Federated ONS Architecture for the Internet of Things - A Functional Evaluation

Sandoche Balakrichenan, Antonio Kin-Foo and Mohsen Souissi
AFNIC (French Network Information Center) R&D, France
{sandoche.balakrichenan, antonio.kin-foo, mohsen.souissi}@afnic.fr

***Abstract*—We present here a Federated ONS (F-ONS) architecture with multiple ONS 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 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 ONS standards to include F-ONS capabilities.**

I. INTRODUCTION

Object Name Service (ONS) provides mapping between the Electronic Product Code(EPC) and the information system corresponding to a given object which could be located anywhere in the Internet. ONS is designed to use the Domain Name System (DNS) protocol and infrastructure

According to the current ONS specifications [1], there is a single ONS root zone (`onsepc.com`), containing the whole ONS name space managed by Verisign Inc.. The concentration of the ONS root governance in the hands of a single entity has raised concerns with some industrial and political communities. The organization controlling the ONS could block certain entities from using the ONS database or monitor the activities of a single/group of companies, since the resolver which does not have in its cache the response/referral for the perceived query should pass through the ONS root for resolution.

The need for an ONS architecture with multiple ONS roots has been expressed and the "EPC ONS Requirements Ad hoc Committee" involving different institutions has been formed to develop the requirements for a federated (*A collection of ONS roots that are sovereign, geographically dispersed and have equivalent functionality*) approach to ONS.

Different proposals [2], [3], [4] have been proposed to distribute the control of the ONS root among several entities and thus eliminate the single root issue. There is no existing infrastructure (either empirical or experimental) to study the feasibility of different ONS root services spread over the Internet. As per our knowledge we are the first to implement an experimental F-ONS platform. The objectives of this platform is:

- Propose modifications to the current ONS specification [1] and test their functionality.
- Perform quantitative tests and study different metrics such as latency, reliability, scalability.
- Benchmark DNS based F-ONS to DNS based single root ONS and DNS based F-ONS to clean-slate alternative architectures such as Peer-to-Peer (P2P) based ONS.

This article describes our proposed modifications to the current ONS specification and different tests run in the F-ONS platform.

II. PROPOSED MODIFICATIONS TO THE CURRENT ONS SPECIFICATIONS [1]

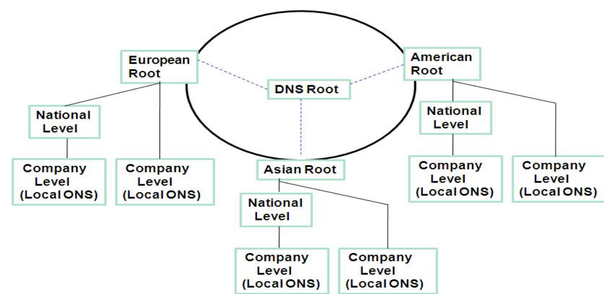

Fig. 1. Proposed F-ONS Architecture used in our Experimental Platform

As per our proposed F-ONS architecture [Figure 1], there should be multiple ONS roots, 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 single company zone or a consortium of companies zone). This design format enables flexibility, wherein companies under a country which is not able to manage its own namespace can have delegation directly from their respective regional root. If there is a national level delegation for a Country, all the companies associated with the GS1 Member Organization (MO) in that Country should get their delegations from their national level zone.

The Fully Qualified Domain Name (FQDN) derived from the EPC is of the following format [As per the current ONS specification [1]], partitioned based on company prefix and item reference:

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

We suggest revising the FQDN format based on individual digit boundaries (thus increasing scalability and caching in comparison with the current classification based on company prefix and item reference) as proposed by [2]

```
4.2.0.0.0.0.2.4.5.2.0.1.3.sgtin.
```

```
                  id.europeanroot.
```

With multiple roots instead of "onsepc.com", appropriate ONS root name (for e.g. "europeanroot") is concatenated at the end of the string when the FQDN is created.

There are multiple scenarios wherein an ONS root zone has to be updated with information pertaining to its peers. For example, let's suppose a GS1 MO "XYZ" is not happy with the European root either for political or technical reason and opts to be delegated under the American root. Both the American and European root are aware that "XYZ" has modified its root. But the Asian root is unaware of this modification. In such scenarios, a level of Co-operation between the different ONS roots is mandatory. To enable Co-operation between the different ONS roots, we propose the use of a Common Mapping Table (CMT) [Fig:2].

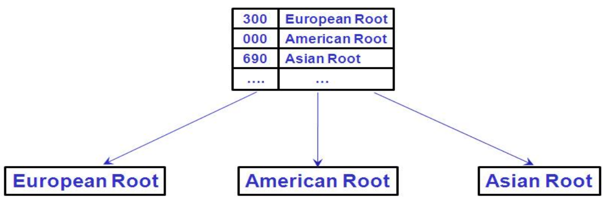

Fig. 2. The Central Mapping Table

The CMT contains an exhaustive list of GS1 prefixes (A GS1 MO associated to a country could be provided a bunch of GS1 prefixes(e.g. GS1 MO for France (300-379) or a single GS1 prefix(e.g. 380 GS1 MO for Bulgaria)) which range from "000" to "999". The file containing the CMT should be stored in a well known location and accessible only by the ONS roots. The GS1 prefixes are inverted and a a "." is introduced between each digit to create a set of DNAME Resource Records (RRs) like:

```
; A sample data of the American root
0.0.3.sgtin.id.americanroot. IN DNAME
           0.0.3.sgtin.id.europeanroot.
0.9.6.sgtin.id.americanroot. IN DNAME
              0.9.6.sgtin.id.asianroot.
```

The information in the CMT could be only used for associating a GS1 prefix to a ONS root (just like knowing that the telephone code "+33" is associated with France) and this data could not be taken advantage for any other purpose.

III. Functional Evaluation of the F-ONS Platform

An RFID reader application reads the EPC from the RFID tag. A local application developed (as part of the experimental platform) converts the EPC into an Uniform Resource Identifier (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 ONS root 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 ONS root 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 root which might have response for the query.

Each root 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.

The demonstration will be done in two phases. In the first phase three real ONS roots ("ons-peer.eu", "ons-peer.com" and "ons-peer.asia") are used to run the tests. Following functionalities are tested.

- A query originating from one ONS root has the response under the same ONS root tree.
- A query originating from one ONS root does not have the response under the same ONS root tree but in one of its peers. This demonstrates the Co-operation between different ONS roots.

The second phase involves modification in the ONS root zone files. Since these ONS roots are managed by different organizations it is impossible to perform the required modifications during the demo. Hence we simulate the different ONS roots ("onsam.test", "onseu.test" and "onsas.test") in our local ONS platform. A web interface control panel is used for configuration changes. Following tests are run during this phase:

- Adding a new GS1 prefix (or) migrating a GS1 prefix from one root to another.
- Adding/removing a root 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. Tests run from the platform have helped us to provide recommendation to the ongoing evolution of ONS standards.

IV. 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] www.epcglobalinc.org/standards/epcis/epcis_1_0_1-standard-20070921.pdf
[2] K. Dean, *Distributed ONS - A Proposal*, 2008.
[3] G. Evdokimov, B. Fabian and O. 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.

Tests : Phase 1

S.NO	Scenario	Originating Root	Test Results
1.	Simple Case	ons-peer.eu	OK
2.	Redirection	ons-peer.eu	OK

Tests : Phase 2

S.NO	Scenario	Originating Root	Test Results
1.	Adding a new prefix (Malta)	onseu.test	OK
2.	Querying Malta	onsam.test	NOK
3.	Querying Malta(After updating the Mapping Table)	onsam.test	OK
4.	Moving Malta from «onseu.test» to «onsas.test»	onsam.test	NOK
5.	Querying Malta(After updating the Mapping Table)	onsam.test	OK
6.	Adding a new ONS root (onsaf.test)	onsam.test	OK

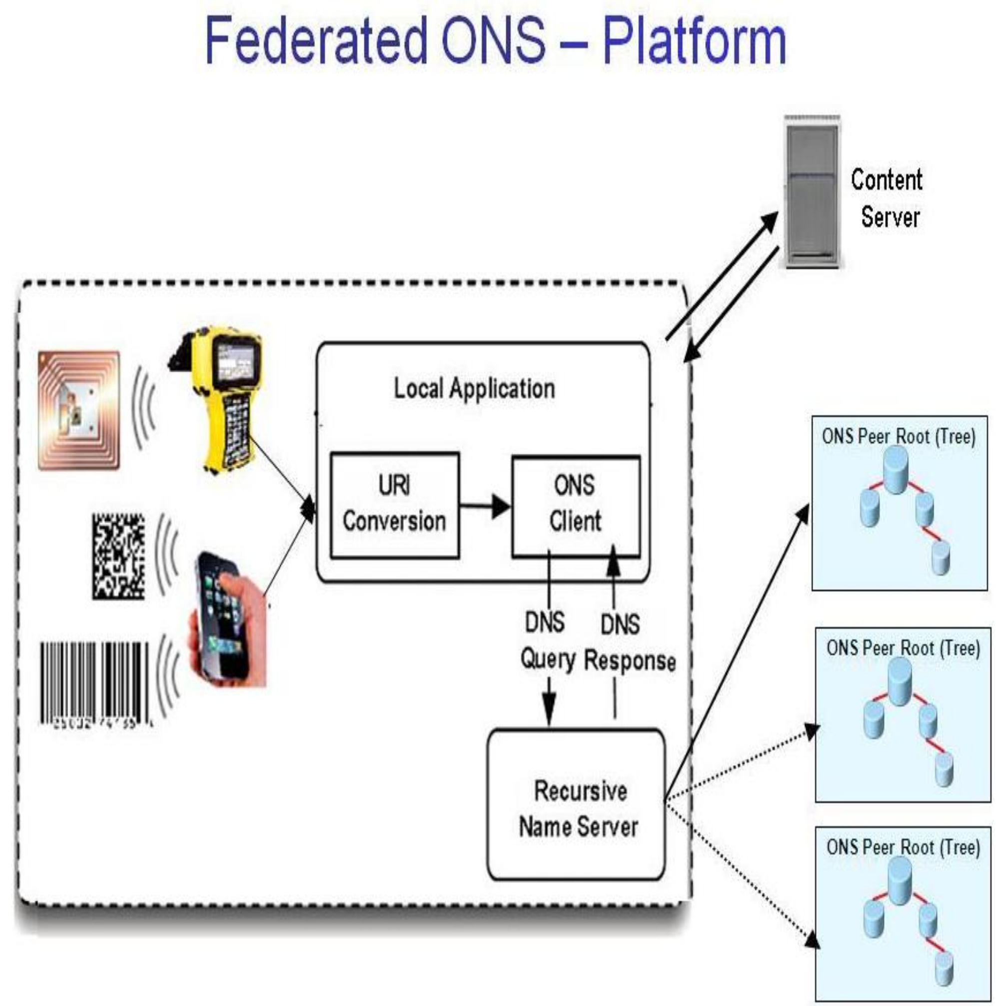

Fig. 3. F-ONS Platform Test Scenarios and Experimental Platform Framework