Core Identifiers Framework Document

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

Management Summary

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 describes the documentary framework. Its purpose is to:

- Provide a common understanding of identifiers, removing confusion;
- Describe guidelines, algorithms, and common semantics;
- Be a reference point for identifier classifications and how they are used; and
- Enable simplification over time.

It is accompanied by a Framework Matrix that lists standards related to identifiers, and classifies them in relation to the requirements and to each other. The Framework Matrix is described in the final section of this document.

Table of Contents

Context

The Open Group - Identity Management Whitepaper [IDMWP] (p. 66):

> There is a compelling need for a set of standards for specifying and exchanging a core identifier.

Definitions

Core Identifier (paraphrased from Open Group - Identity Management Whitepaper [IDMWP], p. 40):

> A core identifier is that essential quality or description, which uniquely and unambiguously identifies a thing or a person within a defined and agreed context.

Common Core Identifier

> A common core identifier is a specific core identifier that is assured of interoperability among domains or systems, according to agreed standards and related policy.

That is; the "core" concept relates to an identifier that has the irreducible minimum of attributes, sufficient to distinguish its subject within the scope of a naming / issuing authority, however that authority may be only implicit and not specifically identified. A "common core" identifier is a core identifier that can be used between different organizations according to agreed industry standards and related policy. It identifies the scope and context within which it is valid, as well as the naming / issuing authority. Thus, it is a core identifier which fulfills interoperability requirements.

Corollary Questions

Is there such a thing as a core identity / core identifier / common core identifier?
If there are such things, what are they and how are they described?

Position Statement

The Core Identifier workgroup, sponsored by The Open Group [OG], The Distributed Management TaskForce [DMTF], and the Network Applications Consortium [NAC], after extended analysis, discussion, and some disagreements, asserts that the concepts of core identifier and common core identifier are valid, as defined.

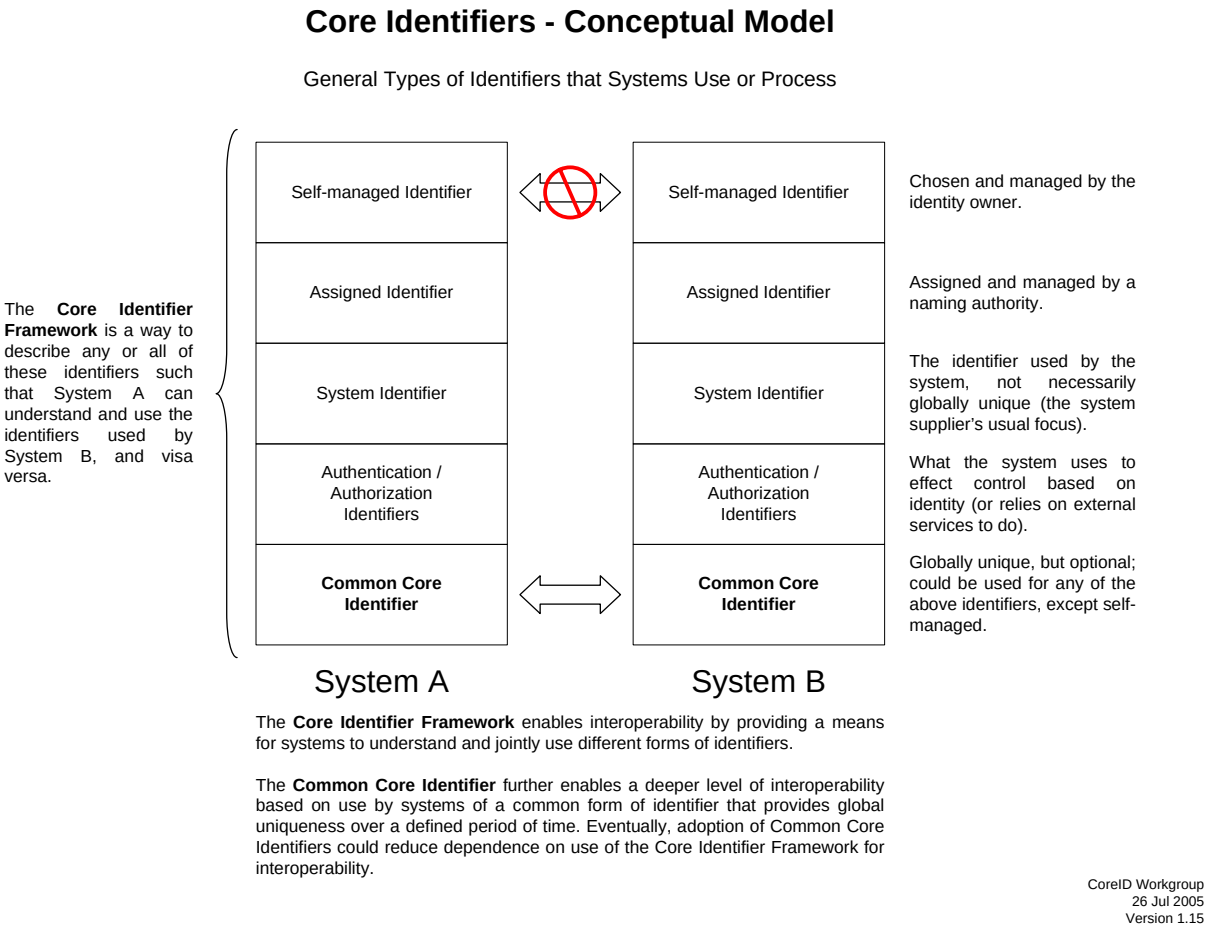
That said, the workgroup also takes the position that there is no one, single core identifier; rather there is a set of core identifiers, which are related to one another. This multiplicity of core identifiers is a necessary result of the mutually exclusive requirements applicable to core identifiers. The group has completed analysis to show that some of these core identifiers are or can be constructed to be common core identifiers, which, by definition, support interoperability among systems across management domains, in conformance with published (de jure / defacto) standards. Thus, the group has fulfilled one of its major objectives.

Business Scenario

The Business Scenario [CIDSCEN] provides a mechanism for discussion of new ideas that is based on easily understandable concepts, and that supports readily comprehensible value statements. In this instance, such ideas and statements are related to identifiers.

Conceptual Model

The following diagram presents the Workgroup's conceptual model for core identifiers:



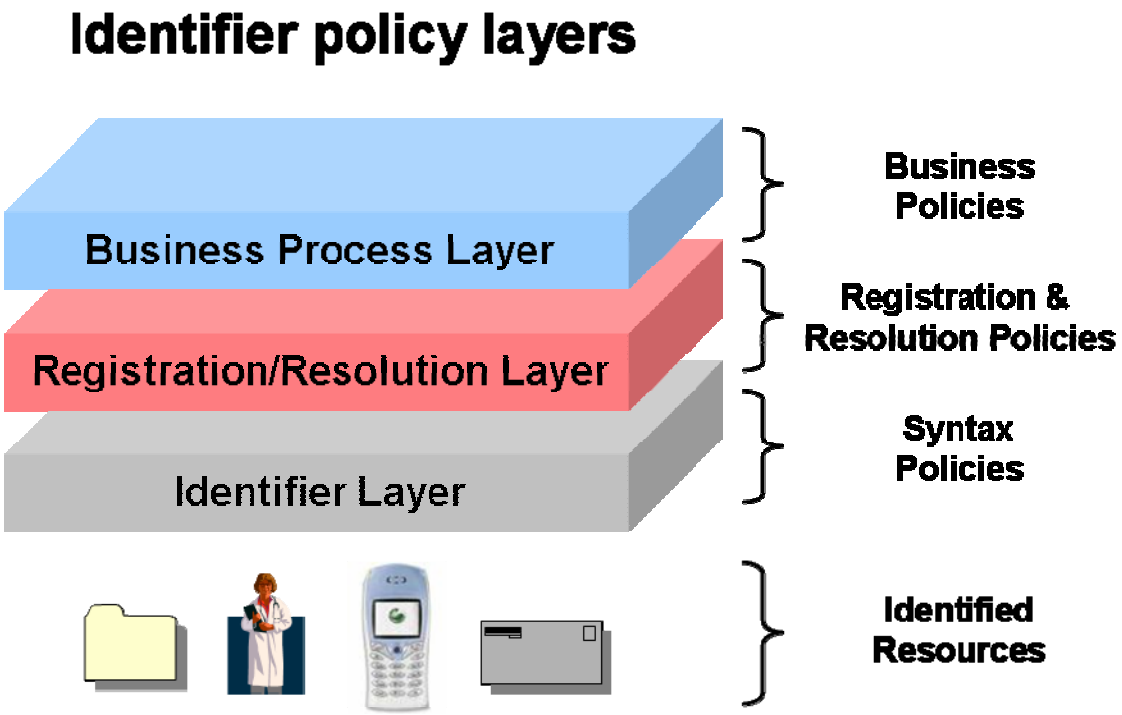
Structural Model

In the structural model for identifiers agreed within the Workgroup, there are three types of policy related to identifiers; Business, Registration & Resolution, and Syntax.

- Business policies for resource identification exist to support other higher-level business policies, e.g., security policies, privacy policies, administrative policies, and the like.
  Examples:
  - Parts MUST be tracked for the lifetime of the part.
  - Principals accessing the intranet MUST be authenticated.
  - Out-of-stock part lists MUST be shared with distributors confidentially.
- Identifier registration & resolution policies are required to support the business policies. They establish the requirements for relating an identifier to: a) an entity or resource, b) metadata describing the entity / resource, or c) other identifiers.
  Examples:
  - The identifier of a part MUST NOT change.
  - An employee MUST be listed in the company directory but MAY change their listed name.
  - A network username MUST have X credential.
  - A filename MUST be [globally/locally] resolvable.
- Identifier syntax policies exist to support identifier registration and resolution policies. In addition, they are necessary for technical and social interoperability and usage.
  Examples:
  - MUST NOT exceed X characters
  - MUST NOT include Y characters

- [MUST/MUST NOT] support delegation
- [MUST/MUST NOT] be [persistent/human-friendly]

The following diagram presents the structural model the Workgroup described above. The Workgroup has used this model in analyzing identifiers and their relationship to the standards identified in the Framework Matrix, described below.



Given knowledge of the business requirements, as described in the Business Scenario, the Workgroup has identified use cases and related business policy requirements for identifiers. This information is basic to the analysis process leading to definition of identifier requirements, given below, and to identification of a set of common core identifiers and related standards.

The results of our analysis are embodied in the framework matrix.

Requirements

The Core Identifier workgroup has agreed on a set of requirements for the core identifier framework and related core identifiers (Business Scenario [CIDSCEN] – Requirements). The requirements set is included here in its entirety to ensure completeness, and to assist in understanding the position and actions recommended later in this paper, and to support the analysis presented in the Framework Matrix.

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.

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 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, and
    e. Identifiers that support specific requirements, e.g., HIP identifiers for Secure Mobile Architecture;
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;
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 can not be guaranteed (for example, it may have been issued by a company that has gone out of business and no longer exists); and
    b. it must be possible to control the amount of information about the subject that can be discovered;
8. Be portable – able to be 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).

Common Core Identifiers

These 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;
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 always represented by some authority that holds sway over him - 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 those people's real identities being revealed - anonymity can be a requirement in some cases;
14. Provide for processing efficiency (for example, fixed length identifiers are more efficient in some situations)
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; and
19. Be assured of interoperability among domains or systems, according to agreed standards and related policy.

Requirements 1-14 apply to all core identifiers. Requirements 15-19 apply in addition specifically to common core identifiers.

The definition of common core identifiers should leverage existing technology where feasible.
Fixed length would be a desirable characteristic.

Additional requirements for the framework and core identifiers may be defined at any time. Such requirements will be added to the list above when they are identified and approved.

Framework Matrix

The framework matrix introduced in this section lists known dejure and defacto standards that are related to identifiers. Further, it classifies them in relationship to the requirements outlined earlier and to each other. The classification presented in the matrix is the final result of our analysis using the requirements and models identified earlier in this paper. The analysis and resulting classification form the essential steps leading to our joint position concerning the identified common core identifiers in the matrix.
This approach has a number of objectives:

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

The Core Identifier workgroup expects and anticipates that publication and review of this Framework Matrix will clarify the existence and relationships among standards related to identifiers and identity. This clarification has clearly identified candidates for core and common core identifiers, or has made it clear that further standardization is required, as well as the requirements such standards must fulfill. Specifically, the work of the OASIS XRI Workgroup [XRI] should go forward along lines currently visible, leading to standards for adornment of several types of identifiers for use as common core identifiers. Other development work may also be required, based on further development of the matrix and of new standards for identifiers. Such an approach is completely in alignment with the Core Identifier Workgroup charter.

This Framework Matrix is a formal standard, approved by the sponsoring consortia, after thorough review and socialization / syndication with other interested and concerned standards bodies (IETF [IETF], OASIS [OASIS], …). As such, it is 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.

One essential use of the Framework Matrix is to guide development of software services that use the characteristics of the named standards 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 mapping must meet established requirements for security, timeliness, integrity, and non-repudiation. 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.

This table is ordered the same as the columns in the framework matrix:

Col ID	Column Name	Description
A.	Standard number	Ordinal number, used only to provide a tag and count for the standards in the table.
B.	Platform	Operating System scope for identifier.
C.	Identifier / Standard Name	Common / short name of identifier or standard.
D.	Identifier / Standard Description	Full name / description of identifier or standard.

Col ID	Column Name	Description
E.	Reference	Text reference to full description of identifier.
F.	URL	Hypertext link to full description of identifier.
G.	Responsible Organization / Contact	Name and contact information of organization responsible for identifier.
H.	Related Standard(s)	Names / links to any related standards.
I.	XRI Representation / Linkage	Hypertext linkage to canonical XRI representation of identifier.
J.	Formats of Identifier	How identifier is formatted, such as number string, dotted decimal, alpha string, alphanumeric string, capitalization rules, etc.
K.	Identifier Type	Type description of identifier, such as digit string, alpha string, alphanumeric string, binary number, etc.
L.	Related Identifier(s) / Type(s) of Identifier(s)	Names of any related identifier(s) / type(s) of identifiers.
M.	Uniqueness	Whether identifier is unique (yes / no), with scope limitations if any.
N.	Persistence Characteristics	Whether identifier is persistent, with scope limitations if any.
O.	Credentials linked with this identifier	Whether identifier has linked credentials and is thus trusted to the degree and with scope specified in the credentials.
P.	Usage Scope	How identifier is / can be used, with scope specification.
Q.	Mapping / Equivalence Checking	Approach for mapping / equivalence checking among identifiers, e.g., through encoding in XRI.
R.	How Generated	How identifier is generated.
S.	How Recognized	How identifier is recognized.
T.	Context for Core	Context in which the identifier is a core identifier.
U.	Core / Non-core / Common Core	Identifier status: Core / Non-core / Common Core.
V.	Rationale	Why identifier is Core / Non-core / Common Core; what would need to change to change status.
W.	Issues / Concerns / Questions / Comments	General comments
X.	Update History	Records update activity and rationale.

The framework matrix elements are specified above. The initial material to fill in the framework is taken from the Open Group Identity Management Whitepaper [IDMWP], and the Core Identifier Workgroup's Business Scenario paper [CIDSCEN]. There are currently 22 standards identified in these sources. As others are identified and approved, they will be included in this list.

Unresolved Issues

No such issues are identified at this time.

References

[CIDSCEN] Business Scenario: Identifiers in the Enterprise. The Open Group, December 2006. http://www.opengroup.org/bookstore/catalog/k061.htm

[IDMWP] White Paper: Identity Management. The Open Group, March 2004. http://www.opengroup.org/bookstore/catalog/w041.htm

[OG] The Open Group http://www.opengroup.org

[DMTF] The Distributed Management Task Force http://www.dmtf.org

[NAC] The Network Applications Consortium http://www.netapps.org

[IETF] The Internet Engineering Task Force http://www.ietf.org

[OASIS] The Organization for the Advancement of Structured Information Standards http://www.oasis-open.org

[XRI] The OASIS Extensible Resource Identifier (XRI) Technical Committee http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xri