# EU-China Joint White Paper on Internet-of-Things Identification

**Identification Technologies for the Internet-of-Things**

# EU-China Joint White Paper on Internet-of-Things Identification


| Date of publication | Document version: |
|---|---|
| 31/10/2014 | V1.0 |


| Dissemination level | | |
|---|---|---|
| **PU** | Public | **X** |
| **PP** | Restricted to other invited experts | |
| **RE** | Restricted to a group defined by the expert group | |
| **CO** | Confidential, only for members of the expert group | |

**Authors (organizations) : China Academy of Telecommunication Research (CATR), Research Cluster on the Internet-of-Things (IERC)**

**Editors**: John Soldatos (Athens Information Technology) and Ge Yuming (China Academy of Telecommunication Research)
**Contributors**:
**EU side:** Claudio Pastrone (Istituto Superiore Mario Boella), Domenico Rotondi (TXT e-solutions), Antonio Skarmeta (University of Murcia), Harald Sundmaeker (Institut für angewandte Systemtechnik Bremen GmbH), Ovidiu Vermesan (SINTEF), Sébastien Ziegler (Mandat International, IoT6, IoT Lab), Peter Kirstein (UCL), Socrates Varakliotis (UCL), Adel Al-Hezmi (Fraunhofer FOKUS)
**China side:** Zhang Xueli (China Academy of Telecommunication Research), Liu Yang (China Academy of Telecommunication Research), Tian Ye (Computer Network Information Center, Chinese Academy of Sciences), Xing Pengfei (Electronic Technology Information Research Institute), Wu Dongya (China Electronic Standardization Institute), Zhang Xu (Article Numbering Center of China), Ma Wenjing (China Electronic Standardization Institute)

**Abstract :**

This paper is a joint effort of IoT experts under the support of EU-China IoT Advisory Group, towards documenting the state-of-the-art on IoT Identification technologies in EU and China, as well as towards providing an outlook for future developments. As a first step the document defines the scope of IoT identification and introduces relevant concepts and mechanisms, including IoT ID Naming, Addressing and Discovery. Accordingly, the development and deployment status of prominent IoT identification technologies in EU and China is reviewed. Furthermore, a range challenges for the future development and evolution of IoT technologies are presented, along with the limitations of existing solutions. The paper ends-up discussing various directions and development guidelines aiming at alleviating existing limitations in areas such as the integration and semantic interoperability of heterogeneous identification technologies, the security of identification and discovery processes, the support of identification and discovery processes for mobile applications and more. Several of these guidelines are already pursued by organizations in China and EU, as part of research and development initiatives.

**Keywords : IoT Identification,IoT ID Naming, IoT ID Addressing, IoT ID Discovery, Ipv6, Handle/DOI, CID, RFID, EPC, DNS, ONS, Semantic Web**

# Disclaimer

# Table of Content

# 1. Acronyms and Definitions

## 1.1. Acronyms

| Acronym | Defined as |
|---|---|
| AMI | Advanced Metering Infrastructure |
| ANCC | Article Numbering Center of China |
| AutoID | Automatic Identification |
| CASAGRASS | Coordination and Support Action for Global RFID-related Activities and Standardisation |
| CATR | China Academy of Telecommunication Research |
| CDI | China Digital Innovation Technology Co., Ltd |
| CESI | China Electronic Standardization Institute |
| CHC | Corporation for Handle Services in China |
| CNIC | Computer Network Information Center, Chinese Academy of Sciences |
| CNNIC | China Internet Network Information Center |
| CNRI | Corporation for National Research Initiatives |
| CID | Communication Identifier |
| COC | Country/Organization Code |
| DNS | Domain Name System |
| DNS-SD | Domain Name System – Service Discovery |
| DOA | Digital Object Architecture |
| DOI | Digital Object Identifier |
| DONA | Digital Object Numbering Authority |
| DTN | Delay-Tolerant Networking |
| EC | European Commission |
| Ecode | Entity Code |
| ENUM | tElephone Number Mapping |
| EPC | Electronic Product Code |
| EPIC | European Persistent Identifier Consortium |
| ETIRI | Electronic Technology Information Research Institute |
| EU | European Union |
| GHS | Global Handle Service |
| HS | Handle System |
| IERC | European Research Cluster on the Internet of Things |
| ISTIC | Institute of Scientific and Technical Information of China |
| IoT | Internet-of-Things |
| ISO | International Standardization Organization |
| LDAP | Lightweight Directory Access Protocol |
| MAC | Media Access Control |
| mDNS | Multicast DNS |
| NIC | Network Interface Card |
| NSC | Naming System Code |
| MPA | Multi-Primary Administrator |
| OGC | Open Geospatial Consortium |
| OID | Object IDentifier |
| ONS | Object Naming Service |
| ORS | Object Resolution System |
| POS | Point of Sale |

| | |
|---|---|
| QR | Quick Response Code |
| RFID | Radio Frequency Identification |
| SCM | Supply Chain Management |
| UUID | Universally Unique Identifiers |
| UPC | Universal Product Code |
| URI | Universal Resource Identifier |
| URN | Uniform Resource Name |
| WFS | Web Feature Service |
| WGSN | China Standardization Working Group on Sensor Networks |
| WMS | Web Map Service |
| WoT | Web-of-Things |

## 1.2. Definitions

**Physical Object (PO)**:
A device with physical existence i.e. a tangible and visible entity.

**Virtual Object (VO)**:
A digital element or component (e.g., computational process or service), which is uniquely identified, provides data and/or performs actions in the scope of an Internet-of-Things application.

**Internet Connected Object (ICOs)**:
Any physical or virtual object that is connected to the internet infrastructure.

**Object Identifier for IoT**:
An object identifier is used to label/tag and uniquely identify a physical or virtual object.

**Communication Identifier for IoT**:
An IoT communication identifier is a label assigned to physical object (e.g., sensor, device), which is used to uniquely identify the device in the scope of its internet communications with other objects.

**Application Identifier for IoT**:
An application identifier is a label (e.g., URI/URL) assigned to an IoT application or services in order to uniquely identify it used in the scope of IoT applications.

**IoT ID Naming**:
Involves the processes of managing ICOs names, assigning names to ICOs and registering them to a naming/directory service.

**IoT ID Addressing**:
The process of mapping between names and identifiers for ICOs.

**IoT ID Discovery**:
Refers to the process of locating and retrieving IoT resources (e.g., services, data) through looking them up to naming/directory services.

# 2. Introduction to IoT Identification

## 2.1. Internet-of-Things Identification Concepts

The Internet-of-Things (IoT) refers to the exploitation of internet technologies for the interconnection of uniquely identifiable objects. Likewise, IoT applications are typically based on the coordination of information and services on a variety of internet-connected-objects (ICO), which include both physical devices (such as sensors) and virtual/logical entities (such as computational processes). Therefore, the availability of mechanisms for the identification of physical and virtual/logical objects is a key prerequisite for the development, deployment and operation of non-trivial IoT applications and services.

The notion of object identification is already extensively used for things in the physical world, such as desktop computers, servers, mobile devices, networking devices (e.g., routers, switches, hubs), network interface cards, energy meters, sensing devices, actuating components, RFID/AutoID readers, tagged items/products, application gateways and more. All these physical objects are associated with an identifier such as a hostname, an IP address or a URI (Universal Resource Identifier). Moreover, the identifier may contain in several cases additional information that conveys the relationship of the thing with other objects (e.g., server hostnames are associated with the NICs that they comprise) and/or their locations.

There are also technologies for identifying logical/virtual objects, such as computational processes, software, services, data items, data stores, web objects, documents, digital objects and more. For example, Web services are identified based on URLs (Universal Resource Locators), while DOIs (Digital Object Identifiers) provide the means for referencing documents and other digital objects.

At its full scale, the emerging IoT paradigm foresees flexible and transparent interactions across numerous physical and logical objects. This requires identification systems that can address the full range of physical and logical/virtual objects outlined above. The identification technologies and solutions outlined above provide a sound basis for IoT identification and are already used in the scope of several IoT applications. However, several challenges are still to be confronted especially when it comes to deploy and operate large scale IoT applications that transcend multiple identification solutions and standards (such as those listed above). In such cases an umbrella Identification Framework for IoT is required.

## 2.2. Taxonomy of IoT Identifiers

A wide array of identifiers suitable for IoT applications are already in place (e.g., RFID tag identifiers, IP addresses, URIs, Handle/DOI) as illustrated in the previous paragraph. It should be noted that these identifier operate at different layers and serve different purposes. In particular, the following classes of IoT identifiers can be distinguished:

- **Object Identifiers (Object IDs)**, which are used for uniquely identifying physical or virtual objects.
- **Communication Identifiers (Communication IDs)**, which are used to identify uniquely devices in the scope of communications with other devices, including internet-based communications.
- **Application Identifiers (Application IDs)**, which are used to identify uniquely applications and services used in the scope of IoT applications.

The following table classifies some popular (IoT) identifiers to the above categories:

| IoT Identifier Type | Examples |
|---|---|
| Application IDs | URIs, URL |

| | |
|---|---|
| Communication IDs | IPv4, IPv6, E.164 |
| Object IDs | EPC, UPC, Handle/DOI, UUID, MAC, URI, URL, Ecode, OID, CID |

**Table 1: Examples of Identifiers for IoT**

Nowadays identifiers of all the above types are typically used in state-of-the-art IoT applications. For example, IPv6 address as communication identifiers are commonly used for identification in the scope of energy management applications based on 6LoWPANtechnology[RFC6775], while barcodes (e.g., UPC) as physical objects identifiers are extensively used in the scope of logistics and point-of-sale (POS) applications. It is also expected that several future applications will have to use identifiers from more than one of the above levels. Hence, this taxonomy is important when defining an ID solution for IoT, since it specifies the scope of the target identifiers, thereby driving the identification functionalities that can be supported.

## 2.3. IoT Identification Technologies

An identification framework for IoT should provide the means for managing the full lifecycle of IoT identifiers, while at the same time enabling their efficient use within IoT applications. To this end, IoT identification is closely associated to the technologies and functionalities listed in the following paragraphs.

### 2.3.1. IoT ID Naming

**Scope**

IoT Identification provides the means to identify objects, when looked up against a naming/directory service that provides a resolution of a name according to a naming system. Names can be thought as labels or attributes assigned to ICOs (physical or virtual objects) in order to enable their individualization within larger sets of objects. In several cases names are organized according to taxonomies or classifications in an hierarchical fashion and according to a well-defined naming system. Names can be also used for groups of objects. The scope of IoT ID Naming includes also mechanisms for assigning names to ICOs and supporting their resolution/mapping to IoT addresses.

**Sample/Indicative Scenario**

The provision of traceability information is essential for several supply chain management applications such as the discovery of defective or unsafe products in the food supply chain. A traceability system allows the provision of traceability information (e.g., the current and past locations of a product, the status of the products across these locations and more). Such information can be looked up using the object identifier of the product. A naming system enables look up of this information on the basis of a name that is assigned to a product. In particular an IoT ID Naming system enables users and solution providers to identify the product through its name rather that via its object identifier (e.g., URI).The process of establishing such a naming system implies the need for managing the association of names to physical identifiers. The management processes define also all the rules that regulate how resources are named and identified, including the mechanisms for secure and authenticated access.

### 2.3.2. IoT ID Addressing

**Scope**

Addresses are used to identify internet-connected-objects (ICOs), while also enabling them to communicate. Furthermore, they can also denote the location of an ICO within a space. IoT ID Addressing entails the assignment and management of addresses/identifiers for ICOs, thereby being also relevant to IoT identifiers. In principle IoT ID Addressing technologies provide the means for mapping identifiers at different levels i.e. object ID, communication ID and application ID.

**Sample/Indicative Scenario**

A great deal of smart energy applications are based on smart meters. A prominent way to formulate a network of smart meters for the implementation of an energy management application is the assignment of a unique IoT address (e.g., an IPv6 address assigned to each of them). Typically, this can be done at the firmware of the smart meter (which is a trend followed by several device manufacturers). This assignment enables smart meters to communicate with application hosts in the scope of an IP network. The assignment of address can be performed at a scalable, plug n' play manner by the manager of the respective administrative domain. In principle, the use of an IPv6 address in this context allows the meter to be accessed by different application entities in their own address space – since any IPv6 termination may have, according to the IPv6 specifications, multiple addresses. This could be very significant to IoT, though we do not yet know if most of the current generation of smart meters has this capability.

### 2.3.3. IoT ID Discovery

**Scope**

IoT ID Discovery refers to the process of locating and retrieving IoT resources (e.g., services, data) in the scope of a large and complex space of ICOs. In this space ICOs can often be linked/networked, in which case the linking could reflect their relationships and dependencies. Discovery is key element of non trivial IoT applications; without discovery, these applications are limited to hard-coded configurations only. As a result, IoT ID Discovery processes alleviate the limitations of fixed configurations and enable dynamic configurable applications. Note also that the IoT ID Discovery process should ideally be efficient and high-performance in the sense that it should discover the most pertinent ICOs for a given task with the lowest possible latency. Therefore, IoT ID Discovery techniques can be classified and distinguished on the basis of the efficiency and performance. Furthermore, in IoT scenarios discovery capabilities are typically supported at two different levels, namely network (node discovery) and application (service discovery) levels.

IoT ID Discovery techniques for non-trivial IoT applications presuppose the existence of automatic mechanisms for registering and updating IoT resources with a directory service. Such mechanisms should be able to ensure that the directory service remains updated for each change in the status of an IoT resource, but also for the emergence/creation of new instances of IoT resources (e.g., new physical or virtual objects). Certain Identifier Resolution Systems like the Handle one considered below, have the capability of requiring authorization to access the attributes of an Identifier. When this property is invoked, as it may well be in IoT, the capability of a generalized access to the status may be inhibited also.

**Sample/Indicative Scenario**

Monitoring pollution levels in urban areas is important for citizens and authorities (e.g., local governments), in their efforts to avoid the adverse implication of air pollution in human health. Nowadays, it is possible to deploy a variety of air pollution sensors that can provide information on parameters such as Nitrogen dioxide ($NO_2$), Carbon dioxide ($CO_2$), Carbon monoxide (CO), Methane (CH4), Ozone (O3) and more. In order to dynamically access and calculate air pollution parameters at a given urban region (e.g., community, neighborhood) the discovery of sensors that monitor the above parameters in the target area is needed. Such IoT ID Discovery functionalities could involve the specification of:

- the target area (e.g., through longitude, latitude, radius) and
- the sensor type(s) that need to be used for the monitoring task,

and would return the list of sensor instances whose values could be used for calculating air quality metrics. This is exactly the type of environment where the device might have, in a system like Handle, multiple identifiers. The device itself might have an Identifier *IDdevice*. However, when part of a monitoring application there may be another Identifier *IDapplication*, which has IDdevice as one of its attributes, and *IPv6address* as another. Two different applications might have quite different authorizations to access the device from different IPv6 routing hierarchies, even if the edge routing is to the same sensor through the same edge network.

## 2.4. Application Areas for IoT Identification

IoT identification technologies are essential for a significant number of IoT deployments in various applications areas. Some indicative examples follow:

- **Energy Management Applications**: State-of-the-art energy management applications (such as smart grids, distributed renewable energy networks) leverage information from a wide range of devices (e.g., stand-alone smart meters, secondary stations) comprising the advanced metering infrastructure (AMI).Such applications are deployed across different scales (e.g., smart homes, smart buildings, smart neighborhood, smart cities), including large scale deployments. The latter take advantage of the large address space of IPv6, its support for robust routing and its compliance to standards (e.g., IEEE 802.15.4g, IETF 6LoWPAN, IEEE 1901.2) in providing reliable communications and data management functionalities as part of smart energy applications. Depending on their scale, regulatory environment and needs, smart energy deployments leverage global or public or private IPv6 address spaces – and even multiple ones at the same time.
- **Supply Chain Management and Logistics**: Several SCM applications are deployed based on AutoID technologies, thereby leveraging identifiers such as UPC, GS1 EPC, ucode and more. The emphasis in these applications lies in the tagging of objects (using some object ID) and accordingly tracking and tracking items for the purpose of improving the efficiency of supply chain processes (e.g., production planning). As already outlined a popular application (both in EU and China) is traceability, which provides complete information about the states of specific objects («things»), including information for both their current and past states. Note that the tag-based identifiers outlined above have been extensively deployed in large scale end-to-end SCM applications. In some industries (liquor, meat and soft drinks), the Government is introducing the Handle system on a large scale as part of their quality monitoring and compliance efforts. This is partly to capitalise on the various authorisation capabilities of Handle to constrain the access to Identifier attributes at different stages of the manufacturing and distribution cycle.
- **Urban Mobility Applications**: IoT technologies in smart cities context are extensively used for managing and optimizing urban mobility. Typical applications include smart parking, traffic management, road monitoring and intelligent transportation systems. Several of these applications leverage application identifiers, while there are also many applications (especially those dealing with transport and logistics) that blend them with RFID/AutoID identifiers.
- **Defense and Intelligence Applications**: Most of the defense and intelligence applications involve geospatial information and deal with the representation and contextual placement of assets, humans, materials and more. Several such applications are developed based on OGC standards (such as WMS and WFS), which commonly use URIs (as application identifiers) in order to refer and manage objects in their geospatial context.

The list of these applications is non-exhaustive. It however makes evident the fact that different applications use identifier types according to their requirements. Note that a structured and more broader list of IoT applications areas can be found in the 2014 edition of the IERC cluster book [Vermesan14].

# 3. State of IoT ID technologies in EU and China

## 3.1. Status in China

### 3.1.1. Technologies for IoT ID Naming

Adopting the international encoding standards and distribution principles, Electronic Product Code (EPC), IP address, E.164 [ITU-T_R_E.164], Uniform Resource Identifier (URI), Uniform Resource Name (URN) and relevant naming systems are already used in IoT field in China, example logistics management, M2M device management and so on. AnIoT ID white paper, which was published by China Academy of Telecommunication Research (CATR) in 2013, has already introduced the relevant situation in detail, which is. In this paper, combining with the new demands of IoT ID applications, we will focus on the newest development status of IoT ID Naming technologies in China, including CID, Ecode etc.

#### 3.1.1.1. CID (Communication Identifier)

The CID (Communication Identifier) system, which is proposed by CATR, is a public user oriented IoT ID Naming system. The CID system is in charge of distribution, management, storage and querying of CID identifiers, which are unique names for ICOs. Each of the CID identifiers consists of three different parts, including Compatibility Domain, Type Domain and Information Domain. The Compatibility Domain and Type Domain are optional fields, but the Information Domain is a mandatory field.

<table>
<tr><td rowspan="2">Compatibility Domain</td><td colspan="2">Country/Organization Code (8 bits)</td></tr>
<tr><td colspan="2">Naming System Code (8 bits)</td></tr>
<tr><td rowspan="2">Type Domain</td><td>Coding Type (4 bits)</td><td>Resource Type (4 bits)</td></tr>
<tr><td colspan="2">Business Type (8 bits)</td></tr>
<tr><td>Information Domain</td><td colspan="2">Information Domain</td></tr>
</table>

**Table 2: Overview of the CID Identifiers**

The Compatibility Domain is design to be compatible with the existing IoT ID service schemes, which consist of 8 bits Country/Organization Code (COC) and 8 bits Naming System Code (NSC). The COC is used to distinguish between different countries and organizations. The NSC is used to distinguish between different naming systems within the same country or organization.

The Type Domain is design to realize the efficient management and statistical analysis of IoT identifiers, distinguishing the coding schemes, naming objects and application areas of different naming systems. The Type Domain consists of 4 bits Coding Type (CT), 4 bits Resource Type (RT) and 8 bits Business Type (BT).The CT is used to specify the numeric scale and coding length of the information domain. The RT is used to specify the type of the named IoT resources, example barcode, RFID, sensor, M2M device etc. The BT is used to specify the application area of the IoT identifiers, example agriculture, manufacture, information etc.

The Information Domain is design to specify the detailed information of the named IoT resources, example identity, attributes etc.

#### 3.1.1.2. Ecode (Entity Code)

Entity Code (Ecode) system is an identification system for Internet of Things, which is proposed by Article Numbering Center of China (ANCC). The Ecode system standards the coding structure and the distribution principle of Ecode identifiers, which is a uniform, compatible coding scheme for ICOs. Each of the Ecode identifiers consists of three different parts, including Version (V), Numbering System Identifier (NSI) and Master Data (MD). The length of NSI and MD is decided by the V of Ecode.

| Ecode | | | | Maximum length | Code type |
|---|---|---|---|---|---|
| V | | NSI | MD | | |
| Ecode-V0 | $(0000)_2$ | 8 bits | ≤244 bits | 256 bits | Binary |
| Ecode-V1 | 1 | 4 digits | ≤20 digits | 25 digits | Decimal |
| Ecode-V2 | 2 | 4 digits | ≤28 digits | 33 digits | Decimal |
| Ecode-V3 | 3 | 5 digits | ≤39 digits | 45 digits | Character |
| Ecode-V4 | 4 | 5 digits | undefined | undefined | Unicode |
| $(0101)_2$~$(1001)_2$ | | Reserved | | | |
| $(1010)_2$~$(1111)_2$ | | Forbidden | | | |
| Note 1: Version and Numbering System Identifier defines the structure and length of the Master Data<br>Note 2: Maximum length is the sum of the length of Version, Numbering System Identifier and Master Data | | | | | |

**Table 3: Overview of the Ecode Identifiers**

The Version, length of 4 bits, is used to distinguish between different coding structures of Ecode systems. It is distributed by the national or universal wide IoT ID management organization uniformly.

The Numbering System Identifier (NSI) indicates the code of different identification system. According to the difference of Versions, the length of NSI could be binary 8 bits, decimal 4 digits and decimal 5 digits. It is distributed by the national or universal wide IoT ID management organization uniformly.

The Master Data is used to specify the identification codes of an industry or an application system. It is managed and maintained by the local management organization of each identification system, including the coding structure and the distribution principle. However, the local management organization should submit the Numbering System Identifier to the national or universal wide IoT ID management organization for records.

#### 3.1.1.3. Handle/DOI

The Handle System, in terms of its namespace and service architecture, is a general-purpose global name service that allows secured name resolution and administration over networks, and is one of the key components of the Digital Object Architecture (DOA), which is a basic information infrastructure that can facilitate interoperability between or among different systems, processes, and other information resources. Under the regulation and support of ITU, Digital Object Numbering Authority (DONA) is established and is responsible for Global Handle Registry (GHR), and authorizes a group of Multi-Primary Administrators (MPAs). Each MPA will run a global root service separately, known as the Global Handle Service (GHS).MPA China was established as one of the top-level management organization of the Handle System, with the headquarter located in the coalition of Electronic Technology Information Research Institute (ETIRI),China Digital Innovation Technology Co., Ltd (CDI), and Corporation for Handle Services in China (CHC), known as Coalition for Handle Services - China, and is responsible for global root services operation and the whole system running and management in China.

#### 3.1.1.4. OID (Object IDentifier)

The OIDis a common encoding strategy recommended by both ISO/IEC and ITU to unambiguous identify an object uniquely in the global range.OID has a very good foundation for global application and could be used in every link of object application process. Now, OID has been successfully used in many fields, such as information security, ehealth service, network management, sensor network and RFID.

In china, National Registration centre for OID (China) is in charge of registration, management, maintenance and international filing work of OID arcs allocated to China under {ISO arc} and {Joint-ISO-ITU arc}, which was established in 2007 with the headquarter located in China Electronic Standardization Institute(CESI). By now, more than 150 top-arc OIDs underneath {ISO arc(1.2.156)} and {Joint-ISO-ITU arc(2.16.156)}allocated to China have been registered by more than 100 IoT technology companies and application organizations throughout ministries, committees, enterprises and research institutes. China Standardization Working Group on Sensor Networks (WGSN) PG5supports the standardization of OID

related issues.In China, 12 national standards have been released and 14 national standards are being drafted up. ITU-T X.oid-iot research project “Guideline for using object identifier for the Internet of Things” has been set up. It is the first IOT Identification standard drafted up by china, which has applied successfully in many industry sectors, such as agriculture field, public health field, forestry field and etc.

### 3.1.2. Technologies for IoT ID Addressing

In this white paper, we will focus on the newest development status of the IoT ID Addressing technologies in China, including DNS and Handle.

#### 3.1.2.1. DNS

The Domain Name System (DNS) is currently the most prominent name service in the Internet. Because of the maturity and stability of the DNS, many name services for IoT ID addressing are also designed based on the principles of the DNS, or directly use DNS infrastructure to construct and improve. For example, the Object Name Service (ONS) used in the EPCglobal Network [EPCglobal], can provide mapping between a GS1 [GS1] Identification Key and associated data or services based on the DNS. The development work of Object Resolution System (ORS) is based on DNS technology. ORS consists of two processes: a general OID resolution process and an application-specific OID resolution process. The general OID resolution process uses the DNS resolution mechanism and DNS resource records. The application OID resolution process has no special restriction for system development. That ensures the flexible, compatible, high-security character of ORS.

In China, China Internet Network Information Center (CNNIC) is responsible for operation, administration and services of fundamental Internet resources (e.g., “.CN” TLD). The “.CN” national top-level domain service platform managed by CNNIC, has 30 distributed nodes at home and abroad. Its average daily DNS query volume achieves about 2.0 billion times. This DNS platform can provide name resolution services with the availability of 100%, and domain name registration and WHOIS services for more than 99.99% of the “.CN” domain name. Currently, they have constructed the China IoT ID root name service platform based on years of accumulated research efforts and maintenance experience in the field of DNS. Through the form of cooperation projects, this root name service platform has provide IoT ID resolve service for furniture business, smart appliances, intelligent monitoring and other application fields in Shanghai, Chongqing, Guangdong, etc.

Based on the above technologies advantages, Computer Network Information Center, Chinese Academy of Sciences (CNIC) has constructed the China IoT ID root name service platform. Through the form of cooperation projects, this root name service platform has provide IoT ID resolve service for smart city, smart home, product life-cycle management and other application fields in Shanghai, Chongqing, Guangdong, etc. In order to implement the centralization of IoT resources, which supports better interconnections among IoT applications, the domain name “.NIOT.CN” is established as the IoT root in China. Accordingly, all of the IoT IDs will be administered within this root domain.

In order to better promote the theoretical research and industrial application for DNS addressing technology, the China Ministry of Science and Technology, Ministry of education, National Development and Reform Commission have already funded a series of related projects. In 2009, CNNIC undertake the CNGI project “Credible Next Generation Internet Domain Name System and its industrialization". Supported by this project, CNNIC established 10 “.CN” top level domain nodes in global to enhance its interoperability for the global DNS system and improve the performance of DNS resolution. Meanwhile, “.CN” top level domain services platform also fully supports IPv4 / IPv6 dual stack resolution services, providing an opportunity for the IPv6 address needed by the Internet of Things. Also in 2009, under the support of National Natural Science Foundation project “Research on Addressing Key Technology in Internet of Things”, Prof. Sun Zhixin from Nanjing University of Posts and Telecommunications, focused primarily on the performance and security aspects of addressing technologies, especially in the constrained network environment (e.g., 6Lowpan). In 2012, under the support of National Natural Science Foundation project “research on the theory and key technologies for the future network architecture”, Prof. Zhang Hongke,

from Beijing Jiaotong University, explores the resolution mapping theory for service ID and connect ID in the future network.

#### 3.1.2.2. Handle

The Handle addressing system is defined as a hierarchical service model. In China, the Handle system has already used in the field of digital libraries, digital museums, digital publishing, etc. The ETIRI, CNNIC, Institute of Scientific and Technical Information of China (ISTIC), Beihang University and some other research institutions and universities have made many contributions on the development and promotion for Handle addressing technologies. In 2006, the Chinese Ministry of Education funded HP Company, Beihang University and others to carry out the China Digital Museum Project, which is aimed at creating a large-scale digital museum union to cover 100 university museum collections. The project adopted DSpace System to storage museum digital content, and used the Handle System to uniquely identify digital resources for the museum, while positioning for copies that may exist in other DSpace instance. From 2007 to 2010, the Chinese Ministry of Science and Technology funded an international cooperation project "Research and Application on Building the Chinese digital object unique identifier system" to carry out the cooperation with CNRI on digital rights management, which established a framework prototype for digital rights management based on DOI/Handle system. Its main idea is to use the security and distributed functions of the Handle system technology, as well as standard Web services interfaces and rights metadata definitions, to support registration and discovery of content rights. Currently, ETIRI is expected to further promote the Handle System in domestic food and drug traceability, equipment life-cycle information integration and management, and other IoT applications.

### 3.1.3. Technologies for IoT ID Discovery

#### 3.1.3.1. Resource discovery in Web of Things

As the use of various devices has become so widespread in IoT networks, it is difficult to access data on these devices in a unified way. The Web of Things (WoT) allows physical devices to be accessed as resources of both the web and services/applications based upon a web-based service environment, as well as through legacy telecommunications.

In 2012, a National Research Project on New Generation Broadband Wireless Mobile Communication System was founded, which is “The Architecture, Key Technologies and Demonstration of the Web-based Wireless Ubiquitous Network Environment” project. Based on the WoT technology, this project defines the interconnection and internetworking interface specification, which makes the data of different devices and systems be shared in a unified message process and format. In order to implement the interface specification, a functional module called WoT adapter or WoT service middleware is developed, responsible for resource abstraction and discovery. Based on this project, two ITU-T recommendations are released as part of the working achievements, ITU-T Y2063 and ITU-T Y2066.

Recommendation ITU-T Y.2063 provides a framework of the web of things (WoT). This Recommendation describes the overview of the WoT and identifies the requirements to support the WoT. In addition, this recommendation specifies the functional architecture including a deployment model for the WoT.

Recommendation ITU-T Y2066 provides the common requirements of the Internet of Things (IoT). These requirements are based on general use cases of the IoT and IoT actors, which are built from the definition of IoT contained in [ITU-T Y.2060]. The common requirements of the IoT are independent of any specific application domain, which refer to the areas of knowledge or activity applied for one specific economic, commercial, social or administrative scope, such as transport application domain and health application domain. The common requirements are also classified into the categories of non-functional requirements, application support requirements, service requirements, communication requirements, device requirements, data management requirements, and security and privacy protection requirements.

#### 3.1.3.2. Device abstraction in M2M

Device abstraction is the process of device modeling and resource parameterized modeling. In order to shield the heterogeneity of different devices, the ontology technology is used to model and describe the devices. Based on the device abstraction, the interoperation between devices and services can be easily implemented, also including the device self-discovery, device self-resolution, device self-aggregating, service discovery and service advertisement. In 2014, the application guidelines for the National Research Project on New Generation Broadband Wireless Mobile Communication System were published, the project of "Research on General M2M device abstraction and semantic specification standardization" was considered as an important research topic.

## 3.2. Status in EU

### 3.2.1. Overview

A wide array of identification technologies are deployed by EU organizations for different types of applications. These include IPv6, tag identifiers (UPC, RFID), DOI/Handle, as well as several application identifiers. The identification technologies are supported by infrastructures developed by European organizations. In addition to investments in these technologies, EU funded research initiatives for IoT are also looking into solutions that can ensure the integration and/or interoperability across multiple identification technologies. In this direction, EC co-funded projects of the European IERC cluster have recently developed and validated several innovative solutions for IoT ID Naming and Identification, which transcend the boundaries of single identification technologies. Following paragraphs provide more information regarding the deployment status and the future outlook of identification technologies in Europe.

### 3.2.2. Technologies for IoT ID Naming

#### 3.2.2.1. IPv6

The European Commission (EC) has acknowledged the importance of providing IPv6 infrastructures and for over a decade taken measures in order to encourage IPv6 deployment. However, IPv6 deployment remains very small comparing to IPv4 (e.g., it was estimated to be approx. 2% in June 2011 and above 4.5% today according to the last statistics of the IPv6 Google stats website (https://www.google.com/intl/en/ipv6/statistics.html). Furthermore, IPv6 is generally present in core networks, but has still very low penetration in the access part. Therefore, the EC has included IPv6 adoption as one of the topics of its Digital Agenda for Europe 2010-2020. In particular, the Digital Agenda underlines the need to support the deployment of IPv6 by public authorities (Action 89), as well as the need to accelerate upgrades of the Internet IPv6 (Action 97).

Note that the established IPv6 infrastructures are not primarily supporting IoT applications. Nevertheless, the momentum of IPv6 and the related commitment of the EC, make it an appropriate enabling infrastructure for IoT. Since 2008, the UDG project developed in Switzerland is mapping virtual IPv6 addresses as unique OID on all sorts of connected devices using different legacy communication protocols such as KNX, ZigBee or X10 (http://www.devicegateway.com). This direction has been validated in the scope of several EU projects, such as IoT6 (http://www.iot6.eu), BUTLER (http://www.iot-butler.eu), Ebbits (http://www.ebbits-project.eu) and IoT Lab (http://www.iotlab.eu), which have showcased how IPv6 and related technologies (i.e. 6LoWPAN, RPL[RFC6550], CoRE [RFC6650], COAP [RFC7252]) can support integrated IoT applications, including applications that comprise non-IPv6 enabled sensors and devices. Since attributes of Handle can be IPv6 addresses, IoT6 has shown a direct connection with the use of IPv6 and Handle together in IoT.

Mandat Inernational and Beijing University of Post and Telecommunication also successfully used IPv6 as global OID to homogenize and simplify access to sensor motes distributed across a joint pilot of IoT testbeds deployed between Europe and China (http://www.ipv6project.com/mibupt/index.php)

[Ziegler01]. Similarly, IPv6 is also used by the IoT Lab project (http://www.iotlab.eu) to integrate several FIRE European testbeds together and to homogenize the addressing and OID of their respective devices.

#### 3.2.2.2. Handle / DOI

The Handle System(HS) (www.handle.net) is a general purpose distributed information system that provides efficient, extensible, and secure identifier and resolution services for use on networks such as the Internet [Kahn06].The creators of the Handle System (i.e. Corporation for National Research Initiative (CNRI)) are closely collaborating with the ITU in evolving the HS and promoting its wider use.
The potential of the HS and the DOIs for unique identification has been acknowledged in Europe, initially in applications that identify and manage electronic documents. For example, it is deployed and used for EC documents by the Office of Publications of the European Community (http://publications.europa.eu/) and by the Multilingual European DOI Registration Agency. Also the European Persistent Identifier Consortium (EPIC) (http://www.pidconsortium.eu/) uses the Handle System for the management of research/scientific datasets.. While, the HS was developed initially with digital documents in mind, it has gradually evolved into a more generic implementation, supporting multiple object types, not just 'digital documents'. It is an operational system with global distribution, many features to aid performance, resilience and scalability. It is being standardised for the ITU under ITU-T Recommendation X.1255[X1255].Recently the EU IoT6 project has researched the use of Handle/DOI for persistent identifiers management, as well as for the scalable and secure management of IoT information. Moreover the richness of the syntax of Handle, and the way its attributes can be secured, has been demonstrated to provide important advantages both in describing legacy IoT subsystems, and in orchestrating multi-process access to them. Full details of that work are given in a number of references – e.g. [Kirstein14], [Varakliotis15].

#### 3.2.2.3. Bar Codes and RFID

Identifiers for AutoID technologies (bar codes, RFID) are extensively used in Europe for several applications. Bar code technology and its applications are at a very mature state, so the majority of the expenditure is on consumables with a smaller share being taken by printers and scanners. For RFID, a great deal of expenditure is still on hardware but also on a combination of services and software. The annual growth of the two technologies is quite different, e.g., approx. 7% per annum for bar code and 14% per annum RFID. The infrastructure behind such large markets is therefore taken into account in any developments towards the Internet of Things. Especially RFID (and its infrastructures) are acknowledged in Europe as forerunners of the Internet-of-Things [Santucci09].
In terms of EU-wide penetration, 17.7% of companies in the top-5 European countries (Germany, France, Italy, Spain and U.K.), across the manufacturing, transportation and retail sectors, had as of 2007 already implemented or piloted RFID (source: IDC European Vertical Market Survey)Manufacturing and logistics were the two sectors with the highest adoption levels, while the retail sector was lagging behind. The most prominent application of RFID in Europe is probably found in public transport, where it is used in most large EU cities [JRC-RFID10]. At the same time, RFID has still growth potential in the logistics and supply chain management sectors, where item-level tagging is leading to an explosion of the RFID/AutoID market.
EU organizations have also a significant presence in the RFID market, with strong actors in most parts of the RFID value chain, from chip manufacturers to label makers and systems integrators [IDTechEx-Das-08]. Furthermore, the EU has invested in several R&D programmes in the scope of the FP7 and ICT-PSP programmes, which results in RFID deployments in multiple sectors, but also the investigation of a wide range of technical, business, privacy, security and standards-related issues. Furthermore, the EC has: (A) Established a Cluster of European RFID Projects (CERP), which included several national and EU-wide projects on RFID and was the forerunner of the IERC cluster for the Internet-of-Things; (B) Financed two Coordination and Support Actions (namely CASAGRAS ((Coordination and Support Action for Global RFID-related Activities and Standardisation - http://www.rfidglobal.eu/)) and GRIFS (Global RFID Interoperability Forum for Standards), which supported collaboration for the development of EU-wide policies on RFID and

fostered synergies for the development of RFID standards. In a similar context, the EC co-funded initiated RfidInEurope (http://www.rfidineurope.eu/) has created a federating platform to the benefit of all European stakeholders engaging in the development, adoption and usage of RFID. The above-listed initiatives and support actions worked also on the transition from RFID to the Internet-of-Things.
RFID operation is regulated by several ETSI standards (see: http://www.etsi.org/technologies-clusters/technologies/radio/rfid), while GS1 standards are also used for the implementation of applications in the areas of supply chain management and traceability. The latter standards have been developed based on feedback from EU traceability stakeholders such as CIMO (European Association of Fresh Produce Importers) and CIAA (Confederation of the Food and Drink Industries of EU).
Recent deployments in the EU tend to integrated RFID identifiers with other types of AutoIDs, such as bar code and QR codes. Nowadays it seems a fallacy to assume that IoT services with require all identifiers (e.g., bar codes) to migrate to the same format (e.g., RFID).

#### 3.2.2.4. URIs and UUIDs

Several Internet-of-Things applications are also using application specific URIs for identifying IoT objects and resources. Typical examples of IoT deployments that use URIs for identification are those implemented by several EC co-funded R&D projects of the IERC cluster (i.e. the European Research Cluster for the Internet of Things) such as FP7 iCore (http://www.iot-icore.eu/), FP7 OpenIoT (http://openiot.eu/), FP7 IoT@Work (https://www.iot-at-work.eu/) and FP7 ebbits.The type of URI identifier used in these projects depends typically on the IoT modeling of resources used (e.g., RDF/ontologies). Some projects also define other types of unique identifiers in the form of UUIDs.
URIs enables applications that integrate multiple identification solutions (e.g., EPC and IPv6). Such integration is considered important for certain classes of applications that transcend the boundaries of multiple heterogeneous IoT systems i.e. IoT systems using different identification technologies.

#### 3.2.2.5. Industry Specific Identification Specifications

In addition to the use of identification systems that are broadly applicable across all sectors and geographic regions, there are cases where of particular industries which impose compliance to normative identification specifications as a means of achieving interoperability and/or economies of scale. For example, the EU FI-SPACE project, which conducts trials in the food-chain exploits standards and guidelines for the identification of animals [FI-SPACE-D500.4.1], such as the international standard “ISO 11784: Radio frequency identification of animals - code structure”. These standards are used in conjunction with RFID technologies and the GS1 identification system.

#### 3.2.2.6 Approaches for Identification of Network Layer Devices

Several IoT applications make use of mechanisms for the identification of network layer devices. As an example, Delay-Tolerant Networking (DTN) is used to address technical issues of interconnecting networks that lack a reliable end-to-end path between the source and destination, and conduct heterogeneity of transport/routing technologies. DTN uses naming, layering, encapsulation, and persistent storage to interconnect heterogeneous portions of a larger network, irrespective of formal layers. In the scope of the DTN architecture nodes have identifiers in the context of the bundle protocol [RFC 5050]. DTN's flexible naming scheme uses a tuple of the form (region, host, application), which is able to identify a host, as well as an application of interest on the host. Various research projects in the EU are addressing this approach of networking, e.g., N4C (Networking for Communications Challenged Communities: Architecture, Test Beds and Innovative Alliances) [http://www.n4c.eu/].

Note that network layer approaches are in general employed for efficiently supporting the interoperability of resource constrained devices, but are not sufficient for delivering application-level IoT innovations e.g., novel services as part of the emerging wave of BigData IoT applications.

### 3.2.3. Technologies for IoT ID Addressing

IoT ID Addressing technologies in Europe are deployed in conjunction with the presented naming and management technologies. As a result a wide array of naming services is deployed, depending on the identification technology used.

#### 3.2.3.1. Domain Name System (DNS)

The DNS system is used for naming as part of general-purpose IPv6 enabling infrastructures. Specific solutions for IoT ID Naming have been demonstrated by EU Research Projects such as FP7 IoT6 which has developed a solution that uses Multicast DNS (mDNS) for discovery of resources at a local level and a distributed hash table (DHT) infrastructure in DNS-SD (http://www.dns-sd.org/) format for looking up resources at global level. This IoT6 solution is appropriate for IPv6 sensor clusters.

#### 3.2.3.2. Object Naming Service (ONS)

The Object Naming Service (ONS) is used in conjunction with GS1 EPC identifiers [RFC5134]. ONS comprises a database and a look-up built on top of DNS. It locates the EPC-IS (Electronic Product Code Information Sharing) repository of the authority that has issued the EPC identifier (i.e. typically the manufacturer of the RFID tagged item). GS1 operates since 2008 the European root ONS platform, which is offered by GS1 to European organizations that have subscribed to EPCglobal. ONS services are used as part of enterprise deployments, but also as part of EU projects (e.g., FP7 SmartAgriFood) for applications such as logistics and traceability.

#### 3.2.3.3. Handle System

Instances of the Global Handle Registry (GHR) are deployed in Europe, along with numerous local handle services (LHS). These provide naming services for the Handle System deployments in Europe, along with the DOI handling agencies. Furthermore, standalone configurations of the LHS exist for the needs of localized IoT testbeds and applications. Also, the FP7 IoT6 project has worked with CNRI to support the evolution of the Handle system towards IPv6.

#### 3.2.3.4. Naming Services based on ontologies

Another direction in IoT ID Naming is based on the linking of IoT systems and/or applications that use different identifiers using common ontologies and a gluing semantic layer. Such deployments map the various IoT resources and identifiers to a common ontology, which accordingly serves as a basis for the provision of naming services. This approach is therefore based on a meta-semantic directory structure, which enables the management, assignment and uses of IoT names according to a common ontology. Such solutionsincur extra overhead for semantically annotating IoT resources (e.g., objects and services), which is the expense of achieving baseline semantic interoperability across diverse IoT systems.

#### 3.2.3.5. Other Naming Systems

Several IoT deployments in Europe are also based on the definition and deployment of custom names for IoT resources as part of conventional/mainstream directory services such as Lightweight Directory Access Protocol (LDAP) [RFC4514], CoAP Resource Directory, and UDDI (Universal Description and Discovery

Interface). A particular interesting approach is one enabling constrained web servers to describe hosted resources, their attributes, and other relationships between links. This approach is based on the CoRE Link Format [RFC6690].

### 3.2.4. Technologies for IoT ID Discovery

Most of the naming and management schemes outlined above come with capabilities for dynamic look-up of resources. For example, ONS provides the means to look-up EPCs against EPC-IS repositories. Furthermore, semantic web technologies (ontologies, RDF, SPARQL) enable the interoperable discovery of resources as outlined in [IERC-AC2-D1]. Also, several EU companies are contributing to the discovery specifications of the OneM2M standardization partnership [OneM2M].Another initiative focusing on IoT ID Discovery is related to the XMPP protocol [RFC6120], [RFC6121]: within the XMPP Standards Foundation, an IoT ID Discovery framework based on XMPP is being specified [XEP-0347].
Several discovery schemes are also researched in the scope of EU projects of the IERC cluster. These research projects emphasize on high-performance and intelligent (non-deterministic discovery). For example, the IoT@Work project performed some initial analysis of the use, in its context, of a semantic content-centric framework enabling cooperative environments where resources can be discovered, queried and inventoried by autonomous objects in a peer-to-peer, collaborative way, without requiring a central control and coordination [Ruta13]. Other approaches have been also introduced by the FP7 FI-WARE project (http://www.fi-ware.org/) which has published a relevant generic enabler (GE) component and CASAGRAS2 (www.iot-casagras.org/), which has been undertaken relevant specification work [Roussos11]). Also, the IoT-A project has implemented, validated and evaluated a range of different approaches based on a resolution infrastructure, which is in-line with the IoT-A reference architecture model [IoT-A-D1.5]. These approaches include:

- A Geographic location-based discovery approach, which shows how a spatial index structure can be used to efficiently retrieve the specified services within a geographic scope. The approach also considers a distributed and federated approach enabling an IoT infrastructure with different operators, which keeps a maximum level of control, but still makes their services discoverable.
- A Semantic web-based discovery approach, which converts service descriptions into a latent factor space with a reduced number of latent factors. The service descriptions are then clustered based on the latent factors. For discovery the request is transformed to latent factors as well and then has to be matched only to the service descriptions in the best matching cluster. This allows the partitioning and distribution of the discovery, resulting in a more scalable solution for semantic discovery.
- A Federation-based discovery and association creation approach, which uses a federated hierarchical location structure for discovery on a semantic basis. For each symbolic location, there is a node in the hierarchy, which is responsible for services whose service area is contained in this location. Semantic discovery only has to be done on those nodes in the hierarchy that overlap with the location scope. Each node only has to match a request to a limited amount of services resulting in a scalable solution.
- M3 and uID-based look-up and discovery approach, which uses the M3 Semantic Information Broker infrastructure for discovering the required services. Semantic Information Broker (SIB) realizes a shared information space. The discovery is based on a two-level approach. In the first step SIB Resolution Service is used for determining which Semantic Information Brokers may have relevant services and in a second step these are contacted for completing the discovery.

Research schemes are not yet deployed at large scale, but indicate the importance of discovery as a means of adding intelligence and sophistication within IoT applications.

# 4. Challenges for the Development of Identification and Naming Solutions for Internet-of-Things in EU and China

Despite the availability of a wide range of naming, addressing and discovery technologies for IoT, the development of complete, robust and effective solutions for IoT identification at a large scale is still in its infancy. Hence, there are still challenges surrounding the development of IoT identification solutions for the emerging wave of IoT applications, which are expected to include large scale applications spanning multiple organizations and in several cases transcending the boundaries of multiple territories. In the sequel we highlight the most important of these challenges as identified from the experience of IoT deployments in both China and the EU.

## 4.1. IoT Identification Challenges

### 4.1.1. Interworking and Interoperability

Several of the existing infrastructures (e.g., IPv6, Handle, EPC/ONS, URIs and Semantic Technologies) for IoT ID Naming, Addressing and Discovery have momentum and a track record of real-life deployments. Furthermore, some of them provide most of the functionalities that are a prerequisite for the operation of IoT applications. Nevertheless, there is no evidence that one of these infrastructures will dominate the IoT identification landscape. Rather, it seems more likely that these identification infrastructures will coexist serving different purposes, application areas and geographical regions. In order to support certain classes of large scale integrated IoT applications, it is therefore required to provide solutions for interworking and interoperability across different identification technologies. Such solutions will enable the development of integrated applications that break the boundaries of state-of-the-art vertical silo applications, towards reducing the fragmentation of IoT data and services. Hence, additional research efforts in this direction are required in both EU and China.

### 4.1.2. Scope of state-of-the-art naming and addressing infrastructures

Most of the existing infrastructures for IoT identification (e.g., IPv6) have not been exclusively designed for IoT environments and applications. Rather they have been inspired by the need to expand the internet address spaces or to digitally track and trace physical objects. As a result, they are not appropriate for dealing with the full range of IoT resources, including virtual objects and IoT services. In several cases extensions to these technologies have been defined in order to address these limitations, such as extensions added through ontologies and semantic technologies. However, it is still challenging to ensure that these extensions can achieve the performance and scalability goals of IoT.

### 4.1.3. National Infrastructures for IoT Identification

Based on the current landscape of technologies for IoT identification, it is very difficult to establish a national wide infrastructure for unique identification i.e. a resilient infrastructure that will not be highly dependent on foreign entities. Indeed, technologies such as Handle/DOI and EPC/ONS depend on infrastructures (e.g., GHR, root ONS) established and operated by third-entities. However, it is possible to operate and manage national wide infrastructures (e.g., LHR, EPC-IS repositories) that facilitate the handling, management and allocation of IoT resources at national level. The possible development of national infrastructures should therefore consider the trade-offs between the effort required to setup/manage national infrastructure and the merits of an independent infrastructure. Because of the widespread acceptance already of systems such as EPC-IS, and the flexibility of systems like Handle, one should investigate the feasibility and utility of defining identifier types that transcend single systems. It is quite feasible to register an attribute of Handles as type EPC-IS. The description of a Handle Digital Object can then utillise the full power of the EPC-IS – related infrastructure and databases.

#### 4.1.4. Performance Considerations

At the current early stage of development of IoT technologies, performance and latency issues are not adequately addressed. These for example include the performance of routing servers and directory servers employed by the various technologies, which should provide decent performance even when they should provide addressing and resolution services for billions of Internet-connected objects. The challenge lies in appropriately dimensioning the amount and capacity of the internet-connected nodes that will provide addressing, directory and discovery services for large numbers of objects. A related issue concerns also the identification of novel distributed approaches supporting large scale IoT deployments in scenarios involving low bandwidth networks and low power devices. The individual components of the candidate systems have investigated their performance and scalability potential. For example the inherent architecture of Handle is identical to that of the DNS, and allows zoned scaling in just the same way. How well that system will perform when the security aspects that Handle can provide are fully utilized is less clear.

#### 4.1.5. Security Challenges

Most of the currently used IoT identification technologies focus on the provision of highly scalable distributed naming and addressing services. Most of these technologies do not put emphasis on the provision of security services over naming and addressing functions. Identification related security functionalities should be provided in the following areas: (A) Authenticated access to naming and identification data as part of look-up and resolution processes; (B) Authorized access to naming and addressing information, through ensuring that the applications that access the identification data have the rights to do so; (C) Ensuring that naming/addressing data are not forged; (D) Encryption of data exchanged between servers in the scope of selected IoT applications; (E) Preventing packet interception i.e. manipulation of IP packets carrying naming or addressing information; (F) Avoiding cache poisoning i.e. possibilities of manipulating information/queries cached within the naming system implementation; (G) Alleviating denial of service caused following manipulation of the IoT identification services; (H) Risks associated with naming assignments such a forging identifiers (e.g., forging QRCodes or RFID identifiers and associating them with hostile services).

Note that mechanisms supporting the above-listed security functionalities should be designed in order to be scalable. This is particularly important given that the enforcement of authorized access to naming and addressing information at a large scale could be a very resource consuming task.

The Handle System can provide insights and experiencing on how to address the above-listed security concern, since in Handle the capability of requiring authentication and authorization if built into the system. Moreover performance has been considered at the same time in several ways. Its local services can be split over multiple servers if needed; its access protocols now support the full RESTful architecture with secure HTTP; its authentication security features include both public/private key and symmetric key cryptography.

### 4.2 Solutions and Recent Developments

#### 4.2.1 Current IoT identification solutions Development in China

Based on a National Founding project from NDRC, CATR, ETIRI, CNIC and ANCC developed a public IoT ID Service Platform, which can provide a compatible name resolution service - Resource Name Service (RNS).

##### 4.2.1.1 System architecture

The platform architecture includes Resolver, Name Server and Information Server. Resolver: IoT ID query software client, which is designed to be a library procedure so that it can be called by any kinds of IoT applications. Its main function includes name conversion, sending query packet and receiving the response packet. In order to make full use of existing DNS infrastructure, all of the IoT identification resolution packets will be converted to standard DNS packets. Name Server: a storage entity of various resources records and provides responses to queries against these records. The Resource Record (RR) refers to the

mapping record of resource identifiers, which may also contain some other auxiliary information. Information Server: a repository of all the detail information corresponding to a special resource. It is also designed to enable events to be captured and queried. In order to improve the efficiency of encapsulating HTTP envelope and high concurrent read/write operations, IS provides RESTful API and stores data based on NoSQL in the platform.

#### 4.2.1.2 Naming mechanism

Two-stage identification structure is designed to solve the heterogeneity problem of current identification technologies, which divide each object identifier into two stages, including Standard Identifier (SID) and the Resource Identifier (RID). The first stage is SID, which refers to the unique identifier for each naming scheme. The Compatibility Domain of CID and the Numbering System Identifier (NSI) of Ecode are both existing SID name spaces. The second stage is RID, which refers to the unique identifier for each ICOs. All of the existing object identification scheme can be directly used as RID. In order to meet the needs of the practical application, most of them have adopted a hierarchical encoding structure.

#### 4.2.1.3 Addressing Mechanism

Correspondingly, in order to solve the heterogeneity problem of current IoT ID Addressing technologies, the RNS platform also requires a two phases IoT ID Addressing technology, including the SID addressing and the RID addressing. The SID addressing, SID query request will be first submitted to a local SID name server, which has been configured in advanced. If cache is not hit, then this local SID name server will forward the query to related SID name server. The returned resource record related to a SID is shown below: RecordSID = {SID, NSD}. In which, Naming Scheme Description (NSD) refers to the semantic description for each naming scheme. The RID addressing, with the help of extracted NSD from the SID resource record, the Resolver can translate different RID into a unified hierarchical resource name (similar to the domain names used in the DNS). Then the corresponding RID resource records will be queried through a standard DNS addressing.

### 4.2.2 Current IoT identification solutions Development in the EU IERC Cluster

#### 4.2.2.1 Integrated Naming and Addressing Solutions based on IPv6

EU IERC projects have recently demonstrated the potential of IPv6 to serve as an infrastructure for unifying various legacy identification technologies. To this end, an IPv6 addressing proxy has been developed, which provides mapping of legacy IoT IDs to IPv6. Furthermore, semantic web interfaces have been deployed over the IPv6 discovery mechanism in order to enable access to names and addresses over the web.

In a further development of the IoT6 project, the Handle infrastructure has been shown to be able to mirror the mapping of the legacy properties onto the Identifier space. In that case the IPv6 addresses need not reveal any information about the IoT end-point configurations, and the IPv6 addressing of the IoT end-points can comply completely with the application policies of the relevant stakeholder. That approach obviates the danger that application-specific stakeholders may claim jurisdiction over part of the IPv6 address space – which might provoke severe conflict with the IETF and others claiming governance rights on the Internet.

#### 4.2.2.2 Integrated Solutions for Semantic Interoperability

Recent developments on IoT identification in the scope of EU's IERC cluster focus on research associated with the development of integrated semantically interoperable applications. During the last two years, several IERC projects have produced cloud-based infrastructures that enable the development, deployment and operation of semantically interoperable applications, notably applications that leverage data and services from multiple heterogeneous IoT systems. For example the IERC OpenIoT project has produced an

open source blueprint infrastructure (available at: http://github.com/OpenIotOrg/openiot/wiki) for semantic interoperability of diverse IoT systems. This infrastructure provides a cloud based directory module, where IoT resources instances are registered based on a URI. URIs are associated with instances of sensors and IoT resources, which all comply to the same ontology, thereby ensuring the semantic unification of diverse resources. Accordingly, a cloud discoverer module operating over the directory enables discovery of resource by location, by location and type, as well as by their URI. The discoverer module operates based on semantic web technologies (i.e. SPARQL is used for querying resources).

The semantic interoperability infrastructures for naming and discovery are validated in the scope of various applications, including several integrated applications for smart cities developed in the scope of IERC projects which have commenced recently. As part of the Horizon 2020 programme, EU has launched a call for new projects that aim to take semantic interoperability of IoT resources to the next level, through enabling large scale federation and interoperability of IoT resources, including data and services residing in multiple cloud infrastructures, as well as IoT resources associated with smart embedded devices and BigData processing. The vision is to ensure a tighter and effective blending of diverse IoT resources into cloud and BigData infrastructures, thereby enabling IoT applications to seamlessly look up and use ICOs residing in different and multiple ICOs gateways, cloud infrastructures and BigData repositories.

# 5 Suggestions and Outlook for the Evolution of Identification Solutions for the Internet-of-Things

In an effort to address the above-listed challenges both EU and China work intensively towards two complementary directions:

- Expanding and extending existing infrastructures for IoT ID technologies
- Researching technological building blocks that could address the technical challenges listed in the previous section.

In the sequel we provide an overview of recent efforts in China and EU, following the presentation of a range of recommendations for the future evolution of IoT identification solutions.

## 5.1 Expansion and Evolution of IPv6

Both China and EU acknowledge the importance of increasing the penetration of IPv6 in future internet infrastructures and have already concrete strategies for boosting this penetration. Early IoT deployments have validated the ability of IPv6 to serve as a global identification infrastructure for the Internet-of-Things. As a result, the IoT community should take advantage of on-going investments on IPv6 deployment, in order to develop large scale IoT applications that transcend multiple administrative domains. To this end, IoT communities should integrate and use technologies that facilitate the deployment of IPv6 for IoT deployments, based on protocols such as Mobile IPv6 (MIPv6) for mobility, IPSec for security, 6LoWPAN for the integration of low-power smart embedded devices and more. Furthermore, emphasis should be paid on technologies that enable the integration of other identification with IPv6. A step in this direction has been realized in the scope of EU's IERC IoT6 project through the implementation of an IPv6 addressing proxy that maps legacy IoT technologies and identifiers (e.g., RFID, Konnex (KNX), X10, ZigBee) to IPv6 addresses [Jara13].Another has been the extension of this to using the same mapping onto the Identifier space [Kirstein14].
IoT could benefit from the fact that IPv6 allows for end-points to have many distinct addresses, compliant with different stakeholder applications. However, to the best of our knowledge, there has been little work on the impact of such usage of addresses on the operation of the IPv6 Internet.

## 5.2 Web Access to IoT ID Naming, Addressing and Discovery Functionalities

In order to facilitate the adoption and wider use of the IoT paradigm, it is essential to ease application development. In this direction EU and China support trends towards opening up IoT functionalities to the large pool of web developers, on the basis of technologies (e.g., IETF CoAP, Semantic Web technologies) that render IoT resources accessible via mainstream web-based interfaces (e.g., RESTFul interfaces). These trends are also in-line with the vision of the Web-of-Things (WoT). It is therefore recommended that IoT ID Naming, Addressing, Management and Discovery functionalities are made accessible through web-based interfaces. Recent projects in both EU and China are in-line with this direction (e.g., through the implementation of recommendation ITU-T Y.2063 and of web/cloud-based discovery functionalities for IoT).

## 5.3 Validation of Semantic Web Technologies for large scale deployment

Both the EU and China sides acknowledge the merit of semantic technologies (ontologies/RDF, SPARQL, LinkedData) towards integrating diverse IoT systems in a way that ensures the semantic interoperability of IoT resources. In terms of identification semantic web technologies are used in order to enable dynamic and intelligent discovery of ICOs and IoT resources across different IoT systems. However, semantic web technologies are still associated with performance and scalability concerns. This asks for their

benchmarking, but also for additional research towards improving their performance without any essential loss in their functionalities.

## 5.4 Handling of Mobility in Discovery

Most of the IoT technologies for discovery are appropriate for resources that reside in fixed, a priori known locations. With only few exceptions (e.g., MIPv6) they do not take into account the mobility of objects and therefore are not appropriate for discovering roaming objects/things. Mobility aspects should be taken into account in the development of IoT ID Discovery techniques, especially since the number of mobile IoT applications (e.g., mobile crowd-sensing) is proliferating. The handling of mobility should not be confined to support for multi-homing, but should also take into account the mobility patterns of the roaming objects. Furthermore, the dynamic relations among objects should be considered, especially in volatile environments where object could dynamically join or leave.

## 5.5 Security Services

As part of Section 3 we have already identified a number of security challenges including authentication, authorization, encryption, prevention of packet interception and cache poisoning and more. IoT ID Naming and Discovery techniques should be therefore enhanced with security schemes that address these challenges, including schemes for authenticated, authorized and tamper proof access to identification information.

## 5.6 IoT Unified Querying Services

Ease of use and friendly interfaces often determine the success of a web service or software. The same situation also applies to IoT identification service. Although heterogeneous IoT ID Naming schemes will coexist for a long term while application developers may also choose a specific resolution service provider according to their own needs, this background knowledge should be transparent for common users. No matter what kinds of identification addressing technologies are adopted in the end systems, a unified IoT ID querying services should be provide to common user. Specifically, we can learn from the DNS design principles, which take its client as a part of the operating system in the form of a library program.

# 6 References

[EPCglobal] EPCglobal, http://www.gs1.org/epcglobal.

[FI-SPACE-D500.4.1] Christopher Brewster, Andreas Füßler, Scott Hansen, Sabine Kläser, Andrew Josey, Daniel Martini, Esther Mie-tzsch, Chris Parnel, Tim Sadowski, Angela Schillings-Schmitz, Monika Solanki, «Guidelines for the use of standards in FI-SPACE», FI-SPACE Project Deliverable D500.4.1, September 2013

[GB/T 26231] Information technology - Open systems interconnection - National numbering system and registration procedures for object identifier (OID).

[GB/T XXXXX-XXXX] Identification System for Internet of Things Entity code (Draft Version).
[Whitepaper2013] Internet of Things ID White Paper, CATR, 2013.

[GS1] GS1, http://www.gs1.org/.

[GS1-2014] GS1 in Europe, External Relations Newsletter, 2nd Quarter, 2014.

[Gubbi13] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Elsevier: Future Generation Computer Systems, vol. 29, no. 7, p. 1645–1660, 2013.

[IDTechEx-Das-08] Das, R. and Harrop, P. (2008), RFID Forecasts, Players and Opportunities, IDTechEx, Cambridge, UK.

[IERC-AC2-D1] Martin Bauer (IOT-A), Paul Chartier (CEN TC225), Klauss Moessner (IOT.est), Nechifor, Cosmin-Septimiu (iCore), Claudio Pastrone (ebbits), Josiane Xavier Parreira (GAMBAS), Richard Rees (CEN TC225), Domenico Rotondi (IoT@Work), Antonio Skarmeta (IoT6), Francesco Sottile (BUTLER), John Soldatos (OpenIoT), Harald Sundmaeker (SmartAgriFood), «Catalogue of IoT ID Naming, Addressing and Discovery Schemes in IERC Projects», electronically available at: http://www.theinternetofthings.eu http://www.theinternetofthings.eu/sites/default/files/%5Buser-name%5D/IERC-AC2-D1-v1.7.pdf)

[IoT-A-D1.5] IoT-A, Deliverable D1.5 – Final architectural reference model for the IoT v3.0, http://www.iot-a.eu/public/public-documents/d1.5/view.

[IoT-A-D4.3] Suparna De (Ed.), Internet of Things Architecture (IoT-A) Project Deliverable D4.3 – "Concepts and Solutions for Entity-based Discovery of IoT Resources and Managing their Dynamic Associations", March 2012.

[IPV6Observatory14] IPV6 Observatory, Final Report, Study Ref: SMART 2011/0059, January 2014.

[ISO/IEC 9834-1] Information technology: open systems interconnection procedures for the operation of OSI registration authorities: general procedures and top arcs of the international object identifier tree.

[ITU-T_R_E.164] ITU-T Recommendation E.164 (05/97), "The international public telecommunication numbering plan".

[ITU-T Y.2066] Recommendation ITU-T Y.2066 (2014),Common requirements of Internet of Things.

[ITU-T Y.2063] Recommendation ITU-T Y.2063 (2012),Framework of the web of things.

[JRC-RFID10] Andrea de Panizza, Sven Lindmark and Pawel Rotter, «RFID: Prospects for Europe Item-Level Tagging and Public Transportation», European Commission, Joint Research Centre (JRC), Institute for Prospective Technological Studies, 2010.

[Kahn06] Kahn, Robert and Wilensky, Robert. "A Framework for Distributed Digital Object Services". International Journal on Digital Libraries, Springer, Volume 6, Number 2, April 2006

[Kelly13] S. T. Kelly, N. K. Suryadevara and S. C. Mukhopadhyay, “Towards the Implementation of IoT for Environmental Condition Monitoring in Homes,” IEEE Sensors Journal, vol. 13, no. 10, pp. 3846 – 3853, 2013.

[Kirstein14] P. Kirstein and S. Varakliotis, “Handling the Internet of Things with Care”. 11th MobiQuitous Workshop on IoT Ecosystems, December 2014, London.

[MSW2004] Mao Wei, Sam X. Sun, Wang Feng, “Technology of Internet Resources Naming and Addressing: Handle System” Application Research of Computers, 2004.

[OneM2M] OneM2M partnership, http://www.onem2m.org/

[RFC 3650] IETF Networking Group, “Handle System Overview”, 2003.

[RFC4514] Zeilenga, K., Ed., "Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names", RFC 4514, June 2006 (http://tools.ietf.org/html/rfc4514).

[RFC 5050] S. Burleigh, «Bundle Protocol Specification», "RFC 5050 (Experimental)", Internet Engineering Task Force, November 2007 (https://tools.ietf.org/html/rfc5050).

[RFC5134] M. Mealling (Network Working Group), «A Uniform Resource Name Namespace for the EPCglobal Electronic Product Code (EPC) and Related Standards», Request for Comments 5134, January 2008.

[RFC6120] Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 6120, March 2011, <http://www.rfc-editor.org/info/rfc6120>.

[RFC6121] Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence", RFC 6121, March 2011, <http://www.rfc-editor.org/info/rfc6121>.

[RFC6550] Winter, T., Ed., Thubert, P., Ed., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, JP., and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", RFC 6550, March 2012, <http://www.rfc-editor.org/info/rfc6550>.

[RFC6690] Z. Shelby,“Constrained RESTful Environments (CoRE) Link Format”, Internet Engineering Task Force (IETF), Request for Comments (RFC) 6690, Standards Track, ISSN: 2070-1721, August 2012.

[RFC6775] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, November 2012, <http://www.rfc-editor.org/info/rfc6775>.

[RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, June 2014, <http://www.rfc-editor.org/info/rfc7252

[Roussos11] George Roussos and Paul Chartier, "Scalable ID/Locator Resolution for the IoT", in the Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing (ITHINGSCPSCOM '11).

[Ruta13] M. Ruta, F. Scioscia, E. Di Sciascio, D. Rotondi, S. Piccione, "Semantic-based Knowledge Dissemination and Extraction in Smart Environments", International Workshop on Pervasive Internet of Things and Smart Cities (PITSaC-2013) - 2013, March 2013 (DOI 10.1109/WAINA.2013.249)

[Santucci09] Santucci, G. (2009), "From Internet of Data to Internet of Things", Paper for the International Conference on Future Trends of the Internet, 28 January 2009.

[Smith12] Ian G Smith, Ovidiu Vermesan, Peter Friess, Anthony Furness; The Internet of Things 2012 New Horizons, ISBN 978-0-9553707-9-3, http://www.internet-of-things-research.eu/pdf/IERC_Cluster_Book_2012_WEB.pdf

[Varakliotis15] S. Varakliotis, P. Kirstein, G. Deiana. "The Use of Handle to Aid IoT Security". 2015 IEEE International Conference on Telecommunications (ICC 2015) - Internet of Things Symposium, June 2015, London, UK.

[Vermesan14] Ovidiu Vermesan and Peter Friess, "Internet of Things – From Research and Innovation to Market Deployment", IERC cluster book, River Publishers 2014.

[XEP-0347] XEP-0347: Internet of Things – Discovery, http://xmpp.org/extensions/xep-0347.html.

[X1255] "X.1255: Framework for discovery of identity management information". Approved in 2013-09. http://www.itu.int/rec/T-REC-X.1255-201309-I

[Ziegler01] Sébastien Ziegler, Michael Hazan, Huang Xiaohong, Latif Ladid; IPv6-based test beds integration across Europe and China.