Handle System and Global Handle Registry

Christophe Blanchi
DONA Foundation

ICANN-58 - Copenhagen March 14th 2017

DONA

Digital Object Architecture

The Digital Object Architecture addresses the following digital information management issues:

- Uniform and interoperable access to heterogeneous information systems, resources or other entities.
  - Identification of digital information including that associate with physical items.
  - Uniform description, search and retrieval capabilities.
  - Extensible typing of data and services.
- Interoperability across heterogeneous information systems.
  - Independent of the specific underlying technologies that host the information.
- Integrated security.
- Highly scalable.

DONA

Background on the DOA

- Started with the work of Kahn and Cerf at CNRI on mobile programs in the 1980s (i.e., Knowbots)
- Elaborated upon in the early 1990s in the Computer Science Technical Reports (CSTR) project.
- Cross-Industry Working Team (XIWT) report in 1997 supported the concept of digital objects and "stated operations" on digital objects (see http://www.cnri.reston.va.us/papers/ManagAccess-1.pdf)
- Received the Digital Id World Award in 2003 for balancing innovation with reality.
- Now being evolved by the DONA Foundation.

DONA

Introduction to the Handle System

- The Handle System is a component of the Digital Object Architecture (DOA) with a defined protocol and data model.
- Basic identifier/resolution system for the Internet, and can be used in other computational environments.
  - Resolves a handle into its associated digital object's current state information
  - Identifier persists when the handle service changes and/or other attributes of the object changes.
- Logically a single system, physically and organizationally distributed.
- Highly scalable.
- Associate stated values, e.g., IP address, public key, URL, metadata, with the identifier.
- Secure resolution and administration using an integrated PKI capability (mandatory in some cases, otherwise optional.
- Optimized for resolution speed and reliability.

DONA

Handle System & DNS

- Both are resolution systems; both work in the Internet and both have extensive collections of data.
- The Handle System is compatible with DNS; handle records may make use of DNS entries; and interoperability with web browsers (that rely on DNS) occurs via proxy servers.
- Local handle services can resolve DNS requests in native form by reaching out to traditional DNS servers; it can also cache the results and regularly update them.
- Client software can access a handle service directly from an application, where appropriate and desirable.
- Where DNSSEC is not available, a DNS request can be mapped internally to a handle request immediately prior to accessing the Internet to take advantage of the security capabilities of the handle protocol.

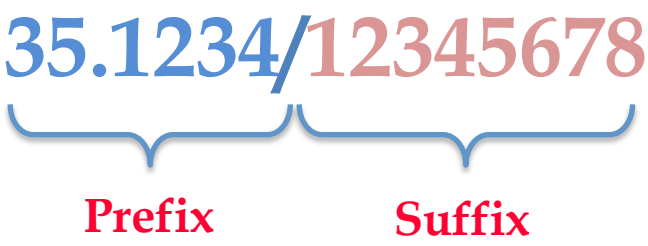
DONA

Handle System Security Features

- Authentication
  - Uses an optional PKI capability.
  - Handle service and client authentication.
- Authorization
  - Handles and associated handle records are administered by organizations or individuals authorized as either global or local handle service providers.
  - A handle service can restrict access to any of its values in a handle record.
- Confidentiality
  - All handle requests and responses can be encrypted.
- Non-Repudiation and Integrity
  - Handle record responses may be signed by the hosting server
  - Certain handle records must be signed by an authorized administrator (such as those records in the GHR); others may be signed as appropriate.
- Audit logs
  - Handle servers log certain metadata.

DONA

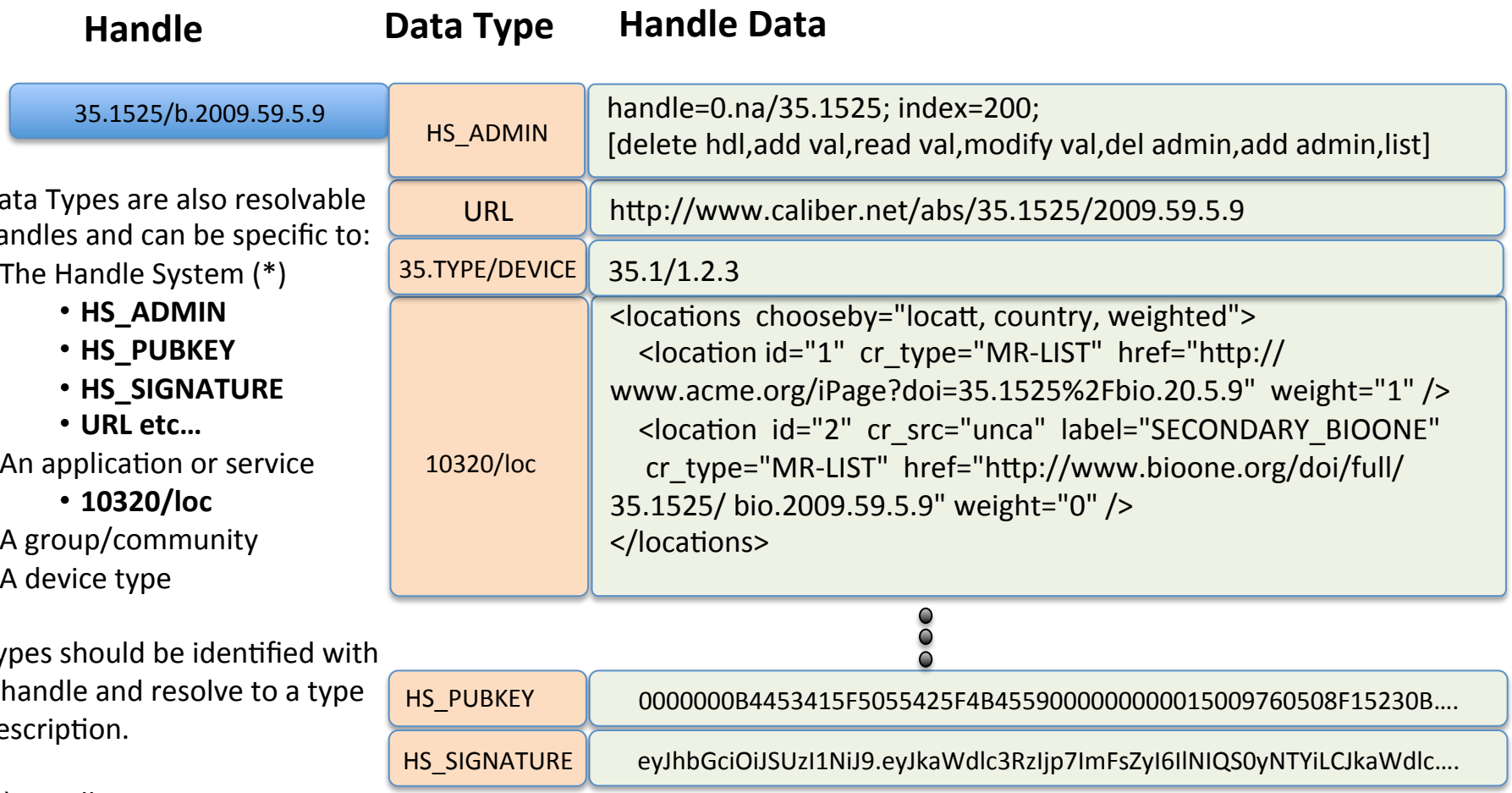
What is a Handle?



- Handles are globally unique and resolvable
  - Prefixes are allotted to local handle service providers; certain prefix handle records are stored in the "**Global Handle Registry**" (GHR) and others by local handle services.
  - A **handle prefix** is typically resolvable by the GHR to one or more ~~an~~ IP addresses for a local handle resolution service; the resolution information could provide public keys, authentication information, etc.
  - The **full handle** is resolvable by the **handle resolution service** into a handle record.
- Character Set: Unicode 2.0; Encoding: UTF-8
- Prefix: Currently allocating only numeric values.
- Suffix: No substantive restrictions.

DONA

Handle Record contains Typed Data



Data Types are also resolvable handles and can be specific to:

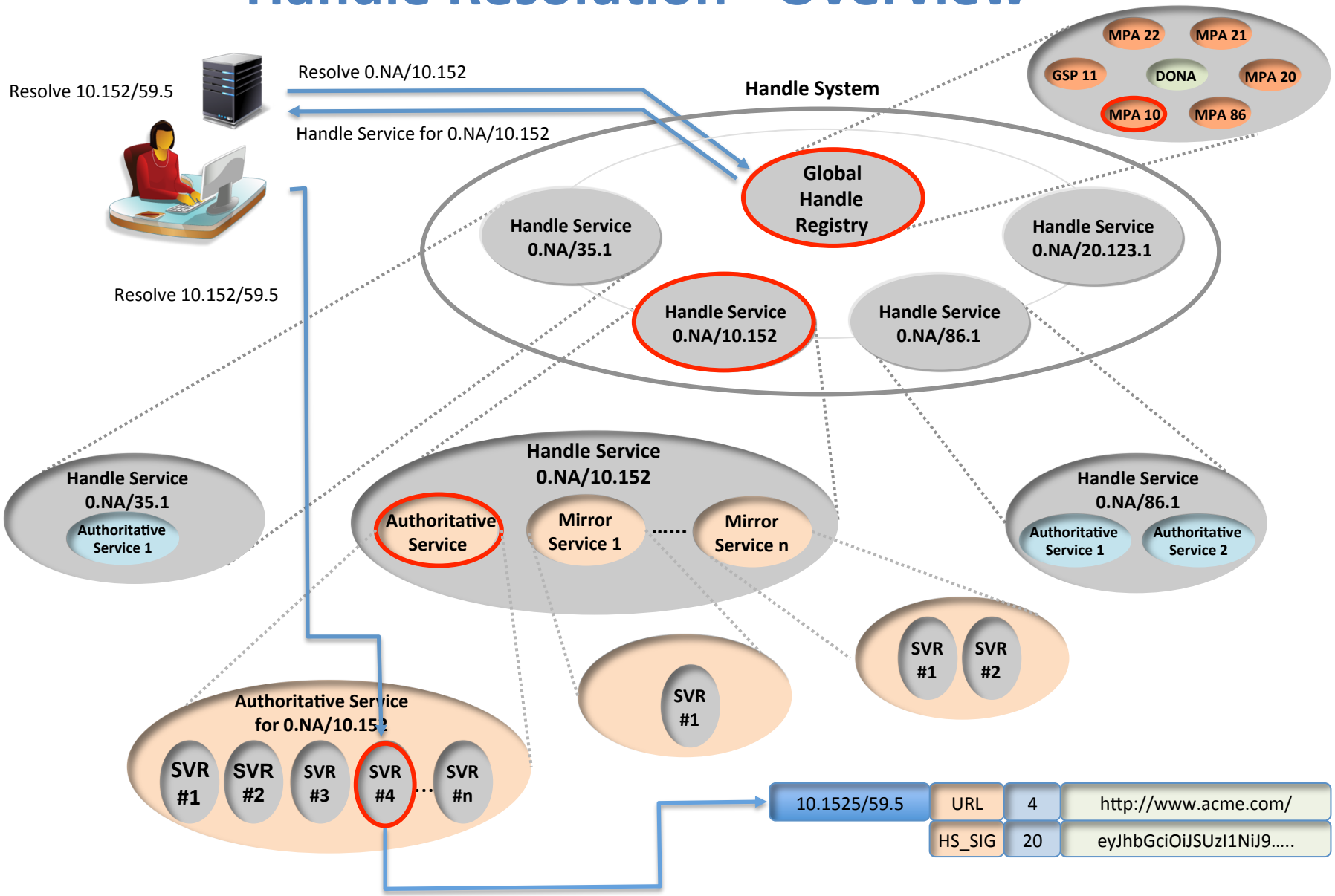
- The Handle System (*)
  - **HS_ADMIN**
  - **HS_PUBKEY**
  - **HS_SIGNATURE**
  - **URL etc…**
- An application or service
  - **10320/loc**
- A group/community
- A device type

Types should be identified with a handle and resolve to a type description.

(*) Handle System types are registered as handles starting with the “0.TYPE/” prefix. (URL -> 0.TYPE/URL)

DONA

Handle Resolution - Overview



Handle Resolution - Service Info Request

Request: Resolve 10.152/59.5

1. Client requests a specific GSP in the GHR to resolve the prefix handle 0.NA/10.152

Global Handle Registry

Security Features:

- **Privacy**: Encrypted client request
- **Authentication**:
  - Cryptographic authentication of the target GSP service
  - Cryptographic authentication of the resolving client
- **Audit trail**: GSP logs the full client request

Handle Resolution - Service Info Response

Client receives the Service Information for the 10.152 Service.

2. The targeted GSP Responds with the Service Information for the 10.152 service.

Global Handle Registry

xccccv	xc	xc	xc	...
xccccv xccx xccx	xc xc xc	xc xc xc	xc xc xc	.. .. ..
xccccv xccx xccx	xc xc xc	xc xc xc	xc xc xc	.. .. ..
xccccv xccx xccx	xc xc xc	xc xc xc	xc xc xc	.. .. ..

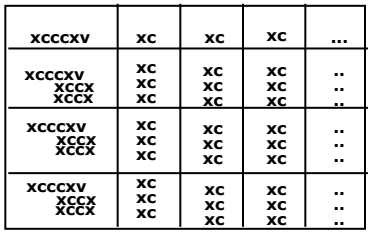
Handle Service Information

Security Features

- **Privacy**: Encrypted client request
- **Authentication**:
  - Cryptographic Authentication of the target GSP service
  - Cryptographic Authentication of the resolving client
- **Audit trail**: GSP logs the full client request

- **Privacy:** Response from GSP is encrypted
- **Authorization:** Response only provides what the authenticated client is allowed to see
- **Non-repudiation:** Service information is signed by the GSP service and it is verified by the client.

Handle Service Information



Handle Services	IP Addresses	Port Number	Public Key	…
Authoritative Service				
Service 1	12.34.45.67	2641	5ec6f944…	…
Service 2	12.34.56.68	2641	55fa26ca…	…
Mirror Service 1				
Service 1	12.45.67.71	2641	C77ee70…	…
Service 2	12.45.67.72	2641	22d81f1…	…
Service 3	12.45.67.73	2641	43a7a1f….	…
Mirror Service 2				
Service 1	32.23.23.12	2641	A80b56…	
Service 2	32.23.23.13	2641	b56757…	

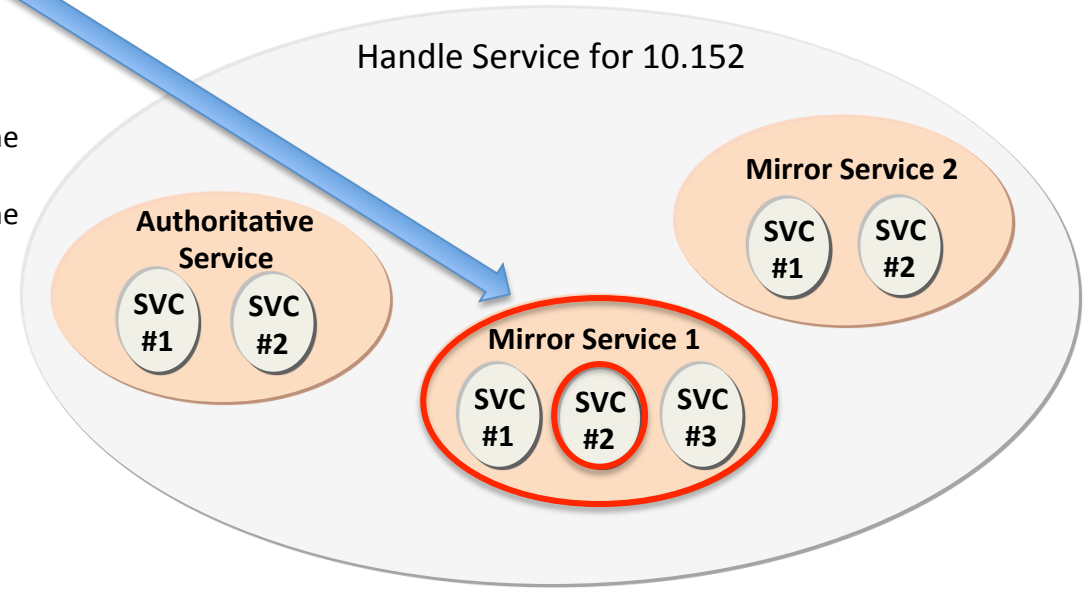
Handle Resolution – Handle Service Request

3. Client queries Server #2 in Mirror Service 1 to resolve 10.152/59.5

Global Handle Registry

Security Features

- **Privacy**: Encrypted client request
- **Authentication**:
  - Cryptographic Authentication of the target LHS service
  - Cryptographic Authentication of the resolving client
- **Audit trail**: LHS logs certain metadata.



Handle Resolution – Handle Service Response

10.152/59.5.9	URL	4	http://www.acme.com/
	HS_SIG	20	eyJhbGciOiJSUzI1NiJ9.....

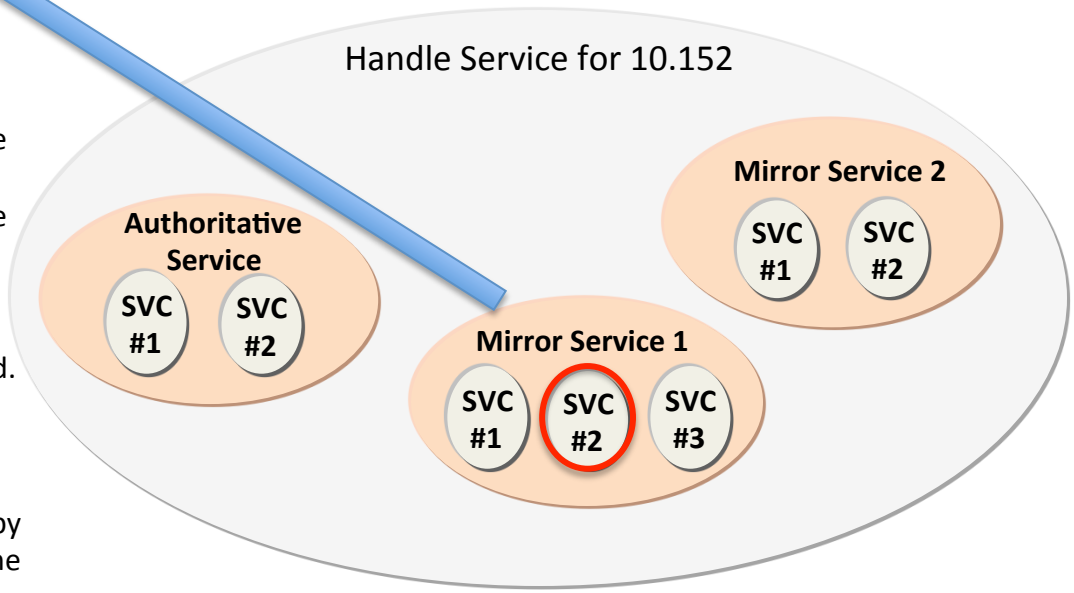
Global Handle Registry

4. Server responds with the 10.152/59.5.9 handle record

Security Features

- **Privacy**: Encrypted client request.
- **Authentication**:
  - Cryptographic Authentication of the target LHS service.
  - Cryptographic Authentication of the resolving client.
- **Audit trail**: LHS logs certain metadata.

- **Privacy:** Response from Mirror is encrypted.
- **Authorization:** Response only provides the values that the authenticated client is allowed to see.
- **Non-repudiation:** Handle record is signed by the Mirror Service and can be verified by the client.



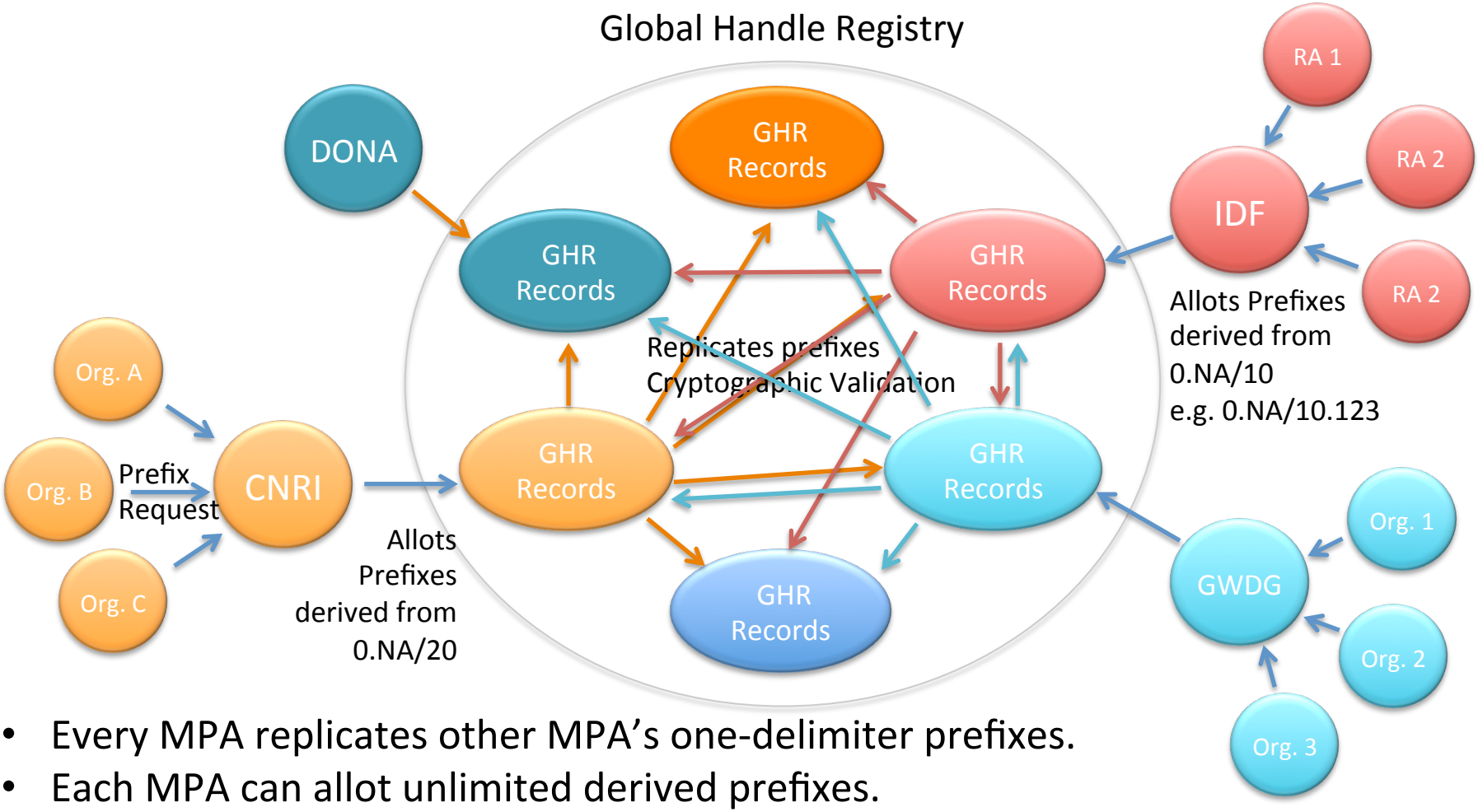
Acme Local Handle Service

Evolution of the Global Handle Registry (GHR)

- The original GHR was developed by CNRI; and operated by CNRI from 1993 - 2015.
- CNRI decided to further enhance and develop the GHR functionality to enable multiple organizations to participate in administering the GHR on a *multi-primary* basis.
- In May 2014, CNRI transferred the right to administer the GHR to the DONA Foundation, a non-profit organization founded by CNRI in Geneva, Switzerland.
- The Multi-Primary GHR first became operational on the 9th of December 2015.

DONA

MPA GHR Operations



- Every MPA replicates other MPA's one-delimiter prefixes.
- Each MPA can allot unlimited derived prefixes.
- An MPA can only allot derived prefixes from its allotted credential.

What is a Providers of GHR Services?

- An organization that is credentialed and authorized by DONA to create derived prefixes from its allotted credential prefix is known as a Multi-primary Administrator (MPA).
- Each such organization is allotted a credential (e.g., “21”) by DONA and authorized to provide GHR Services in accordance with DONA Foundation Policies and Procedures.
- Each such organization can create an unlimited number of derived prefixes from its credential and allot them to organizations to provide local handle services.
- The GHR Services verify and replicate all valid prefixes created/ modified in the GHR from the other MPAs.

The Role of the DONA Foundation

- Based in Geneva Switzerland.
- Provides coordination, software, and other strategic services for the technical development, evolution, and application of the Digital Object Architecture (DOA) with a mission to promote interoperability across heterogeneous information systems.
- DONA promotes ITU Recommendation X.1255, a standard based on the DOA, as well as the use of the DOA across many different countries, domains, and industries through pilot projects and other efforts in the public interest.
- Makes DOA standards and/or software publicly accessible to further their development and adoption.
- Credentials new MPA candidates.
  - Multistakeholder representation, geographical distribution, etc.

DONA

Foster Community Interests and Development

- DONA works with others to enable the development and availability of relevant standards, and reference software implementations in connection with the Handle System and other components of the Digital Object Architecture.
- Examples are:
  - IoT: development of identifier-based approaches to authenticate, type, describe, and foster interoperability.
  - Big Data: data identification, data typing, data type registries.
  - Authentication of distributed resources: development of a generic handle model and libraries for authenticating digital resources.
  - Using the Handle System as a bridge to other identifier resolution systems.

DONA

Thank You!