard(s)	IRI
Characteristics	
XRI Representation, meeting Common Core ID Requirements	PURL does not define a new URI scheme but uses the http scheme. Following is an example of a persistent XRI that incorporates a PURL http URI: `xri://!!1000!1234.a1b2/!(http://purl.oclc.org/OCLC/PURL/FAQ)`

Formats of Identifier (Canonical/Other)	To aid in the development and acceptance of URN technology, OCLC has deployed a naming and resolution service for general Internet resources. The names, which can be thought of as Persistent URLs (PURLs), can be used both in documents and in cataloging systems. PURLs increase the probability of correct resolution and thereby reduce the burden and expense of catalog maintenance. PURLs look like URLs (they are URLs). Functionally, a PURL is a URL. However, instead of pointing directly to the location of an Internet resource, a PURL points to an intermediate resolution service. The PURL resolution service associates the PURL with the actual URL and returns that URL to the client. The client can then complete the URL transaction in the normal fashion. In web parlance, this is a standard HTTP "redirect".
Type of Identifier	Generalized/Internationalized Character String
Related Identifier(s)/ Type(s) of Identifier(s)	URI, XRI, IRI, all related specifications.
Uniqueness	Within registration scope.
Persistence Characteristics	Based on service provider, essentially unlimited.
Usage Scope	General
Mapping/Equivalence Checking (Canonical)	Case ignore string match to check equivalence between identifiers.
How Generated	Per RFC specification
How Recognized	Per RFC specification
Analysis	
Context for Core	General usage.
Core/Non-core/Common Core	Core, Common Core
Rationale	Meets all requirements for common core. Limited scope, not recommended.

4.14.5 HTTP

Description	
Classification Number	14.5
Identifier/Standard Name	IRI Scheme: *http*
Platform	General
Identifier/Standard Description	ITEF RFC 2616: HTTP The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. It is a generic, stateless, protocol which can be used for many tasks beyond its use for hypertext, such as name servers and distributed object management systems, through extension of its request methods, error codes, and headers. The HTTP protocol defines the http URI scheme.
Reference	IETF RFC 2616: Hypertext Transfer Protocol – HTTP/1.1, R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee, June 1999.
URL	www.ietf.org/rfc/rfc2616.txt
Responsible Organization/Contact	IETF Secretariat c/o Corporation for National Research Initiatives 1895 Preston White Drive, Suite 100 Reston, VA 20191-5434, USA Tel: +1 703 620 8990 Fax: +1 703 620 9071 Email: ietf-info@ietf.org
Related Standard(s)	IRI
Characteristics	
XRI Representation, meeting Common Core ID Requirements	Although a canonical XRI representation of an *http* URI has not yet been defined, any resource identified using the *http* URI scheme may be represented using XRI cross-reference syntax. Following is an example of a persistent XRI that incorporates an *http* URI: `xri://!!1000!1234.a1b2/!(http://example.com/example/resource?id=247)`
Formats of Identifier (Canonical/Other)	HTTP URIs – commonly known as URLs (Uniform Resource Locators), although this term is now deprecated by the W3C – are a URI scheme (IETF RFC 3986) defined by the HTTP protocol specification (IETF RFC 2616).
Type of Identifier	Generalized/Internationalized Character String
Related Identifier(s)/ Type(s) of Identifier(s)	URI, XRI, IRI, all related specifications.

Uniqueness	Globally unique identifiers.
Persistence Characteristics	Unspecified, thus based on service provider, essentially unlimited.
Usage Scope	General
Mapping/Equivalence Checking (Canonical)	Per RFC
How Generated	Per RFC specification
How Recognized	Per RFC specification
Analysis	
Context for Core	General usage.
Core/Non-core/Common Core	Core
Rationale	Meets all requirements for common core except persistence over time. Protocol binding with no specified persistence, not recommended.

4.14.6 HTTPS

Description	
Classification Number	14.6
Identifier/Standard Name	IRI Scheme: *https*
Platform	General
Identifier/Standard Description	IETF RFC 2818: HTTPS This memo describes how to use TLS to secure HTTP connections over the Internet. Current practice is to layer HTTP over SSL (the predecessor to TLS), distinguishing secured traffic from insecure traffic by the use of a different server port. This document documents that practice using TLS.
Reference	IETF RFC 2818: HTTP over TLS, E. Rescorla; May 2000.
URL	www.ietf.org/rfc/rfc2818.txt
Responsible Organization/Contact	IETF Secretariat c/o Corporation for National Research Initiatives 1895 Preston White Drive, Suite 100 Reston, VA 20191-5434, USA Tel: +1 703 620 8990 Fax: +1 703 620 9071 Email: ietf-info@ietf.org
Related Standard(s)	IRI
Characteristics	
XRI Representation, meeting Common Core ID Requirements	Although a canonical XRI representation of an *https* URI has not yet been defined, any resource identified using the *https* URI scheme may be represented using XRI cross-reference syntax. Following is an example of a persistent XRI that incorporates an *https* URI: `xri://!!1000!1234.a1b2/!(https://example.com/example/resource?id=247)`
Formats of Identifier (Canonical/Other)	Identical to the HTTP scheme except for the use of *https* as the scheme identifier.
Type of Identifier	Generalized/Internationalized Character String
Related Identifier(s)/ Type(s) of Identifier(s)	URI, XRI, IRI, all related specifications.
Uniqueness	Globally unique identifiers.
Persistence Characteristics	Based on service provider, essentially unlimited.
Usage Scope	General
Mapping/Equivalence Checking (Canonical)	Per RFC

How Generated	Per RFC specification
How Recognized	Per RFC specification
Analysis	
Context for Core	General usage.
Core/Non-core/Common Core	Core
Rationale	Meets all requirements for common core except persistence over time. Protocol binding with no specified persistence, not recommended.

4.15 User Principal Name (UPN)

Description	
Classification Number	15
Identifier/Standard Name	User Principal Name (UPN)
Platform	Windows (Active Directory)
Identifier/Standard Description	Microsoft User Principal Name A logon name type of a user on a Windows 2000 or Windows Server 2003 network. The user principal name consists of the user object name used in Active Directory, followed by the at (`@`) symbol and then, typically, the Domain Name System parent domain. For example, `Jeff Smith` in the `Fabrikam.com` domain tree might have the user principal name `jeffsmith@fabrikam.com`.
Reference	Microsoft MSDN Library
URL	msdn.microsoft.com/library/default.asp?url=/library/en-us/dsglossary/adsi/u.asp
Responsible Organization/Contact	Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399, USA Tel: +1 800 642 7676
Related Standard(s)	DNS, Kerberos, pkix, X.509
Characteristics	
XRI Representation, meeting Common Core ID Requirements	No recommended form is available; at present there is no strong incentive to specify this format.
Formats of Identifier (Canonical/Other)	Per IETF RFC 822
Type of Identifier	Fully qualified logon name. The UPN suffix by default represents the Windows domain and Kerberos realm that "owns" the security principal account. If the UPN is abstracted to an arbitrary namespace, then the UPN must be resolved in the Active Directory Global Catalog to determine the actual domain/realm. UPN is almost never the same as the email name and does not have the same meaning in any case.
Related Identifier(s)/ Type(s) of Identifier(s)	Related to Kerberos Name, also related GSS-API Subject Name, and to SSPI Subject Name. These are not exact equivalences, however.
Uniqueness	Globally unique by default.

Persistence Characteristics	Limited. By default, UPN is stable as long as the security principal account is not relocated to another domain. If the UPN suffix is abstracted to an arbitrary namespace, then UPN does not change with account relocation but requires Global Catalog resolution to determine actual domain/realm.
Usage Scope	Within an Active Directory forest under all circumstances. Across forest boundaries as long as UPN suffix default is used. Throughout any WS-Federation-based trust fabric.
Mapping/Equivalence Checking (Canonical)	Case ignore string match to check equivalence between identifiers.
How Generated	By default, UPN is system-generated as the concatenation of operating system user name, and "@" delimiter, and the fully-qualified domain name of the account domain in which the account is created.
How Recognized	By local system.
Analysis	
Context for Core	MS Systems
Core/Non-core/Common Core	Core
Rationale	Proprietary, lack of persistence, re-assignability, etc. Not common core due to limited domain.

4.16 ObjectGUID

Description	
Classification Number	16
Identifier/Standard Name	ObjectGUID
Platform	Windows (Active Directory)
Identifier/Standard Description	Object-Guid: The unique identifier for an object.
Reference	Microsoft MSDN Library
URL	msdn.microsoft.com/library/default.asp?url=/library/en-us/adschema/adschema/a_objectguid.asp
Responsible Organization/Contact	Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399, USA Tel: +1 800 642 7676
Related Standard(s)	[IETF RFC 4122]
Characteristics	
XRI Representation, meeting Common Core ID Requirements	No recommended form is available; at present there is no strong incentive to specify this format.
Formats of Identifier (Canonical/Other)	Per IETF RFC 4122
Type of Identifier	Stable, unambiguous object reference in Active Directory
Related Identifier(s)/ Type(s) of Identifier(s)	UUID
Uniqueness	Globally unique
Persistence Characteristics	Valid through CY 3400.
Usage Scope	MS systems
Mapping/Equivalence Checking (Canonical)	N/A
How Generated	MS AD
How Recognized	MS AD
Analysis	
Context for Core	MS Systems
Core/Non-core/Common Core	Non-core
Rationale	Same as UUID.

4.17 Security Identifier (SID)

Description	
Classification Number	17
Identifier/Standard Name	Security Identifier (SID)
Platform	Windows (Active Directory)
Identifier/Standard Description	Microsoft Security Identifier (SID) A data structure of variable length that uniquely identifies user, group, service, and computer accounts within a forest. Every account is issued a SID when the account is first created. Access control mechanisms in Windows 2000 identify security principals by SID rather than by name.
Reference	Exchange 2000 Server Resource Kit
URL	www.microsoft.com/technet/prodtechnol/exchange/2000/library/reskit/part5/c23host.mspx
Responsible Organization/Contact	Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399, USA Tel: +1 800 642 7676
Related Standard(s)	None identified.
Characteristics	
XRI Representation, meeting Common Core ID Requirements	No recommended form is available; at present there is no strong incentive to specify this format.
Formats of Identifier (Canonical/Other)	N/A
Type of Identifier	N/A
Related Identifier(s)/ Type(s) of Identifier(s)	N/A
Uniqueness	Unique within scope of domain.
Persistence Characteristics	Per MS
Usage Scope	MS Systems
Mapping/Equivalence Checking (Canonical)	Per MS
How Generated	Per MS
How Recognized	Per MS
Analysis	
Context for Core	MS Systems
Core/Non-core/Common Core	Non-core

Rationale	Proprietary

4.18 UID

Description	
Classification Number	18
Identifier/Standard Name	UID
Platform	UNIX or POSIX operating systems
Identifier/Standard Description	User ID A non-negative integer that is used to identify a system user. When the identity of a user is associated with a process, a user ID value is referred to as a real user ID, an effective user ID, or a saved set-user-ID.
Reference	The Single UNIX Specification, Version 3; **<sys/types.h>**, *getuid*(), *setuid*(), et al.
URL	www.unix.org/version3
Responsible Organization/Contact	The Open Group 44 Montgomery St., Suite 960 San Francisco CA 94104-4704, USA Tel: +1 415 374 8280 Fax: +1 415 374 8293
Related Standard(s)	POSIX, Linux
Characteristics	
XRI Representation, meeting Common Core ID Requirements	No recommended form is available; at present there is no strong incentive to specify this format.
Formats of Identifier (Canonical/Other)	Binary number
Type of Identifier	UID is a non-negative 32-bit integer
Related Identifier(s)/ Type(s) of Identifier(s)	In common usage, UID is mapped to UNIX *username*. Username is used for human/machine interactions and UID is used for machine/machine interactions.
Uniqueness	Unique only within scope of identity management implementation; e.g., for standalone systems UID is unique within that system. For a NIS or NIS+ system, UID is unique within a NIS domain for all systems within that domain.
Persistence Characteristics	UID is used to map security principals to resource policy in Access Control Lists (ACLs) or to groups. There is no referential integrity for UIDs in ACLs or groups. UIDs persist for the life of an account within a system. Best practice requires that UIDs not be re-assigned for the life of the system unless some mechanism of re-ACL'ing is put in place to reconcile deletions/re-assignments for all groups and resources within the system.

Usage Scope	See “Uniqueness”.
Mapping/Equivalence Checking (Canonical)	Bitwise comparison.
How Generated	UID is serially assigned within some arbitrarily assigned range. Generally, there is little or no system assistance in assuring non-duplication unless supported by an external provisioning system.
How Recognized	UID is recognized by the context in which it is used in administrative tools, APIs, and protocols.
Analysis	
Context for Core	UNIX or Linux operating systems
Core/Non-core/Common Core	UID is a core identifier with UNIX or Linux operating systems. Core, but not Common Core.
Rationale	Meets requirements for core identifiers. Not common core because it is system-specific, not interoperable across systems.

4.19 GID

Description	
Classification Number	19
Identifier/Standard Name	GID
Platform	UNIX or POSIX operating systems
Identifier/Standard Description	Group ID A non-negative integer, which can be contained in an object of type **gid_t**, that is used to identify a group of system users. Each system user is a member of at least one group. When the identity of a group is associated with a process, a group ID value is referred to as a real group ID, an effective group ID, one of the supplementary group IDs, or a saved set-group-ID.
Reference	The Single UNIX Specification, Version 3: **<sys/types.h>**, *getgid*(), *setgid*(), et al.
URL	www.unix.org/version3
Responsible Organization/Contact	The Open Group 44 Montgomery St., Suite 960 San Francisco CA 94104-4704, USA Tel: +1 415 374 8280 Fax: +1 415 374 8293
Related Standard(s)	POSIX, Linux
Characteristics	
XRI Representation, meeting Common Core ID Requirements	No recommended form is available; at present there is no strong incentive to specify this format.
Formats of Identifier (Canonical/Other)	Binary number
Type of Identifier	GID is a non-negative 32-bit integer.
Related Identifier(s)/ Type(s) of Identifier(s)	In common usage, GID is mapped to UNIX *groupname*. Group name is used for human/machine interactions and UID is used for machine/machine interactions.
Uniqueness	Unique only within scope of identity management implementation; e.g., for standalone systems GID is unique within that system. For a NIS or NIS+ system, GID is unique within a NIS domain for all systems within that domain.

Persistence Characteristics	GID is used to map groups of security principals to resource policy in Access Control Lists (ACLs) or to other groups. There is no referential integrity for GIDs in ACLs or groups. GIDs persist for the life of an account within a system. Best practice requires that GIDs not be re-assigned for the life of the system unless some mechanism of re-ACL'ing is put in place to reconcile deletions/re-assignments for all groups and resources in the system.
Usage Scope	See "Uniqueness".
Mapping/Equivalence Checking (Canonical)	Bitwise comparison.
How Generated	GID is serially assigned within some arbitrarily assigned range. Generally, there is little or no system assistance in assuring non-duplication unless supported by an external provisioning system.
How Recognized	GID is recognized by the context in which it is used in administrative tools, APIs, and protocols.
Analysis	
Context for Core	UNIX or Linux operating systems
Core/Non-core/Common Core	GID is a core identifier with UNIX or Linux operating systems. Core, not Common Core.
Rationale	Meets requirements for core identifiers. Not common core because it is system-specific, not interoperable across systems.

4.20 International Mobile Subscriber Identity (IMSI)

Description

Classification Number	20
Identifier/Standard Name	International Mobile Subscriber Identity (IMSI)
Platform	Mobile Telephony (GSM/UMTS)
Identifier/Standard Description	An international identification plan for mobile terminals or mobile users of public networks enabling roaming capabilities.
Reference	ITU-T Recommendation E.212
URL	www.itu.int/ITU-T/publications/recs.html
Responsible Organization/Contact	ITU Place des Nations CH-1211 Geneva 20 Switzerland Tel: +41 22 730 51 11 Fax: +41 22 730 65 00
Related Standard(s)	None

Characteristics

XRI Representation, meeting Common Core ID Requirements	No recommended form is available; at present there is no strong incentive to specify this format.
Formats of Identifier (Canonical/Other)	A decimal number of up to 15 digits. The first 3 digits are the Mobile Country Code (MCC) followed by a 2 or 3-digit (depending on the country) Mobile Network Code (MNC). The remainder of the numbers up to the maximum length is the Mobile Subscriber Identification Number (MSIN).
Type of Identifier	String of decimal digits, maximum length 15 digits.
Related Identifier(s)/ Type(s) of Identifier(s)	International Mobile Equipment Identifier (IMEI) is a similar number which uniquely identifies a GSM or UMTS handset device (the association between IMEI and IMSI will change if the SIM is removed from one device and put in another).
Uniqueness	Globally unique for all GSM and UMTS mobile phone subscribers. Currently around 2bn IMSIs are in use.
Persistence Characteristics	Not specified.
Usage Scope	See “Uniqueness”.
Mapping/Equivalence Checking (Canonical)	String comparison.

How Generated	MCC is defined by E.212. MNC is allocated by national telecommunications regulators. MSIN is allocated by the network operator.
How Recognized	In context of mobile phone transmissions.
Analysis	
Context for Core	Mobile telephone systems
Core/Non-core/Common Core	Core, but not Common Core.
Rationale	Meets requirements for core identifiers. Not common core because it is system-specific, not interoperable across systems.

5 Conclusions and Recommendations

5.1 Conclusions

Examination of the Core Identifier Framework Matrix supports the following conclusions:

1. Many identifier forms can be appropriately mapped to the Extensible Resource Identifier (XRI), reinforcing the suitability of XRI as the common identifier form.

2. There are two specifications that could be appropriate for the global common core identifier form, as they fully satisfy the requirements that the Core Identifier Work Group has identified. These are:

    a. Certain forms of the XRI, which is being developed in the XRI TC at OASIS. Generally, XRI identifier forms meet the requirements for common core identifiers, except for the requirements for persistence and for uniquely indicating the issuing authority. These two requirements can be met through use of appropriate XRI constructs. Some specific forms that meet the requirements are indicated in the matrix.

    b. The UUID Pair, which is not currently the subject of formal standardization activity.

3. There are several other standards related to IRI schemes and URN namespaces that satisfy the requirement for common core identifiers. The primary reason that the Core Identifier Work Group does not recommend these identifiers for general use is that they are linked in one way or another with particular user groups, usage domains, or protocols, and thus are not directed at general/universal usage. The Core Identifier Work Group has concluded that universal usage is the most appropriate domain for common core identifiers, making this limitation significant.

5.2 Recommendations

The above conclusions lead directly to the following recommendations:

1. Reference mappings of existing identifier forms to XRI should be documented and published as standards. Appropriate bodies to carry out this work include The Open Group, the NAC, the IETF, and OASIS.

2. Further work should be undertaken to select a particular identifier form as the global common core identifier. This work should:

    a. Be conducted in large part by the vendors of products that will use common core identifiers

    b. Include pilot implementations, in line with normal open standards practices

3. Make contact with appropriate standards groups to seek support for the Core Identifier Work Group conclusions and recommendations, and be endorsed through the Sponsoring Consortia (the Distributed Management Task Force (DMTF), the Network Applications Consortium (NAC), and The Open Group).

A Mapping of Identifiers to Requirements

A.1 Introduction

This appendix provides a detailed analysis of how the identifier forms identified in Chapter 4 map to the requirements identified in Chapter 3. The reader should review appropriate standards sections (e.g., Section 4.16, Object GUID) to gain an understanding of the rationale for the classification assigned to each identifier.

The core/common core identifier requirements are listed here, with brief reference titles appended. These titles are repeated in the table as references to the full requirement statement.

Core identifiers must:

No.	Title	Requirement Description (from Chapter 3)
1	Portability	Be portable – able to be issued by one organization and used by others, based on cross-organization standards.
2	Name Form	Have a clear, unambiguous name form.
3	Identity Only	Convey no meaning other than that they identify someone or something; there should be no need to parse names.
4	Free of Constraints	Impose no constraints on directory namespace.
5	De-Centralized Authority	Be easily generated without reliance on complex interactions with some central authority.
6	Free of Language Link	Not be tied to any language or cultural environment.
7	Flexibility	Be flexible enough to accommodate different business models.
8	SSO Integration	Be able to be integrated into single sign-on systems where security and privacy of the identifier information is critical.
9	Representation	Allow for the fact that an individual is usually represented by some authority that holds sway over him – his credit card company, government, etc.
10	Compatibility	Be compatible with federated identity standards.
11	Generality	Be applicable to things as well as to people – anything that needs to be subject to access control policy, not just a person, can be a security principal.
12	Applicability	Be applicable to groups as well as to individuals.
13	Anonymity	Allow for anonymity – there is a need for "friendly handles" that can be used to refer to people in transactions without revealing their real identities; anonymity can be a requirement in some cases.

No.	Title	Requirement Description (from Chapter 3)
14	Efficiency	Provide for processing efficiency (for example, fixed-length identifiers are more efficient in some situations).

Common core identifiers must, in addition:

No.	Title	Requirement Description (from Chapter 3)
1	Persistence	Be persistent over time.
2	Uniqueness	Uniquely distinguish an entity within a global scope.
3	Authority	Uniquely distinguish the issuing authority, which is within the same scope.
4	Representation	Be capable of representation in common identifier form syntax.
5	Interoperability	Be assured of interoperability among domains or systems, according to agreed standards and related policy.

The analysis is carried out in a tabular format that places the requirements across the top and the protocols down the left side of the table. Each table cell contains one of four items:

- Yes – for situations where the identifier clearly *does* satisfy the requirement.
- No – for situations where the identifier clearly *does not* satisfy the requirement.
- Yes or No with a number – the number identifies a note giving rationale that is required to make the situation clear. The rationale statements follow the table, in numeric order.
- Blank – for situations that have not been evaluated.

In the following table, a single "No" is enough to disqualify an identifier standard for Core/Common Core status. Thus, the analysis for each protocol stops when the first "No" is entered, starting from the left side of the table, and further cells are not evaluated. Note that the Core Identifier Work Group recommends a specific subset of all the possible common core identifiers for further development.

A.2 Analysis Table of Core Identifier Requirements

(Bold indicates recommended common core identifiers.)

Count	Classification	Characteristic	Portability	Name Form	Identity Only	Free of Constraints	De-Centralized Authority
	No.	Standard	1	2	3	4	5
1	4.1	OS User Name	Yes	Yes	Yes	Yes	Yes
2	4.2	Email Address	Yes	Yes	Yes	Yes	Yes
3	4.3	X.500 Distinguished Name	Yes	Yes	Yes	No	
4	4.4	Domain Component Name	Yes	Yes	Yes	No	
5	4.5	SPKI/SDSI Name	No[1]				
6	4.6	DCE Name	Yes	Yes	Yes	Yes	Yes
7	4.7	HIT	Yes	Yes	Yes	Yes	Yes
8	4.8	Universal Identifier	Yes	Yes	Yes	No	
9	4.9	IUID	Yes	Yes	Yes	No	
10	4.10	RFID	No				
11	4.11	URI	Yes	Yes	Yes	Yes	Yes
12	4.12	XRI	Yes	Yes	Yes	Yes	Yes
13	4.13	URN	Yes	Yes	Yes	Yes	Yes
14	4.13.1	URN: UUID/GUID	Yes	Yes	Yes	Yes	No
15	4.13.2	URN: UUID Pair	Yes	Yes	Yes	Yes	Yes
16	4.14	IRI	Yes	Yes	Yes	Yes	Yes
17	4.14.1	IRI Scheme: *hdl*	Yes	Yes	Yes	Yes	Yes
18	4.14.2	IRI Scheme: *doi*	Yes	Yes	Yes	Yes	Yes
19	4.14.3	IRI Scheme: *ark*	Yes	Yes	Yes	Yes	Yes
20	4.14.4	IRI Scheme: *purl*	Yes	Yes	Yes	Yes	Yes
21	4.14.5	IRI Scheme: HTTP	Yes	Yes	Yes	Yes	Yes
22	4.14.6	IRI Scheme: HTTPS	Yes	Yes	Yes	Yes	Yes
23	4.15	User Principal Name (UPN)	No				
24	4.16	ObjectGUID	Yes	Yes	Yes	Yes	No

Count	Classification	Characteristic	Portability	Name Form	Identity Only	Free of Constraints	De-Centralized Authority
25	4.17	Security Identifier (SID)	No				
26	4.18	UID	No				
27	4.19	GID	No				
28	4.20	IMSI	No				

Count	Classification	Characteristic	Free of Language Link	Flexibility	SSO Integration	Representation	Compatibility
	No.	Standard	6	7	8	9	10
1	4.1	OS User Name	Yes	Yes	Yes	Yes	Yes
2	4.2	Email Address	Yes	Yes	Yes	Yes	Yes
3	4.3	X.500 Distinguished Name					
4	4.4	Domain Component Name					
5	4.5	SPKI/SDSI Name					
6	4.6	DCE Name	Yes	Yes	Yes	Yes	Yes
7	4.7	HIT	Yes	Yes	Yes	Yes	Yes
8	4.8	Universal Identifier					
9	4.9	IUID					
10	4.10	RFID					
11	4.11	URI	Yes	Yes	Yes	Yes	Yes
12	4.12	XRI	Yes	Yes	Yes	Yes	Yes
13	4.13	URN	Yes	Yes	Yes	Yes	Yes
14	4.13.1	URN: UUID/GUID	Yes	Yes	Yes	Yes	Yes
15	4.13.2	URN: UUID Pair	Yes	Yes	Yes	Yes	Yes
16	4.14	IRI	Yes	Yes	Yes	Yes	Yes
17	4.14.1	IRI Scheme: *hdl*	Yes	Yes	Yes	Yes	Yes

Count	Classification	Characteristic	Free of Language Link	Flexibility	SSO Integration	Representation	Compatibility
18	4.14.2	IRI Scheme: *doi*	Yes	Yes	Yes	Yes	Yes
19	4.14.3	IRI Scheme: *ark*	Yes	Yes	Yes	Yes	Yes
20	4.14.4	IRI Scheme: *purl*	Yes	Yes	Yes	Yes	Yes
21	4.14.5	IRI Scheme: HTTP	Yes	Yes	Yes	Yes	Yes
22	4.14.6	IRI Scheme: HTTPS	Yes	Yes	Yes	Yes	Yes
23	4.15	User Principal Name (UPN)					
24	4.16	ObjectGUID					
25	4.17	Security Identifier (SID)					
26	4.18	UID					
27	4.19	GID					
28	4.20	IMSI					

A.3 Analysis Table of Common Core Identifier Requirements

(Bold indicates recommended common core identifiers.)

Count	Classification	Characteristic	Common Core Persistence	Common Core Uniqueness	Common Core Authority	Common Core Representation	Common Core Interoperability
	No.	Standard	15	16	17	18	19
1	4.1	OS User Name	No	No	No	No	No
2	4.2	Email Address	No	No	No	No	No
3	4.3	X.500 Distinguished Name	No	No	No	No	No
4	4.4	Domain Component Name	No	No	No	No	No
5	4.5	SPKI/SDSI Name					
6	4.6	DCE Name	Yes	Yes	Yes	No	No
7	4.7	HIT	Yes	Yes	No		
8	4.8	Universal Identifier	Yes	Yes	No		
9	4.9	IUID					
10	4.10	RFID					
11	4.11	URI					
12	4.12	XRI	Yes	Yes	Yes	Yes	Yes
13	4.13	URN	Yes[3]	Yes[3]	Yes[3]	Yes[3]	Yes[3]
14	4.13.1	URN: UUID/GUID	Yes	Yes	No	No	No
15	4.13.2	URN: UUID Pair	Yes	Yes	Yes	Yes	Yes
16	4.14	IRI	Yes[3]	Yes[3]	Yes[3]	Yes[3]	Yes[3]
17	4.14.1	IRI Scheme: *hdl*	Yes[3]	Yes[3]	Yes[3]	Yes[3]	Yes[3]
18	4.14.2	IRI Scheme: *doi*	Yes[3]	Yes[3]	Yes[3]	Yes[3]	Yes[3]
19	4.14.3	IRI Scheme: *ark*	Yes[3]	Yes[3]	Yes[3]	Yes[3]	Yes[3]
20	4.14.4	IRI Scheme: *purl*	Yes[3]	Yes[3]	Yes[3]	Yes[3]	Yes[3]
21	4.14.5	IRI Scheme: HTTP	No	No			
22	4.14.6	IRI Scheme: HTTPS	No	No			
23	4.15	User Principal Name (UPN)					No
24	4.16	ObjectGUID			No	No	No

Count	Classification	Characteristic	Common Core Persistence	Common Core Uniqueness	Common Core Authority	Common Core Representation	Common Core Interoperability
25	4.17	Security Identifier (SID)					No
26	4.18	UID					No
27	4.19	GID					No
28	4.20	IMSI					No

A.4 Notes to the Tables

1. SPKI/SDSI Name is deprecated due to inactivity.

2. URI and IRI form a framework for identifier schemes or namespaces, and are not specific identifiers, themselves. Certain schemes, as noted, fulfill all requirements for common core identifiers.

3. This is a scheme or namespace within the URI/IRI context. It meets common core requirements, but is not recommended due to linkage with particular user groups, usage domains, and protocols, and thus it is not directed at general/universal usage. The Core Identifier Work Group has concluded that universal usage is the most appropriate domain for common core identifiers, making this limitation significant.