Digital Object Architecture and the Handle System

ICANN Office of the CTO

Alain Durand

OCTO-002
14 October 2019

TABLE OF CONTENTS

Executive Summary

The Digital Object Architecture (DOA) is an overall architecture for managing digital objects with an associated unique persistent identifier. In this context, digital objects are defined as a sequence or set of sequences of bits. The DOA resulted from the work by Dr. Robert Kahn and Dr. Vinton Cerf at the Corporation for National Research Initiatives (CNRI) in the late 1980s.[1]

The DOA has three core components: the identifier/resolution system, the Digital Object Repository system, and the Digital Object Registry system containing metadata about the repository objects. The Handle System is the original name of the identifier/resolution system of the DOA. Its governance is coordinated by the DONA Foundation, a Geneva-incorporated nonprofit organization founded by CNRI.

The Handle System and the DONA Foundation are the elements of the DOA that are closest to ICANN organization’s role helping coordinate the Internet's system of unique identifiers. This report will focus on those two elements to better understand the technology and its usage, innovation, and limitations. This report is not intended to endorse the technology nor offer any recommendations regarding its operation. It is based on the set of publicly available technical documents, an analysis of the code published on CNRI website, and a number of interviews with Dr. Robert Kahn and his team at CNRI.

The DONA Foundation combines governance roles that have traditionally been separated in the Domain Name System (DNS) world: creation and coordination of the registries, technical evolution of the protocol, policy development, and operation of the Global Handle Registry, the equivalent of the root zone in the DNS. With the exception of Board meetings, there is little visibility into their activities. As of March 2019, the DONA Foundation has not yet made available public documents describing in detail many DONA Foundation processes or policies, such as the exact roles and responsibilities of Multi-Primary Administrators (MPAs) – the rough equivalent of top-level domains in the DNS world – as well as the details about the requirements and selection process to become an MPA, the procedure in case of an MPA failure, and how keys underpinning the cryptography to secure the system are managed.

CNRI has made available (under a specific license) a royalty-free implementation of each of the DOA components, including the Handle System. However, the DOA protocol suite is not standardized by a Standards Development Organization like the Internet Engineering Task Force (IETF) or the Institute of Electrical and Electronics Engineers (IEEE). The only published descriptions of the Handle System protocols are outdated and are not in sync with what is currently implemented. In 2016, the DONA Foundation committed to make documentation of the protocol suite publicly available. As of March 2019, the documentation remains incomplete.

This lack of a formal and open specification allows for some degree of flexibility in deployments of the DOA by specific industry verticals, such as publishing or the film industry. However, without such documentation, building another independent, interoperable implementation of the various components of the DOA would be impractical, making the DOA difficult to deploy universally as a generic Internet solution like the DNS or the Web.

[1] Robert E. Kahn and Vinton G. Cerf, An Open Architecture for a Digital Library System and a Plan for Its Development, The Digital Library, Volume I: The World of Knowbots (DRAFT), March 1988.

Introduction

This report assumes the reader is familiar with the Domain Name System (DNS). Where applicable, it includes comparisons of parts of the Digital Object Architecture (DOA) to the DNS from technological, operational, and governance perspectives.

ICANN RESEARCH ACTIVITIES RELATED TO THE DIGITAL OBJECT ARCHITECTURE

The Research Department of ICANN org's Office of the Chief Technology Officer (OCTO Research) started to look at the DOA in 2015 at the request of segments of the ICANN community. Over the course of that year, Alain Durand, a Principal Technologist with OCTO Research, had a number of interactions, including one-on-one conversations with Dr. Robert Kahn, the inventor of DOA, and his team at the Corporation of National Research Initiatives (CNRI). At the end of 2015, ICANN org obtained a DOA prefix, the equivalent of a DNS top-level domain in DOA, from CNRI and started running an experimental Local Handle Service.

During this time, OCTO Research prepared a number of reports for senior management at ICANN org and for the ICANN Board of Directors. In March 2017, Durand gave a presentation on DOA at the ICANN58 Public Meeting in Copenhagen, Denmark. Christophe Blanchi, the DONA Foundation's Executive Director, presented the DONA Foundation perspective to the ICANN community.

This document was written in 2017 and revised in early 2019.

Over the last several years, Study Groups 17 & 20 (SG17, SG20) at the International Telecommunications Union (ITU) have generated significant discussion around the DOA technology. However, despite the substantial discussions, few public technical documents exist about the DOA.

In a 2016 Board meeting, the DONA Foundation committed to make documentation of the protocols publicly available. The Digital Object Interface Protocol (DOIP) specification was published in November 2018.[2] As of March 2019, documentation on the Identifier/Resolution Protocol (IRP), which is at the core of the Handle System, is still not available.

The only published descriptions of the Handle System protocol have become outdated. In 2003, the Internet Engineering Task Force (IETF) published "Informational" Requests for Comment (RFCs) describing version 2.1 of the Handle System protocol: RFC3650, RFC3651, and RFC3652.[3] The IETF declined to put those documents on the Standards track.

The Handle System protocols have since evolved. The 2017 version was 2.10. What has changed between the current version and earlier versions can be found only in the *readme* files contained in the software distribution for each release. At the time of this writing, the RFCs describing the protocols have not been updated. The CNRI implementations of the three DOA

[2] https://www.dona.net/sites/default/files/2018-11/DOIPv2Spec_1.pdf

[3] https://www.ietf.org/rfc/rfc3650.txt, https://www.ietf.org/rfc/rfc3651.txt, and https://www.ietf.org/rfc/rfc3652.txt

components are readily available free of charge using a CNRI specific license.[4] The China Internet Network Information Center (CNNIC) is reported to have created a C/C++ implementation of the Handle System that offers “secure DNS resolution via the Handle System protocol.”[5] The CNNIC work was done under National Science Foundation (NSF) award number 0334140 from 2003, listing Kahn as principal investigator and CNRI as sponsor.[6] However, it appears this implementation has not been released publicly. OCTO Research has not found any other publicly available implementations of the DOA protocols outside of the CNRI one.

As a result, it is not easy to separate the protocol description from CNRI’s implementation choices. The technical analysis section of this report is based on version 2.1 of the Handle System protocol described in RFC3651, augmented by numerous technical discussions between OCTO Research and the CNRI team. Although CNRI has given feedback on this document, this report is not endorsed by CNRI.

This report focuses on the Handle System, the identifier component of the DOA, the element most relevant to ICANN org’s role coordinating the Internet's unique identifiers. It reflects the author’s best efforts at understanding DOA in general, and the Handle System in particular. The author acknowledges that there might be errors, misinterpretations, or misunderstandings.

[4] http://www.handle.net/hnr_documentation.html and http://www.handle.net/HNRj/HNR-9-License.pdf
[5] “Naming and Meaning of Digital Objects,” Proceedings of the Second International Conference on Automated Production of Cross Media Content for Multi-Channel Distribution (AXMEDIS 2006), Norman Paskins, http://www.doi.org/topics/060927AXMEDIS2006DOI.pdf
[6] https://nsf.gov/awardsearch/showAward?AWD_ID=0334140

1 About This Report

The aim of this report is to inform readers about DOA, not to take a position or make any specific recommendations regarding the architecture, technology, or operational components of the DOA system. This document is the result of gathering and examining as much unbiased and verifiable technical information as possible to better understand the DOA technology and its usage, innovation, and limitations. The focus of this report is mostly on the identifier/resolution system and its governance structure, which are the components that are closest to the ICANN org's role helping to coordinate the Internet's system of unique identifiers.

- Section 2 introduces DOA and Handle System terminologies and various acronyms and explains how they relate to one another.
- Section 3 provides a high-level architecture overview.
- Section 4 gives a timeline of DOA evolution.
- Section 5 explores who is using DOA.
- Section 6 examines DOA governance.
- Section 7 details handle prefixes.
- Section 8 offers a deep dive into the Handle System technology.
- Section 9 contains tables that present a side-by-side comparison of the Handle System to the DNS.
- Section 10 lists related publications.

2 Acronyms and Terminology

Some specialized terminology is centered around the Handle System, and the more recent terminology is centered around the DOA. Where applicable, the link between the two sets of terminology will be explained.

Digital Object (DO). A sequence of bits, or a set of sequences of bits, with an associated unique persistent identifier.

Digital Object Architecture (DO Architecture, DOA). The name of the overall architecture for managing digital objects.

DO Identifier, or Digital Object Identifier. The term *Digital Object Identifier* is the formal way to refer to a DO Identifier and consists of a prefix and a suffix separated by the first forward slash (/) in the string. A Digital Object Identifier is also known as a handle and the terms are interchangeable.

DOI. The acronym DOI is a registered trademark of the International DOI Foundation (IDF), The IDF is a nonprofit organization in the United States originally set up to support the publishing industry. The IDF was one of the earliest adopters of selected components of DOA, including the Handle System.

Digital Object Interface Protocol (DOIP). The protocol that a client uses to interact with a digital object housed on a server.

Digital Object Registry (DO Registry). A specialized digital object repository that contains metadata records about other digital objects.

Digital Object Repository (DO Repository). A digital object service that implements the required functionalities to manage digital objects. This term typically refers to the management software (and the repository service it provides) and is independent of the actual storage technology being used.

DONA Foundation.[7] A nonprofit foundation in Geneva, Switzerland, responsible for the oversight and administration of the Global Handle Registry and for the evolution of the DOA.

Global Handle Registry (GHR). A registry that contains all handle prefixes without delimiters and all one-delimiter prefixes created by Multi-Primary Administrators (MPAs). In this context a delimiter is a dot (.). The operation of the GHR is called the GHR service. The GHR is a DO Repository.

Handle. In the DOA, handle is a term interchangeable with Digital Object Identifiers.

Handle Record. The actual data, or digital object, describing the handle, that is stored in a DO Repository, typically a GHR or LHS.

[7] DONA is not an expandable acronym.

Handle System. A trademark of the DONA Foundation referring to the identifier/resolution system administered by the Foundation.

Local Handle Service (LHS). A network service provided by an organization (or user) that serves handle records. The term LHS comes from early Handle System specifications. The term LHS is interchangeable with DO Repository.

Multi-Primary Administrator (MPA). An organization that has been authorized by the DONA Foundation to allot handle prefixes. [8]

Prefix. A string of labels, the first typically being a number, separated by dots.

Suffix. A character string representing a locally unique name assigned to a digital object in the local DO Repository or LHS.

[8] "Allotment" is a term of art used by CNRI and the DONA Foundation. It is roughly equivalent to "allocation" in the DNS world.

3 Architecture High-Level Overview

The DO Architecture introduces the concept of a digital object. In its simplest form, a digital object is a structured sequence of bits. The DO Architecture defines the concept of a Digital Object Identifier (DO Identifier) as a persistent identifier associated with the digital object.

The DO Architecture specifies mechanisms for storing and retrieving digital objects. The system includes an infrastructure for managing information in digital form on the Internet and consists of three primary components and two protocols:

DOA COMPONENTS:

- An identifier/resolution system (the Handle System). Handles are identifiers that act as pointers to digital objects or their components.
- Digital Object Repositories (DO Repositories), which store digital objects.
- Digital Object Registries (DO Registries), which are used to define collections of digital objects that can each exist across one or more DO Repositories and store metadata related to them.

DOA PROTOCOLS:

- The Digital Identifier/Resolution Protocol (IRP). It was known earlier as the Handle System Protocol. It is used for resolving Digital Object Identifiers.
- The Digital Object Interface Protocol (DOIP). It specifies a standard way for clients to retrieve and manipulate digital objects.

Handles and Digital Object Identifiers are interchangeable terms. They are somewhat similar to DNS names. A handle consists of a *prefix* and a *suffix* separated by the slash (/) character as: prefix/suffix.

4 Timeline

Late 1980s. Dr. Robert Kahn and Dr. Vinton Cerf authored a report on mobile programs on the Internet. They called these mobile programs *knowledge robots* (or *knowbots* for short). The report was called “An Open Architecture for a Digital Library System and a Plan for Its Development," *The Digital Library Project, Volume I: The World of Knowbots, (DRAFT),* March 1988.[9]

1992. CNRI was funded by the U.S. Defense Advanced Research Project Administration (DARPA) to carry out a Computer Science Technical Reports (CSTR) Project, which involved funding the development of digital libraries of computer science technical reports at five major U.S. universities.[10] CNRI’s proposal involved a strategy for linking these digital libraries with an architecture derived from their work on Knowbots, but with the mobility aspect temporarily sidelined. This effort led to the development of the DOA.

1995. Dr. Robert Kahn and Prof. Robert Wilensky first described important aspects of DOA in a seminal paper called “A Framework for Distributed Digital Object Services,” originally published in *D-Lib Magazine* in 1995.[11] Several earlier versions of the paper were made available to the participants in the CSTR project starting in early 1994. The paper was later republished in 2006 in the *International Journal on Digital Libraries,* (2006) 6(2): 115-123.[12]

Early 2000s. The Handle System was first proposed to the Internet Engineering Task Force (IETF) during the mid-1990s. Around 2003, during discussions on *Uniform Resource Names* (URNs), the IETF looked at the Handle System, but IETF leadership decided against putting it on the Standards Track.[13] Instead, the then-current Handle System documents describing version 2.1 of the protocol were published as informational Requests for Comment (RFCs): RFC3650, RFC3651, and RFC3652.[14] The Internet Engineering Steering Group (IESG) inserted the following note in RFC3650, RFC3651, and RFC3652:

> “Several groups within the IETF and IRTF [Internet Research Task Force] have discussed the Handle System and its relationship to existing systems of identifiers. The IESG wishes to point out that these discussions have not resulted in IETF consensus on the described Handle System, nor on how it might fit into the IETF architecture for identifiers. Though there has been discussion of handles as a form of URI [Uniform Resource Identifier], specifically as a URN, these documents describe an alternate view of how namespaces and identifiers might work on the Internet and include characterizations of existing systems which may not match the IETF consensus view.”

2013. The International Telecommunication Union - Telecom (ITU-T) published recommendation X.1255 "to provide an open architecture framework in which identity management information can be discovered".[15] This recommendation was developed in ITU-T

[9] http://hdl.handle.net/4263537/2091

[10] The five universities were Carnegie Mellon University, Cornell University, Massachusetts Institute of Technology, Stanford University, and University of California, Berkeley.

[11] http://hdl.handle.net/4263537/5001

[12] https://www.doi.org/topics/2006_05_02_Kahn_Framework.pdf

[13] The rationale behind this decision is unclear due to conflicting accounts of events.

[14] https://tools.ietf.org/html/rfc3650, https://tools.ietf.org/html/rfc3651, and https://tools.ietf.org/html/rfc3652

[15] ITU-T Recommendation X.1255, Framework for discovery of identity management information, ITU-T, 09/2013

Study Group 17. It is a framework, not a specification document. It is based on the DO Architecture but does not mandate that DOA protocols should be used.

2014. CNRI created the DONA Foundation to assume the administrative responsibility for the Global Handle Registry (GHR) and the evolution of DOA. CNRI subsequently transferred the relevant intellectual property to the DONA Foundation, including trademarks (Handle Systems, GHR, DONA), domain names (dona.net), X.509 certificates, and software needed to run the GHR. Around the same time, the DONA Foundation signed a Memorandum of Understanding (MoU) with the International Telecommunications Union (ITU). The MoU called for the ITU to temporarily assist in maintaining the GHR continuity of operations if for some reason DONA was unable to perform that service until it could be restored.

2015. The DONA Foundation put in operation the system of Multi-Primary Administrators (MPAs). Each MPA is responsible for the administration of its portion of the GHR. CNRI is one of the MPAs.

5 Who Is Using the Digital Object Architecture?

Known applications of the Digital Object Architecture include:

- The publishing and content industry, through the International DOI Foundation (IDF), uses handle technology as a framework to manage digital objects of various formats, including movie clips or books. A handle record typically points to information about publications, such as the author and available publication formats.[16] More recently, DOI identifiers have been used to identify entertainment objects such as movies.[17] From its inception, the IDF has used CNRI to register, operate, and resolve its prefixes via a DOA web proxy operated by CNRI. All DOI prefixes start with 10. The syntax for a DOI name is defined by ISO 26324:2012.[18]

- The American Psychological Association is an example of an organization using DOI prefixes to reference its publications.[19]

- The Motion Picture Association of America (MPAA), which represents the U.S. television, video, and movie industries, uses the Entertainment Identifier Registry (EIDR).[20] EIDR catalogs metadata about its creative assets and uses DOA implementations to simplify the automation chains that involve studios, suppliers, and third parties. EIDR is a member of the IDF, so it relies on CNRI to run and operate its handle prefix 10.5240. The code that CNRI operates for EIDR embeds custom business logic that, for example, detects similar entries and flags them as potential duplicates. In 2017, EIDR maintained almost a million digital objects.

- The Max Planck Institute in Germany has another known DOA deployment, using it to catalog the results of scientific experiments.[21]

- The China Academy of Information and Communication Technology (CAICT) has been tasked to use DOA to implement the China Industrial Internet Initiative as part of the Action Plan for Industrial Internet Development (2018 - 2020).[22] In 2017, CAICT and the Coalition for Handle Services in China cohosted the DOA Development Forum in Shenzhen and another 29 November–1 December in 2018.[23]

- MPA number 77 is being operated in Russia by the state-owned telecom Rostelecom. The GHR server and a proxy resolver are up and running, the local registry should be operational in 2019.[24] Both are running software from CNRI. Early tests will focus on food production factories.

[16] Sometimes, these can be found at a level removed from the handle record, e.g., a publisher's webpage for a publication information.
[17] DOI is a registered trademark of the IDF.
[18] https://www.iso.org/standard/43506.html
[19] Publication Manual of the American Psychological Association, Sixth Edition.
[20] http://www.mpaa.org/mpaa-content-creators-and-tech-firms-promote-universal-digital-ids-for-movies-and-tv-shows/
[21] https://doi.mpdl.mpg.de
[22] http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757016/c6212005/content.html
[23] The coalition is one of the global Multi-Primary Administrators of the Handle System.
[24] https://ghr.doinet.ru/

The above examples demonstrate that DOA deployments happen mostly in vertical markets. This is different from general purpose technologies such as DNS or the web that are deployed across the entire Internet.

6 Digital Object Architecture Governance

6.1 Creation of the DONA Foundation

In January 2014, the DONA Foundation was created to assume responsibility for evolving the DOA and overseeing the administration of the Global Handle Registry (GHR), the root of DOA's identifier/resolution system. The DONA Foundation is incorporated and operates in Geneva, Switzerland.

In conversations, Dr. Robert Kahn explained that the decision to incorporate in Switzerland was a choice made by CNRI to find a jurisdiction that had the potential to be acceptable to organizations that were unwilling to use the Handle System under U.S. jurisdiction.

The DONA Foundation assumes a combination of coordination and management roles which are still being defined. Many of these roles have traditionally been separated in the DNS world.

DONA Foundation Role	DNS Equivalent
MPA authorization, credentialing, and coordination	Registry/registrar contracts with ICANN org
Protocol evolution	IETF standardization process
Policy development	ICANN policy development processes
Global Handle Registry MPA operators	Combination of Internet Assigned Numbers Authority (IANA) Root Zone Manager, Root Zone Maintainer, and Root Server Operators

Notably, the DONA Foundation manages the root key of the Handle System. It is contained in the 0.0/0.0 handle record.[25] This is the equivalent of the DNS Key Signing Key (KSK) that ICANN org manages.

6.2 DONA Foundation and ITU

In June 2014, the DONA Foundation entered into a Memorandum of Understanding (MoU) with the ITU.[26] This MoU identified three areas where the ITU agreed to assist, if requested:

- Secretariat support.
- Public policy input.
- Support to ensure the continued operation of the GHR if DONA Foundation is unable to carry out its functions due to an event like bankruptcy. Support would continue until such time as the overall DONA Foundation functions could be reconstituted under the supervision of the Swiss Government and the successor to the DONA Foundation could reassume operation of the GHR.

[25] How this key is actually managed, stored, and if or how it is updated is not publicly documented.
[26] https://www.itu.int/md/S15-CL-C-0094/en

Dr. Kahn explained in conversation the public policy provision with this example: the DONA Foundation might turn to the ITU for input on defining a country.[27] This public policy approach could be important in the future if, for example, the DONA Foundation were to decide to use letters instead of digits to delegate future MPA prefixes that represent country codes.[28]

The third provision of the agreement has been a source of controversy. If, for any reason, the DONA Foundation fails, the ITU would be responsible for ensuring the continued operation of the GHR until a successor organization to the DONA Foundation is found. Critics of the ITU or the DONA Foundation or both have raised the following issues:

- The ITU would have an operational role (although temporary), and the ITU Council would probably have to approve such an effort. It is unclear what would happen if the ITU Council were to not approve the effort.
- This scenario might set up a potential conflict between the DONA Foundation Board members' fiduciary duties to maximize assets in case of failure and the MoU provision for a reconstruction by the ITU, which might or might not achieve full value of those assets.[29]

6.3 DONA Foundation Organization and Documentation

It is worth noting that the DONA Foundation is still very young and its governance structures will likely evolve over time, just like the ICANN structures did.

Beyond summaries of minutes from annual Board meetings, the DONA Foundation has not yet made much information publicly available. At its July 2016 Board meeting, the DONA Foundation agreed to assume responsibility for standardizing the core protocols of the DOA and announced their intention to publish the standards.[30] The Digital Object Interface Protocol (DOIP) specification was published in November 2018.[31] Documentation for the Identifier/Resolution Protocol (IRP), which is at the core of the Handle System, was still not available in March 2019.

The DONA Foundation concentrates several roles whose equivalents have been spread across multiple organizations in DNS governance. There is little visibility into the DONA Foundation's activities, including its current model of governance, which is under development. In 2017, the DONA Foundation web site was little more than a single page, not listing much information. However, more information can now be found on the DONA Foundation web site.[32] In particular, it now includes a *Frequently Asked Questions* section answering a number of questions about the foundation and the technology.[33]

[27] The UN and the ISO-3166 Maintenance Agency are the accepted authorities on country names and codes, not the ITU.

[28] To date, there is no evidence the DONA Foundation has plans to do so.

[29] That claim was made several times to the author in various conversations. The author has not been able to independently verify its validity.

[30] https://www.dona.net/sites/default/files/2017-09/Summary_of_Board_Minutes_July_5-6%2C_2016.pdf

[31] https://www.dona.net/sites/default/files/2018-11/DOIPv2Spec_1.pdf

[32] http://www.dona.net

[33] https://www.dona.net/faq#dona

As of March 2019, the DONA Foundation has not yet made public documents describing many important DONA processes or policies, such as the exact roles and responsibilities of MPAs, the requirements and selection process to become an MPA, procedures in case of an MPA failure, and how keys underpinning the cryptography to secure the system are managed.

7 Handles, Prefixes and Registration

7.1 Handles

Handles and Digital Object Identifiers are interchangeable terms.

The Handle System as described in RFC3650 can be seen as a federation of local name resolution systems that associates (resolves) a handle. The handle is a pointer to a digital object which can be conceptualized as an indexed series of blocks of data of various types. Some types are predefined, such as a Uniform Resource Locator (URL), an email address, a cryptographic signature, or a public key. Other types can be user-defined.

7.2 Handle Prefix

A handle *prefix* is a unique dot-separated Unicode character string, UTF-8 encoded. To ensure uniqueness, prefixes must be registered in a global database, the same way that unique DNS names must be registered in top-level domain registries.

One of the Handle System's main features is that prefixes do not include names. Dr. Kahn explains that the Handle System "does not rely on name semantics". For example, organization names are usually not included in handle prefixes. To date, except for a few special (and primarily administrative) cases, prefixes contain only digits.

Dr. Kahn offered three reasons for that choice:

- Human-readable names often refer to organizational structures that change over time, thus defeating the DOA design goal of providing persistent identifiers.
- Human-readable names are often associated with intellectual property and trademarks. CNRI did not want such controversies to hamper the development of the DOA technology.
- Human-readable names in different languages are only meaningful to those who are familiar with these languages.

However, nothing in the prefix definition, DOA protocols, or implementation restricts handles from using non-numeric prefixes. In the future, the DONA Foundation could adopt a policy to allow the use of non-numeric characters. So far, it appears that the DONA Foundation has no intention to do so.

Prefixes can have zero or more dots, called delimiters, as shown in the examples below:

11738	zero-delimiter prefix[34]
10.1038	one-delimiter prefix
20.500.1234	two-delimiter prefix

[34] Since 2016, the DONA Foundation allots zero-delimiter prefixes only to Multi-Primary Administrators (MPAs). The example is ICANN org’s experimental prefix with was allotted in 2015.

7.3 Handle Suffix

A handle *suffix*, sometimes called a *local-name*, is a unique name assigned to a digital object. There are no real restrictions on the format of a suffix. The *suffix* is comparable to either a label in a DNS zone or the local part of an URL.

EXAMPLES

11738/ithi	Resolves to a handle record containing the URL: https://www.icann.org/ithi
10.1038/nphys1170	Resolves to a handle record containing the URL: http://www.nature.com/nphys/journal/v5/n1/full/ nphys1170.html

A handle points to a digital object. To point directly to a specific attribute of a digital object, a handle can be qualified with an index using the syntax *prefix/suffix#index*, where *#index* is a number.

This example shows details of a digital object pointed to by the handle 10.1038/nphys1170.

Handle.Net®
Handle Values for: 10.1038/nphys1170

Index	Type	Timestamp	Data
1	**URL**	2009-01-3 10:20:06Z	http://www.nature.com/nphys/journal/v5/n1/full/nphys1170.html
700050	**700050**	2009-01-3 10:20:06Z	2009010205576
100	**HS_ADMIN**	2009-01-3 10:20:06Z	Handle=0.na/10/1038; index=200; [delete hdl, read val, modify val, del val, add val, modify admin, del admin, add admin, list]

7.4 Handle Persistency

The DONA Foundation often cites persistence as one of the key benefits of the Handle System.[35] It cites studies that show that in a short period of time, URLs can break for many reasons including changes to organizational structure, company name, and ownership. To address this issue, one of the DOA's design goals was to provide persistent identifiers. Persistent handles remain unchanged even if the underlying objects they refer to change or get moved to a new location or become under another's administrative control.

To achieve persistency, DOA is using a convention for designing handles.

CONVENTION FOR HANDLE PREFIXES:

- Use numbers, not names. Names tend to reflect organizations, which can change over time.

[35] https://www.dona.net/digitalobjectarchitecture

CONVENTION FOR HANDLE SUFFIXES:

- Use a flat, non-hierarchical name space. Structures reflect organizations, which tend to change over time.
- Use object identifiers that are as generic as possible. For example, one MPA uses what looks like a hexadecimal hash. 10.5240/7487-C990-425F-D706-1785-J is a handle for the movie "Top Gun."

When used as design criteria, the above convention helps make handles persistent. This convention is separate from the underlying DOA technologies and could be replicated in the DNS or any other naming system.

7.5 Multi-Primary Administrator (MPA)

Until December 2015, CNRI was the only entity registering handle prefixes in the Global Handle Registry (GHR). Every single prefix was registered in a unique database managed by CNRI. A handle prefix allotment was typically a single number with no dots. If a derived prefix (including dots) was subsequently required, CNRI would register it in the GHR.

In the Handle System, information is represented in the form of digital objects. Thus, a prefix registration appears in the form of a digital object in the GHR with the handle 0.NA/*prefix*.[36] For example, the 11738 ICANN org experimental prefix is stored in the GHR as 0.NA/11738, as shown below.

Handle.Net®
Handle Values for: 10.1038/nphys1170

Index	Type	Timestamp	Data
100	**HS_ADMIN**	2019-07-03 18:46:34Z	handle=0.NA/20.ADMIN; index=200; [create hdl,delete hdl,read val,modify val,del val,add val,modify admin,del admin,add admin]
101	**HS_ADMIN**	2015-11-20 20:00:37Z	handle=0.NA/11738; index=200; [create hdl,read val,list]
200	**HS_VLIST**	2015-11-20 20:00:37Z	300:0.NA/11738
2	**EMAIL**	2015-11-20 20:00:37Z	alain.durand@icann.org
1	**HS_SITE**	2016-12-07 23:15:14Z	0001020A000280020000000000000001000000046465736300000018416C61696E2773207465737420656E7669726F6E6D656E740000000100000001000000000000000000000000605F2409000001B90000000B4453415F5055425F4B45590000000000000150976050 8F15230BCCB292B982A2EB840BF0581CF50000008100FD7F53811D75122952DF4A9C2EECE4E7F611B7523CEF4400C31E3F80B6512669455D402251FB593D8D58FABFC5F5BA30F6CB9B556CD7813B801D346FF26660B76B9950A5A49F9FE8047B1022C24FBBA9D7FEB7C61BF83B57E7C6A8A6150F04FB83F6D3C51EC3023554135A169132F675F3AE2B61D72AEFF22203199DD14801C70000008100F7E1A085D69B3DDECBBCAB5C36B857B97994AFBBFA3AEA82F9574C0B3D0782675159578EBAD4594FE67107108180B449167123E84C281613B7CF0

[36] The 0.NA prefix is an example where characters after the first dot are not digits. In this example, NA stands for Numbering Authority.

Handle.Net®
Handle Values for: 10.1038/nphys1170

			9328CC8A6E13C167A8B547C8D28E0A3AE1E2BB3A675916EA37F0BFA213562F1FB627A01243BCCA4F1BEA8519089A883DFE15AE59F06928B665E807B552564014C3BFECF492A0000008100BFF8ADDAAED6A4534053346C9D4ADDCE8C167D2AEDB5043A0EACFACC1541E9D74E1A02CC954B05745AE3707537D032E659413B72D69FA8B58C103C093F7E39A2D3CCCDBAA99703CE46EE45AFC035D8A2AF5C5D5B8BEE67A994E9B5FFF4F7F317B5C25C90F9915A8176617E75491C2845E50A45BB164F62B2D5AC24AC9D64F4520000000303010000A51020000000A51030200001F40
300	**HS_PUBKEY**	2016-12-07 23:15:14Z	0000000B5253415F5055425F4B4559000000000000003010001000001010088A8F4CB2EB9DBAE55FF2AE9DF74F8A649889345BC7E83D009F65FD7A873CAB736195BA1373BF4923AC189514527872626948152373AFFE9CEF56C61340E46BAB39AED1599F6D2BF89A1AAFABD707B1A50D99750776C343039BD368A9FF1001801398D80CF5DB6E192697351B0EFB935F73DD497AC6E581C028405367ED530FB57D0AEABD5D163D74526DA61270A42034539EE731B97EE1A696A4623346EC6C713335FADA53BE60339E1501CB30040474D7920E0C6DFEF8A4D61D1D4B58EF2A9DF027609C3AF57DE98B7F35B27EAE7DC7FFF9484C35265AE26E100CD4EF7DEF6E0DF3B6808576EF5D60F785792A61DC96C6B613C8DEF0BE96779B0A8F4E1A94300000000
400	**HS_SIGNATURE**	2019-07-03 18:46:34Z	eyJhbGciOiJSUzI1NiJ9.eyJkaWdlc3RzIjp7ImFsZyI6IlNIQS0yNTYiLCJkaWdlc3RzIjpbeyJpbmRleCI6MTAwLCJkaWdlc3QiOiJJZFFkeUVaN1EvMTJMemZvQnRtTzFtZXBtcDQwUlBaTHRGYjhKS3lDRXdrPSJ9LHsiaW5kZXgiOjEwMSwiZGlnZXN0IjoiVzZTWDJqcTRMNndKS3RTOEQzVlVFWi9yK3Z0bkZ5b2JpQnllUitMci9SZz0ifSx7ImluZGV4IjoyMDAsImRpZ2VzdCI6Ilk5eVpqY0pCdWpoU21YY2xFczl0U3N4M0hDalpXS2NrajVEVEw0bE02ZHc9In0seyJpbmRleCI6MiwiZGlnZXN0IjoiYllXRzJYWE5rZEZQTms2a2RoM2RqdlJMcm5NRjVKSXJBeUVmN3AxejhkMD0ifSx7ImluZGV4IjoxLCJkaWdlc3QiOiJhYUE5T2tuaVNURXZ6bXE2QVlweFZwL010dWQrcEtrcTZPTXpHSWlybm9zPSJ9LHsiaW5kZXgiOjMwMCwiZGlnZXN0Ijoia0hxclBDdm5xYmZwcER5SmNNaThOTENNSk1mU1BPYlY2NDgxT2E2R21VYz0ifV19LCJjaGFpbiI6WyIwLk5BLzIwIiwiMC5PUFMvMTE3MzgiXSwiaXNzIjoiMzAxOjAuTkEvMjAiLCJzdWIiOiIwLk5BLzExNzM4IiwiZXhwIjoxNjg4MzIzNTkxLCJuYmYiOjE1NjIxNzg5OTEsImlhdCI6MTU2MjE3OTU5MX0.fmj4IjOwNlcA56lffc4aUYe5foEXNaRhY_KNDDVFHX_kmNV3Lx6USoWmZprJuxO3ak_9iDln2yk6_crSaMYvg8APTsJQ_ErPZfC8HrQUxee3PIoLGvciVjBO3setmptpfLwYWbWDD-6lwbcBEwgYjt9gXsh0GVF96aGdP1FV97_2mgT7qqZbhe_Ae1mo1o4Jwgkmsxz1t6_mjylMv5qsEgkXUWEmVpYv00Fa5o6EozxD8LzEL-2d_c_Nw-f1zVX2JV-fQlmXz3lmcQGTOlWEw2vv4Lg0d3tskpxqBvY6108T1VYzkfr9YeziHHzNMcylj5lArluGJQKQdTz5NBdj8w

Starting in 2016, the DONA Foundation adopted a system where multiple registration authorities, called Multi-Primary Administrators (MPAs), could register prefixes they are responsible for in the GHR. Each MPA is allocated a zero-delimiter prefix (e.g., a number without dots), called a credential, and it is authorized to allot prefixes derived from this credential. For example, in 2016, the DONA Foundation allotted credential 20 to CNRI, so all new prefixes that CNRI creates will be one-delimiter prefixes starting with 20 *dot*. CNRI will be responsible to register those in the GHR. That way, there should be no conflicts between the registrations of the various MPAs, and each MPA can focus on managing the part of GHR for which it is responsible.

To become an MPA, organizations must sign an "MPA Service Agreement" with the DONA Foundation. In conversations, Dr. Kahn indicated that each MPA pays an annual fee of CHF 75,000.[37] He added that the Foundation expects to sign up about 10 to 12 organizations as MPAs. As of July 2017, 8 organizations had entered into MPA Service Agreements with the DONA Foundation. At that time, the DONA Foundation website listed 8 MPAs without mentioning which zero-delimiter prefix they had been allocated.[38] In March 2019, the list included 9 MPAs:[39]

- 20: Corporation for National Research Initiatives (CNRI), signed 3 April 2015.
- 86: Coalition for Handle Services – China (ETIRI, CDI and CHC), signed 9 December 2014.
- 21: Gesellschaft für Wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG), signed 9 February 2015.
- 10: International DOI Foundation (IDF), effective 1 January 2016.
- 22: Communications and Information Technology Commission (CITC), effective 1 July 2016.
- 25: Smart Africa Alliance, a joint initiative between the Smart Africa Secretariat and the Rwanda Utilities Regulatory Authority (RURA), effective 19 October 2016.
- 27: MISAVA Agency for Digital Identifiers (MISADI), effective 16 October 2016.
- 44: Tunisian Internet Agency (ATI), effective 22 June 2017.
- 77: Public Joint-Stock Company Rostelecom, effective 10 September 2018.

The minutes of the DONA Foundation Board of Directors meeting of 3 and 4 July 2014 indicate that the ITU was designated as an MPA. [40] However, the ITU never signed the MPA Service Agreement and the DONA Foundation does not consider it to be an MPA. Still, the ITU operates a portion of the GHR in accordance with its approved mission, primarily for internal services. They use zero-delimiter prefix 11 that CNRI allotted to the ITU before the creation of the DONA Foundation.

The details of the agreements between those organizations previously listed and the DONA Foundation are not published on the DONA Foundation’s website. Dr. Kahn said that the basic agreement template is made available to prospective MPAs upon request. The exact roles and responsibilities of MPAs are also not public; however, Dr. Kahn points to a few common characteristics:

- MPAs are allocated a zero-delimiter prefix under which they register prefixes.
- Each MPA must keep a copy of the entire GHR.
- All zero-delimiter and one-delimiter prefixes must be resolvable in the GHR.
- Prefixes with two or more delimiters are not presently hosted in the GHR but are intended to be hosted in a Local Handle Service provided by the corresponding MPA.

Very few details are publicly available concerning the operation of the MPAs. In particular, there is no public version of a Service Level Agreement (SLA), published procedures if an MPA goes

[37] It is unclear if the DONA Foundation has other sources of revenues.
[38] https://www.dona.net/mpa/
[39] https://www.dona.net/mpas
[40] https://www.dona.net/sites/default/files/2017-09/Summary_of_Board_Minutes_July_3-4%2C_2014.pdf

out of business, security or policy requirements for the operation of the MPA, how and when statistics will be published, etc. According to DONA Foundation Board minutes of July 2018, MPAs are coordinated through the DONA Coordination Group (DONA-CG), which was formally established as an internal body of the Foundation during that meeting.

7.6 CNRI as an MPA

CNRI appears to be the only MPA that openly accepts registrations for the general community.

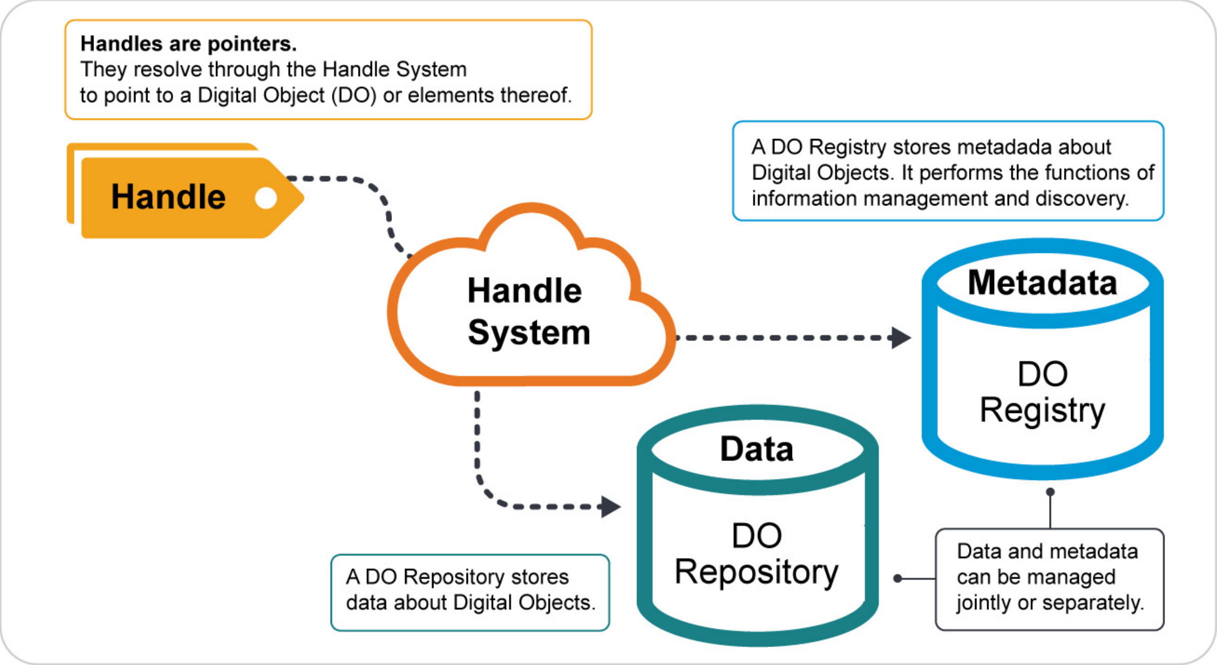
The fee structure for registration at CNRI is currently: a USD 50 one-time initial fee to register a prefix and USD 50 per year, meaning that each prefix costs USD 100 the first year and USD 50 in subsequent years.[41]

CNRI typically creates one-delimiter prefixes. It does not generally allow prefix owners to create derived prefixes (e.g., two delimiters or more) of their own prefixes. As such, a prefix holder usually goes back to CNRI and pays an extra fee to register any derived prefixes. This is an operational choice by CNRI, not a technological limitation; the current implementation allows for delegating authority to third parties to create derived prefixes themselves.

[41] http://www.handle.net/payment.html

8 Technical Analysis of the Handle System

The rest of this document will focus on a technical analysis of the Handle System as a key component of the DO Architecture. This document will not expand much in the other components of the DO Architecture: the DO Repository and the DO Registry. The Handle System is comparable to the DNS. Both are a hierarchical, globally distributed database and lookup system.


Handles are pointers.
They resolve through the Handle System
to point to a Digital Object (DO) or elements thereof.
Handle
Handle System
A DO Registry stores metadada about
Digital Objects. It performs the functions of
information management and discovery.
Metadata
DO Registry
Data
DO Repository
A DO Repository stores
data about Digital Objects.
Data and metadata
can be managed
jointly or separately.

8.1 Implementation and Protocol Documentation

The DOA protocol suite is not standardized by a Standards Development Organization like the Internet Engineering Task Force (IETF) or the Institute of Electrical and Electronics Engineers (IEEE). DOA appears to be less specified when compared to Internet standards. The lack of a formal and open specification allows for some degree of flexibility that is well-suited to the adoption of the technology by specific industry verticals.[42] However, it also typically hinders the general deployment of the technology, as it is difficult to build interoperable implementations from scratch.

CNRI has released under a CNRI-specific license,[43] a royalty-free implementation of each of the DOA components: The Handle System, the DO Repository, and the DO Registry.[44] This mitigates (to a point) the lack of published current specifications for all DOA components. No other publicly available implementations of any of the Handle System components are known to exist.

[42] It is worth noting that interoperability across verticals was not a design requirement of CNRI.
[43] http://www.handle.net/HNRj/HNR-9-License.pdf
[44] http://handle.net, http://dorepository.org, and http://doregistry.org

The Digital Object Interface Protocol (DOIP) specification was published in November 2018.[45] As of March 2019, the Identifier/Resolution Protocol (IRP) - that is, the core protocol of the Handle System, replacing or updating RFC3650, RFC3651, and RFC3652 - is still not published.

Without the complete set of documentation of every protocol and data model, building another independent, interoperable implementation of the Handle System would require reverse engineering the current CNRI implementation and keeping track of future changes.

8.2 Original GHR Model: Global Handle Registry and Local Handle Services

As mentioned previously, the Handle System refers to a federated identifier/resolution system, at least conceptually. The prefix part of a handle can be seen as designating the party authorized to create suffixes pointing to digital objects, *beneath* that prefix. The suffix part of a handle is stored in one or more Local Handle Services (LHSs), also known as the DO Repository. It is operated directly by the owner of the prefix or a third party authorized by the owner of the prefix.

In the original design before the introduction of the MPA concept, resolving a handle was conceptually a two-step process:

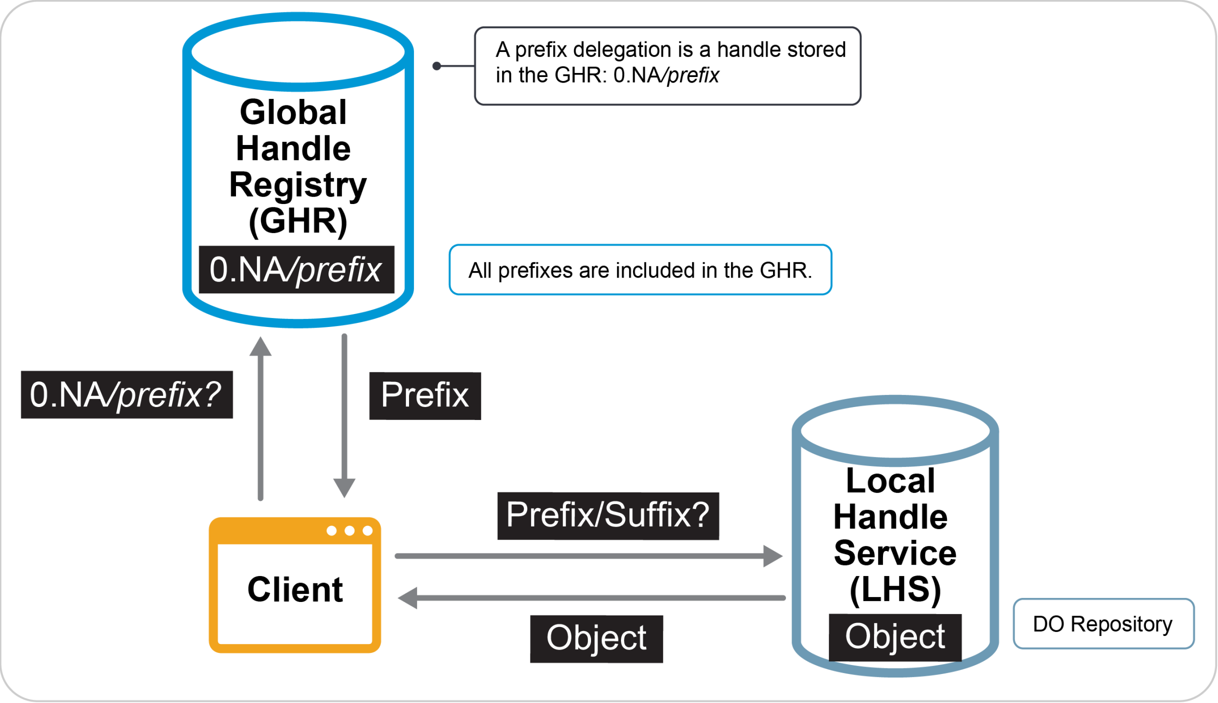
1. Query the GHR (using the prefix) to obtain the address of the Local Handle Service responsible for the handle record for the digital object from the prefix.

2. Query that Local Handle Service for the handle record containing the relevant state information for the desired digital object.

Before the creation of MPAs, CNRI would run the GHR as a DO Repository. All prefixes were registered as prefix handle records in the GHR. Prefix *n* would be stored as a handle record with the handle 0.NA/*n*. That handle record would contain, among other things, the IP addresses of sites (or servers) hosting the associated Local Handle Service. That Local Handle Service would be responsible for storing and providing upon request the actual handle record for identifiers starting with prefix *n*. Those identifiers might lead to the requested digital object, potentially at some location other than the server providing the Local Handle Service.

[45] https://www.dona.net/sites/default/files/2018-11/DOIPv2Spec_1.pdf

GHR/LHS: Original Design


Global Handle Registry (GHR)
0.NA/*prefix*
A prefix delegation is a handle stored in the GHR: 0.NA/*prefix*
All prefixes are included in the GHR.
0.NA/*prefix?*
Prefix
Client
Prefix/Suffix?
Object
Local Handle Service (LHS)
Object
DO Repository

8.3 Resolution: IRP

As of March 2019, the documentation of the Identifier Resolution Protocol (IRP) is not available on the DONA Foundation website. However, IRP is the new name of the Handle System protocol. Early versions of that protocol were documented in RFC3650, RFC3651, and RFC3652 in 2003. An analysis of those RFCs is made with the caveat that current implementations depart from this original specification.

The Handle System protocol, the identifier/resolution component of the DO Architecture, appears to be modeled on the idea of a central authority and delegated assignments. This idea is also central to the DNS.

The Handle System Protocol uses TCP and UDP port 2641.[46] UDP tends to be used for messages smaller than 512 bytes. Larger ones only use TCP. This is broadly similar to how DNS makes use of TCP and UDP port 53.

To learn about and receive periodic updates on general service information about the GHR – including relevant IP addresses, ports, and public keys – Handle System clients send a query to the GHR upon start-up. This initial query is sent to the GHR by selecting a GHR endpoint from a list of IP addresses, ports, and public keys that match previously known endpoints of the GHR Service. This is not unlike how DNS resolution servers bootstrap. The servers start with a list of pre-configured IP addresses of the DNS root servers and make a priming query to at least one of those IP addresses to fetch the current list of DNS root servers.

[46] https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt

8.4 Resolution: MPA Evolution (2016)

In the original design, handle resolution was a two-step process, involving the GHR and a Local Handle Service. The original GHR model can scale to a very large number of prefixes (estimated to a minimum of one billion, according to CNRI).[47] Both registration of the prefixes and the operation of the GHR were originally performed by a single administrative authority, CNRI.

In 2014, the DONA Foundation decided to authorize multiple entities called Multi-Primary Administrators (MPAs) to perform the public-facing role of registration and operation of providing the GHR Services. In this new model, the GHR contains the credentials allotted to the all the MPAs. Then, each MPA runs a GHR Service, which is an instance of the GHR registry. In those instances, the MPAs are responsible to include the list of the one-delimiter prefixes they allotted. Those are then synchronized with the other MPAs. Thus, each GHR Service contains all prefix handle records for the zero-delimiter and one-delimiter prefixes. The MPA version of the GHR went into operation in December 2015.

For these zero-delimiter and one-delimiter prefixes, the resolution process remains a two-step process, as described in Section 8.3. For prefixes with two or more delimiters, the resolution process adds an additional step:

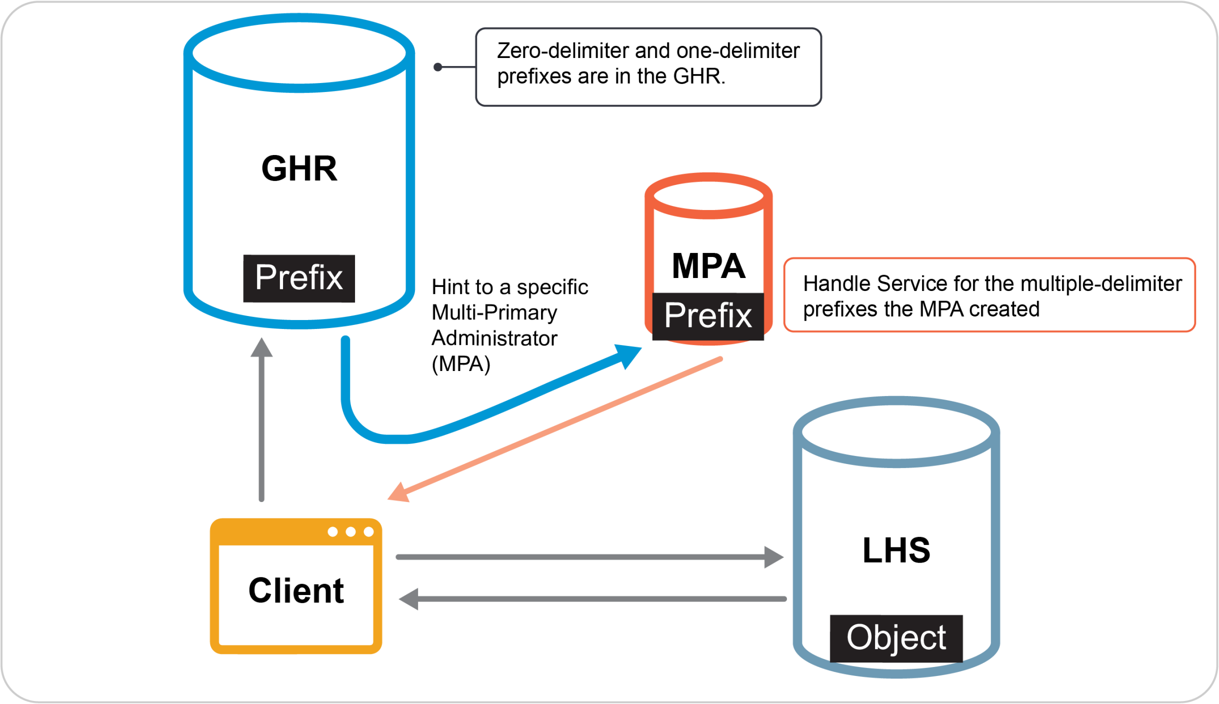
1. Request the prefix handle record for the queried prefix from any of the MPA GHR Services. The response contains a hint that typically redirects to a Local Handle Service operated by the organization authorized to provide the MPA GHR Service on behalf of the relevant MPA.
2. Ask the MPA-operated Local Handle Service about the same prefix handle. The response now redirects to the Local Handle Service in charge of that prefix.

3. Ask that Local Handle Service for the handle record for the identifier.

The vast majority of handle prefixes are zero-delimiter or one-delimiter prefixes, so the two-step process is still the norm in 2019. However, this situation might change in the future. For example, CNRI now allocates two-delimiter prefixes starting with 20.500. Those new prefixes with two or more delimiters require the three-step resolution process.

[47] Two reasons explain why the GHR can scale: (1) only a limited amount of information is kept about each prefix, and (2) the GHR itself is sliced according to a methodology described in section 8.5.2.

Resolution for Multiple-Delimiter Prefixes


Zero-delimiter and one-delimiter prefixes are in the GHR.
GHR
Prefix
Hint to a specific Multi-Primary Administrator (MPA)
MPA
Prefix
Handle Service for the multiple-delimiter prefixes the MPA created
LHS
Object
Client

8.5 DO Registry Scaling

Each DO Registry (GHR, LHRs) in the overall system can host vast quantities of data and should be able to sustain a heavy volume of queries. This scaling is achieved through two techniques: replication and slicing.

8.5.1 Replication

Handle Service replication is similar to the use of mirroring by DNS secondary servers; the entire set of handle records can be replicated at multiple sites. Providers of Local Handle Services can determine their own replication strategies. The DONA Foundation controls replication of GHR Services. Each MPA replicates prefix handle records from the GHR Services of all other MPAs. In doing so, it accepts entries from other MPA's GHR Services only if those MPAs created them under the original prefix allotted to them.

Local Handle Services that are responsible for identifiers beginning with prefix *n* are registered in the handle record for 0.NA/*n*, which is stored in the GHR. In that handle record is a list of functionally identical Local Handle Service sites that can be queried to access the desired handle record. When presented this record, the Handle System client will decide which site to choose. How to make that selection is left to the client implementation, just like a DNS recursive resolver makes an implementation-dependent decision on how to choose among different DNS servers listed in the Name Serve (NS) records for a zone.

8.5.2 Slicing

Slicing in the Handle System has no direct equivalent in the DNS world. Slicing enables splitting digital objects contained in a handle registry at a given site into multiple servers at the same site. Each slice holds a non-overlapping subset of the handle registry, and the combination of all slices contains the entire handle registry data set.

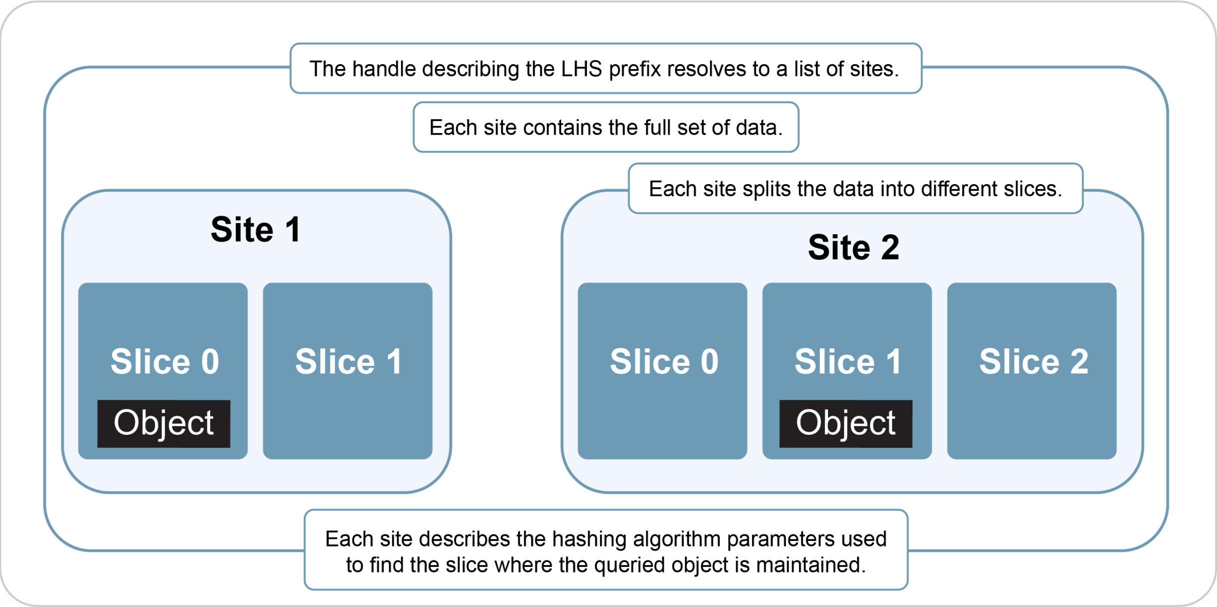
Note: Slicing, just like replicating the data on multiple sites, can be applied to either the GHR Service or to Local Handle Services.

Slicing performs two functions:

- It divides (almost equally) the data set among multiple servers.
- It splits the query load among each slice.

To decide into which slice the object must go, the handle registry applies a hash function to all or part of the handle. The Handle System Service definition version 2.1 documented in RFC3651 specifies that MD5 provides this hashing function.[48]

Handle Registry Scaling (Applies to GHR, LHS)



The handle describing the LHS prefix resolves to a list of sites.
Each site contains the full set of data.
Each site splits the data into different slices.
Site 1
Slice 0
Object
Slice 1
Site 2
Slice 0
Slice 1
Object
Slice 2
Each site describes the hashing algorithm parameters used to find the slice where the queried object is maintained.

Note that each site can use a different number of slices. The choice of how many slices to use is determined by the administrator of the specific site replicating the prefix to be resolved.

[48] https://tools.ietf.org/html/rfc3651

The same hash function must also be performed on the client. The parameters of the hash function to be used for a given site are found in the site description.

According to conversations with Dr. Kahn and his team, slicing has not been used much, if at all. Current servers are powerful enough to handle the largest existing Local Handle Systems. Also, slicing is not guaranteed to be effective because splitting the set of records does not necessarily split the query load. For slicing to work efficiently, the assumption is that queries are evenly distributed among the full set of objects, which may or may not be the case.[49] If the queries cover many different digital objects, the load will be fairly distributed among the servers. However, if only a small subset of digital objects is queried multiple times, chances are that those queries will hit some servers but not others, defeating the purpose of spreading the load.

8.6 Security, Keys, and Key Management

Security in the Handle System, just as in the DNS, is based on data security and transport security. In the DNS, DNSSEC provides data security. Transport security is provided by TSIG (RFC2845) and DNS over TLS (DOT, RFC7858) or DNS over HTTPS (DOH, RFC8484).[50] In the Handle System, transport security and data security are built in the client/server protocol.

Two sets of keys play an important role in the Handle System. First, there are the keys to the various servers used for transport security to authenticate messages. GHR and LHS servers can be authenticated using their public keys (or X.509 certificates). Those public keys (or X.509 certificates) are registered as part of the site description of the queried handle prefixes.

Secondly, there are keys used to provide data security. That second set of keys starts with the root key, contained in the 0.0/0.0 handle record, which the DONA Foundation manages. The root key is used to sign the various MPAs' keys. When an MPA allots a handle prefix to a LHS, that MPA signs the LHS key with its MPA key. This mechanism builds a chain of trust that operates very similarly to DNSSEC.

Note: there is no documented mechanism describing how the root key contained in the 0.0/0.0 handle record is managed, nor how it could be rolled in the future.

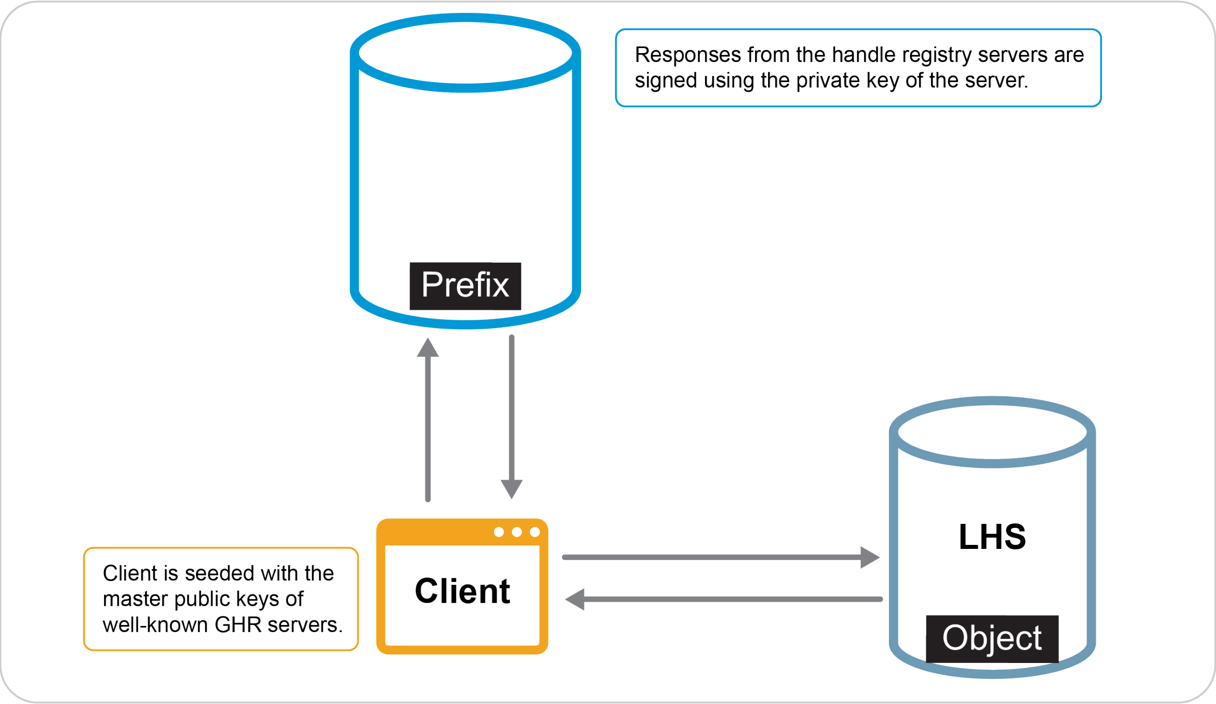
Just like the DNS, the Handle System needs a bootstrapping mechanism. At boot time, the current CNRI Java client implementation uses a list of well-known GHR servers and queries them for the handle record 0.NA/0.NA, which contains the up-to-date list of current GHR servers. This mechanism is similar to the DNS priming query mechanism used by DNS resolvers at start-up to discover the list of root name servers.

However, unlike the DNS, the Handle System goes further: the 0.NA/0.NA handle record also includes the various public keys used by the Handle System, enabling the client to automatically update its key set when querying for that handle record. If the client possesses an old key, the data returned by the GHR server will be signed by the private key corresponding to that old key. This mechanism allows the client to automatically update the keys of the GHR servers.

[49] If there are large numbers of stored and queried objects, there is a high probability that the hash function will spread the load equally.
[50] https://tools.ietf.org/html/rfc2845, https://tools.ietf.org/html/rfc7858, and https://tools.ietf.org/html/rfc8484

This automated update mechanism works for regular, scheduled, key updates. In the event that one of the keys were to be compromised, the system would keep operating but some level of coordination between the MPAs would be needed for rekeying. The details of this operation would vary depending on which key is compromised.

Resolution/Security: Client Validation



Responses from the handle registry servers are signed using the private key of the server.

Client is seeded with the master public keys of well-known GHR servers.

8.7 In-Band Object Management

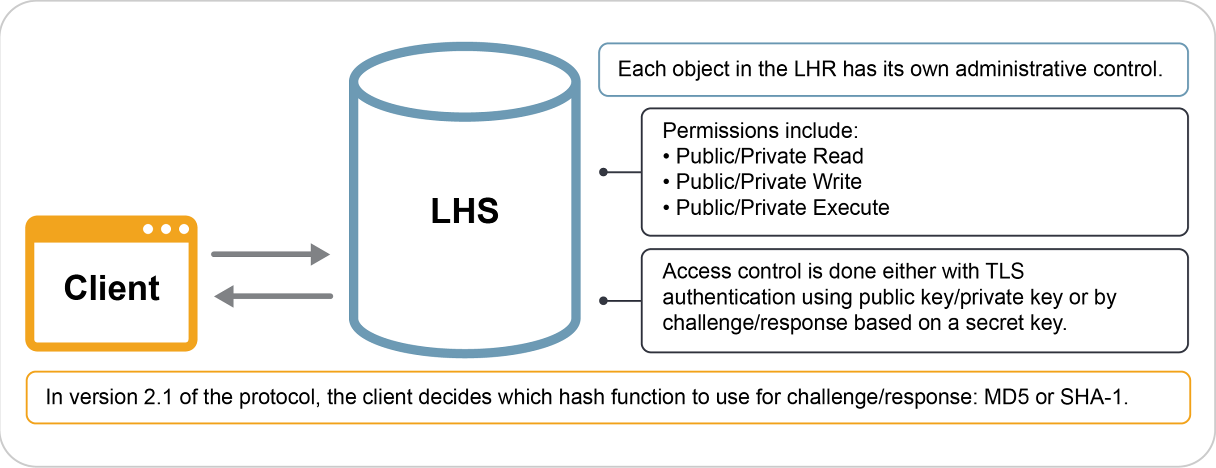
In the DNS world, managing and resolving DNS names are usually separate processes.[51] In the Handle System world, the same protocol can cover both.

In the Handle System, each element of a digital object (digital object attribute) can be controlled in-band by setting administrative read/write/execute privileges on the digital object itself. In version 2.1 of the protocol, an administrator can set permissions of a digital object to the values as shown in the diagram below.[52]

[51] One exception would be the use of dynamic DNS updates as detailed in https://tools.ietf.org/html/rfc2136

[52] Security experts might be concerned about providing execute privileges.

Object Management: Same Channel as Resolution



Each object in the LHR has its own administrative control.

Permissions include:
- Public/Private Read
- Public/Private Write
- Public/Private Execute

Access control is done either with TLS authentication using public key/private key or by challenge/response based on a secret key.

In version 2.1 of the protocol, the client decides which hash function to use for challenge/response: MD5 or SHA-1.

Using the native protocol, clients and servers exchange messages on port 2641. Messages are authenticated using a challenge-response mechanism based on a cryptographic hash, or message digest. In RFC3652, the *Handle System Protocol (ver 2.1) Specification* states that the client decides which hash function to use: MD5 or SHA-1.[53] However, the *Handle.Net (Version 8.1) Technical Manual* of the current Handle System implementation from CNRI states that authentication is based on HMAC-SHA1:

> "Handle.Net software version 8 will by default use PBKDF2-HMAC-SHA1 to generate a derived key from the secret key, and then use HMAC-SHA1 to generate the MAC.[54] Older software will use the SHA1 hash of the secret key concatenated with a challenge concatenated again the with secret key."[55]

The security properties of authentication based on MD5, SHA-1, and HMAC-SHA1 are different. HMAC-SHA1 hashing avoids the significant cryptographic weaknesses of MD5 and SHA-1 hashing. However, because current servers might have to deal with both old and new clients, a malicious actor might be able to force a server to use the weaker protocol and thus break the authentication (known as a *downgrade* attack). The alternative is to not require newer servers to be interoperable with older clients.

8.8 Out-of-Band Object Management: DOIP

The easiest way to manage digital objects is not through the in-band method, but through an out-of-band protocol, known as the Digital Object Interface Protocol (DOIP). DOIP is a client/server protocol. DOIP version 2 specification is available on the DONA Foundation website.[56]

[53] https://tools.ietf.org/html/rfc3652 (section 2.2.3)
[54] MAC is an acronym for message authentication code.
[55] http://www.handle.net/tech_manual/HN_Tech_Manual_8.pdf (section 1.4.1)
[56] https://www.dona.net/sites/default/files/2018-11/DOIPv2Spec_1.pdf

The DOIP protocol can be tunneled over any secure transport layer. Transport Layer Security (TLS) is listed as the minimum requirement to run DOIP. Objects can be described as a JavaScript Object Notation (JSON) serialization.[57] Other forms of serialization can be used, but a DOIP request or response must lead with a JSON segment.

Site administrators could turn off the administration of the database via the in-band IRP protocol and instead authorize administrative requests over HTTPS using the JSON REST API, relying on TLS authentication.

8.9 Handle System Clients and Proxy Servers

To resolve identifiers, a Handle System client is needed to interact with the rest of the Handle System. Aside from the Java client that CNRI provides with its handle software distribution, and some earlier C versions developed by CNRI and CNNIC, there are no other known native Handle System clients. There also do not appear to be any operating systems or web browsers that natively support handles. Instead, plug-ins and proxies are used.

8.9.1 Firefox Plug-In

CNRI developed a plug-in for the Firefox browser.[58] Like all plug-ins, it must be manually installed, greatly reducing its usefulness in deploying handles on a large scale.

The plug-in introduced a new URI method: hdl://*handle*.[59] For example, after manually installing the Firefox plugin, typing hdl://11738/ITHI would reach the ICANN org Identifier Technologies Health Indicator (ITHI) project webpage. However, this URI method was never formally standardized via the IETF.

The API which the plug-in was coded against has also since been deprecated and, after the release of Firefox version 53, the plug-in no longer functions. This now defunct plug-in was not a full client; it was relaying the queries over HTTP to a proxy server.

8.9.2 Proxy Servers

Besides using the CNRI Java client, the only practical way to resolve handles today is to send the request over HTTP or HTTPS to a proxy server. A proxy server accepts HTTP or HTTPS appropriately formatted requests and converts them into native handle requests on port 2461. Responses are typically cached in the proxies before being returned to the proxy service users.

An example of a DOA adopter recommending the use of a proxy is the American Psychological Association (APA). In 2014, the APA changed its cross-reference syntax recommendations from using a DOI URI method to using an HTTP method that makes use of a proxy.[60] For example,

[57] https://tools.ietf.org/html/rfc7159
[58] A plug-in is a third-party add-on piece of software that an end user needs to install.
[59] https://tools.ietf.org/html/rfc3986
[60] Publication Manual of the American Psychological Association, Sixth Edition

the reference for the document “rmh0000008” went from doi:10.1037/rmh0000008 to use the proxy form http://dx.doi.org/10.1037/rmh0000008. Note: the DOI URI method was never standardized.[61]

Another example of proxy server use can be found in RFC7669, which states that “the standard way to look up a DOI is to use the public HTTP proxy at https://dx.doi.org.”[62] RFC7669 gives this example: https://dx.doi.org/10.17487/rfc1149.

Anyone can use the set of handle.net proxy servers run by CNRI. For example, the ICANN org’s 11738/ithi handle can be resolved by using the URL https://hdl.handle.net/11738/ithi. Obviously, using proxies creates a dependency for the Handle System on the Internet and on the DNS.

PRIVACY IMPACT OF PROXIES

The use of proxies may raise a number of privacy concerns. Proxy logs may contain user resolution history. If the proxy has a cache, it might contain resolved data, potentially in clear text as the proxy acts as a *man in the middle* for communication between the client and the server.

In the DNS world, one could argue that there is a similar situation with DNS recursive resolvers. The logs of those servers also contain users’ resolution history. However, privacy-conscious users may opt to run their own DNS recursive resolvers instead of relying on the one provided by their Internet service provider or another third party.[63] Similarly, privacy-conscious Handle System users would have to install their own proxy servers. Today, there are many readily available DNS resolver implementations to do this, which is not the case for the Handle System.

8.9.3 Deployment Considerations

The absence of widely available Handle System client implementations creates a deployment challenge. Native Handle System clients could be implemented and distributed, but a significant hurdle remains to make those clients part of standard operating system or browser distributions. The lack of client implementations and a deployed base limits the incentive to deploy DOA servers, which further discourages the distribution and uptake of DOA clients.

[61] URI schemes are usually defined based on specific (web) applications. Since the DNS is not a web application, it doesn’t have a URI scheme defined. Similarly, as a general-purpose identifier/resolution service, the Handle System might not need a URI scheme. A specific Handle application, like one based on the DOI, might require a URI scheme.
[62] https://tools.ietf.org/html/rfc7669
[63] There are cases where ISPs block port 53 and make running a local DNS recursive resolver impossible.

9 Comparison: Handle System vs. DNS

The following tables compare the Handle System and the DNS.

9.1 Protocol

	Handle System	DNS
Syntax	Dot-separated UTF-8	Presentation format: dot-separated letter/number/ hyphen for hostnames
Identifier Length	No protocol specified length limitation	Name format: maximum label length 63 octets, maximum domain name length 255 octets
Transport	UDP/TCP port 2641, HTTP/HTTPS port 8000	UDP/TCP port 53, DNS over TLS port 853 (DOT) DNS over HTTPS (DOH)
Resolution	GHR LHS Replication Caching server Slicing	Root servers Authoritative servers Secondary servers Caching resolvers
Granularity of Data Administration Delegation	Per object	Per DNS zone unless Dynamic Updates are enabled, in which case per resource record set.
Data Management	In-band: Object management is done using either challenge-response and a message digest between the client and the server Out-of-band: JSON Admin REST API over Transport Layer Security (TLS)	In-band: DNS dynamic updates Out-of-band: DNS zone management
Data Objects	Extensible indexed types, predefined or opaque (as relevant only to the producer and the consumer of the data)	Defined RR types, private use types

9.2 Security and Privacy

	Handle System	DNS
Security/ Authentication Considerations	Transport security model + Data Security In-band access control	Data security model (DNSSEC) + Transport Security (TSIG)
Automatic Key Rollover Mechanism	Client automatically downloads new keys from GHR, message is signed using old key.	RFC5011 Root KSK management and ceremonies
Privacy	Relying on proxies creates a privacy concern.[64] Deploying DOA clients is difficult: there are no native operating system or browser implementations.	Recursive resolvers share the same privacy issues as proxies. (Privacy-conscious users may opt to run their own resolvers.)

9.3 Governance

	DOA	DNS
Registration	MPAs	Separation of registries and registrars
Protocol Extensions	DONA	IETF
Policy Development	DONA	ICANN
Operation	DONA/CNRI/MPAs	Root, TLD, and resolver operators

[64] Privacy-conscious DOA users may choose to operate their own proxies.

10 More Information

10.1 Web Resources

DONA Foundation:	http://www.dona.net/
Handle System:	http://www.handle.net/
DO Repository:	http://dorepository.org
DO Registry:	http://doregistry.org

10.2 RFCs and Articles

RFC2136, Dynamic Updates in the Domain Name System, Internet Engineering Task Force, April 1997.

RFC2845, Secret Key Transaction Authentication for DNS, Internet Engineering Task Force, May 2000.

RFC3650, Handle System Overview, Internet Engineering Task Force, November 2003.

RFC3651, Handle System Namespace and Service Definition, Internet Engineering Task Force, November 2003.

RFC3652, Handle System Protocol (ver 2.1) Specification, Internet Engineering Task Force, November 2003.

RFC5011, Automated Updates of DNS Security (DNSSEC) Trust Anchors, Internet Engineering Task Force, September 2007.

RFC7159, The JavaScript Object Notation (JSON) Data Interchange Format, Internet Engineering Task Force, March 2014.

RFC7669, Assigning Digital Object Identifiers to RFCs, Internet Engineering Task Force, October 2015.

RFC7858, Specification for DNS over Transport Layer Security, Internet Engineering Task Force, May 2016.

RFC8484, DNS Queries over HTTPS, Internet Engineering Task Force, October 2018.

Robert E. Kahn and Vinton G. Cerf, An Open Architecture for a Digital Library System and a Plan for Its Development, The Digital Library, Volume I: The World of Knowbots (DRAFT), March 1988.

Robert Kahn and Robert Wilensky, A Framework for Distributed Digital Object Services, *International Journal on Digital Libraries*, 2006 (originally published in D-Lib Magazine, 1995).

DOIP, DIGITAL OBJECT INTERFACE PROTOCOL SPECIFICATION v2, DONA Foundation, November 2018. https://www.dona.net/sites/default/files/2018-11/DOIPv2Spec_1.pdf

Other relevant documents about DOA can be found on the DONA Foundation web site.[65]

[65] https://www.dona.net/suggested-reading-documents

ICANN.ORG

ICANN.ORG