Georgia Tech School of Public Policy
Ivan Allen College of Liberal Arts

Internet Governance Project

DIGITAL OBJECT ARCHITECTURE AND THE INTERNET OF THINGS: GETTING A 'HANDLE' ON TECHNO-POLITICAL COMPETITION

Karim Farhat

Abstract

The promise of vast new markets has created an array of alliances and consortia to develop competing standards and protocols for the Internet of Things (IoT). The ITU - DONA Foundation alliance is one such example. DONA's Digital Object Architecture (DOA), a name-attribute binding service for managing distributed databases, presents itself as a potential solution for IoT challenges. But this proposed solution has been greeted with intense political opposition. Some have even called it an "Authoritarian Internet Power Grab." This working paper aims to answer the question of why a 1990s-vintage technical proposal regarding naming and addressing has generated such polarization. Although part of a broader debate on critical IoT considerations, deconstructing the politics of the DOA debate will help uncover whether it is a viable competing technology for the IoT or, as its critics argue, a threat to multistakeholder Internet governance.

DOA and the Internet of Things

Introduction

While nothing in the Internet of Things (IoT) is certain, most imagined futures suggest a multistakeholder model of governance and policymaking. This approach is intended, at least in theory, to resolve problems of collective action under the umbrella of private sector leadership in standards development and lightweight government oversight.[1] As an array of standards-setting organizations are strategically positioning themselves to address competition in the IoT space, a previously obscure alternative has emerged from the annals of 1990s-Internet Engineering Task Force (IETF) mailing lists. The standard in question is known as Digital Object Architecture (DOA), or sometimes as the *Handle System,* and has recently been the subject of heated exchanges on Internet fora.[2] Some of the alarmist outcries depict the resurgence of the Handle System as threatening "to kill off the diverse ecosystem of coexisting or competing identifiers."[3] Other critics have dubbed the sponsor of DOA, the DONA Foundation, a purveyor of "snake oil" and its service platform as an "authoritarian Internet power grab."[4] Proponents of DOA however, tout the

---

[1] The Department of Commerce (DoC) and State department have been officially operating under the principle of private sector leadership since the 1997 Framework for Global Electronic Commerce which concluded that it was "unwise and unnecessary for governments to mandate standards for electronic commerce". W3.org. (1997). *A Framework for Global Electronic Commerce*. [online] Available at: https://www.w3.org/TR/NOTE-framework-970706. This method was followed twenty years later in the NTIA's IoT proceeding. See, NTIA.doc.gov. (2017). *Fostering the Advancement of the Internet of Things*. [online] Available at: https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf

[2] DOA and the Handle system are not technically synonymous: the former is a higher-level abstraction of the actual architecture, and the latter is a key general purpose resolution mechanism for it. Think of it as packet-switching vis-a-vis TCP/IP - both denote semantic and technical differences but are practically very similar. Trade publications are using DOA and the Handle System interchangeably which created some undue confusion. IETF members were even using DOI and the Handle System synonymously in the 1990s.

[3] Lazanski, D. (2016). *The Problem With the United Nations Setting Tech Standards for Your Internet Devices*. [online] Council on Foreign Relations. Available at: https://www.cfr.org/blog/problem-united-nations-setting-tech-standards-your-internet-devices

[4] Rutkowski, A. (2016). *Selling DONA Snake Oil at the ITU*. [online] Circleid.com. Available at: http://www.circleid.com/posts/20161025_selling_dona_snake_oil_at_the_itu
Dourado, E. (2016). *How Russia and the UN are actually planning to take over the Internet*.

"security and scalability properties" of a "highly efficient infrastructure" that is capable of addressing looming IoT problems.[5]

The aim of this article is to critically evaluate claims that the Handle System, conceived and developed at the Corporation for National Research Initiatives (CNRI) and embraced by the International Telecommunications Union (ITU), threatens multistakeholder Internet governance through its potential impact on the IoT. The overarching questions motivating this effort are:

- Why has a seemingly obscure technical proposal regarding naming and addressing on the Internet generated such intense opposition?

- Is the issue at hand merely a technical deliberation or is the conflict motivated by other, more political concerns?

Doubtless, the technical and the political are interrelated. Evidently, DOA constitutes some form of institutional competition between - at the risk of oversimplification - two polarized global factions involved in Internet governance. One centers on the U.S. government and Western Europe as well as the private sector and the IETF. The other revolves around the ITU, BRIC countries and a growing number of developing nations. We can arguably conceive of two different hypotheses explicating the Handle System today. Either 1) it is a viable technology that will only succeed if it does its job better than the competing alternatives or 2) it is a threat to multistakeholder Internet governance through its strategic alignment to address the IoT.

I will attempt to address these considerations in this paper, starting with an overview of the Handle System and outlining relevant questions it raises. Then, I briefly revisit some of the original proposals around Uniform Resource Identifiers (URI), Uniform Resource Locators (URL) and Uniform Resource Names (URN) which are crucial to understanding the Handle System and DONA Foundation's positions on Internet governance today. I end on what the Handle System proposes to solve for the IoT including what I believe to be the substantive takeaways out of this whole affair.[6]

[online] TheHill. Available at: http://thehill.com/blogs/congress-blog/technology/295320-how-russia-and-the-un-are-actually-planning-to-take-over-the.

[5] Roussos, G. and Chartier, P., 2011, October. Scalable id/locator resolution for the iot. In Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing (pp. 58-66). IEEE.

[6] I thank Hascall 'Chip' Sharp for assistance with preliminary research and Dr. Milton Mueller for comments that improved the manuscript.

The issue is especially relevant today for a host of reasons. First, DOA is gaining prominence as a contender in the IoT governance space, especially through the International DOI Foundation it enabled.[7] The DONA Foundation is the Handle System's equivalent to the Internet Corporation for Assigned Names and Numbers (ICANN). Based in Geneva Switzerland, the Foundation's mission is "to provide management, software development, and other strategic services for the technical coordination, evolution, application and other use in the public interest around the world of the Digital Object Architecture…"[8] DOA arguably became a stone in the shoe of multistakeholder governance advocates because renewed interest and adoption is emanating from BRIC and developing countries - especially in the latter part of 2016. The Russian Federation is pushing for DOA in ITU Plenipotentiary conferences and World Telecommunication Standardization Assemblies (WTSAs) as a way of combating counterfeiting. Recently, Brazil, South Africa, Saudi Arabia, Rwanda, Tunisia, and Ghana have all endorsed DOA as evident from the 2016 ITU Session of the Council.[9]

---

[7] The most prominent of which is the International DOI Foundation (IDF) that consists of several consolidated international publishing trade associations that unified the digital publishing supply chain through a modified version of the Handle System. The IDF includes CrossRef (scholarly journal consortium covering most of the available literature); the Office of Publications of the European Community (EC documents); MEDRA (Multilingual European DOI Registration Agency) as well as Nielsen BookData, R.R. Bowker, et al (bibliographic data - ISBN). Notable deployments include the Library of Congress (LoC) and the Defense Technical Information Center (DTIC), the Organisation for Economic Co-operation and Development (OECD), etc. Kumar, V., 2009. Comparative evaluation of open source digital library packages. In *OSLS 2009: National Seminar on Open Source Library Solutions, held on 16-17 January 2009 at Dept. of Library and Information Science, Banaras Hindu University, Varanasi, India*.

[8] DONA Foundation. (2014). *Dona Foundation Statutes*. [online] Available at: https://www.dona.net/documents/public/144fc0bf2534/DONA_Foundation_Statutes.pdf

[9] South Africa signed a Multi-Party Administrator (MPA) service agreement with the DONA Foundation, Rwanda followed in South Africa's stead and recently signed an agreement to acquire DOA and become a GHR.
Wyngaardt, M. (2016). *Cwele urges African govts to close the digital divide*. [online] Engineering News. Available at: http://www.engineeringnews.co.za/article/cwele-urges-african-govts-to-close-the-digital-divide-2016-10-17/rep_id:4136.
Muvunyi, S. (2016). *New system to enhance digital management*. [online] The New Times Rwanda. Available at: http://www.newtimes.co.rw/section/article/2016-10-21/204637.

The Russian delegation commented that: "Indeed, the arguments expressed during the discussions at that meeting appear in fact to reflect a wish to maintain a monopoly and not allow any competition in the management of Internet resources, in particular in regard to IoT deployment." Saudi Arabia commented that they encourage the ITU "to reach out to all industries and sectors, in particular those in the developing countries, to provide them with technical assistance, including assistance related to the applications based on DOA."
Itu.int. (2016). *Proposals regarding the master framework agreement (MoU) between ITU and*

Recent undertakings by the DONA Foundation, most notably the signing of a Memorandum of Understanding (MoU) with the ITU and the WTSA-16, were met with fierce antagonism by some Washington telecommunications policy pundits and opponents of the old ITU regime.[10] WTSA-16 was seen as a break in the ITU's technology-neutral stance. Second, and perhaps more importantly, the Handle System and DOA are part of a broader, more meaningful debate on critical IoT considerations including security and privacy, device shelf-life, and persistent identifiers.[11] Finally, the Handle System alternative could help catalyze the discussion over the future of networking and infrastructure concerns for the IoT.

The Handle System: a history

The original impetus behind DOA stems back to the 1980s when the Corporation for National Research Initiatives (CNRI) was working on a digital libraries program.[12] The Defense Advanced Research Projects Agency (DARPA) funded CNRI in a collaborative effort with different research universities to help digitize existing collections and homogenize different e-libraries under a unified archival system. This requirement prompted and solidified the Handle System's *raison d'être* as a distributed system for the secure management of libraries, digital documents and archival records. It is perhaps best to think of the Handle System as "a name-attribute binding service with a specific protocol for securely creating, updating, maintaining, and accessing a distributed database."[13] In

---

the DONA Foundation. ITU-SG CL Contributions 89 and 93. [online] Available at: https://www.itu.int/md/S16-CL-C-0089/en.

[10] Most notably the US delegation at the ITU expressed support for termination of the Master Framework Agreement, including a voluntary contribution from the DONA Foundation to ITU in support of activities related to the Digital Object Architecture at the 2016 Plenipotentiary ITU. Itu.int. (2016). *Proposals regarding the master framework agreement (MoU) between ITU and the DONA Foundation. ITU-SG CL Contribution 78.* [online] Available at: https://www.itu.int/md/S16-CL-C-0089/en.

[11] The Handle System includes the open protocol, the namespace and the reference implementation of the actual protocol. DOA refers to the overarching protocol architecture.

[12] Their knowbot program which helped guide the DOA effort. Cnri.reston.va.us.(2014). *Knowbot Programs*. [online] Available at: https://www.cnri.reston.va.us/knowbot_programs.html

[13] As described in RFC 3650. Refer to informational RFCs 3650 for a more thorough overview and 3651 and 3652 for more detailed operational analysis.
Sun, S., Lannom, L. and Boesch, B., 2003. *Handle System Overview (RFC 3650)*. Technical report, The Internet Society (ISOC)–IETF.
Sun, S., Reilly, S. and Lannom, L., 2003. RFC 3651: Handle system namespace and service definition.

other words, it was designed to be an expert librarian. However, some of the inherent properties of DOA afforded it more potential than a boilerplate archivist, not the least of which was the name-attribute bind that distinguishes it from DNS and other naming schemes.

Developers of the Handle System were adverse to the original DNS design on ontological grounds. DNS, they claimed, "conflated addresses to serve two purposes:" a designator for a resource's *location* and another for its *identity*.[14] With the benefit of some hindsight, features that were found wanting in the IETF suite were added to DOA, including persistence,[15] multiple entry points for a service with a single handle,[16] and access control by design.[17] These value differences led to a fundamental divergence and competition between the two networking schemes. Beyond the technical trade-offs implied by the end-to-end principle, the DNS tradition ensured a network that is mostly agnostic to the resource in question and is more concerned with reliable addressing. With DOA however, the digital resource is considered the "first class citizen" as I further elaborate in the next section.

Handle Syntax

The primary Handle namespace identifier consists of two parts: a prefix - administered at the Global Handle Registry (GHR) – and a suffix designating the local namespace - which is managed at the Local Handle Service (LHS) level.[18]

Sun, S.X., Reilly, S., Lannom, L. and Petrone, J., 2003. RFC 3652: Handle system protocol (ver 2.1) specification. *The Internet Society (ISOC)-IETF, Tech. Rep.*

[14] Paskin, N. (2007). *ITU Focus Group on Identity Management Geneva [PowerPoint presentation]*. [online] Doi.org. Available at: https://www.doi.org/doi_presentations/070207-ITU-Handle.ppt.

[15] Lack of persistence most commonly looks like the infamous HTTP error 404: by tying a resource to a local file path on a server as part of that URL, if the resource changes location, the URL breaks.

[16] Better load distribution by referencing an HS Caching service in the Handle metadata.

[17] For example, despite being as potentially scalable and distributed as the DNS, access control features can be setup in a way where a user needs authorization before they can read the attributes of an identifier, this has obvious applications to the copyright industry. Varakliotis, S., Kirstein, P.T. and Deiana, G., 2015, June. The use of Handle to aid IoT security. In *Communications (ICC), 2015 IEEE International Conference on* (pp. 542-548). IEEE.

[18] The full handle record has more fields including indexes for data types, metadata, cryptography, etc. This paper only includes a minimal technical description. For a graphical representation of the global Handle System, refer to the following presentations:

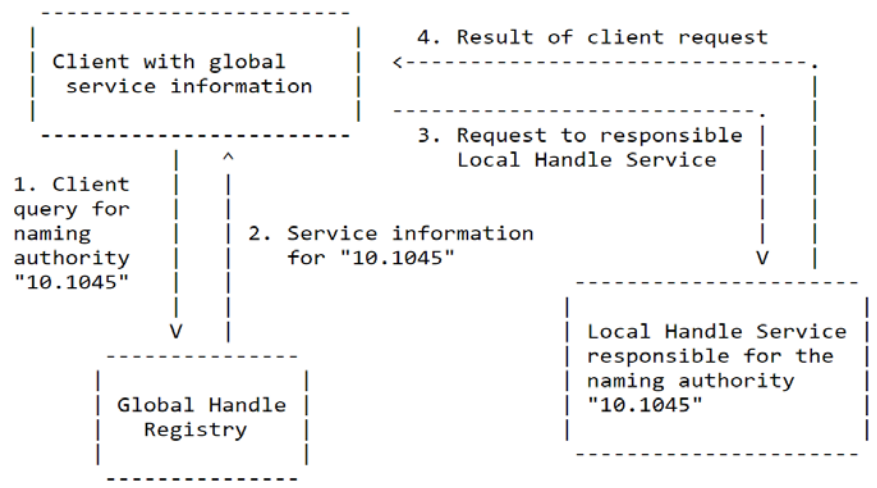
Lannom, L. Handle.net. (2008). *2008 Handle System Workshop. [PowerPoint presentation]*. [online] Available at:

The GHR serves as the root authority for LHRs. It assigns prefixes, describes how the servers are distributed and replicated and provides service information for the LHRs. LHRs and the GHR share certain characteristics, however, including that they may consist of one or more replicated services sites (handle servers which may be a cluster of low powered systems), which have the same set of handles distributed among each other through a hashing mechanism (RFC 3651). Note that the GHR functions are logically centralized but physically distributed.

For example:

<Handle> = <NamingAuthority> "/" <LocalName>

A handle might be 123/itu.pdf. Once a prefix is reserved with the GHR, the handle is globally unique and resolvable by a handle service into a set of typed values i.e. an object.[19] DOA achieves resolution either using DNS or the Handle.Net software (currently HN_v8.1).[20] The following figure provides a simple outline of how a handle is resolved:



(Fig. 1 from RFC 3650)

---

http://www.handle.net/workshop_08/presentations/HDL_WrkshpIntro_June08.ppt
Blanchi, C. (2016). *Digital Object Architecture and The Handle System*. [online] Diplomacy.edu. Available at: https://www.diplomacy.edu/sites/default/files/Technical%20Innovation%20-%2025-4-2016%20-%20Christophe%20Blanchi.pdf.

[19] Prefixes may be of any length and may include different numbering schemes. Shorter prefixes (1-3 digits) are usually reserved for major projects (such as the prefix <loc> for the Library of Congress), or for countries.

[20] The Handle System does not require DNS, but it can leverage it through a proxy server. Other middleware also include handle caching servers.

Handle System structure and governance

As of 2010, the Handle System resolved on average 68 million direct requests per month using the Handle software and another 50 million relayed by DNS.[21] Despite achieving a significant number of resolutions, the global DNS resolves more in a day than DOA resolves in a year, so we are still very far from what can be considered an effective competition. The Handle System is logically decentralized (and hierarchical) around the GHR cluster but physically and organizationally distributed across service sites. The Handle System is also modular, i.e. it works with other protocols on different layers and can make use of a variety of other features (including non-repudiation, layered access control or multiple attributes) to fit a given application. The initial design was a patented system[22] "that respects and protects rights, interests and value"; in other words, it was clearly poised to address Digital Rights Management (DRM) as we saw with DOI and later with the Entertainment Identifier Registry (EIDR) and other schemes.[23] Recently, the Handle System underwent significant changes in its governance structure, but its fundamental values remain the same.[24]

In December 2015, the handle userbase requested the decentralization of prefix creation across multiple organizations. A new 'Multi-Primary GHR architecture' was developed through the creation of the DONA Foundation in Geneva to oversee all operations. Under the new governance structure, CNRI, which previously had the sole authority to create all new prefixes, now shares administration with other entities that entered a service agreement with DONA as Multi-Primary Administrators (MPA).[25] Only the DONA board can authorize

---

[21] Hassanmahomed, T. (2010). *Identifying and retrieving digital objects: A Study of the Handle System*. [online] Delaat.net. Available at: http://www.delaat.net/rp/2009-2010/p05/report.pdf.

[22] The Handle System's patent only recently expired.

[23] Paskin, N. (2007). *ITU Focus Group on Identity Management. [PowerPoint presentation]*. [online] Doi.org. Available at: https://www.doi.org/doi_presentations/070207-ITU-Handle.ppt.

[24] Itu.int. (2006). *ITU-T Workshop on Digital Identity for Next Generation Networks*. [online] Available at: https://www.itu.int/md/T05-TSB-CIR-0118/en.

[25] There are five Multi-Primary Administrators (MPAs) as of 2016, including CNRI, the IDF the GWDG in Germany, the Communications and Information Technology Commission (CITC) of Saudi Arabia and the Coalition for Handle Services (ETIRI / CDI / CHC), a Chinese consortium funded by the Chinese Ministry of Industry and Information Technology (CDI). According to minutes from a DONA Foundation board meeting in July 2016, "the current goal is to increase the number of MPAs to approximately twelve (12) in the next few years" i.e. one less than there are DNS root servers. Note that MPAs sub-delegate assigned numbers just like Regional Internet Registries (RIRs).
Dona.net. (2016). *Dona Foundation Board of Directors Meeting, Summary of the Minutes*. [online] Available at:

new MPAs however. MPAs are organizations credentialed and authorized by DONA to create and administer their own prefixes thereby adding an extra layer of hierarchy and data redundancy within the GHR in what they refer to as Multi-Primary GHR Architecture.[26]

The DONA Foundation likes to keep reminding us of the "non-Proprietary Status of the Digital Object Architecture."[27] Any individual or organization can join the system by becoming a Local Handle Service (LHS) and request prefixes after signing the Handle.Net Public License Agreement (ver. 1) for the use of the software. While it is true that software licensing is 'open' it comes with a caveat: a paid subscription service and the threat of license termination at "CNRI's sole discretion." Subscription involves paying a one-time $50 Registration Fee (for each new prefix allotted), followed by an annual Service Fee of $50 per prefix.[28] The astute reader would have recognized how reminiscent this situation is of the ICANN regime for domain names; i.e., a single root that accredits registrars and registries and imposes fees upon them for doing so.

At this point, you may be asking yourself: why would the ITU be interested in all of this? In a workshop on Digital Identity for Next Generation Networks in December 2006, the ITU stated "the network level and in general lower layers have not been addressed sufficiently with regard to digital identity, and this remains a weak point in standardization and research."[29] This excerpt from the MoU signed between the ITU and the DONA Foundation is a little more telling:

> *"ITU will provide assistance to the DONA Foundation with respect to public policy issues and questions referred to it by the DONA Foundation; provide secretariat services to the DONA Foundation in support of the*

https://www.dona.net/documents/public/eb347173ba31/2016%20DONA%20Board%20Sumary%20Minutes.pdf

[26] Blanchi, C. (2016). *Digital Object Architecture and The Handle System*. [online] Diplomacy.edu. Available at: https://www.diplomacy.edu/sites/default/files/Technical%20Innovation%20-%2025-4-2016%20-%20Christophe%20Blanchi.pdf.

[27] Dona.net. (2017). *DONA Foundation Statement Non-Proprietary Status of the DO Architecture*. [online] Available at: https://www.dona.net/documents/public/750a25a26b83/Statement%20re-proprietary%20DOA.pdf

[28] Handle.net. (2017). *Handle.Net Registry*. [online] Available at: http://www.handle.net/payment.html.

[29] Bertine, H. and Sarma, A. (2006). *Digital Identity for Next Generation Networks*. [PowerPoint presentation]. [online] ITU.int. Available at: https://www.itu.int/dms_pub/itu-t/oth/06/04/T06040060020001PDFE.pdf.

> *mission in accordance with applicable ITU rules and regulations including cost recovery (…) ITU will accept the DONA Foundation's voluntary contribution of, and thereafter hold, the IPRs and licences [sic] in GHR technology and software which are sufficient to enable ITU to reconstitute the GHR system as necessary. The voluntary contribution of licensing rights for this purpose will be administrated by ITU (…) All DOA-based applications and solutions with external entities will be undertaken based on the principle of full cost recovery and some aspects of revenue generation for ITU.*[30]

It's no secret that the ITU is struggling to maintain its relevance and revenue stream in the 21st century.[31] As the ICANN model can tell us, there are obvious monetary advantages to becoming a naming authority, especially when dealing with a subscription model. DOA is already deployed in the UN system, and the ITU is envisioning applications in anti-counterfeiting, copyright and "the traceability of the flow of funds."[32] Usually, with uniquely assigned resources, one pays a fee for maintaining an entry in a registry and the periodic nature of the fees also makes it possible to know who is active and remove free-riders. This is currently the case with DNS: ICANN charges licensing fees to approved top level domain registries as well as fees for accrediting registrars, who in turn bill their customers for individual domain name registrations.[33] Attacks on DOA being a "lucrative global money making operation" could be just as easily be pointed towards the ICANN regime.[34] But are the servers making real-time handle resolution necessary? Couldn't we just leverage DNS for DOA and leave it at that? The end-to-end model of networking was designed to allow open competition at the application layer; therefore, DONA has a right to compete. A more pertinent question also comes to mind. The DONA Foundation recognizes

---

[30] Itu.int. (2015). *Digital Object Architecture (DOA) and the master framework agreement between ITU and the Dona Foundation*. [online] Available at: https://www.itu.int/md/S15-CL-INF-0013/en.

[31] Drake, W.J., 2000. The rise and decline of the international telecommunications regime. *Regulating the global information society*, pp.124-177.

[32] Itu.int. (2015). *Digital Object Architecture (DOA) and the master framework agreement between ITU and the Dona Foundation*. [online] Available at: https://www.itu.int/md/S15-CL-INF-0013/en.

[33] Registries such as VeriSign, are organizations that manage top-level domain names (.com and .net for VeriSign) by creating extensions, setting the rules and working with registrars to sell domain names to the public. Registrars are authorized organizations that sell domain names to the public.

[34] Rutkowski, A. (2016). *Selling DONA Snake Oil at the ITU*. [online] Circleid.com. Available at: http://www.circleid.com/posts/20161025_selling_dona_snake_oil_at_the_itu/.

that informational RFCs 3650-1-2 are now “in need of updating” and regards the ITU’s X.1255 as a stepping stone towards eventual complete standardization.[35] But why was the Handle System not actually standardized in the IETF? It would have undoubtedly granted the entire DOA architecture more positive network externalities and would have saved CNRI the trouble of having to travel the disused ITU road. Did “rough consensus and running code” not apply for DOA? For that matter, why was the Handle System mostly ignored outside of its original usage-contexts of data management? The answer to this and the previous question takes us back to the original URL-URN-URI debate at the IETF.

The Handle System forks from the IETF

The original discussions over web-based identifiers delved into ontological debates on the meaning of an ‘object’: is a URI denoting the object itself or a representation of that object and how is a distinction between the two made?[36] For instance, if a URI is identifying a news article and if that news article is updated the next day, should the URI change because the article changed? It was agreed that an identifier could denote a location of a resource (a URL), or its name regardless of its location (a URN).[37] Therefore, a URI was either a URL, which identifies resources by network location through a particular access protocol such as HTTP or FTP, or it is a URN which is a persistent, location-independent identifier assigned within specific namespaces by a given authority and held at the Internet Assigned Numbers Authority (IANA). The point of URNs was to have unique and persistent identifiers even after the resource which they identify ceases to exist or becomes unavailable. For example, any resource with a random URL such as http://www.foobar.com/baz/frob.html risks having the reference link invalidated if a web site administrator changes the location of that resource. Using a URN, however, (say in the ISBN namespace) would provide users with persistence. Over time, the importance of this additional level of hierarchy decreased, and URL/URI were used interchangeably.

Back in 2001, the World Wide Web Consortium (W3C) released a paper in an attempt to clarify some of the distinctions between web-based identifiers. Given that the Handle/DOA issue was still prevailing, they included an

---

[35] Itu.int. (2013). *Framework for discovery of identity management information*. [online] Available at: https://www.itu.int/rec/T-REC-X.1255-201309-I.

[36] (M. Mealling 2017, personal communication, 13 May).

[37] Arms, W. (1996). *URN Agreement Check List*. [online] Lists.w3.org. Available at: https://lists.w3.org/Archives/Public/uri/1995Dec/0007.html.

"unregistered NIDs" (Namespace IDs) category which accounts for "bonafide Namespace IDs that just haven't bothered to even explore the process of registration" [with the IETF]. The paper went on to refer to the Handle System as "the most prominent case that comes to mind," and speculated that "[the Handle System] has not been registered because it is not clear to the owners whether it should be registered as a URI scheme or as a URN namespace."[38] Clearly, the Handle system was part of the original URN discussions but was never standardized at the IETF. Why not? The latest attempt to finalize the URN standards-track, RFC 8141, (April 2017) does not even mention the Handle system and contains no provision for any rogue, unregistered URNs. It seems that as far as the IETF is concerned, Handle/DOA no longer exists. What happened in the interim?

Hints at the answer can be found in the original IETF working group mailing-lists. These suggest that the Handle system's promoters were equivocating on its URN registration intentionally.[39] Although readers should examine the original mailing list archive for a richer coverage of the exchanges, the following excerpt summarizes the crux of the discussion. Michael Mealling of the original IETF-URN working group writes:

> *DOI (handles) were actually part of the URN discussions way back in '93. (...) Larry Lannom [the Director of Information Services and Vice President at the Corporation for National Research Initiatives] was there in all of the meetings. He knows full well that key parts of the URN design were specifically put there to accommodate handles. Contrary to what some in the DOI world think, DOIs have always been valid URNs and could have easily sidestepped this entire discussion and issue by simply registering as a URN namespace. The only reason I can come up with that they wouldn't want to do that is that they see the entire URN space as competition for their namespace (sorry guys, I'm tired of not calling it as I see it). (...) I can see no other reason for this request than their attempt to create a monopoly namespace that will compete directly against URNs and other standards.*[40]

Mealling goes on to refer to the large amount of "business development I've seen being done by CNRI (a non-profit!) in other for a," which leads him to

---

[38] W3.org. (2001). *URIs, URLs, and URNs: Clarifications and Recommendations1.0*. [online] Available at: https://www.w3.org/TR/uri-clarification/.

[39] Lists.w3.org. (2003). *Re: DOI and the non-IETF tree*. [online] Available at: https://lists.w3.org/Archives/Public/uri/2003Sep/

[40] Ibid.

believe that “they are attempting to build their own proprietary, CNRI-run alternative to URIs (complete with a private DNS-like root!).”

Larry Lannom of CNRI wrote in reply:

> *“(...) I can't speak for others, but I am not being disingenuous. I can assure you that the DOI community and the various handle system users are not alone in wondering which way to go with the various url/urn/uri questions. In terms of the handle system, we are on what we consider to be a logical path and in front of any kind of IETF id registration is the complete specification of the system itself in the form of informational RFCs. You may have received different impressions over the years from other people at CNRI, but any course changes were due to our own indecision, not to any grand Machiavellian schemes.*

In reply, Mealling voiced suspicions about CNRI’s repeated refusal to register the Handle System as a URN namespace within IETF standards.[41] Based on the current direction of the Handle System’s governance structure, it should come as no surprise to hear Michael Mealling say 17 years later that Robert Kahn – co-inventor of TCP/IP and father of DOA – was motivated to develop and control his own URN technology for business purposes. According to Mealling, Kahn “was looking at what Verisign had been able to do, Network Solutions, with having a monopoly and how much money it generated and that was his play.”[42]

The Handle System and IoT

DOA and the Handle System were initially conceived with something else in mind: the management of libraries and digital documents. The Handle System is, in fact, a very efficient means of achieving what it was originally designed to do: act as a library repository and information retrieval system with persistent identifiers. Even the IETF and Internet Society (ISOC) use it for those purposes. Once you bring that mix into the IoT space, however, the scale changes by many orders of magnitude, and concerns such as security, privacy, and efficiency become paramount. In other words, there are many reasons to continue ignoring it. Although most industry players regard the idea of having globally unique identifiers as a means of trusted authentication for IoT as a good

---

[41] Ibid. It is worth noting that this review would not have been possible without the IETF’s open and archived deliberation process. In comparison, processes of the ITU and the DONA Foundation lack transparency, as noted in Sharp, C. (2016). *Overview of the Digital Object Architecture (DOA)*. [online] Internetsociety.org. Available at: https://www.internetsociety.org/sites/default/files/ISOC-DOA-Overview-20161025-A4-3_0.pdf

[42] (M. Mealling 2017, personal communication, 13 May).

one, as far as we know no private sector software company is currently considering applying DOA to Internet of Things solutions. Major global industry standards bodies have developed their own specialized tagging platforms and have rejected the use of DOA to combat counterfeiting.[43] The currently preferred method of secure resolution is that of 802.1AR "Secure Device Identity" that leverages Certificate Authorities (CA). Although this method is far from perfect as CAs are susceptible to spoofing, they are often supplemented with different schemes such as including hardware-level signature to establish a 'chain of trust.'[44]

Proponents of DOA contend that their solution not only is viable but is, in fact, a better functioning technology.[45] Theoretically, the Handle architecture could contribute to unifying part of the IoT within a single structured address and identifier space. However, we currently lack any real-world applications of the required scope and scale. DOI provides a significant real-world application, but its scale is far lower than DNS and its ability to scale up to levels anticipated for widespread IoT applications is speculative. Claims that the Handle System is more secure are also speculative. The Handle System actually leverages the same tools for secure communications (PKI, TLS, SSH, etc.) as the rest of the Internet and is susceptible to the same types vulnerabilities as regular DNS. As of 2016, the Handle software requires utilization of Java 6 which has a known vulnerability.[46] In terms of speed and efficiency, a network engineering student at the University of Amsterdam ran a simple comparative deployment of handles and DNS, and concluded that "resolution [of the Handle System] is not as fast as DNS and (…) it does not always efficiently handle fail-over when a [sic] LHS server fails to respond, but it still resolves the handles eventually. Fail-over would require much more effort with other systems, like DNS, when comparing

---

[43] (C. Sharp, 2017 personal communication, 24 February). The GSMA use the International Mobile Equipment Identity Database (IMEI DB).

[44] Including Cisco's Trusted Platform Module, Intel's Trusted Execution Technology or the upcoming Bootstrapping Remote Secure Key Infrastructures (BRSKI), an ongoing collaboration between Juniper Systems and Cisco for a new method of key distribution on non-constrained IoT devices (class 2+). (E. Lear 2017, personal communication, 27 February).

[45] Researchers at CNRI conceptualized Strong Authentication schemes Based on PKI and Handles. Reilly, S. and Tupelo-Schneck, R., 2010. Digital object repository server: A component of the digital object architecture. *D-Lib Magazine*, *16*(1/2).

[46] Rogers, D. (2016). *Dead on Arrival? What's next for IoT security?*. [online] Blog.mobilephonesecurity.org. Available at: http://blog.mobilephonesecurity.org/2016/10/dead-on-arrival-whats-next-for-iot.html.

to [sic] the simple setup needed for the Handle system."[47] Being tied up in political issues interferes with an objective technical evaluation. So far, the need for running a large-scale testbed for DOA seems to be outweighed by its cost.

Now for the big question: do the Handle System and its governance structure constitute a threat to the open Internet through potential applications in the (IoT)? Given that policy for DOA is now shared between the DONA board and the ITU, some observers see a danger that 'special' stakeholders or nation states gain leverage on a system of governance shrouded behind a veil of politics.

In our opinion this is not a severe threat. IoT standards are a complex space with many moving parts. Given how high the commercial stakes are and how many different interests are involved with Standards Development Organizations, the ITU/DONA Foundation marriage is only one amongst many alliances, and DOA is only one amongst many technologies.[48] The alarmist arguments have the DONA Foundation achieving a highly improbable trifecta: centralizing power through MPAs/governments which cherry-pick online content; bypassing existing governance processes and transferring decision-making to an inter-governmental rather than multi-stakeholder process. It's not clear how they could ever pull this off. Despite being an intergovernmental treaty-based organization, the ITU has no dictatorial powers when it comes to enforcing standards on the hundreds of equipment manufacturers, software developers and users across the board.

We saw a lot of similar flag waving about an ITU takeover of the Internet in 2012. The ITU's revision of its International Telecommunication Regulations (ITRs) during the World Conference on International Telecommunications (WCIT-12) was also supposed to pose a huge threat.[49] Two years later, similar arguments were made about the IANA transition, which was supposed to deliver the Internet to Russia, China or the ITU. But in both cases, the threat was

---

[47] Hassanmahomed, T. (2010). *Identifying and retrieving digital objects: A Study of the Handle System*. [online] Delaat.net. Available at: http://www.delaat.net/rp/2009-2010/p05/report.pdf

[48] Other notable unions include the Open Connectivity Foundation, the LoRa and AllSeen alliances, and the Industrial Internet Consortium.

[49] Mueller, M. (2012). *Threat Analysis of ITU's WCIT (Part 1): Historical context* |. [online] Internetgovernance.org. Available at: http://www.internetgovernance.org/2012/05/24/threat-analysis-of-itus-wcit-part-1-historical-context/

Mueller, M. (2012). *Threat analysis of WCIT part 2: Telecommunications vs. Internet* |. [online] Internetgovernance.org. Available at: http://www.internetgovernance.org/2012/06/07/threat-analysis-of-wcit-part-2-telecommunications-vs-internet/.

overstated, if not invented. The basic institutions and models of Internet governance are unchanged. The only time the ITU arguably got close to successfully controlling the root of the Internet naming system was between 1996-1997, when it was cooperating with the Internet Society and the IETF.[50] In other words, despite the current tendency for some countries to laud DOA and lament the lack of multilateralism in Internet governance, this is really an issue of technical and economic competition, and the ITU and DOA are in a weak position. Although a close monitoring of how DOA unfolds is warranted, the whole affair should not be blown out of proportion as I summarize next.

Conclusion

There are three essential takeaways from the recent reemergence of DOA:

1. The ITU/DONA alliance is just one of many competing approaches to the IoT. Although clearly in competition with DNS and the ICANN regime, this competition seems to be more about generating revenue for the Handle system developers than controlling the identifier system. Handle System backers seem to have opted out of the mainstream IETF standards process in order to be able to cash in if it succeeds. Exiled from the IETF and ISOC circles, they turned towards the ITU. The ITU has a congruent interest in generating revenue and in maintaining its relevance. Thus, ITU and DONA's need for a sandbox outside of the ISOC/ICANN regime to compete is understandable. But the fact is, both DOA and ITU are relatively isolated in the overall Internet governance regime and the IoT business. DOA does not constitute a significant threat to the existing frameworks.

2. When it comes to applying DOA to Industrial IoT, there are few if any signs of DOA adoption by the private sector outside the original usage-context i.e. DOI. The IoT standardization process is extremely complex and diverse at the moment. It faces the same challenges as many other standards which combine aspects of both public and private goods. The method of standards' production is "a societal choice of significant

[50] In the race to control the DNS root zone file in the mid-1990s, the International Ad Hoc Committee (an alliance between ITU, ISOC, IAB, INTA and WIPO) and its gTLD-MoU proposal could have shifted the balance towards intergovernmental control.
Mueller, M. (2002). *Ruling the Root: Internet governance and the taming of cyberspace,* Ch.7 The Root in Play. MIT Press.

consequence."[51] If history serves, companies will strive for market dominance by focusing on tightly guarded proprietary technology that is developed in-house. Technical considerations of efficiency are secondary to having an exclusionary competitive edge when it comes to, say, interoperability across supply chains. However, proprietary standards have trouble realizing network externalities, and as development matures, innovative products become more standardized through alliances, consortia and SDOs. As for open standards developed at the IETF, public benefit is always produced but those standards mostly give an edge for private firms (such as Cisco, Huawei, Ericsson Nokia or Juniper Systems) whose engineers moonlight at the IETF. In that sense, IoT development will likely face a variety of competing alternatives that coexist serving different applications and jurisdictions.

3. The U.S. Department of State through its Bureau of Economic and Business Affairs' Office of International Communications and Information Policy (EB/CIP) has a distinct position when it comes to the ITU and Internet governance. For example, the U.S. was unequivocal in wanting to remove any mention of DOA from the outline report of the WTSA October 2016 conference[52]. Moreover, I have it on good authority that after an MoU was signed between the ITU and Georgia Tech's Center for Development and Application of Internet of Things Technologies (CDAIT), the State Department asked Cisco (who are on the board of CDAIT) to clarify their position and refrain from encouraging DOA-related activity. The U.S. has a vested interest in keeping the status quo when it comes to Internet governance and U.S. companies feel the pressure to stay in-line with that agenda. The implication is not only that western private companies have an additional incentive to stay away from DOA, but also that the U.S. government shares as much responsibility for politicizing the DOA vs. DNS choice as the ITU does.

There are many IoT considerations still open for debate. The National Telecommunications and Information Administration (NTIA) process on 'Fostering the Advancement of the Internet of Things' is one of those fora where the conversation is ongoing and the mainstream U.S. government/private sector

---

[51] Congress, U.S., 1992. Office of Technology Assessment. Global Standards: Building Blocks for the Future. *TC-F-512, Washington DC, US Government Printing Office*.

[52] Internetsociety.org. (2016). *ITU WTSA 2016 Outcomes An Internet Society Perspective*. [online] Available at: https://www.internetsociety.org/sites/default/files/ISOC-WTSA16-Outcomes-20161122.pdf.

view is being synthesized in an authoritative albeit non-binding process.[53] It should be noted that although anyone can get involved in the open multistakeholder meetings none of the alarmists or anyone from the Handle System ecosystem raised any arguments for or against DOA[54]. In fact, none of the workshop members even brought the issue up despite alluding to the need for open and scalable architectures.[55] As we wait for the dust to settle on the IoT standards war, we can at least hope for some progress to emerge based on the results of those deliberations. In the meantime, we can encourage people with strong feelings about DOA to discuss its merits or flaws in the NTIA process or other fora.

[53] NTIA.doc.gov. (2017). *Fostering the Advancement of the Internet of Things*. [online] Available at: https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf

[54] NTIA.doc.gov. (2016). *National Telecommunications and Information Administration workshop on Fostering the Advancement of the Internet of Things*. [online] Available at: https://www.ntia.doc.gov/files/ntia/publications/09012016-iot-workshop.pdf.

[55] Ibid.