Experiemental Evaluation of a Proposed Federated Object Naming Service Architecture

Sandoche BALAKRICHENAN, Antonio KIN-FOO and Mohsen SOUISSI
AFNIC R&D
Paris, France
{*sandoche.balakrichenan, antonio.kin-foo, mohsen.souissi*}*@afnic.fr*

***Abstract*—The Electronic Product Code (EPC) network is a collection of technologies designed and implemented to build an Internet of physical objects. Object Naming Service (ONS), a directory based on the Domain Name System (DNS) is one of the important components of the EPC network. Given an object carrying an RFID tag (compatible to EPCglobal standards), and based on its EPC, the ONS allows storing and looking up information system associated with that object from the Internet. This facility could profit both business as well as ordinary users. But the issue is that at present there is a single ONS root zone, and the ONS namespace is completely controlled by a single organization. Such a solitary control over the ONS root has raised concerns among businesses and political communities who worry that the organization controlling the ONS namespace could block businesses from certain countries or involve in industrial espionage. They have expressed the need for a Federated ONS (F-ONS) architecture.**

In this article, we present the F-ONS architecture with multiple ONS peer roots. This architecture is evaluated in an experimental platform developed and implemented by us. The objective of this platform is to design, develop and evaluate technical solutions for managing the ONS in a completely decentralized fashion (Federated model). The tests run demonstrates Co-operation between multiple ONS peer roots to access the servers containing the appropriate information. The experiments done in this platform has enabled us to provide feedback to the ONS standardization committee which is in the process of revising the current ONS standard to include F-ONS capabilities. Finally we explain how it is possible to use the implemented F-ONS platform for legacy object identification systems other than EPCglobal standards.

***Keywords*-ONS; DNS; Internet of Things;**

I. INTRODUCTION

Internet of Things (IoT) encompasses several meanings depending on the communities/technologies being involved. In the context of this article, IoT addresses mapping `physical objects` to the `information systems` related to the object using the existing Internet infrastructure.

IoT is made possible by different technologies such as RFID, sensors etc. Our focus initially here is only on RFID capable objects typically associated with an RFID tag. The tag contains an identification key which is structured by different object identification schemes and the Electronic Product Code (EPC) is one such scheme. The EPC specifies a global object identification scheme intended to uniquely identify any object in the world.

Information about the object is not stored in the tag itself but stored in different servers distributed across the Internet. The network of physical objects achieved by integrating an EPC to each object is called the `"EPC network"`.

The EPC Network is composed of three key elements: EPC Information Services (EPC-IS), EPC Discovery Services (EPC-DS) and the Object Name Service (ONS). ONS is a global look up service that provides mapping between the EPC and the information system corresponding to the object which could be located anywhere in the Internet. ONS as of now is designed to use the Domain Name System (DNS) protocol and infrastructure and therefore it has the same hierarchical architecture as that of DNS.

According to the current ONS Standard v. 1.0.1 [1] by EPCglobal standardization body, there is a single ONS root zone (`onsepc.com`), containing the whole ONS name space managed by Verisign Inc.. Under this single ONS root there could be delegation at different levels providing distribution of the overall ONS database.

Political and technical issues pertaining to a `"single root"` scenario, is a *deja vu* in the DNS case. The contract between the US Department of Commerce and the Internet Corporation for Assigned Names and Numbers (ICANN) gives the US government the final authority on what appears or does not appear in the DNS root (DNS ”root” refers to the root of the domain name tree and is denoted by a single dot (”.”)). The US government could potentially remove a country from the DNS root and therefore from the Internet. While it is extremely unlikely that the US Government would use this authority, it is unacceptable to other nations that one country should have such control over the Internet.

Similarly a country/organization which controls the ONS root could block certain entities from using the ONS database. It could also monitor the activities of a single/group of companies, since the resolver which does not have in its cache the the response/referral for the perceived query should pass through the ONS root for resolution. There is a possibility that the ONS root controller passes on this monitored information to the competitors resulting in industrial espionage or use it for economic intelligence.

With such rapid development of RFID technologies and the vision that IoT will be a part of the future computing and

communications, governance of the ONS gains importance, especially when it comes to who manages the ONS root and how? It is currently considered by certain political and/or industrial actors (mainly in the RFID area), that concentration of the ONS root governance in the hands of a single entity is a major issue, which for instance hinders the deployment of an ONS infrastructure that is accepted by everyone. The need for a distributed ONS Architecture has been expressed and the "EPC ONS Requirements Ad hoc. Committee" involving different institutions has been formed to develop the requirements for a Federated approach to ONS. That is to say, a collection of ONS roots that are sovereign, geographically dispersed and have equivalent functionality.

Here is an overview of the High-Level Requirements proposed by the "EPC ONS Requirements Ad hoc. Committee" that has to be taken into consideration for implementing a Federated ONS (F-ONS) architecture:

1) There SHOULD not be a single authority controlling the complete ONS namespace.
2) There SHOULD be multiple ONS Peer Roots (OPRs) each controlling a part of the ONS namespace.
3) No OPR has a privileged position over its peers.
4) Every peer in the federation SHALL provide necessary connections to support a seamless resolution of ONS queries.
5) If any peer level zone is to be updated such as addition, removal, delegation change etc., all the other peer zones in the ONS federation MUST be notified in a timely fashion prior to the update.
6) The proposed architecture MUST support queries in cases where the separation between the company prefix and the Item reference is not known.
7) The proposed architecture and the existing single root ONS model SHOULD inter operate with each other.
8) The proposed architecture SHOULD be able to resolve identifiers other than the EPC.
9) The proposed architecture SHOULD support a dynamic service definition model.
10) Privacy, Security and integrity SHOULD be taken care of.
11) It SHOULD be ensured that global performance of the ONS end-to-end service meets the requirements of the user applications.

This article will first try to address the ONS governance issue. For this reason, we initially discuss the current ONS architecture and existing literature on proposals trying to solve the ONS governance issues [II]. In section [III] we explain the modification that we proposed to the existing ONS standard for a F-ONS architecture. Based on our propositions we set up three OPRs in the Internet to implement a F-ONS platform and the different experiments conducted on this platform are explained in section [IV]. The current ONS standard supports only the EPC identification scheme. Our objective is to demonstrate that the proposed F-ONS architecture should be able to resolve object identifiers using any identification scheme. In section [V] the possibilities of how other legacy identification schemes could resolve the service associated to the object using the F-ONS platform are explained.

II. Background

A. The current ONS Standard v. 1.0.1 [1]

As explained earlier, ONS is a part of the EPC network, which uses DNS to resolve the information/services about an object from its EPC. In order to be used in the DNS, the EPC must be converted to a Fully-Qualified Domain Name (FQDN).

Conversion from EPC to FQDN follows different steps. An RFID reader reads the RFID tag-equipped object and typically returns the HEX representation of the EPC. This value is then converted to binary form. The binary value is then decoded according to EPC specifications [1] to extract the decimal values and finally, formatted to return a meaningful representation of the EPC called the Uniform Resource Identifier (URI) representation. The URI example shown here is of a common tag encoding format, the Serialized Global Trade Identification Number (SGTIN).

```
urn:epc:id:sgtin:3102542.000024.46595
```

The URI can be broken down as follows:

Table I
EPC URN FORMAT EXPLAINED

Field	Description
urn	Indicates that data is of Uniform Resource Name(URN) format standard
epc	Indicates that data is of EPC format standard
id	Indicates that the data is an EPC identifier
sgtin	Indicates that data is an SGTIN tag
3102542	The Company prefix
000024	Item Reference
46595	Serial Number

The company prefix (3102542) can be partitioned into two parts. The first three digits (310) also called as "GS1 prefix", identifies the Country (i.e. GS1 Member Organization (MO) of a particular country) and the second four digits (2542) which identifies the company in that country. An analogy can be made for GS1 prefixes with the telephones codes for each country. If the first three digits of the company prefix is between 300-379, then it is assumed that the company is associated with the GS1 organization in France. Similarly for each country (there are still countries which are not assigned with GS1 prefixes) a three digit value is assigned. A Country can have a bunch of values (e.g. France) or a single value

(e.g. 380 for Bulgaria). The GS1 prefixes range from 000-999.

Ignoring the "Serial number", (Since ONS resolution stops at the `item` level) the URI is rewritten as follows:

```
000024.3102542.sgtin.id.onsepc.com
```

"onsepc.com" is appended at the end to represent the existing single ONS root service.

While resolving a FQDN of the above type, if the DNS resolver has complete/part knowledge of the server corresponding to the FQDN in its cache, it sends the query to the particular server. If its cache does not have any knowledge of the FQDN, then the query is directed to the DNS root. With the current ONS architecture, the DNS root will refer the resolver to the ONS root `"onsepc.com"`. The ONS root will refer the resolver to the EPCIS which has authoritative data corresponding to the query.

B. Existing work on distributing the ONS authority

There is not much literature studying a F-ONS architecture. According to our knowledge, there are only three articles [2], [3] and [4] which discuss about it.

Kevin Dean from GS1 Canada [2], put forth two proposals for a F-ONS architecture. The idea is to have different OPRs based on regions or the countries. Actually this article has served as a basis for part of our work. The drawback in [2] is that one of the root being assigned as a default callback root (i.e if an OPR could not obtain information for an incoming query it will ask a designated default callback OPR). This scenario gives a privileged position for one OPR over the others. The article [2] also does not take into account how an OPR informs its peers in the event of a modification in its zone.

[3] proposes a delegation structure similar to the DNS but based on regions.The `Regional Multipolar ONS architecture` proposed by them tries to address the single ONS root issue. A drawback that we could cite is that a query that needs to be redirected (Refer to subsection [III-D] for further information about need for redirection) to another regional root is based on Name Server (NS) Resource Records (RRs). In case of a modification of the identity of the NS, it should be immediately updated to other regional root zones. Updations/modifications of the NS can occur frequently and we feel that it could be operationally cumbersome. Another issue with their proposal is that the ONS client/resolver MUST be configured to interrogate a particular root NS based on the region where the resolution originates. Similarly in case of modification of the name of the regional root NS all the ONS clients at that particular region should be updated. This is also a major operational issue.

[4] proposes setting up ONS operations under any existing Top Level Domains (TLDs) in the DNS. Thus by default a decentralized ONS service is possible. The issues with this proposal is that

- The callback is always on the default OPR, i.e. onsepc.com.
- There is no concrete policy mentioned how the different OPRs will communicate and update in case a new OPR is added.

The different work mentioned above does not discuss the implementation methods of their proposals or try to address how ONS could resolve object identifiers using identification schemes other than EPC.

III. Design consideration for a F-ONS architecture

In the following subsections we will explain in detail the reason the different functionalities (or) options that was chosen for implementing the F-ONS architecture.

A. DNS vs Distributed Hash Tables (DHT)

The first option to look into was whether to choose an evolutionary or disruptive approach. The evolutionary approach is based on the DNS software and infrastructure as per the current ONS standard version 1.0.1 [1]. The disruptive approach is based on DHT. The reason for choosing DHT as an alternative solution is that it uses the Peer-to-Peer concept, thus enabling multiple OPRs to operate at the same hierarchical level. The tabular column [II] below compares DNS vs. DHT with respect to different functionalities. The comparison has been made based on the literature [7].

Table II
DNS vs DHT

Functionalities	**DNS**	**DHT**
All OPRs are equal	yes, but there is a feeble dependence on the DNS root	All OPRs are in Same level
Adding/removal of OPRs	Need to have policies defined and followed by all OPRs	Needs to contact other OPRs already in the network to join. Similarly on removal need to update DHT
Caching	Can cache the hierarchy itself	Can cache only the data
Availability	Performs well in case of random attacks or server shut down	In case of orchestrated attacks performs better
Ease of Deployment	Use the existing DNS infrastructure	Need to build an infrastructure

According to the table [II] for basic functionalities, DHT performs in no major way better than DNS. ONS based on DNS is a proven architecture, whereas ONS based on DHT is still in its nascent stage. In case of implementing a F-ONS architecture based on DNS, it is highly possible to give concrete results within stipulated time. Whereas in

DHT it is still not proven in the production stage in a scale as DNS is proven today. The WINGS [8] project which has funded the work explained in this article also has a working package studying the disruptive approach which does not come within the scope of this article.

B. Proposed F-ONS Architecture

In order to have multiple authoritative sources for the ONS namespace, we propose certain modifications in the current ONS Standard v. 1.0.1 [1] .

As per our proposed architecture [Fig: 1], there should be multiple OPRs, each managed by a regional (e.g. based on continents) organization. Below the root there should be zone delegations to either national or local organizations (e.g., a national zone, a single company zone, a consortium of companies zone, etc.).

Initially there would be direct delegations from the (regional) OPR zone (e.g. European regional OPR) to company local ONS zones, without an intermediate hierarchy. Later, countries that chose to manage a national-level ONS zone - a sort of *ONS TLD* - would get a delegation from their (regional) OPR and give ONS zone delegation to the companies under it.

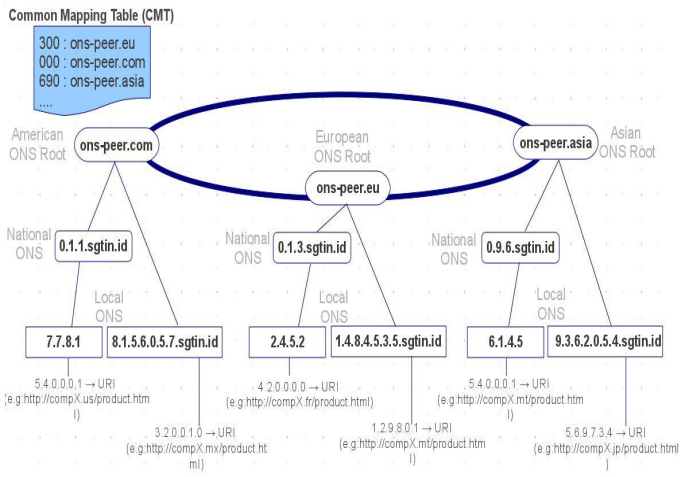

Figure 1. OPRs in the Internet

This design format [Fig:1] enables flexibility, wherein companies under a country which is not able to manage its own namespace can have delegation directly from their respective regional OPR. If there is a national level delegation for a Country, all the companies associated with the GS1 MO in that Country should get their delegations from their national level zone.

If in case a Country does not want to be under a regional OPR, it could have its own national level OPR and all the companies associated with GS1 MO in that Country should get their delegations from their national level OPR.

As indicated in the figure [Fig:1] we have three OPRs ("ons-peer.eu" representing the European region, "ons-peer.asia" representing the Asian region and "ons-peer.com" representing the American region). The delegations under the OPRs confirm to the design format that we have explained in the previous paragraph.

C. Revising the EPC derived FQDN format

We also propose to revise the FQDN format "000024.0614141.sgtin.id.ons-peer.eu" as per the current ONS standard [1] based on individual digit boundary as follows:

```
urn:epc:id:sgtin:3102542.000024.46595 --->
4.2.0.0.0.0.2.4.5.2.0.1.3.sgtin.id.ons-peer.eu
```

Since there are multiple OPRs, the string identifying the current centralized ONS root service ("onsepc.com") has to be replaced by a string identifying the OPR under which the query originates. For example, if the query originates in the European region, `"ons-peer.eu"` will be appended at the end of the string as per the architecture [Fig:1].

The advantage in the modification is that the application which performs the conversion from the RFID tag identifier to the FQDN format as explained in [subsection II-A] does not need to identify the delimiter between the company prefix and the item reference. Another advantage is that revising the FQDN format based on individual digit boundaries increases scalability and caching in comparison with the current classification based on company prefix and item reference. Also, the proposed revision tries maintain a generic format which also envisions the possibility of being agnostic to identifiers other than the EPC.

D. Communication within the ONS root peers

Since each OPR is the authoritative source for only its namespace, there arises a possibility where a query originating from one OPR wants to have information about a product in its peer namespace. This calls for mechanism to enable communication between the different peers at the root level.

For example let's take an example of a user in Europe who wants have information about a Chinese product and use the proposed F-ONS architecture. Since the query originates in Europe, during the conversion process the FQDN will be appended with the string pertaining to the European root server as follows:

```
5.4.0.0.0.1.6.1.4.5.0.9.6.sgtin.id.
                          ons-peer.eu.
```

For the above query, the DNS resolver initially interrogates "ons-peer.eu". To redirect the query to "ons-peer.asia" (since the query is for a Chinese product and assuming

China is under the Asian OPR), "ons-peer.eu" needs to know that the query is destined for the Asian OPR. With the help of GS1 prefix (last three digits "0.9.6" of the query is the Chinese GS1 prefix "690" inverted and "." inserted between the digits), "ons-peer.eu" can identify that the query is destined to China which is under the Asian OPR. To map a GS1 prefix to the corresponding OPR and to append the appropriate OPR name to the query (in this case: 5.4.0.0.0.1.6.1.4.5.0.9.6.sgtin.id.ons-peer.asia), there need to be a mechanism possible with the existing DNS database.

Using DNAME [9], the redirection could be done based on GS1 prefix as follows:

```
0.9.6.sgtin.id.ons-peer.eu. IN  DNAME
                0.9.6.id.ons-peer.asia.
```

The facility with DNAME is that there is no necessity for each OPR to have the knowledge about the zone information of its peers. The only necessity is that there should be DNAME redirection RRs for all the GS1 prefixes. Each OPR will have the DNS RRs for all the GS1 MO other than the MO that it is authoritative for.

E. In the event of modification of the Zone in the OPR

There are multiple scenarios where an OPR has to be updated with information pertaining to its peers. For example, let's suppose a country "XYZ" is not happy with the European OPR either for political or technical reason and opts for the American OPR. Both the American and European OPR are aware that "XYZ" has modified its association. But the Asian OPR is unaware of this modification and for all queries for "XYZ" hitting the Asian OPR will be redirected to the European OPR. In this case, the European OPR will redirect the query to the American OPR with n+1 required redirections ("n" being the case where all the OPRs are updated with the modifications in their OPR zones). But there are scenarios wherein the query resolution may lead to failure if there is a lack of co-operation between the different peers at the root level.

In order for each peer to be updated with modifications occurred in their peer root zones we propose three methods: Push, Pull and Bilateral updates. For the push and pull methods we propose the use of a Common Mapping Table (CMT), designed of the following format:

```
;serial:2011061500 (YYYYMMDDSN)
;default:ons-peer.asia
; onseu
300-379:GS1 France:ons-peer.eu
[..]
; onsas
690-695:GS1 Chinese:ons-peer.asia
[..]
; onsam
000-019:GS1 US:ons-peer.com
[..]
```

This mapping table contains an exhaustive list of all GS1 prefixes (From 000-999). This file should be stored in a well known location and accessible only by the OPRs. It has to be noted that the CMT is just an `allocation root`. For example the International Telecommunication Union(ITU) allocates the telephone code for each country whereas each country has its own routing procedures to route the telephone calls. In this case, the ITU is an allocation root for the telephone codes. Whereas in DNS, the DNS root is used for routing the query to its appropriate target and it is a `resolution root`. We have to reiterate this point since the reader might think that CMT will have a privileged position over the existing OPRs. The CMT is not used for resolution and in no way the CMT has a privileged position. The contents of the CMT will be used by each OPR just to update itself the modifications occurred in any of its peer.

Each OPR downloads the CMT. It creates a local copy of the CMT. Using this local copy it creates DNAME RRs which are used for DNAME redirection [subsection III-D]. In case there is a modification for a GS1 prefix in any of the OPR, it notifies the CMT. The CMT gets updated appropriately and increments the serial number for each update.

Each OPR downloads the CMT at a scheduled period and compares the serial number of the downloaded CMT with the local version. In the event of the serial number from the downloaded copy is greater than the serial number of the local copy, the local CMT is rewritten with the downloaded one.

If there is any change it rewrites the local version with the downloaded CMT. This we name it as "Pull" method.

In the "Push" method the CMT is pushed to all the OPRs at a stipulated time. Then each peer performs the same process as explained in the pull method.

In bilateral updates, each OPR has the access identifier of its peers. Whenever there is any modification to a OPR it notifies the modification to its peers which in turn updates their zones. There is no need for a CMT here. As of now we have tested only the pull method.

IV. THE F-ONS PLATFORM

Based on the propositions made in the section [III], three different OPRs (see [Fig: 1), are implemented. The European OPR (ons-peer.eu) and its delegations were configured/implemented in a physical server in the same Local Area Network (LAN) and located in the suburbs of Paris. The American OPR (ons-peer.com) and its delegations are configured/implemented in four different servers (OPR, national level, local under the national level delegation and direct company level delegation from the OPR). These machines are distributed over two different LAN's and physically located in the city of Caen in Northern France.

Similarly the Asian OPR (ons-peer.asia) is also distributed in four different servers on two different LAN's. These four servers are also situated in the city of Caen. The servers for the American and Asian OPR and its delegations is shared by other test applications whereas the server for the European OPR and its delegations is dedicated for the F-ONS tests. [Fig. 2] shows the functional details of the F-ONS platform.

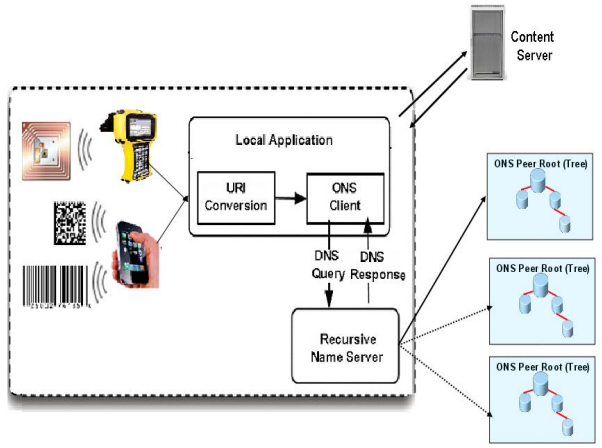

Figure 2. F-ONS Platform

An RFID reader application reads the EPC from the RFID tag. A local application developed (as part of the F-ONS platform) converts the EPC into an URI format as specified in the current ONS specification [1]. The URI is then converted in to a FQDN (based on individual digital boundaries). At the end of the generated FQDN string, appropriate OPR name is concatenated. The ONS client interrogates the DNS using the FQDN. The final response for the query is a Naming Authority Pointer (NAPTR) RR. The regular expression of the NAPTR RR contains the service (e.g. web service) associated to the EPC. When the OPR interrogated does not have the response under its ONS tree it refers the query (using DNAME RRs created with the help of the CMT) to the concerned OPR which might have response for the query.

Each OPR has a daemon which periodically downloads the CMT. It then compares the CMT with its local copy. If there is a difference in the serial number between the local copy and downloaded version of the CMT, the local copy is overwritten by the downloaded version. Using the new version of the CMT the daemon automatically rewrites the DNAME RRs in the ONS root zone file.

A. *Functional tests*

Following functionalities are tested on the F-ONS platform successfully:

- A query originating from one OPR has the response under its tree.
- A query originating from one OPR does not have the response under it but in one of its peers. This demonstrates the Co-operation between different OPRs.
- Adding a new GS1 MO (or) migrating a MO from one OPR to another.
- Adding/removing an OPR from the federation.

The above tests successfully demonstrates that each ONS roots are sovereign and independent, and also there is Co-operation between different roots without the real possibility of blocking or involving in business intelligence. Other than RFID, the platform can also be used for testing one and two-dimensional barcodes. Reviewing with the High-level requirements defined in section [III] below is the tabular column which compares the F-ONS platform with the high level requirements.

Requirements	**Status**
No Single Authority	OK
All ONS peer roots are equal	OK
Transparency between different peer roots	OK
Interoperability between F-ONS and current ONS standard	OK
Support in case where the separation between Company prefix and Item reference is not known	OK
Dynamic Service definition	OK
Accommodation of non GS1 identifiers	ToDo
Uniqueness of the object identifier	ToDo
Privacy/Security/Integrity	ToDo

B. *Quantitative tests*

It is very important to identify the similarities and difference between the quantitative tests run on the F-ONS platform and the production environment. If we look into the literature for DNS quantitative test, measurements were done in the Internet or DNS behavior traces have been collected and then replicated in the lab and measured. The difficulty in testing the F-ONS architecture is non availability of empirical traces that can be replicated in the test environment. The WINGS F-ONS platform based on DNS involves network which belong to a university and two companies having higher bandwidth than a normal user. The delegated nameservers for each OPR is in the same campus. Due to previously mentioned constraints, the quantitative results obtained by us will not be the same as perceived by an F-ONS user.

But we have done certain tests by stressing the DNS cache servers and then sending queries at predetermined intervals to get an idea of the time taken for resolution of a particular query. The detailed explanation of the quantitative tests cannot be explained within the scope of this paper. This will be the subject of a future article.

V. Using the F-ONS platform for object identifiers other than EPC

Object identifiers have different characteristics. They could be based on different types of identifier schemes, identifier allocation rules, their uniqueness scope and opaqueness. A generic identifier (e.g. RFID, bar code, NFC) even in an unrelated business processes should be identified without the need for an existing mapping technique. The requirement is all types of object identifiers should be supported by the proposed F-ONS architecture. This will lead to a wider adoption of F-ONS in a real world business process.

A. Use cases on how the proposed architecture could be used for identifiers other than EPC

It will be nearly impossible to have one global identification scheme for all the objects in the world. The main reason for this is because there are industries which are using their proprietary object identification schemes for a long time. It is quite impossible to convince them to move to a newer object identification system. Another difficulty is that it will require consideration of a wide variety of object identification schemes to achieve a global object identification schema. One possible solution is to map different identifiers to one generic identification schema. For this, each object identifier should be identified of its original coding schema and then an appropriate mapping technique be used to map it to the generic identification schema. This method will be successful only for already known identifiers. For unknown identifier types a flexible identifier translation method should be developed. The second possible solution is to identify a query of its identification scheme and redirect to a server which manages that scheme. In case of EPC it will be the OPR. Below we will explain how it can be done with two other legacy identification schemes.

1) Unique Code (ucode) [10]: An example of a ucode is :

```
00001C0000000000000001000285E7A6E3
```

The ucode network is a closed network with multiple hierarchy similar to the DNS. The root part of the server hierarchy, along with the infrastructure of ucode space and ubiquitous ID architecture is managed by the Ubiquitous ID Center. This is like one of the OPR. We can call this an ucode OPR. There are number of ucode OPR called ”ucode resolution servers”.

A special device called ”Ubiquitous Communicator” is needed to read the ucode and search services/information related to the ucode in the ”ucode resolution servers”. An example of the output could be an URL containing information about the object.

To inter-operate the proposed F-ONS platform with the ucode resolution servers, we need:

- the ucode resolution servers accessible on the Internet
- the ONS client is able to identify the RFID tag that is read is an ucode
- the server (at the ucode network) which is responding with the information/service about the ucode should be able to respond to the querying source.

If the above requirements are met, it is quite possible the proposed F-ONS and the ucode network are inter-operable.

2) ISO Object Identifier (OID): An example of OID is:

```
urn:oid:1.0.15961.12.1 $=>$ IATA
     Baggage Identification Number (BIN)
00176367789 $=>$ Unique BIN for
                        a flight HKG-DBX-LGW
```

Combining the BIN and the unique BIN for the flight provides us a baggage that can be uniquely identified. Hence it could be combined as follows: urn:oid:1.0.15961.12.1.00176367789. This obtained value could be converted into a FQDN as follows 1.0.1.5.9.6.1.1.2.1.0.0.1.7.6.3.6.7.7.8.9.oid.ons-peer.eu if the flight is under European jurisdictions. The OID has a hierarchical architecture that can be well used in the ONS

In the two use cases explained before we try to understand how legacy identification schemes could inter-operate with the proposed F-ONS architecture. The authors acknowledge that it is very difficult to get into the nuances of the different identification schemes within the scope of this article. The authors also acknowledge that they don’t have a deep knowledge of the object identification schemes described in subsection [V-A2 and V-A1]. The point to demonstrate here is that the F-ONS platform is not constrained to EPC identification scheme, but it is open and agnostic to resolution of other types of object identification schemes. The necessity is for further studying and testing the interoperability of different types of object identification schemes with the F-ONS platform.

VI. Contribution

The contribution from this work are :

An IoT scenario where the objects are associated with RFID technology and confined to EPC identification scheme.

- Have developed an experimental platform which satisfies the high level requirements of the EU stakeholders.
- This work has contributed to the ”EPC ONS Requirements Ad hoc. Committee”.
- Have exteded ONS to resolve one and two-dimensional barcodes.
- Experience from this work are helping us to provide recommendation to the ongoing evolution of ONS standards.
- The source code developed as part of this project will be given to the community open source license

VII. Conclusion & Future work

In this article we explore the requirements and challenges in implementing a F-ONS platform. The aim of developing

this platform is to test different features required for a F-ONS system and to demonstrate that several ONS roots can fully co-operate together and safely share the management and the governance of the EPC network. To our knowledge from studying the related literature, this is the first work that has implemented and tested a distributed set up for resolving object identifiers using ONS to its information system in the Internet. We have tried to solve a certain set of high level requirements put out by the stakeholders.

The proposed F-ONS model does not reinvent the wheel. It is based on the existing DNS software and infrastructure. This platform could be implemented easily and used in a production environment without much hassles.

There are mutliple object identification schemes which have been in use for some time. Our experience from interacting with the clients who use object identifiers for business, we come to know that it is highly improbable that they will switch to a single global identification scheme. If that was possible, it would have been easier. But that possibility is highly unlikely. In this article we also show the possibility of how the proposed F-ONS platform could be interoperable fro different types of object identifiers. The only addition is that they need to have some additions to their resolver which is the ONS client.

F-ONS has a valid economic model because there is interest for this type of service both for business as well as normal user. Lot of research issuers like security, privacy and integrity needs to be solved. Also it is important to study how the ONS client could identify and classify different object identification schemes. It could be done on a case by case basis for legacy identification schemes but what about new identification schemes?

ACKNOWLEDGMENT

This work is carried out within the framework of a French national research project (Ref:ANR-09-VERS-015) : ANR WINGS (http://www.wings-project.fr)

REFERENCES

[1] http://www.epcglobalinc.org/standards/ons

[2] *Distributed ONS - A Proposal*, 2008.

[3] GSergei Evdokimov, Benjamin Fabian and Oliver Gunther *Multipolarity for the Object Naming Service* , In proceedings of IEEE International Conference on e-Business Engineering (ICEBE), 2007

[4] *Finding your way in the Internet of Things*, An Afilias Whitepaper, September 2008.

[5] Mealling, M.; RFC 3402 - *Dynamic Delegation Discovery System (DDDS) Part Part Two: The Algorithm., October 2002*

[6] Mealling, M.; RFC 3403 - *Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database., October 2002*

[7] Vasileios Pappas, Dan Massey, Andreas Terzis and Lixia Zhang - A Comparative Study of the DNS Design with DHT-Based Alternatives, In proceedings of IEEE INFOCOM, 2006

[8] http://www.wings-project.fr

[9] Crawford, M.; RFC 2672 - *Non-Terminal DNS Name Redirection., August 1999*

[10] http://www.uidcenter.org