IERC Activity Chain 2 DELIVERABLE D1

"Catalogue of IoT Naming, Addressing and Discovery Schemes in IERC Projects"

IERC Activity Chain	**Naming, addressing, search, discovery**
Deliverable Reference Number	**IERC-AC2-D1**
Deliverable Title	**Catalogue of IoT Naming and Addressing Schemes in IERC Projects**
Revision Number	**V1.7**
Deliverable Editor(s)	**John Soldatos (OpenIoT)**
Authors / Contributors	**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)**

Dissemination Level		
PU	**Public**	

Revision History

Rev.	Author(s)	Project(s)	Date	Changes
V0.1	J. Soldatos	OpenIoT	02/7/12	Table of Contents
V0.15	Antonio Skarmeta	IoT6	23/7/12	IoT6 Contribution
V0.2	J. Soldatos	OpenIoT	30/7/12	Introduction and OpenIoT Input
V0.21	J. Soldatos	OpenIoT	15/9/12	Changes in the structure / Abstract
V0.3	Paul Chartier, Richard Rees	CEN TC225	01/10/12	Addressing Schemes Considered in CEN TC225
V0.4	M. Bauer	IOT-A	02/10/12	Contribution from the IoT-A project
V0.45	D. Rotondi	IoT@Work	02/10/12	Contribution from the IoT@Work project
V0.5	K. Moessner	IOT.est	04/10/12	Contribution from the IoT.est project
V0.55	Harald Sundmaeker	SmartAgriFood	09/10/12	Inputs from SmartAgriFood Project
V0.6	C. Pastrone	ebbits	15/10/12	ebbits Contribution
V0.65	D. Rotondi	IoT@Work	16/10/12	Updates to the IoT@Work contribution
V0.7	J. Soldatos	OpenIoT	19/10/12	Updates to OpenIoT contribution, First Taxonomy of the solutions
V0.8	J. Soldatos	OpenIoT	21/10/12	Questionnaire in Appendix 1
V0.85	Francesco Sottile	BUTLER	26/10/12	Inputs from the BUTLER Project
V0.9	J. X. Parreira	GAMBAS	26/10/12	Contribution from the GAMBAS Project
V.95	Nechifor, Cosmin-Septimiu	iCORE	30/10/12	Contribution from the iCore Project
V0.99	C. Pastrone	ebbits	08/11/12	Additions to ebbits contribution
V1.0	J. Soldatos	OpenIoT	08/11/12	First complete version
V1.1	C. Pastrone	ebbits	19/11/12	ebbits Revisions
V1.2	J. Soldatos, All	All Projects	18/12/12	Finalization following the IERC AC2 WebEx Conference
V1.3, V1.4	J. Soldatos, All	All Projects	27/12/12	Minor Corrections
V1.5, V1.6	J. Soldatos, Antonio Skarmeta, Francesco Sottile	All Projects	22/01/13	Version after Quality Control of the Deliverable
V1.7	J. Soldatos	OpenIoT	31/01/13	Version for Release

Abstract

This document provides a catalogue of different naming, addressing and discovery schemes for the Internet-of-Things (IoT), notably schemes that are currently researched, validated and used by IERC projects. As part of this document each of the contributing projects has provided an overview of the addressing and discovery solution(s) that it deploys, along with an assessment of each solution in terms of its migration and scalability. The various schemes include solutions based on legacy standards, semantic solutions that rely on emerging standards, as well as radically new solutions that focus on new propositions beyond existing and on-going standardizations efforts. A clustering of the various solutions is also performed on the basis of the different naming and addressing standards that they adopt, as well as on the basis of their semantic power. Despite the heterogeneity of the various schemes, the projects' solutions feature several commonalities (e.g., the use of naming standards such as URIs/URNs), and reveal certain trends (e.g., the use of semantic web approaches for IoT resource discovery). The document ends-up recommending areas for further research and investigation. At the same time, it briefly outlines the Activity Chain's roadmap towards the elicitation and documentation of best practices associated with the deployment and use of the IoT naming, addressing and discovery solutions.

Table of Contents

Table of Tables

Table of Figures

Abbreviations

AC	Activity Chain
AIDC	Automatic Identification and Data Capture
ARM	Architecture Reference Model
CoAP	Constrained Application Protocol
CVO	Composite Virtual Object
DHT	Distributed Hash Table
DNS	Domain Name Service
DOI	Digital Object Identifier
ebbits	Business Based Internet-of-Things and Services
EDIFICE	Electronic Data Exchange Forum for Companies with interest in Computing and Electronics
EDMA	European Diagnostics Manufacturing Association
EFPIA	European Federation of Pharmaceutical Industries Association
EHIBCC	European Health Industry Business Communications Council
EIB	European Installation Bus
ENS	Event Notification Service
EPC	Electronic Product Code
EPCIS	Electronic Product Code Information Sharing
EUCOMED	European Confederation of Medical Devices Association
GSN	Global Sensor Networks
IATA	International Air Transport Association
ICO	Internet Connected Object
iCORE	Empowering IoT through Cognitive Technologies
IEEE	Institute of Electrical and Electronic Engineers
IERC	European Research Cluster on the Internet of Things
IETF	Internet Engineering Task Force
IoPTS	Internet of People, Things and Services
IoS	Internet-of-Services
IoT	Internet-of-Things
IOT-A	Internet of Things – Architecture
IOT6	Universal Integration of the Internet of Things through an IPv6-based Service Oriented Architecture enabling heterogeneous components interoperability
IPv6	Internet Protocol version 6
ITS	Intelligent Transportation Systems
KPIs	Key Performance Indicators
LOD	Linked Open Data
mDNS	Multicast DNS
NFC	Near-Field Communications
OCLC	Online Computer Library Center
Odette	Organisation for Data Exchange by tele-transmission in Europe
OGC	Open Geospatial Consortium
ONS	Object Naming Service

OpenIoT	Open Source blueprint for large scale self-organizing cloud environments for IoT applications
OSS	Open Source Software
OWL	Ontology Web Language
P2P	Peer-to-Peer
QoS	Quality-of-Service
RDF	Resource Description Framework
REST	Representational State Transfer
RFID	Radio Frequency Identification
SaaS	Software-as-a-Service
SCE	Service Creation Environment
SGTIN	Serialized Global Trade Item Number
SIR	Sensor Instance Registry
SLP	Service Location Protocol
SmartAgriFood	Smart Food and Agribusiness
SOR	Sensor Observable Registry
SPARQL	Simple Protocol and RDF (Resource Description Framework) Query Language
SSN	Semantic Sensor Networks
STIS	Smart Things Information Services
SWE	Sensor Web Enablement
UPU	Universal Postal Unit
URI	Universal Resource Identifier
UUID	Universally Unique IDentifier
VO	Virtual Object
WSDL	Web Services Description Language
WSN	Wireless Sensor Networks

Executive Summary

The present document is the first deliverable of the second Activity Chain (AC2) of the European Research Cluster on the Internet of Things (IERC). IERC AC2 focuses on naming, addressing and discovery technologies for Internet Connected Objects (ICO), with the ultimate goal of introducing a reference addressing and discovery scheme for IoT applications, along with a set of best practices for adopting existing addressing and discovery solutions in practical IoT applications. The purpose of the present deliverable is to provide a catalogue of the naming, addressing and discovery schemes which are used by the IERC projects that contribute to (AC2). This catalogue provides a taxonomy of the various schemes, through identifying the commonalities and differences of the solutions used by the contributing projects. The understanding of the different options is a first step to a bottom up process of specifying a reference mechanism for addressing and discovery, which could complement the IoT Architecture Reference Model (ARM) specified by the IOT-A project in the scope of the first activity chain (AC1) of the IERC.

A total of eleven IERC/IoT projects have contributed to this deliverable, including ebbits, GAMBAS, iCore, IOT-A, BUTLER, IoT.est, IOT6, IoT@Work, OpenIoT, SmartAgriFood, CEN TC 225. These projects have different research goals and address a wide range of different IoT applications. Due to their different research agendas, they also feature differences in terms of the naming, addressing and discovery schemes that they implement. In particular:

- ebbits exposes physical devices, sub-systems and cloud services as services or a composition of services. In this way, virtual devices/sub-systems could be created with no direct link to any specific physical resource. Virtualization has been realized by specifying a semantic-free addressing layer based on unique identifiers. The project exploits semantic techniques and attribute-based service descriptions to provide discovery features.
- GAMBAS uses URIs to identify both data and devices according to the Linked Data paradigm, while it lists URIs (along with semantic information) to a directory in order to enable discovery of resources. Discovery relies on semantic technologies, as well as a distributed query processing framework.
- iCore is currently implementing a DHT (Distributed Hash Table) structure as a means to realizing a flat naming space (semantics based), along with fast access to relevant ICOs (based on semantic search using the SPARQL language). To this end, the project makes also use of the Smart M3 approach (http://smart-m3.sourceforge.net/), yet the iCore architecture allows for multiple implementation options.
- IOT-A is prescribing the IERC (general) reference architecture and therefore focuses on providing support for multiple naming, addressing and discovery schemes rather than introducing a single solution. Hence, IoT-A prescribes and promotes the use of existing naming (e.g., URIs) and addressing solutions (e.g., IPv4/IPv6). It also proposes three different schemes for resource discovery including geo-

location based discovery, semantic web based discovery and a federating approach to resource discovery. The latter is based on a federating architecture and hierarchical clustering.

- BUTLER is following and adopting IOT-A's work on naming, addressing and discovery. Hence, it uses URIs and IP addresses, while opting for the geo-location discovery approach to IoT resource discovery.
- IoT6 (as its name indicates) is focused on the investigation and use of IPv6 technologies for IoT. Hence, it adopts IPv6 addresses for addressing and DNS techniques for naming. Furthermore, it uses DNS-SD (Service Directories) and mDNS (Multicast) for resource discovery. However, it also acknowledges the merit of semantic techniques and will attempt to deploy them as well.
- IoT.est focuses on the testing of IoT solutions. The project uses common URIs to uniquely identify objects that may be used in the service creation. In terms of addressing and discovery it uses a Service Registry and Search interfaces which are accordingly used by other components of the IoT.est testing environment.
- OpenIoT promotes semantic approaches to naming, addressing and discovery. The project's solution is based on the creation of a distributed directory service which will include semantically annotated resources. The latter will be addressed on the basis of URIs and will be searched (as part of the discovery process) using the SPARQL language.
- IoT@Work is focused on manufacturing solutions and hence has developed an entity manager that can handle with hierarchies of entities/resources relevant to manufacturing applications. At the same time, the project supports event-driven access to resources, along with semantic web technologies for discovering IoT resources.
- SmartAgriFood uses unique URLs and URNs for addressing shared resources such as EPCs (as available on products, packaging material, etc.). It also relies on the ONS protocol and techniques for resolving URNs and EPCs. Furthermore, the project exploits a semantic approach (based on SPARQL and the principles of Linked Data) for the discovery of resources.
- CEN TC 225 is focused on AutoID solutions focusing on the exploitation of existing legacy naming and addressing schemes (IPv6, DNS/ONS, URNs, DOI). At the same time the project pays emphasis in the provision of support for a long term migration from the legacy applications.

A more detailed presentation of the above schemes can be found in following sections of this document. Despite the heterogeneity of the various schemes, the projects' solutions feature several commonalities (e.g., the use of naming standards such as URIs/URNs), and reveal certain trends (e.g., the use of semantic web approaches for IoT resource discovery). These commonalities and trends are presented as part of the taxonomy attempted in the deliverable. Following the taxonomy and based on the above trends, the deliverable identifies a number of issues and functionalities that should be explored in the next stages of the AC2 work. As part of these next steps, the deliverable ends-up with a questionnaire for soliciting inputs on key naming, addressing and

discovery requirements from other projects, beyond the list of 11 projects contributing to this deliverable. This questionnaire is included as an Appendix to this document.

1. Introduction

1.1 Document Purpose and Scope

The second Activity Chain (AC2) of the European Research Cluster on the Internet of Things (IERC) focuses on naming, addressing, search and discovery mechanisms for IoT. Among the main objectives of AC2 is to create a catalogue of naming, addressing and discovery schemes, which can be deployed in the scope of large scale open loop applications. The AC2 will also explore best practices associated with the deployment of naming, addressing and discovery in non-trivial IoT applications. Furthermore, it will investigate the possibility of integrating and/or federating multiple addressing schemes towards a scalable unified solution that could be deployed regardless of underlying technology and application domain. The activity chain is currently supported by eleven FP7 projects (ebbits, GAMBAS, iCore, IOT-A, BUTLER, IoT.est, IOT6, IoT@Work, OpenIoT, SmartAgriFood, CEN TC 225).

The present document is the first deliverable of the IERC AC2. It aims at describing the different naming, addressing and discovery schemes developed and used by the contributing IERC projects, while at the same time providing insights on their functionalities, added-value and potential applications. The description of the naming and addressing mechanisms of each project covers issues associated with the scalability of the solution, as well as insights on the effort for migrating to these solution (from legacy systems and solutions). Note that migration and scalability are two issues that receive special attention within the IERC and EU's IoT Expert Group, but also within the global IoT community as a whole.

The purpose of the documentation of the project's solution is to identify commonalities and potential synergies, which could later use to resource pooling, joint works, as well as the elicitation of best practices based on the experiences of the various projects (and their related IoT deployments). As a first step to this direction, the present deliverable attempts to classify the various efforts on the basis of the intelligence and semantic power of the corresponding naming/discovery schemes. This taxonomy is a first step towards identifying synergies and eliciting best practices. The identification and documentation of best practices will be the subject of future deliverables of IERC AC2.

1.2 Target Audience

The target audience for the present document includes:

- **Projects participating in the IERC and their members**: FP7 projects on IoT could greatly benefit from the adoption of effective naming and discovery schemes. The present document illustrates several naming and discovery schemes used and/or researched by other projects, which they could take into account in the scope of their research and development tasks.

- **EC IoT stakeholders:** The naming and addressing solutions of the IERC projects, along with their consolidation are of interest to other groups in the EU working on IoT technologies and policies, such as the IoT Expert Group.
- **Researcher and Engineers working on IoT:** Researchers and engineers implementing IoT solutions will be interested in the contents of the deliverable, in order to understand alternative ways of implementing naming and addressing in the scope of their IoT solutions.

1.3 Document Structure

The document is structured as follows: Section 2 provides a short introduction to the goals of the activity chain, including a short roadmap and milestones towards achieving these goals. Section 3 is devoted to the documentation of the naming, addressing and discovery schemes that are researched, deployed and used by the contributing projects. Section 4 attempts a categorization of the presented naming and addressing schemes on the basis of the intelligence and semantic capabilities offered by the presented schemes. Section 5 highlights the main issues and gaps associated with the presented schemes and identifies areas for further research and contributions. Finally Section 6 concludes the document.

2. Overview of IERC AC02 «Naming, addressing, search and discovery»

2.1 Scope of the Activity Chain and Target Outcomes

The scope of the second activity chain of the IERC (AC02) covers naming and addressing schemes for IoT, as well as search and discovery mechanisms for resolving ICO (Internet-Connected Objects) and discovering their capabilities. The activity chain will produce best practices and guidelines for using existing and emerging addressing and discovery schemes for IoT applications, while paying emphasis to the following aspects:

- The need to ensure smooth migration of legacy applications (such as AutoID and WSN applications) to the proposed/introduced IoT addressing and discovery schemes.
- The required scalability of the schemes, as a result of the need to address highly distributed and massively scalable IoT applications.

As part of the activity chain several addressing and naming schemes will be explored on the basis of relevant activities of the participating projects. However, IERC AC02 will also endeavour to introduce a reference scheme for naming and addressing, which could be applicable to a range of different IoT applications. This reference scheme could serve as a general meta-scheme that could be customized for different domains and applications. The generality and the level of implementation detail of this reference scheme will be explored during the evolution of the activity chain.

2.2 Methodology

In order to achieve its objectives, the activity chain will work on the basis of the following steps:

- The creation of a catalogue of naming, addressing and discovery schemes used in IERC project. This catalogue will provide a list of candidate solutions, while also facilitating the identification of the relative strengths and weaknesses of the various schemes.
- The elaboration of different best practices associated with the adoption and use of the various schemes in different applications. The best practices should address different aspects including functionality, implementation/deployment flexibility, scalability, ease of migration, technological longevity and more.
- The development of a reference naming, addressing and discovery scheme, which will provide a framework for development and customizing addressing / discovery solutions for IoT applications. Special emphasis will be paid in the interoperability and federation of heterogeneous IoT solutions, towards unified integrated and global naming, addressing and discovery services for IoT resources.

The present deliverable serves the first of the above steps, and will be used as input to the second and third steps outlined above.

2.3 Relevant Standards

This deliverable presents the main naming, addressing and discovery schemes that are used by the IERC projects that participate and contribute to AC02. In most cases these projects adopt and rely on existing or emerging standards for their ICO addressing and discovery needs. Therefore, the following standards are very relevant to the schemes presented in this deliverable:

- The **Object Naming Service (ONS) introduced by EPCglobal**, which describes a Domain Name System used to locate authoritative metadata and services associated with the SGTIN (Serialised Global Trade Item Number) portion of a given Electronic Product Code™ (EPC). ONS is used by projects and applications that are based on RFID/AutoID technologies. In addition to ONS, familiarity with EPC and the EPCglobal architecture and standards is a key to understanding several of the approaches adopted by the various projects.
- **The IPv6 (Internet Protocol version 6)**, the latest revision of the Internet Protocol (IP) which is developed by the Internet Engineering Task Force (IETF). IPv6 uses 128-bit for addressing thereby leading to a virtually unlimited number of addresses, which can accommodate the addressing needs of IoT applications and services.
- Standards introduced by **Sensor Web Enablement (SWE)**, notably in relation to the [Jirka09], [Bröring11]:
    - **Sensor Instance Registry (SIR)** for harvesting, managing and transforming sensor metadata and
    - **Sensor Observable Registry (SOR)** for managing the semantics of the phenomena observed by sensors.
- Proposed standards introduced by the **W3C Semantic Sensor Network Incubator Group**. These include [Taylor2011]:
    - A standard ontology used to describe sensors and sensor networks for use in sensor network and sensor web applications.
    - Standard methods for using the ontology to semantically enable applications developed according to available standards such as the Open Geospatial Consortium's (OGC™) and the Sensor Web Enablement (SWE) standards.
- **W3C ontologies and the Resource Description Framework (RDF)**, as a framework for describing resources and their relationships (as required in several IoT applications).

As a result, familiarity with these standards and mechanisms can greatly facilitate the understanding of the schemes presented in this document.

2.4 Interaction with other Activity Chains

The IERC targets the development of a pan-European approach to the development of IoT solutions. The various activity chains are expected to provide several key building blocks of this approach and therefore deal with thematic aspects of IoT architectures and solutions. As a result, activity chains are expected to interact with each other in order to ensure that their developments are complementary, compatible and in-line with

the overall goals of the IERC. In this context, AC02 will be interacting closely with the following activity chains:

- The IERC AC01 on «Architecture Approaches and Models», which focuses on the specification of an Architecture Reference Model (ARM) for Internet-of-Things applications. The reference schemes to be produced in AC02 should be compatible to the ARM introduced by the IoT-A project in AC01.
- The IERC AC04 on «Service openness and interoperability issues / semantic interoperability», which explores interoperability issues between IoT services and applications. Interoperability is closely related to addressing and discovery, given that interoperable IoT naming, addressing and discovery schemes is a prerequisite for the development of large scale solutions.

Interactions with other activity chains may also be identified during the evolution of the AC02 work.

3. Catalogue of Naming, Addressing and Discovery Schemes in IERC Projects

3.1 ebbits (http://www.ebbits-project.eu)

3.1.1 Project Overview

Enabling business-based Internet of Things and Services – ebbits is a four years Integrated Project funded by the European Commission within the 7th Framework Programme in the area of Internet of Things and Enterprise environments. ebbits started in September 2010 and will end in August 2014.

The ebbits project aims to develop architecture, technologies and processes, which allow businesses to semantically integrate the Internet of Things into mainstream enterprise systems and support interoperable real-world, online end-to-end business applications. More specifically, the ebbits platform is based on a Service-oriented Architecture and intends to support interoperable business applications with context-aware processing of data separated in time and space, information and real-world events, people and workflows, optimisation using high-level business rules, end-to-end business processes or comprehensive consumer demands. This results into the actual convergence of the Internet of People (IoP), the Internet of Things (IoT) and the Internet of Services (IoS) into the "Internet of People, Things and Services (IoPTS)" for business purposes.
ebbits is fostering major innovations within the following areas:

- Physical World Sensors and Networks – supporting semantic interoperability among heterogeneous physical world technologies and enterprise systems and defining P2P-based scalable network architecture featuring opportunistic communication paradigms;
- Data and Event Management – providing a Layered P2P Event Management Architecture capable of handling of physical, network, application and business events and supporting rule-based service orchestration;
- Centralised and Distributed Intelligence – defining standardised frameworks for fusing sensor data and integrating in business process and adopting ontology-based context models to promote self-awareness approaches;
- Semantic Knowledge Infrastructure – supporting hybrid querying and real-time reasoning also connecting many conventional data sources to semantic models;
- Frameworks for Business Process Life Cycle Management – taxonomy, metrics and solutions for production optimisation and food traceability.

The resulting platform is being demonstrated in end-to-end business applications featuring connectivity to and online monitoring of a product during its entire lifecycle. The project will develop, implement and demonstrate two ebbits IoPTS applications, one demonstrating real-time optimisation metrics, including energy savings, in manufacturing

processes, the other demonstrating online traceability with enhanced information on food.

3.1.2 Naming, Addressing and Discovery Solutions

ebbits IoPTS applications deal with a potentially huge amount of real word "resources" including any kind of smart objects, hardware devices, sensors, actuators, processing components, sub-systems, people and places but also with digital world "resources" which represent the real world ones and are able to expose their relevant basic or composed capabilities. All these resources need to have common naming and addressing schemes as well as lookup and discovery services to enable global reference and access to them.

3.1.2.1 Naming and addressing

In ebbits, physical devices, sub-systems and cloud services are all viewed as a service or a composition of services. In this way, virtual devices/sub-systems could be created with no direct link to any specific physical resource. For this kind of resources, strict privacy and security requirements have been identified also influencing their naming, addressing and as well as discovery mechanisms.

Entities

ebbits introduces the concept of entities as static resources which need to be monitored throughout their whole lifecycle. For instance, as far as the food traceability scenario is concerned, cattle could be considered as entities, starting from the farm to the slaughterhouse and ending up at a restaurant. As the aim is to be able to link data from different systems to the same "resource", this needs to have static EntityID during the relevant complete lifecycle. Although these issues do not completely refer to the naming and addressing definition, there are some direct links.

In the IoPTS vision, business boundaries fade. In fact, every business process involves different proprietary sub-systems, which are certainly not going to be replaced in the near future. In order to interact with such existing sub-systems, an additional decoupling layer is required to connect the relevant capabilities and offer composed services.

In such a scenario, the key task of ebbits entity management is to uniquely and in persistent way identify the resources, store this information together with basic set of resource attributes and support the lookup operations. Of course the compatibility with specific identification schemes adopted within the business process should be preserved, so that such IDs are member of the basic set of attributes related to the entity's identity. Accordingly, in ebbits, the identity of a given entity is defined by an EntityID that can be seen as a compound consisting of the following parts:

- UUID – it is generated automatically when an entity is registered in ebbits system (e.g. urn:ebbits:id:0123456789abcdef);
- Local ID – it identifies the entity in the local domain of the resource provider (e.g. herd number (CHR):animal ID);

- List of aliases – it represents the list of Local IDs that identifies the same entity;
- List of resources according to Relation Type X – it is the list of Entity IDs (UUIDs) that identify resources which are in the X relation (e.g. part-of property) with the original (identified) resource.

The Entity Manager (refer to the figure below) is the element implementing the entity management functionalities within the overall ebbits architecture and is composed of the following parts:

- Resource Directory - responsible for creating unique UUID as part of ebbits ID and registering newly created EntityIDs in the local database of the Entity Manager.
- Mapping&Relation Service - maintaining the alias relations between ebbits unique identity and different local IDs, as well as different relations between ebbits identities (e.g. part-of).
- Lookup Service – responsible for the communication infrastructure of Entity Managers according to the peer-to-peer architecture and offering ebbits-wide Lookup service.

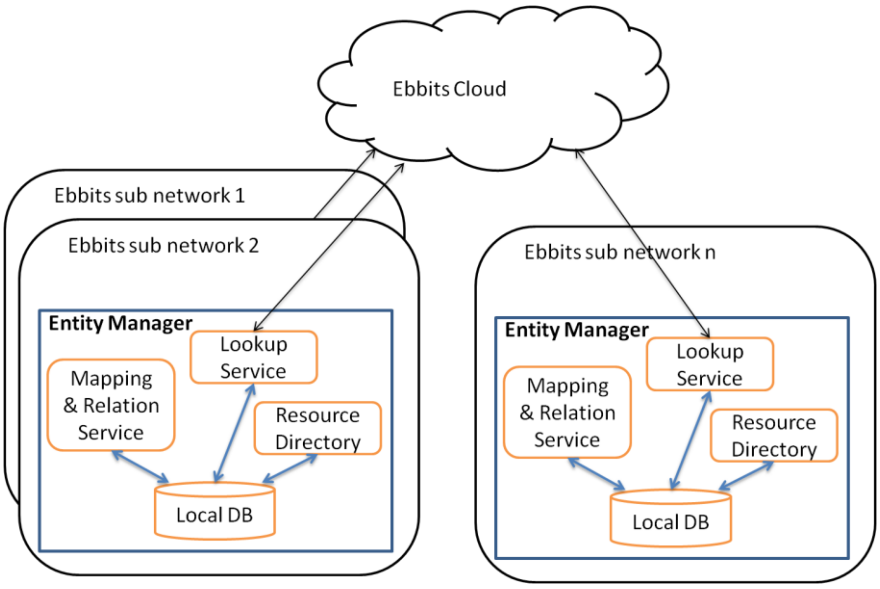

Figure 1: Architecture of ebbits Entity Manager

Virtualization

As smart objects and sub-systems providing any kind of service in an IoPTS architecture, which may be linked to some human, the identity of objects and sub-systems has to be protected in the same way as would be that of a human. This mainly influences privacy requirements, e.g. position tracking or accounting. In order to cope with such kind of issues, ebbits builds on virtualization.

This notion of virtualization targets not only at abstractions of physical devices and sub-systems (thus defining virtual resources) but also at decoupling the mechanisms supporting addressing and identification, thereby introducing services which refer to addressable entities whose actual identity cannot be assigned to their addresses by default. For example, different devices could be combined into a logical representation

that exposes the functionalities offered by the physical objects but appears in ebbits as one service.

Virtualization has been realized within the ebbits middleware by applying the concept of a semantic-free addressing layer that uses HIDs to address services. As HIDs neither do provide any information about the resources they represent nor can be assumed to be persistent, they allow addressing entities without tracking them – thereby enabling the creation of "virtual" devices/entities exposed as services.

More specifically, an HID is a number of 4 blocks of 32 bit each. The first 3 blocks are used for context information and the last block is used for networking. In fact, HIDs serve only the purpose of addressing but are not adopted as identifiers needed to recognize known entities. This is intended as a clear separation of addressing and identification and helps to overcome privacy problems which occur from the usage of static addresses.

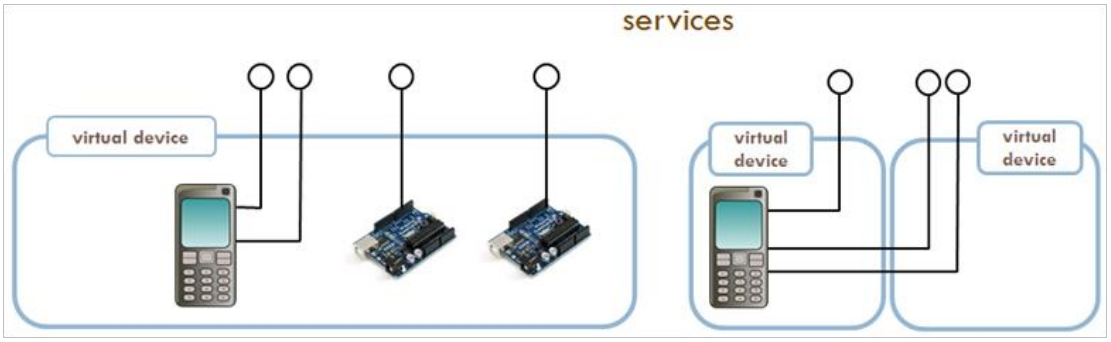

Figure 2: Virtualization of devices

3.1.2.2 Discovery

There are two types of discovery features available in ebbits, namely semantic discovery, mainly for local entity resolution, and attribute-based discovery for global resolution.

Semantic discovery capabilities offered within ebbits basically leverage on semantic descriptions of entities and services. To this aim a specific OWL-Lite-based ontology has been derived to support the modelling of device services, device capabilities (e.g., hardware properties, software description, security properties and energy profiles), discovery features provided by low-level communication protocols (e.g., Bluetooth, ZigBee, UPnP), groups of devices logically aggregated to provide more advanced application level functionalities, quality of service aspects and applications. Such ontology representation is used in runtime for device discovery, searching for specific services or devices and for retrieving all information required for the service calls by using simple SPARQL queries. Advanced searching features are then supported: the execution of query retrieves the more matching candidates, which could be further investigated by heuristically comparing possible additional information.

Instead global discovery leverages on an attributes-based description of services. As mentioned, global service discovery should take privacy-

related aspects into account as it may be exploited for tracking or accounting. In attribute-based discovery, a query containing a set of attributes names and corresponding values is broadcasted in the network. The security requirement is that only the party holding the searched attributes understands the message and can then answer it. In this way even if an adversary sees the query and the answer, it is still computationally hard to decide what the searched attributes were and what attributes the answering entity has. In the proposed solution, Bloom-filters are used for the queries as they do not reveal the original query values. They also provide the possibility to freely choose the set and order of attributes to include into a query. Even if the queried entity does not have some of the attributes requested, he can still check whether he fits the rest of the attributes and can respond to the request.

3.1.3 Migration Solution

ebbits also takes into account the need for migration from legacy solutions. In general, ebbits builds on existing sub-systems and solutions and rather adds a decoupling layer instead of replacing specific components. This concept is actually reflected into the definition of the overall ebbits architecture. Then, particular components specifically implement the presented concept:

- Entity Manager – it handles the identification of entities within ebbits while supporting existing identification schemes e.g., the one based on Electronic Product Code and defined within EPCGlobal;
- ebbits Gateway – this component enables the integration of heterogeneous technologies and sub-systems into the ebbits environment;
- Enterprise Hub – it allows the integration of existing business systems into ebbits framework.

3.1.4 Scalability

As already mentioned ebbits framework is being designed to operate in an IoPTS environment where a potentially huge number of real world resources could be interconnected and interact with each other through the Internet. To deal with scalability aspects, a kind of hierarchy has been introduced in the overall framework. More specifically, the way hierarchy is supported within the ebbits middleware is through the usage of contexts. In fact, HIDs can be used to define different levels of context and to elect an ebbits component in charge of managing all the operations related to a specific level. In this way, ebbits sub-networks can be created.

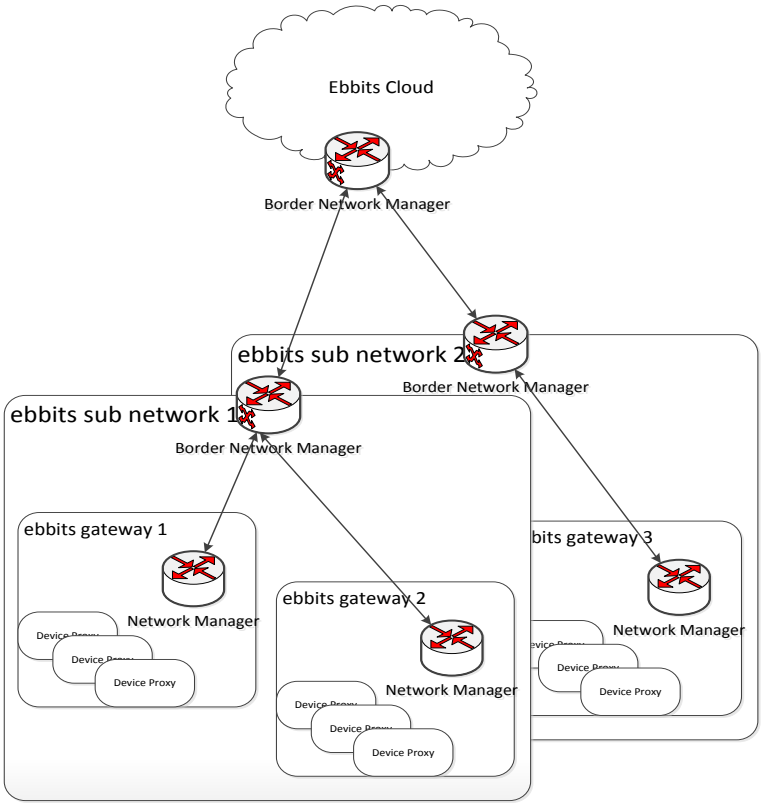

Figure 3: Example of deployed ebbits network

The actual physical deployment of the ebbits network configuration reported in the figure above could then represent e.g., different manufacturing sites each with their own ebbits gateways managing different objects and sub-systems. Routing among different sub-networks is provided by the Border Network Managers.

The proposed approach supports better performance and more flexible security management.

3.1.5 Indicative Applications

The ebbits framework is being validated in two major application scenarios: manufacturing and food traceability.

As far as the manufacturing process is concerned, the main idea is to have access to the different types of devices including e.g., robots, PLC, rolls, elevators, present in the different production stations composing a production line. Note that a more fine-grained access to information coming from the shop floor allows for a better understanding of production efficiency, with a major focus on energy aspects.

Concerning food traceability, the possible applications relate to the accessibility of the information about a specific product throughout its lifecycle from the farm to the fork. Two representative example scenario

sub-sets are reported in the following:

- A costumer is buying some meat in a shop and wants to use his personal devices to access all the information available about the meat, such as which farm it comes from, when it was slaughtered etc.
- A customer has a smart fridge in his home able to monitor which pieces of meat are present. The fridge could display which meat would need to be consumed e.g., because the best before date is coming close. In addition, the same fridge could be notified that the retailer would need to recall a specific batch of meat e.g., because of issues in storage operations. The final customer could then receive a proper warning.

3.2 GAMBAS (http://www.gambas-ict.eu)

3.2.1 Project Overview

The overall objective of the GAMBAS project is the development of an innovative and adaptive middleware to enable the privacy-preserving and automated utilization of behaviour-driven services that adapt autonomously to the context of users.

This middleware will contain a flexible context recognition framework that is able to capture the context of users (e.g. location, activity, plans, intents), a suite of security protocols to enforce the user's privacy when sharing context information as well as a recommendation system to largely automate the selection of relevant services available to the user.

At the core of the middleware there will be an interoperable data model to represent context information and a scalable data processing infrastructure to query and aggregate context information and to integrate context into services. Moreover, a discovery mechanism will be in place to find relevant data sources to fulfil the user's requests.

In following section we present the model that is used to represent and access the data, while also making the data discoverable.

3.2.2 Naming, Addressing and Discovery Solutions

To achieve data interoperability, GAMBAS will develop a unified representation of the heterogeneous data and their data sources, following the Linked Open Data principles. The unified view will consist of basic vocabularies and ontologies that will cover all aspects of generated data and Internet Connected Objects (ICOs). The goal is to have the ICOs themselves store their generated data locally in the form of Linked Data, by using the vocabularies and ontologies developed. We will extend existing ontologies like the W3C SSN (Semantic Sensors Networks) ontology to describe the data and the objects.

In the GAMBAS project special care will be taken to provide complete, yet compact data descriptions that are suitable for resource constrained devices. Moreover, our middleware focuses on service recommendation based on user's immediate context, which requires dealing with streams of data. For that matter our data representation will allow the representation of dynamic and temporal data aspects.

Data discovery will be enabled by means of exchanging the descriptions of the data and of the data sources. The GAMBAS middleware will contain a discovery service where devices can publish their semantic descriptions, as well as additional privacy information. Each device can control how much information is published in the discovery directory. This allows devices to find relevant data, without knowing a priori the data's particular location. Our distributed query processing framework uses the discovery directory to retrieve a list of relevant data sources for a particular query. It then sends the query requests to those selected sources, and retrieves the results. We use the SPARQL query language to query both the discovery directory and the data sources.

In summary, the naming, addressing and discovery solution of the GAMBAS project are handled as follows:

- **Naming**: URIs to identify both data and devices, following the Linked Data paradigm.
- **Addressing**: Each data source is assigned a unique URI. For discovery, these URIs will be listed in a discovery directory, together with semantic descriptions of the data and data source.
- **Discovery**: A discovery service will allow objects to publish their semantic descriptions, as well as additional privacy information. Our distributed query processing framework uses the discovery directory to retrieve a list of relevant data sources to a particular query. This allows devices to find relevant data, without knowing a priori the data's particular location.

3.2.3 Migration Solution

By following the Linked Data principles, the data and objects described in GAMBAS can be easily integrated with other Linked Data collections. Further devices that wish to connect to the GAMBAS middleware will require semantic descriptions. The GAMBAS data acquisition framework together with the GAMBAS ontology can be reused or extended in this case.

Devices will be equipped with a query processor that uses both SPARQL and a SPARQL extension to handle continuous queries over stream data. The processor will be accessible to other devices in the middleware via RESTful SPARQL endpoint interfaces.

3.2.4 Scalability

To enable scalability the GAMBAS framework will develop Linked Data storage and query processing capabilities for ICOs. This will also improve privacy, since each ICO will be responsible for storing its own data. It can therefore decide which data is disclosed to which ICOs. We will build a data storage framework based on state-of-the-art approaches that will also comply with limitations imposed in terms of memory, processing power, battery life, etc. A query processing framework will also be developed following the same guidelines. Even though the query processing capability at each device will be limited, distributed query processing techniques will be explored to offer a more powerful processing framework among the ICOs.

3.2.5 Indicative Applications

The GAMBAS naming and addressing solution will be applied to the public transport domain.

Current transport infrastructures are saturated due to the growing number of vehicles over the last decades. This leads to increased traffic congestion, accidents, delays and larger pollution emissions.

All these challenges have led to huge research efforts in the area of Intelligent Transportation Systems (ITS). ITS applies advanced communication, information and electronics technology to solve transport problems. The purpose of ITS is to take advantage of the appropriate technologies to create "more intelligent" roads, vehicles, public transport systems and also "users".

Travelling people nowadays often carry personal smart devices like mobile phones with them. These devices are equipped with various sensors and store information about their user's intentions/future plans - e.g. in a calendar, task list, etc. Therefore, they have become a very interesting source of information for urban mobility management, and in particular for public transport operations. In the GAMBAS project we integrate data from citizens with the data from public transport provider to not only improve the operations of a public transport network and in general urban mobility, but also to improve citizens' quality of life, enabling a better organization of their time according to the interpretation of human intentions.

3.3 iCore (http://www.iot-icore.eu)

3.3.1 Project Overview

iCore (Internet Connected Object for Reconfigurable Ecosystems) is an FP7 Objective 1.3 Integrated Project started in October 2011. The project will run for 36 months until September 2014.

iCore's aim is to provide the foundations, architecture and functionality for a cognitive management paradigm for the IoT. A cognitive system has the ability to dynamically select its behaviour (managed system's configuration), through self-management/awareness functionality, taking into account information and knowledge (obtained through machine learning) on the context of operation (e.g., internal status and status of environment), as well as policies (designating objectives, constraints, rules, etc.). In the light of the above, cognitive technologies constitute a unique and efficient approach for addressing the technological heterogeneity and obtaining context awareness, reliability and energy efficiency. Cognitive technologies have been applied to the management of diverse heterogeneous technologies (e.g., wireless access, backhaul/core segments). iCore will apply this successful paradigm for solving problems that are particular to the Internet of Things.

Therefore, new IoT-oriented cognitive functionality will be provided, which will be part of the service layer of the Future Internet.

3.3.2 Naming, Addressing and Discovery Solutions

The "7 trillion devices for 7 billion people" paradigm yields that the handling of the amount of objects that will be part of the IoT requires suitable architecture and technological foundations. The Internet-connected sensors, actuators and other types of smart devices and objects need a suitable communication infrastructure. While other projects have set out to define architectures or reference models to ensure interactions and facilitate information exchange, as well as test facilities (such as Smart Santander), there is a significant lack in terms of management functionality and means to overcome the technological heterogeneity of the capillary networks. This is essential for the IoT, in order to enhance context awareness (by being able to exploit more objects), and also render high reliability (through the ability to use heterogeneous objects in a complementary manner for reliable service provision), energy efficiency (through the selection of the most efficient and suitable objects from the set of heterogeneous ones, and, in general, through the optimal management of a large population of resource constrained devices) and security in these distributed networks of cooperating objects. The sheer numbers of objects and devices that have to be handled and the variety of networking and communication technologies, as well as administrative boundaries that have to be supported do require a different management approach.

iCORE builds his own concepts on top of three fundamental "bricks": Virtual Objects (VO) as one-to-one virtualization of real world things allowing service like access (in line with current IoT standardization efforts in the space of RESTful services) ,Composite Virtual Objects (CVO) – mesh aggregations of Virtual Objects realized by the cognition based iCORE factory in order to deliver coherent service response to outer world of a certain iCORE instance (identified as user space where most of the users are applications and services), and Services (as a level capable to map outer world demands and sensed evolution in service demands).

Both VO and CVO concepts ask for a combination of semantics with object oriented approaches, allowing the existence of template-ing mechanism, instances, activation/de-activation of services. All those actions are supported by registries at both VO and CVO level allowing meaningful exploration of search space.

As per current perspective an appropriate structure covering needs is based on DHT (Distributed Hash Table) in order to insure a flat naming space (semantics based) and fast access to relevant VO's (SPARQL searches).

As a base of work stays also Smart M3 approach (http://smart-m3.sourceforge.net/) but the architecture allows multiple implementation options.

3.3.3 Migration Solution

iCORE builds the grounding of architecture on IoT-A core values and architectures. Therefore, cognitive stack delivered will follow IoT-A adding side capabilities where the cognition may boost service demands matching, cooperative use or resources and services, and smart capabilities (both inner world on optimization space, and outer world on advanced interaction due to specific capabilities like stream processing).

3.3.4 Scalability

The VO addressing capabilities (available as API in "ICORE kernel") offers the mechanisms to the VO fabric and CVO level to discover and access the VOs that are in the proximity of an iCore instance, where the proximity concept is expressed by the Service Logic Level.

The VO level addressing and naming scheme must ensure high availability of the data. This principle is achieved if the user data request are answered quickly and reliable using a route by name protocol. The routing protocol must find the shortest path to the VO and in the same time it should avoid failed or overloaded servers. Another issue that VO addressing should solve is the trustworthiness. In other words the VO clients (mainly the CVOs) need the certainty that they get information from a reliable source.

The infrastructure of the iCore system is not static and long-lived, such as classical enterprise systems because the services offered by the VOs constantly degrade, vanish or even re-appear. This dynamic characteristic of the system implies the need for immediate and automated discovery of VOs and services offered by VOs as well as their dynamic management.
The crucial challenge of the VO level (more precisely VO fabric) is to find the VO (VOs) that offer the adequate services for solving a particular task required by a CVO.

As per current state of research an iCORE instance might easily scale in terms of both data volume and involved services per instance. Due to on-

going convergence between IoT and Cloud Computing the future seems belong to a combination between naming expressiveness based on semantic technologies and elastic capabilities of Cloud based solutions.

3.3.5 Indicative Applications

One of the most relevant family of use cases is Logistics, due to the fact that large business value chains asks for logistic solutions, with specific constraints in terms of space, conditions, combinations of goods per warehouse space and freight. iCore is addressing one such a use case highlighting the realization of cognition by specific technological meanings (e.g. Complex Event Processing in combination with Machine Learning).

iCore considers the involvement of different actors for example along the chain of provisioning with fresh products of retail businesses or sensitive pharma products.

iCore technology allows all stakeholders to gain information that can optimize their business processes, like resource planning and stock management:

- The multi-modal sensors are combined into VO's/CVO's presenting the status and quality of the products, taking into account the environmental conditions around the products.
- It reuses VO's/CVO's representing the products to find out the storage requirements and compartments in transport vehicles or warehouses are autonomously adapted to e.g. the optimal temperature conditions.
- A food retailer manages its fresh food stock (e.g. strawberries) based upon the remaining shelf-lifetime of products. This information is retrieved by using sensors added to the perishable foods.

The iCore technology allows "management by exception", without knowledge of the products optimal storage conditions:

- During transportation, hazardous goods must be treated differently and the CVO of the total plane/truck load will warn if goods are present that are reactive when stored together.
- Upon arrival of the equipment, the hospital uses product status information represented by CVOs to decide whether or not to accept the equipment.

3.4 IoT-A (http://www.iot-a.eu/)

3.4.1 Project Overview

The project acronym "IoT-A" stands for "Internet of Things - Architecture". IoT-A is a 3 year Integrated Project that is part of the FP7 ICT European Research Program in the area of Internet of Things. It started in September 2010 and will end in August 2013.

IoT-A proposes the creation of an Architectural Reference Model (ARM) together with the definition of an initial set of key building blocks.

Together they are envisioned as crucial foundations for fostering a future Internet of Things. Using an experimental paradigm, IoT-A will combine top-down reasoning about architectural principles and design guidelines with simulation and prototyping to explore the technical consequences of architectural design choices.

The IoT-A ARM consists of a Reference Model, a Reference Architecture and Best Practice. The Reference Architecture explains the core aspects of the IoT domain that do not change and are independent of concrete technologies. The Reference Architecture identifies the key aspects, functionalities and design choices an architect developing an IoT system architecture faces. The Best Practice recommendations are there for helping such an architect in developing a concrete IoT architecture by showing what design choices to make depending on given requirements and constraints. Overall, the goal is to give a framework to discuss and design interoperable IoT systems. Using the common reference, the critical interaction points can be identified early in the design process and available design choices can be evaluated taking into account the recommendations in the Best Practice part.

As IoT-A is looking at an Architectural Reference Model, it identifies the high-level architectural aspects, also with respect to naming, addressing and discovery, it explores the design space and, as part of Best Practice, it gives recommendations what approach to take when deriving a specific IoT Architecture depending on given requirements and constraints. In addition, IoT-A is further exploring typical instances of architecture building blocks like a Resolution Infrastructure. Here a special focus lies on the discovery aspect.

3.4.2 Naming, Addressing and Discovery Solutions

In the Architectural Reference Model, IoT-A has defined components for discovery, look-up and name resolution on the service level. In addition, the communication model of the Reference Model includes an IoT communication stack that defines an ID layer.

With the ID layer, a convergence point in the communication stack has been defined that enables an identifier/locator split, i.e., unlike in the traditional IP architecture, where and IP address is both used for identifying a communication endpoint as well as being the basis for routing messages to this endpoint, identifier and locator are separate aspects. For example, an identifier may remain the same over the lifetime of a communication endpoint, whereas the locator may change with the point of attachment to the network, which may be changing according to the mobility of the device that implements the communication endpoint.

The functional view of the Reference Architecture identifies the IoT Service Resolution and the VE Resolution functional components in the IoT Service and Virtual Entity functional groups respectively. The functional groups represent two abstraction levels that are depicted in Figure 4.

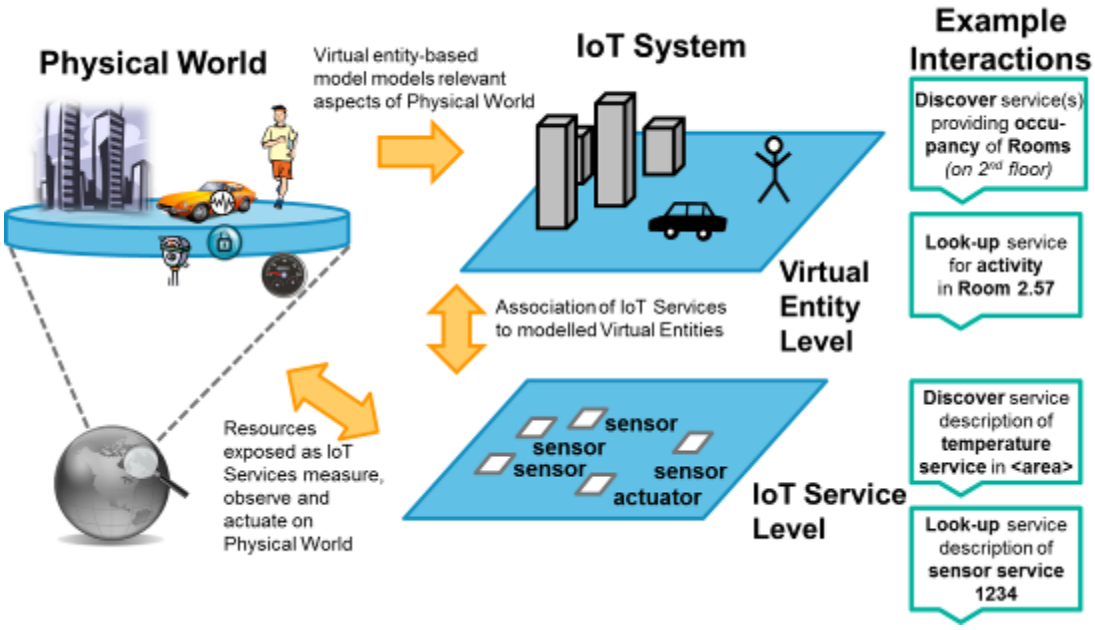

Figure 4: Virtual Entity and IoT Service Abstraction Levels

The IoT Service Level contains the IoT Services that expose sensor and actuator resources that provide information or enable actuation respectively. The IoT Service Resolution component provides discovery, look-up and id-resolution functionalities on this level. Figure 4 shows two example requests: *Look-up service description of sensor service 1234* and *Discover service description of temperature service in <area>*. A resolution request would resolve the service identifier, e.g. 1234, to the locator with which the service can be accessed, e.g. http://myservice.com:9080/temp". While this abstraction level is suitable for certain classes of IoT applications, there are other types of applications that profit from a higher abstraction level.

The Virtual Entity level models Physical Entities of the real world with their properties modelled as attributes. Applications can now look-up or discover Virtual Entities representing Physical Entities, e.g. in their environment, without having to know them beforehand, but just specifying what kind of Virtual Entity they are interested in together with the IoT Services that can provide the respective service. The relations between Virtual Entities, their attributes and Services are called associations. The VE Resolution enables the look-up and discovery of the services (as part of the associations) based on the Virtual Entity or the type of Virtual Entity respectively. Figure 4 shows two example requests: *Look-up service for activity in Room 2.57* and *Discover service(s) providing occupancy of Rooms (on 2nd floor)*.

- **Naming:** IoT-A is looking primarily at identifiers, i.e. a *name* that also serves the purpose of identification. The purpose of identifiers is to uniquely identify an object. This is true for everyday life (like license plate numbers identifying cars) as well as for the digital world (like MAC addresses identifying a network adapter). Identifiers are a handy representation of the object and allow to reference or address the object for example in database or in communication protocols. In order

to fulfil this purpose, identifiers must be unique. Sometimes the uniqueness is only given inside a certain scope (like ZIP codes which are only unique inside one country). In this case uniqueness must be ensured either implicitly by the context or explicitly by a second identifier.

Identifiers can be constructed in different ways:
- random data
- hierarchical identifier
- encoding additional information (e.g. timestamp, locator)
- by cryptographic operations (e.g. hash of public key)

Of course, identifiers can also mix several of these concepts. Additionally, some identifier types allow serving additional purpose like routing, locating, binding to other identifiers.

As IoT-A targets a general reference architecture, we do not prescribe a certain identification scheme. Different systems following an architecture that is based on the reference architecture may have different requirements regarding identification and so it would be problematic to force a single one. Instead we discuss general approaches with their respective properties.

In general there are two different approaches for an identification scheme for an IoT. The first approach is reusing an existing identification scheme. As an example (from the Internet/Web world): devices are identified by IP addresses, services are identified by URLs. However, this small example immediately illustrates that such an approach only works in homogeneous environments. For example, RFID tags do not have an IP address and thus the offered services can also not be addressed via URLs.

The second approach is defining a new identification scheme, independent of existing schemes. In this case, there are two possibilities for bridging between the new identification scheme used inside the IoT-A architecture and the identification schemes used by concrete IoT:
- Mapping: The existing identifiers are be mapped to the newly defined identifiers. In this case, entities providing the mapping functionality are required.
- Container: The existing identifiers are embedded into a universal container format. In this case, translating between new and existing identifiers performed by wrapping and unwrapping respectively.

In both cases, it must be taken into the account that the new identifier might not offer some functionality, which the original identifier included. Typical examples for this are hierarchical structuring, locator, cryptographic information.

The definitions of all lookup and resolution functions are based on the assumption that there is an identification scheme. For IoT deployment an appropriate identification scheme has to be used.

- **Addressing:** IoT-A has not developed its own addressing solution and is rather relying on existing addressing schemes like IPv6, IPv4 and other solutions, possibly employing gateways for translating between addressing schemes.

- **Discovery:** IoT-A has been investigating different approaches to discovery that can be applied to both the IoT Service and the Virtual Entity abstraction level. Interesting approaches and respective configurations have now been selected for implementation and further evaluation, i.e., we have fixed certain parameters to make an implementation feasible, but are now aiming for a more in-depth evaluation.

  - *Geo-Discovery approach:* Discovery of IoT Services and Virtual Entities based on geographic coordinates plays an important role in IoT scenarios as they relate to the physical world, where the question of *where* something is – often with respect to one''s own location – is of key importance. The geographic discovery is also often highly selective with respect to number of IoT Services or Virtual Entities returned, as there may be millions of temperature services registered in an IoT system, but there may be only a few that cover (parts of) a specified geographic area.

    An efficient geographic index is needed to efficiently find IoT Services according to their service areas or Virtual Entities according to the location of their physical counterpart. As geographic areas are indexed instead of geographic points, an index structure handling geographic areas is needed. For the implementation we have decided to use an R-Tree index structure. As a true Internet of Things will include a large number of players, we assume that also the Resolution Infrastructure will not be operated by a single entity, but a multi-tenant solution is needed. Therefore, we are investigating different configurations, e.g. with a hierarchy of catalogue and resolution servers, where catalogue servers know the areas covered by the resolution servers, whereas the resolution servers store the service descriptions and associations respectively.

  - *Semantic Web approach:* The idea of the semantic approach is to semantically specify requests as well as service descriptions and associations and match them for discovering the desired services and associations. For efficiency reasons, latent factors are calculated for service descriptions and associations, reducing the original information to a much smaller vector. These vectors are used for clustering the service descriptions and associations. When receiving a request with a specification, again the latent factors are calculated to determine the cluster, where possible matches can be

found. And only for the elements of this cluster a precise matching is performed.

- *Federation-based approach:* The federation-based approach is also based on semantic technologies, but assumes a federated architecture. A federation is conceptually represented as a directed acyclic graph with no undirected cycles, where each non-source vertex has an in-degree strictly equal to 1 and an out-degree above or equal to 0. The nodes composing the federation denote places.

  The approach uses a hierarchical clustering approach with a matching based on semantic distance in combination with a routing table in each node. This enables the efficient discovery of associations and services within the federation.

- The *domain-based approach* that focused on a hierarchical domain structure has been discontinued due to the proposing partner leaving the project.

3.4.3 Migration Solution

The discussed approaches are general approaches that can be employed for identification and discovery in the Internet of Things. As a first step, the IoT-A Architectural Reference Model allows mapping existing solutions into a common structure, helping to identify possible problems, e.g. relating to the integration of existing systems. It also helps in suggesting possible solutions, e.g. how gateways can be used for bridging different systems, and what alternatives can be pursued depending on the specific requirements. Since we focus on an Architectural Reference Model, we do not present a single solution with a migration path to that solution, rather we present a framework and some recommendations how a solution can be found given specific requirements.

3.4.4 Scalability

Since IoT-A is looking at Internet of Things; scalability is a very important aspect that will also be at the focus of further evaluations to be conducted before the end of the project. These evaluations are intended to verify the following observations concerning the different approaches. The geographic discovery approach aims at enabling a highly scalable discovery based on a geographic index structure and a high selectivity. The hierarchical distribution with catalogue servers is designed to enable this also in a multi-tenant scenario with a large number of tenants.

The semantic approach uses clustering to achieve a higher scalability. The federation-based approach aims at using the federated structure together with the fact that in the Internet of Things the locality with respect to places is of great importance to achieve scalability for typical requests.

3.5 BUTLER (http://www.iot-butler.eu)

3.5.1 Project Overview

The project acronym BUTLER stands from uBiquitous, secUre inTernet-of-things with Location and contExt-awaReness. BUTLER is a 3-year Integrated Project funded by the European Commission within the 7th Framework Programme in the area of Internet-Connected Objects. BUTLER started in October 2011 and will end in September 2014.

BUTLER's concept is to develop a natively secure, pervasive, energy-efficient and optimized context-aware opened architecture, by bundling and integrating IoT technologies and services to transparently learn and infer the behaviours and needs of users, acting on their behalf of and protecting them so as to improve their quality-of-life. More in particular, the BUTLER project aims to:

a) Improving/creating enabling technologies to implement a well-defined vision of secure, pervasive and context-aware IoT, where links are inherently secure (from PHY to APP layers) applications cut across different scenarios (home, office, transportation, health, shopping etc.), and the network reactions to users are adjusted to their needs (learned and monitored in real time).
b) Integrating/developing a new flexible smartDevice-centric network architecture where platforms (devices) function according to three well-defined categories: smartObject (sensors, actuators, gateways), smartMobile (user's personal device) and smartServers (providers of contents and services), interconnected over IPv6.
c) Building a series of field trials, which progressively integrate and enhance state-of-the-art technologies to showcase BUTLER's secure, pervasive and context-aware vision of IoT.

In addition to above reported R&D innovations, BUTLER and its External Members Group will also aggregate and lead the European effort in the standardization and exploitation of IoT technologies.

3.5.2 Naming, Addressing and Discovery Solutions

Along the first year of the BUTLER project, not so much effort was devoted to naming, addressing and discovery solutions. However, some preliminary ideas, mainly based on the IoT-A approaches, have been taken into consideration. These functionalities will be investigated in more detail along the second year of the project in order to complete the final design of the horizontal version of the BUTLER architecture and give support to the development phase of the BUTLER system.

Similar to the IoT-A project, BUTLER is going to use a representation of the physical world by means of virtual entities. The physical world is composed of physical entities that could be any object (e.g., a car, a human, a bottle, etc.) or environment (e.g. a room, a building, a car park etc.). Thus, an association between physical entities and virtual entities is necessary in order to allow the user to interact with the physical world and

meet his goals. In particular, this association is achieved for instance by embedding into the physical entity one or more ICT devices that allow the user to take information from it and change its status. Note that a device can be composed of sensors, which are able to provide information from the physical entity they monitor, and actuators, which are used to modify the state of a physical entity. To sum up, the association between physical and virtual entities is important in look-up and discovery process. In addition, since IoT entities and related services are spread globally, there must be a sort of identification and resolution infrastructure to identify and discover devices and services that allow accessing information about entities and controlling them.

Following paragraphs illustrate how BUTLER is going to deal with naming, addressing and discovery.

- **Naming**: Name is a label or an attribute of an object used to uniquely identify it within a large set of objects. Names are also used to identify groups of objects or subset of objects. It is important to distinguish the difference between naming and addressing. Naming is the procedure of assigning a name to an object while addressing refers to placing the object into the space, or in other words refers to a way to access the object. Thus, naming and addressing are strongly linked between each other. In fact, a common naming and addressing scheme should be employed. For example, given in input the name of an object, the resolution infrastructure should be able to find the corresponding address to be used by the involved communication protocols. Since the BUTLER scenario is not uniform, existing naming approaches are not suitable. In fact, the involved entities in BUTLER are heterogeneous in terms of communication technologies, computational capabilities, and degree of mobility. Note that BUTLER defines three set of devices namely, smart objects, which are constrained devises such as sensors and actuators, smart mobiles, which are user's personal devices, and smart servers, which provides contents and services. Moreover, the BUTLER system should be able to operate transparently and seamlessly across different vertical domains such as smart home, smart transport, smart shopping, and so on. Therefore, given this horizontal scenario, it is not easy to reuse existing IoT naming schemes such as IP address to identify devices and URI to services because smart objects do not have enough resources. Therefore, in order to solve this problem, BUTLER is going to use gateways that mediate the data exchange between constrained smart objects and web applications. In particular, the address mapping between smart objects (e.g. WSN nodes) and applications is performed at the gateway by employing IPv6 mapping functionalities. Thus, a SOA middleware approach can be utilized in the BUTLER project that guarantees flexibilities and provides higher level abstraction. Moreover, this middleware solution will be augmented by restful interfaces to support semantic description.
- **Addressing**: Similar to IoT-A, BUTLER is not going to develop its own addressing scheme and it rather relies on the existing IPv6 one. As mentioned in the previous paragraph, gateways are employed to

translate between IPv6 and other addressing schemes used by the underlying communication technologies.

- **Discovery**: Different discovery approaches for IoT already exist in the literature. One approach that BUTLER is going to investigate is the Geo-Discovery one proposed by IoT-A as it is suitable for mobile and context-aware scenarios identified within BUTLER. Moreover, this approach is supported by the fact that BUTLER applications are enabled by accurate localization algorithms and a generic user is often interested in discovering services that are close to its location or to its final destination. Thus, the knowledge of geographic coordinates plays an important role to better selecting the physical world of interest.

3.5.3 Migration Solution

As presented in the previous subsection, BUTLER will use gateways for bridging different technologies to IPv6. Thus, this approach permits the migration of different legacy technologies to a common IPv6 abstraction. In particular, the gateways will implement an addressing proxy module that defines IPv6 mapping for the native addressing of legacy technologies. Additionally, this approach allows interoperability among heterogeneous objects independently of the underlying communications technology used.

3.5.4 Scalability

Scalability is an important feature to be guaranteed in IoT applications. Regarding addressing scheme, BUTLER will use IPv6 addresses. Scalability is achieved by adopting gateways with IPv6 mapping functionalities that allow the integration of non IPv6 compliant smart objects (e.g. based on IEEE 802.15.4, RFID and NFC communication technologies). As far as discovery is concerned, in agreement with the IoT-A project, the proposed Geo-Discovery approach is highly scalable and provides high selectivity. In fact, since this method is based on absolute coordinates of IoT objects, it is possible to select the region of interest by using the perimeter's coordinates of the region as input of the discovery functionalities. Thus, this approach results to be efficient in terms of communication and energy consumption. Moreover, the Geo-Discovery approach is suitable for mobility scenarios like the ones identified in BUTLER, where the users move across different vertical IoT scenarios. One point to take into consideration is that all devices and context data need to be continuously geo-referrenced.

3.5.5 Indicative Applications

Firstly, BUTLER aims at demonstrating several pervasive and context-aware information systems in different vertical domains including:

- Smart Home/Office (e.g., saving energy comfortably, interacting with appliances, monitoring and controlling, etc.).
- Smart Health (e.g., monitoring medicine intake, personalized diabetes assistance, monitoring health parameters, etc.).

- Smart Shopping (e.g., managing spark deals, getting advice on buying goods, updating consumer profiles, etc.).
- Smart City (e.g., managing parking space, remotely paying parking meter, etc.).
- Smart Transport (e.g., notification of bus arrival, notification of car traffic jam, monitor available reserved seats in public transport, etc.).

Finally, BUTLER aims to design and demonstrate the first prototype of a comprehensive, pervasive and effective context-aware information system, which will operate transparently and seamlessly across the above vertical domains towards a unified smart horizontal urban environment.

3.6 IoT6 (http://www.iot6.eu/)

3.6.1 Project Overview

IoT6 stands for "Universal Integration of the Internet of Things through an IPv6-based Service Oriented Architecture enabling heterogeneous components interoperability". IoT6 is a 3 years FP7 European research project from October 2011 until September 2014.

It aims at exploiting the potential of IPv6 and related standards (6LoWPAN, CORE, COAP, etc.) to overcome current shortcomings and fragmentation of the Internet of Things. Its main challenges and objectives are to research, design and develop a highly scalable IPv6-based Service-Oriented Architecture to achieve interoperability, mobility, cloud computing integration and intelligence distribution among heterogeneous smart things components, applications and services. Its potential will be researched by exploring innovative forms of interactions such as:

- Multi-protocol integration & interoperability with heterogeneous devices.
- Device mobility and mobile phone networks integration, to provide ubiquitous access and seamless communication.
- Cloud computing integration with Software as a Service (SaaS).
- IPv6 - Smart Things Information Services (STIS) innovative interactions.
- Information and intelligence distribution.

The main outcomes of IoT6 are recommendations on IPv6 features exploitation for the Internet of Things and an open and well-defined IPv6-based Service Oriented Architecture enabling interoperability, mobility, cloud computing and intelligence distribution among heterogeneous smart things components, applications and services, including with business processes management tools. The project will integrate an end-user perspective with the targeted realization of a green and smart IPv6 building for the validation in a real environment.

3.6.2 Naming, Addressing and Discovery Solutions

Following paragraphs illustrate how IoT6 deals with naming, addressing and discovery of IoT resources:

- **Addressing**: IoT6 considers global IPv6 addresses to identify and interconnect any two objects. IoT6 proposes three solutions for enabling the translation of the proprietary identifiers of smart objects from legacy technologies to homogeneous IPv6 address. For smart things as IEEE 802.15.4 device, this adaptation solution is implemented by means of the 6LoWPAN standard [Montenegro2007]. To provide this integration in legacy technologies (e.g. Bluetooth Low-Energy, KNX, X10, CAN and RFID), we propose two adaptation solutions called Glowbal-IP [Jara2012] and IPv6 Addressing Proxy [Zamora2010]. These solutions offer support for an auto-configuration process to avoid the manual definition and maintenance of tables in border routers, making them more scalable and dynamic.
- **Naming**: IoT6 proposes to use Domain Name System (DNS) which is the most suitable naming solution in Internet. DNS presents a naming solution where no additional infrastructure, in addition to the current DNS servers, is needed, and merely requires that resources be enabled with an IP-based addressing. We provide a novel mechanism with maximum lifetime of the cacheable DNS entries in order to allow dynamic registration from smart objects to DNS servers. Following a similar way to DNS, IoT6 defines a lightweight solution for resource directory (RD) based on CoAP [Shelby2011]. This RD is used as a repository for Web Links to the resources hosted on the smart objects, which are acting as Web Servers through their REST/CoAP interfaces.
- **Discovery**: IoT6 proposes DNS-SD (Service Directories) [Cheshire2011DNS-SD] and mDNS (Multicast) [Cheshire2011mDNS] as main solutions for global and local discovery operations. In the global scope, we provide an optimization of DNS-SD which is scalable to enterprise deployments, since it is defined a centralized server per enterprise, building or in an IoT deployment to a room level. In the local scope, mDNS is integrated with a DHT (Distributed Hash Table) [Balakrishnan2003] mechanism to provide load balancing, scalability, and robustness when extending the search and discovery operations to the global scope. Also, in the local part of the operations, we incorporate the optimizations by lmDNS which is specifically designed for smart objects. The DHTs are structures to store key/value mappings across a set of nodes, which in turn pertain to the overlay network that hosts the DHT. For our approach we decided to use Chord [Stoica2001], a widely used and well-known overlay network routing algorithm and DHT across the research community. Moreover, we consider another tendency to define global discovery mechanisms based on semantically linked data and thus driven by ontologies and vocabularies (e.g., OWL). These systems provide a powerful mechanism to store and query complex information and are based on RDF (Resource Description Framework) [Klyne2004] and SPARQL (Query Language) [Prudhommeaux2008].

3.6.3 Migration Solution

IoT6 project propose two mechanisms (Addressing-proxy and Glowbal-IP) to permit the migration of a wide spectrum of legacy technologies with proprietary protocols to a common IPv6 abstraction. Addressing-proxy defines an IPv6 mapping for the native addressing of legacy technologies. The mapping has been carried out initially for a representative home automation technology i.e. X10, a building automation technology i.e. EIB/KNX, an industrial technology i.e. CAN, and finally a logistics and identification technology i.e. RFID. For wireless sensor technologies (i.e. IEEE 802.15.4 and Bluetooth-Low-Energy) which are not offering direct IPv6 or 6LoWPAN support can be adapted in a similar way with the presented Glowbal-IP protocol. This mechanism allows the global communication and interoperability with any object independently of the technology used.

3.6.4 Scalability

The IoT6 project provides a high scalability in terms of number of connected objects, anticipating the growing number of Internet of Things devices. The IoT6 solutions enable the management of billions or trillions of identifiable "things" communicating with one another with an increased communication among terminals and data centres. This project proposes scalable addressing and communication solutions based on IPv6 compliant standards such as 6LoWPAN, Glowbal-IP and Addressing-Proxy. As abovementioned, these solutions support the dynamic maintenance of tables in border routers, making them more scalable.

Moreover, IoT6 provides a decentralized architecture based on DNS-SD and mDNS that allows the distribution of the information about the services and location of the deployed smart objects based on their domain or anchor point. It defines services in a local level through mDNS and in a global level through the hierarchical delegation of domains servers to locally managed repositories with DNS-SD. These local repositories can be located at the border routers from solutions such as 6LoWPAN, and consequently managed repositories. Thereby, it can be managed locally their information but accessible globally through the Internet architecture.

3.6.5 Indicative Applications

IoT6 project was designed to enable a multi-domain compliant solution. The developments of IoT6 project is proposed for heterogeneous technologies on the context of Internet of Things. IoT6 project considers a wide set of IoT applications, including:

- Building automation.
- Smart electrical grid.
- Telemedicine and e-Health.
- Business process management tools.
- RFID tags & smart things information service (such as EPCIS).
- Wireless sensor networks (WSN).
- Audio / video components.
- Cloud computing associated with Software as a Service (SaaS).

- Safety and security.

3.7 IOT.est (http://www.ict-iotest.eu)

3.7.1 Project Overview

To date implementations of Internet of Things architectures are confined to particular application areas and tailored to meet only the limited requirements of their narrow applications. The ICT workprogramme highlights the importance of interoperability between the silo solutions and different technologies used in these disjointed sectors. Sensors/objects that provide information or perform as actuators implementing actions in the real world are plentiful and the range of communication technologies, networking protocols, information types and data formats used to exchange information or control data is vast. To overcome technology & sector boundaries and therefore dynamically design and integrate new types of services and generate new business opportunities requires a dynamic service creation environment that gathers and exploits data and information from sensors and actuators that use different communication technologies/formats. To accelerate the introduction of new IoT enabled business services (in short IoT services) an effective dynamic service creation environment architecture needs to provide:

1. Orchestration, i.e. composition, of business services based on re-usable IoT service components,
2. Self-management capable components for automated configuration and testing of services for "things",
3. Abstraction of the heterogeneity of underlying technologies to ensure interoperability.

IoT.est develops a test-driven service creation environment (SCE) for Internet of Things enabled business services. The SCE will enable the acquisition of data and control/actuation of sensors, objects and actuators. The project will provide the means and tools to define and instantiate IoT services that exploit data across domain boundaries and facilitate run-time monitoring which enables autonomous service adaptation to environment/context and network parameter (e.g., QoS) changes. At the core of IoT.est is the need to interact and connect to objects and the digital representations of things, for the service creation and run-time facilitation the availability of unique names and addresses is a must. Discovery mechanisms plat a similarly important role in the service lifecycle.

IoT.est will prototype its major concepts and will evaluate the results for exploitation towards future IoT service creation, deployment and testing products.

3.7.2 Naming, Addressing and Discovery Solutions

IoT.est does not explicitly investigate approaches and solution for naming, addressing and discovery, rather the project exploits available

approaches. For example looking at current Internet of Things service platforms, they consider two main technology approaches one based on extended heavy weight Web Services (SOAP/WSDL) and one using the capabilities exposed by the REST architectural style. Both approaches have been considered from both functional and non-functional criteria point of view. The majority of considered aspects stress specific subjects like resource-constrained devices, reliability of data or naming and addressing strategies. From this point of view, the REST approach is considered more appropriate due to low footprint, simplicity of the messaging style, openness to common Web technologies and easiness for developers. As a consequence most of the current standardisation is made around REST interfacing model. At the same time from integration point of view, the IoT.est addresses both models of services together with semantic annotation capabilities. Given this choice of platform, the naming, addressing and discovery choices made in IoT.est are rather standard choices:

- **Naming**: IoT.est uses common URIs to uniquely identify objects that may be used in the service creation.
- **Addressing** and **Discovery** uses a Service Registry and Search interfaces which include three interfaces for other components to use: service registration interface, service search interface and service query interface. These interfaces are used by the Service Composition Environment, Service Runtime and IoT.est Services components. The service search interface is an intermediary between service discovery requests and the service discovery component which performs service search, recommendation and ranking based on the semantic service descriptions. The service query interface accepts requests on service lookup/update/remove and forwards them to the respective processing components. The semantic descriptions of the services in the registry will be updated according to the requests.

3.7.3 Migration and Scalability

As already outlined IoT.est uses existing naming and addressing schemes rather than introducing new ones. Therefore, the project does not explicitly investigate a migration and scalability solution associated with its test environment.

3.8 IoT@Work

3.8.1 Project Overview

The designers of industrial automation systems have always faced the challenge of configuring a highly complex and demanding communication network as well as an IT security subsystem. This is a critical and costly activity, often performed manually, that is required to avoid failures that can lead to costly production interruptions or malfunction that can endanger involved humans.

IoT@Work aims at designing an IoT architecture that takes into account the needs of the industry and factory automation systems, and specifically their networking and communication issues, improving their flexibility and reliability through what we call plug and work IoT. Specific features to be explored and developed by the IoT@Work project are related to factory automation systems auto-configuration and improved security.

An IoT@Work enabled factory shop floor should make the life of an automation expert or engineer easier, reducing operative and capital expenditure. Transforming automation devices into *Internet-enabled things* automation experts will not have to care of configuring the bits and bytes exchanged between these things during the design and commissioning phases. The self-configuring Internet of Things (IoT) will hide most of the complexity of network protocols that are needed to properly configure a device from a network and operational point of view.

3.8.2 Naming, Addressing and Discovery Solutions

3.8.2.1 Overview

In the following we provide a quick summary of the naming issues in the IoT@Work Event Notification Service (ENS). These issues are related to the management of events the ENS collects and manages in an industrial production environment. In order to properly manage the collected events they are arranged in so called Namespaces that have a hierarchical structure in which nodes could identify physical objects(e.g.: PLCs, robots, etc., as well as applications) or objects aggregations (e.g.: production cells, production lines, etc.), or even virtual entities (e.g.: robot's model, software modules, etc.). The IoT@Work namespaces nodes need to be properly identified as quickly summarised below.

3.8.2.2 IoT@Work ENS

Event-driven architectures are rapidly becoming one cornerstone of modern distributed systems due to their ability to support organisations in setting up information systems that proactively react to the changing environment. Event-driven architectures support enterprises in deploying business or production processes that have low latency and are highly reactive.

Traditional systems, and the manufacturing ones in particular, are based on pull interaction patterns, i.e. synchronous request/response (often based on client/server RPCs), while event-driven architectures normally adopt a publish/subscribe model that pushes event's notifications to interested listeners. The corresponding communication patterns are therefore unidirectional, asynchronous and fire-and-forget, which promote the use of highly decoupled systems in which the only relevant issues are related to well-defined message semantics.

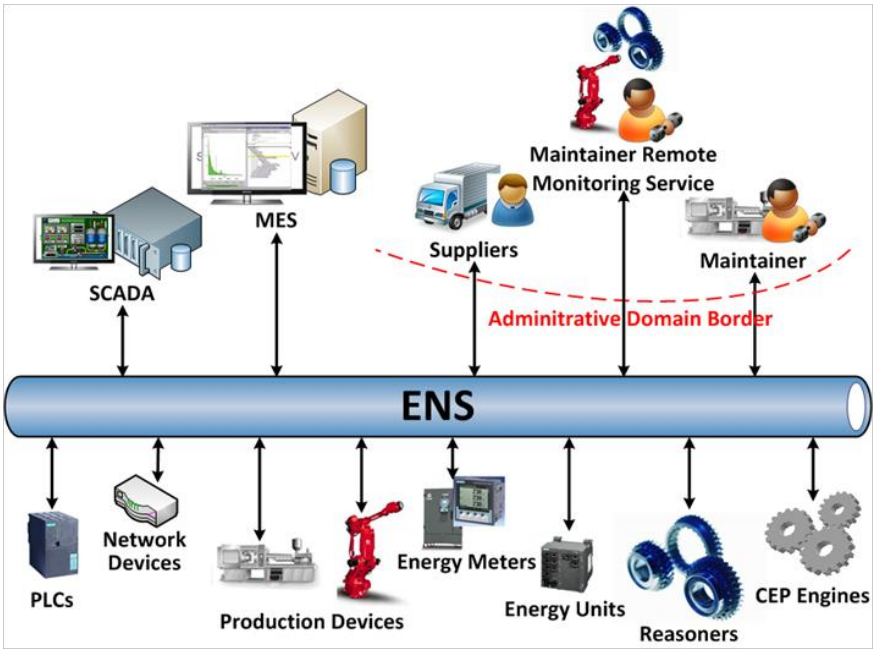

Figure 5: Overview of the Notification Service Approach used in the scope of IoT@Work Project

As depicted in Figure 5, all devices and services publish their relevant events to a common middleware in charge of dispatching specific subsets to properly identified and authorized applications and services.

The proposed approach, therefore, brings the data to the interested parties, instead of bringing the parties to the data. This reversed approach in data provision has significant impacts both on the system's security and on controlling what data is provided to whom.

The Event Notification Service is a functional component that acts as a common collector and distributor of events coming from disparate sources (i.e. Publishers) and dispatched to listeners (e.g. Subscribers/Consumers). The functionalities provided by the ENS are similar to the one offered by a generic asynchronous messaging middleware server. Anyway the ENS is not only an asynchronous message-oriented server but can be considered an active component of an Event-Driven Architecture as it fully supports the key features of that paradigm (e.g.,: Broadcast communication, Timeliness, Asynchrony, etc.).

The IoT@Work ENS is based on the AMQP protocol being this one of the few standards for MOMs and perhaps the only one to provide at the same time both a model and wire-level standard, support for several message exchange patterns and payload transparency.

3.8.2.3 IoT@Work ENS Namespaces

The ENS uses namespaces to organize the published events. A namespace is devoted to organize a specific set of events independently from other namespaces and relating to a specific need and/or scenario (for example

data that reports energy consumptions of production devices can be organized in a specific namespace named Energy Monitoring Namespace).

In order to provide to ENS subscribers flexibility in identifying subsets of events in a given namespace, each namespace has a hierarchical structure (see Figure 6) that is functional to production needs only. Therefore each namespace can be represented by a tree structure.

Each publisher publishes its events for a specific namespace under a well defines leaf node. As events can be generated only by physical objects (e.g. shop floor devices or even applications), leaf nodes in namespaces represent "physical" entities.

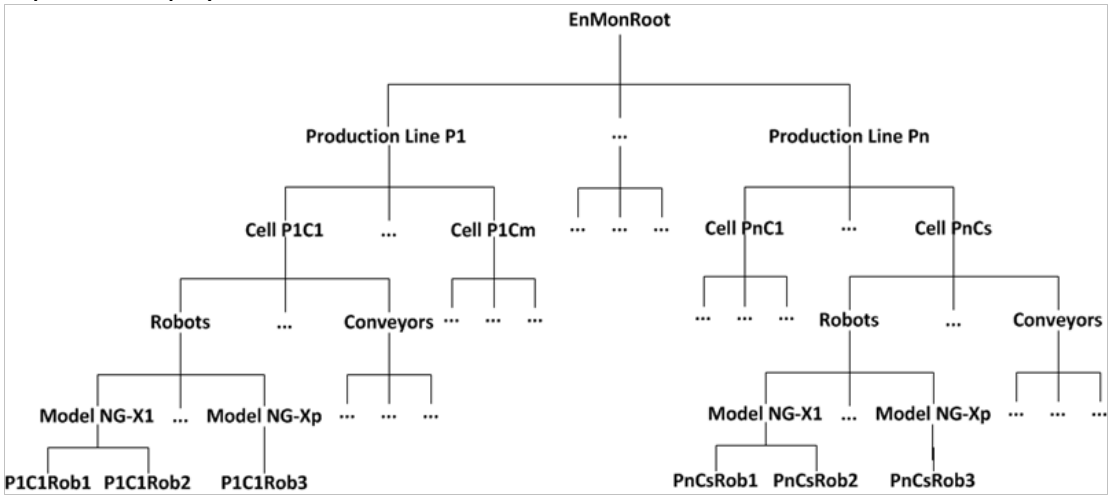

Figure 6: An example of IoT@Work ENS namespace

Intermediate nodes in a namespace, instead, represent aggregations or virtual entities that are useful to simplify subscribers "area of interest" within a given namespace.

The way nodes, both leaf and intermediate, are identified in different namespaces are potentially completely uncorrelated. Therefore while leaf nodes, which are tied to physical objects, are normally named in the same way in different namespaces, intermediate nodes, as well as the namespace hierarchy, can be completely different among namespaces.

Each node in an ENS namespace has the following set of attributes:

- **Name**: the identifier of the node.
- **Description**: a free-text description of the entity represented by the node.
- **EntityURI**: an URI that points to a semantically enriched description of the entity represented by the node. For example a Root Node could have semantically enriched information like: objective of the namespace, people/roles in charge of managing the namespace, etc., while an Intermediate Node information describing the purpose of the subtree.
- **A URI** that points to meta-data useful for subscribing applications to properly manage and process the published events. For example for an

energy monitoring namespace these meta-information can detail the unit of measure, accuracy, etc. of the published measured data.

Figure 7 highlights an example of events' publishing by a physical object (in the figure a robot of Model NG-X1 and identified as PC1C1Rob1) under an energy monitoring namespace.

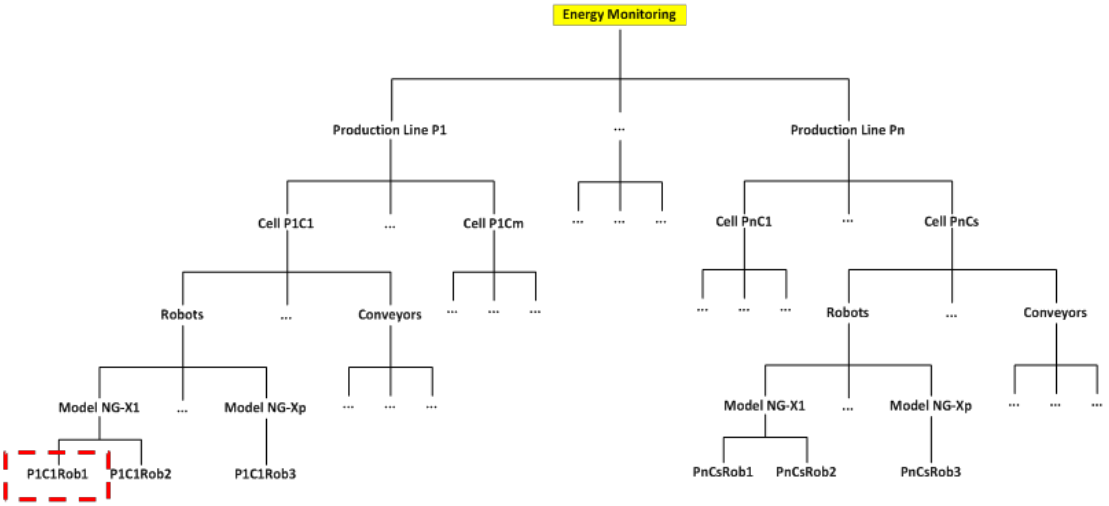

Figure 7: IoT@Work ENS namespace publishing

The events at lower hierarchical levels are aggregated at each upper level. Therefore a subscriber to an intermediate node will receive events of all dependent nodes. Figure 8 for example exemplifies such kind of subscriptions; indeed a subscriber that specifies as the namespace's subset of its interest something like "Energy Monitoring.*.Cell P1C1" will receives all events published under the leaf nodes of "Cell P1C1".

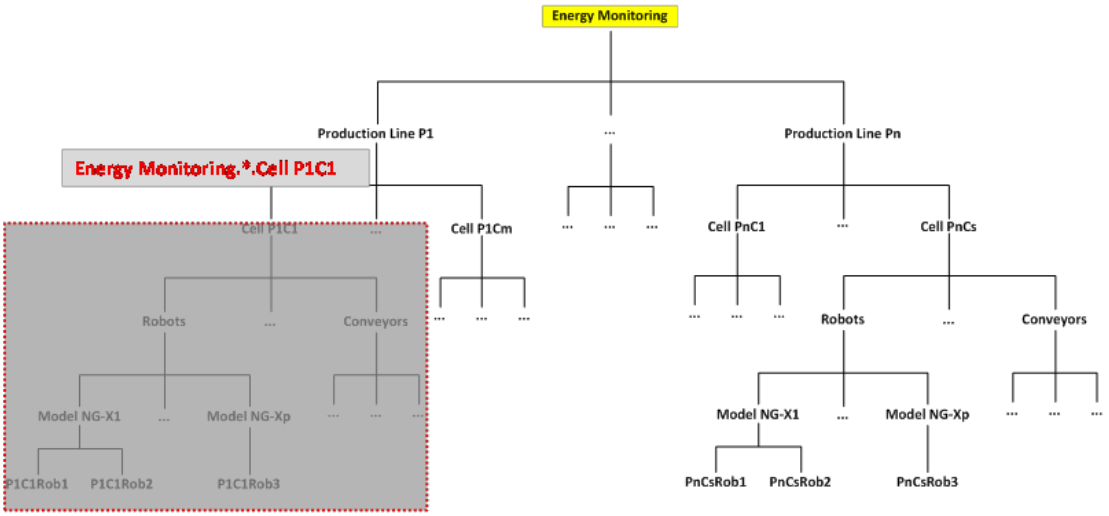

Figure 8: IoT@Work ENS namespace subscription to a branch

Figure 9 instead exemplifies a more complex events' subscription where a subscriber is interested to all events generated by robots of a specific model ("Model NG-X1" in the figure). To this end the subscriber declares to the ENS as the events' subset of its interest in this namespace something like "Energy Monitoring.#.Robots.Model NG-X1".

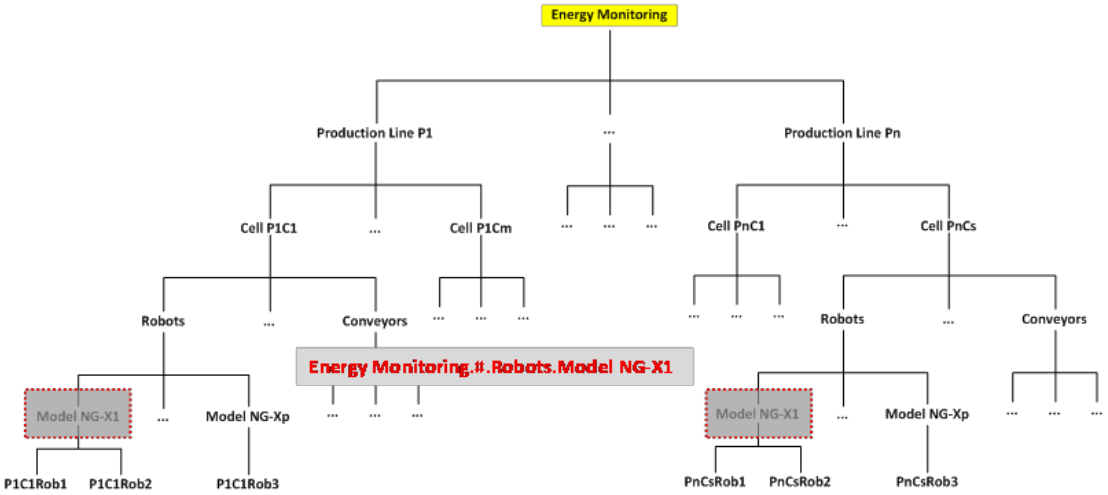

Figure 9: IoT@Work ENS namespace subscription to a more complex subset

As evident from the above discussion and examples, in IoT@Work ENS namespaces naming is a crucial elements for efficiently managing events' filtering and aggregation, even if our system doesn't mandate specific constraints regarding the naming hierarchical structure and name contents apart from avoiding using meta-characters (i.e. characters having special meanings like ".", for structuring the naming hierarchy, and "*" or "#" for expressing filtering).

3.8.2.4 IoT@Work Directory Service

The IoT@Work Directory Service objective is a service focused on *quickly* provide a set of information (e.g.: short description, location, active services, etc.) on a given device deployed in the manufacturing plant.

The *quickly* term has been used to highlight that this service has to be accessible not only via traditional access means (i.e. browser on a PC and URL), but also using more intuitive means like pointing the device for which I need the information (see Figure 10), so that it can be more effective in a production environment in which people (workers, or line supervisors) can acquire those information while moving in their working environment using a mobile device (phone, tablet, etc.).

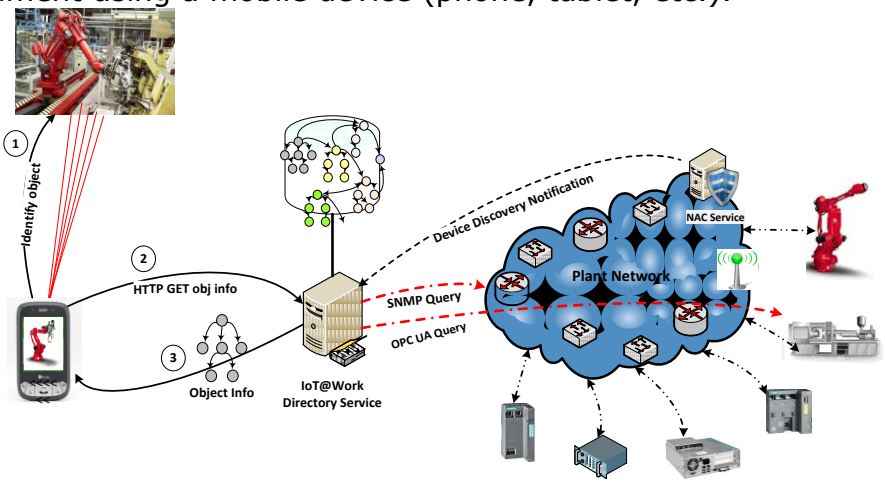

Figure 10: IoT@Work Directory Service

The entities managed by this service can be layered as follows:

- *physical entities*: these are objects (Things) deployed within the production environment that are characterized by having not only a digital ID (i.e. something that identifies them within the IoT@Work digital environment), but also some physical representation of this ID;
- *virtual entities*: objects that have an identity but do not have a physical counterpart. for example virtual entities can represent application services, locations, etc…;
- *relationships*: links between objects that conveys information about objects;
- *primitive elements*: basic data type (e.g.: numbers, strings, URLs, etc.);

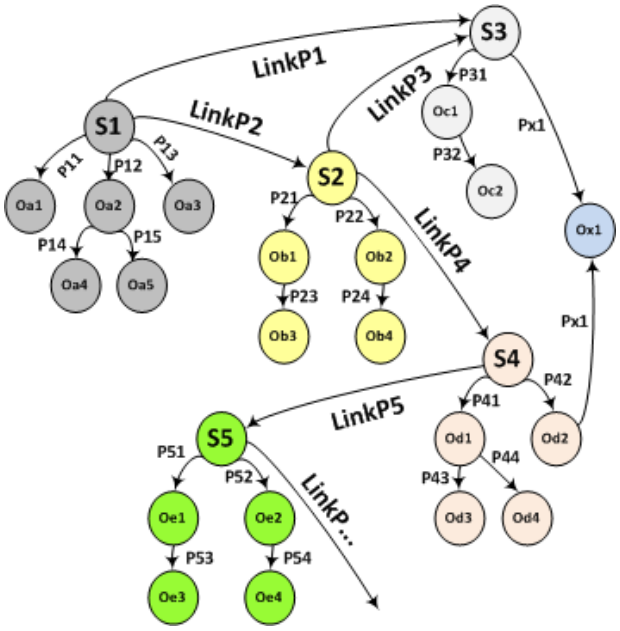

Figure 11: IoT@Work Directory Service Data Model

The IoT@Work Directory Service Data Model (sketched in Figure 11) is in line with:

- T-Engine Forum *uCode* Relation Model;
- W3C RDF (Resource Description Format).

Entities naming issues in the IoT@Work Directory Service are not critical (being RDF oriented each entity in the system is identified by a URI); while proper ontologies and taxonomies are critical being the founding element for a significant *intelligent* and dynamic processing.

3.8.3 Migration Solution

Integration with the IoT@Work ENS system requires that events' sources (publishers) and events' consumers (subscribers) adhere to the ENS access procedures, which are not complex, and provides some additional, optional, metadata for published events. To easy the integration both on the publisher as well as subscriber sides TXT e-solutions SpA provides a Java, OSGi compliant, library that supports all communication phases (i.e.

ENS connection setup, including client authorization check, connection usage for events publishing/consuming, connection release). The ENS does not set any constraint on the kind of data associated to events.

The IoT@Work Directory Service exposes a set of REST APIs through which its features (e.g. entity query, search, entity data updates, etc.) are made available.

3.8.4 Scalability

In order to support scalability the IoT@Work ENS service is based on the AMQP protocol (Advanced Messaging Queuing Protocol - http://www.amqp.org/) that offers a set of standard features (e.g. *Virtual Host*, filtering, …) to address scalability. Additionally the IoT@Work ENS makes use of the RabbitMQ (http://www.rabbitmq.com) implementation of the AMQP specification. Being based on the Erlang programming language (http://www.erlang.org/), the RabbitMQ additional has built in features for parallel execution, reliability, etc.

The IoT@Work Directory Service, as a REST service, does not have *front end* scalability issues, being possible to deploy multiple instances of the service. The *back end* system (e.g. the Directory Service database) presents instead scalability issues both related to the complexity of the entities to be managed (entities with different attributes, relationships among entities, etc.) and to the potentially relevant data to be managed. To address these issues our Directory Service is based on a NoSQL database (specifically OrientDB - http://www.orientdb.org) which is able to natively manage graphs, replication and data sharding.

3.8.5 Indicative Applications

The ENS, as described above, is well suited for all application contexts in which collection of data and their dispatching to a, potentially dynamic, set of consuming applications is a key factor. As compared to more traditional message broker's solutions, our ENS provides a more advanced, and flexible, access control based on the use of capability tokens, as well as the structuring of collected events in disjoint, and autonomous, *namespaces*.

The IoT@Work Directory Service, as the name implies, is suited for contexts where rapid access to a set of not-so-dynamic information related to *entities* is required.

3.9 OpenIoT (http://openiot.eu)

3.9.1 Project Overview

The main goal of OpenIoT is to research and deliver a middleware platform for the formulation of sensor-cloud infrastructures, where IoT services can be provided on-demand and in a utility based fashion.

OpenIoT will therefore enable the storage of sensor and ICO data within cloud computing infrastructures, while at the same time providing mechanisms for the on-demand selection of sensors and data streams.

OpenIoT will enable the dynamic orchestration of Internet-Connected Objects in response to requests for IoT services. As a typical example one can image a «Sensing-as-a-Service» functionality, on the basis of on-demand queries that retrieve and combine data from multiple distributed sensors. The OpenIoT middleware platform will be implemented and offered as Open Source Software (OSS).

Naming, addressing and discovery solutions are at the heart of the OpenIoT operation, given that the on-demand fulfilment of service requests requires the discovery of sensor and ICO resources. In the sequel we describe the OpenIoT naming and addressing solutions.

3.9.2 Naming, Addressing and Discovery Solutions

OpenIoT uses semantically annotated ICO (Internet-Connected Objects), which conform to the structure of the OpenIoT ontology (described in deliverable D3.1) of the project. The OpenIoT ontology is based on the W3C SSN (Semantic Sensors Networks) ontology and supports discovery of sensors and ICOs data and resources on the basis of the SPARQL language. In particular, the OpenIoT ontology enhances the W3C SSN ontologies on the basis of concepts pertaining to cloud computing and the OpenIoT applications. Note that the SSN ontology provides the means for describing sensors, their accuracy and capabilities, as well as related observations and methods used for sensing. The SSN ontology is sensor-centric, yet the term sensor is not restricted to sensing devices but it comprises hardware devices, sensing systems, scientific computational models, human run laboratory setups and generally anything that senses (no matter whether it is a physical or virtual sensor).

All sensors and ICOs in OpenIoT are announced to a semantic triple store (which serves as a directory service) and comply with the OpenIoT ontology. Note that sensors and ICOs in OpenIoT are typically interfaced to the cloud system via the Global Sensors Networks (GSN) open source middleware (http://sourceforge.net/apps/trac/gsn/). Hence, sensors and ICOs are initially represented based on the addressing options of the GSN middleware i.e. on the basis of their geographic location and type.

Within the OpenIoT cloud system each sensor and ICO is registered on the basis of a unique identifier, which maps to a URI (Universal Resource Identifier). The URI corresponds to an entity described based on the OpenIoT ontology, while it can be also linked to other URIs (i.e. semantically annotated resources) on the basis of the Linked Data Paradigm [Heath2011]. Overall, the naming, addressing and discovery solution of the OpenIoT project is based on the following elements:

- **Naming**: The naming infrastructure of OpenIoT is based on the use of unique URIs that point to the full structures with sensors/ICOs

properties. URI's are therefore used as names for things (including both resources and data).
- **Addressing**: OpenIoT maintains a list of unique identifiers for the various ICOs / sensors residing in the sensor cloud.
- **Discovery**: Discovery takes places on the basis of semantic queries formulated in the SPARQL language. Based on SPARQL queries, the OpenIoT directory services reason over the triple store and return lists of triples (URIs) that are appropriate for the service (SPARQL query) at hand. The discovery process provides RDF information related to URI's that are looked up by machines or people. Note that the use of linked RDF data is possible, which can provide pointers to other (linked) URI's thereby enabling discovery of other related things of the web of data. As part of this process the linking of real world data to existing data on residing on the linked data cloud (and on the basis of Linked Data principles).

3.9.3 Migration Solution

The OpenIoT addressing and discovery solution relies on the registration of sensors within its W3C compliant directory services. As a result, OpenIoT compliant sensors migration can be based on enhancing sensors with capabilities for announcing themselves to the OpenIoT directory service, thereby making them searchable by applications and services. This implies a non-trivial effort for enhancing the SSN directory with the classes and properties on new sensors. In order to alleviate this effort, OpenIoT will develop an interface from the GSN middleware to the OpenIoT service directory, in order to effectively automate the integration of any GSN compliant sensor. At the same time, OpenIoT will augment the number and type of GSN drivers, which will broaden the base of sensors that could be automatically announced/migrated to the OpenIoT service directory and associated discovery services.

A number of additional measures and tools can be developed to ease migration including:
- The use of on-line (web based) tools.
- The provision of REST APIs enabling semantic annotation and interfacing to the OpenIoT directory services.
- The support of RESTful direct access to the Semantic Entities (residing in the OpenIoT sensors directory).

The development of such tools have been already undertaken in background projects/efforts of the partners (see [Pfisterer11] and [Karnstedt12]), and this experience will be used to develop similar solutions in OpenIoT. Note that as part of the SPITFIRE project [Pfisterer11], there has been also an effort to use machine learning techniques for semantic annotation, in an effort to semi-automate this step. Such (semi-)automation could give a significant boost to the migration of the range of existing and future sensors in the OpenIoT semantic directory.

3.9.4 Scalability

The OpenIoT system is under development and hence there are no factual results about the scalability of its addressing and discovery subsystem. The project is designing for scalability (in terms of the number of sensors that can be supported) based on the use of several distributed instances of the GSN middleware (i.e. sensors in OpenIoT are first attached to GSN nodes and then announced to the directory) and based on the use of the scalability of the cloud where OpenIoT is hosted. While these measures are expected to provided scalability in terms of the sensor instances supported, additional scalability concerns may emerge due to the semantic nature of the system, which provides capabilities for provenance and quality reasoning. OpenIoT will exploit reasoning over its ontology in order to filter sensors and observations (e.g., select sensors that deliver specific measurements (e.g., air temperature or wind speed), filter according to the characteristics of the deployment (e.g., select sensors deployed in a specific region) and more. In these areas there will be a need to identify scalability issues and constraints, given for example that several spatial qualitative decision problems are NP-hard [Renz07].

3.9.5 Indicative Applications

The OpenIoT naming and addressing solution will be deployed in three different application domains, in particular:

- Smart City / Smart Campus applications, where the discovery schemes will be used to dynamically discover and link/reserve objects within a smart campus.
- Manufacturing applications, notably applications where multiple sensors will be dynamically discovered and combined in order to calculate specific Key Performance Indicators (KPIs) associated with the manufacturing operations (e.g., utilization of machines, manufacturing performance, production order execution monitoring).
- Smart Farming / Agriculture applications, which will dynamically gather information and compute crop-related parameters based on the multiple distributed wireless sensors.

3.10SmartArgiFood (http://www.smartagrifood.eu/)

3.10.1 Project Overview

The SmartAgriFood project aims at the realization of a fundamental change in the agri-food sector by exploiting innovative technologies towards a Future Internet. This goes far beyond the adoption of single functionalities by certain actors, but to provide an entire set of enablers that will support the agri-food chain actors as well as all of us, as anyone represents a consumer. The agri-food chain wide dimension and specific goals can be summarized as follows:

- Increase the effectiveness of farming procedures and globally increase the availability of food for all,

- Enabling also small farmers to become global actors in trading their supplies on a global market place,
- Dramatically reduce the waste in food logistics considering both the local as well as the global distribution of produce that continuously undergoes a quality change/decay over its life cycle in very short time periods, compared to other business domains,
- Avoid the distribution and consumption of harmful food, which, for example, has been contaminated with bacteria or pesticides,
- Assure the trust of consumers in a sustainable food production, providing a profound evidence of e.g. the origin, quality and applied procedures, and
- Establish a new dimension of communication in the food chain; enhancing the collaboration from farm to fork and at the same time opening a new dimension of feedback from fork to farm, enabling the realization of a new services and revenue models never thought of before.

Especially the consumer shall be enabled to control its supply in a new dimension that will assure the delivery of fresh food. In this context of international and even global supply chains, the unique identification of supplies remains a challenge in terms of both organizational and technical matters. The usage of approaches for naming and addressing needs to cope with the dynamic collaboration of actors in chains as well as the specific quality requirements to assure safe and healthy food as well as to target at the better usage of the global resources.

3.10.2 Naming, Addressing and Discovery Solutions

Naming, addressing and discovery of resources in the scope of SmartAgriFood are handled as follows:

- **Addressing**: Shared resources between stakeholders within the SmartAgriFood scope are based on unique URLs and URNs. These URIs can represent EPCs (as available on products, packaging material, etc.) and companywide used range of numbers.
- **Naming**: To discover data sources for a named IoT entities discovery different approaches are used. The most prominent technique is the use of an ONS server, which facilitates the functionality of a DNS server to resolve the URN of an entity to a set of URIs pointing to data sources and services. This standardized way of lookup has one big disadvantage: If someone has information about a given product, but the owner of the EPC is not willing or does not care to add it to an ONS server, other users might not be able to discover this information. To overcome this disadvantage SmartAgriFood extends this functionality by a high scalable P2P approach in which every user of the IoT-P2P-Network has the ability to attach information to the given entity.
- **Discovery**: To allow the discovery of resources SmartAgriFood is focusing on a semantic approach, which is based on the principles of Linked Data. This enables the decentralised storage of data, while allowing a highly flexible and powerful way of querying this data (SPARQL). On top of that the semantic storage of data also allows the

reasoning and therefore the creation of new knowledge about the given resources.

3.10.3 Migration Solution

The solution targeted by SmartAgriFood is not to replace existing applications within companies, but to integrate different existing solutions and increase the accessibility of available information currently "hidden" within. While this directly implies the need of converters between different formats, SmartAgriFood focus on the implementation of existing standards to reduce the amount of work to be done. Moreover SmartAgriFood offers the ability to not just only transfer pure data from one entity to another, but to enrich the data with the information about how they can be presented.

3.10.4 Scalability

The SmartAgriFood project targets at a highly scalable approach in terms of number of connected objects, information sources and related services. To achieve this SmartAgriFood doesn't build on a centralized storage and communication system, hence a single point of failure. Instead the project builds on a decentralized and open P2P architecture, which shall allow the easy integration of new systems and a failsafe (on peer level) operation.

3.10.5 Indicative Applications

The developed services are targeting a wide range of users beside the traders and retailers:

- Farmers.
- Software Development Companies.
- Associations.
- Consumers.
- Standardization bodies.
- Government Policy.
- Certification.
- App Developers.
- Food Chain Service Providers.
- Equipment Providers.

Also the intended IoT applications represent a heterogeneous set of different types regarding focus, targeted users and devices:

- End consumer apps.
- Tracking and Tracing.
- Asset management.
- Farm management.

3.11 CEN TC 225

3.11.1 Project Overview

CEN TC225 AIDC technologies are responsible for developing European standards for automatic identification technologies. It currently comprises of five working groups covering:

- ***Optical readable media***, which includes bar code and optical character recognition technologies.
- ***Security and data structures***, from the edge data capture through to the interrogator or reader device interface application.
- ***Automatic ID applications***, addressing potential pan-European AIDC applications.
- ***RFID, RTLS and on-board sensors***.
- ***Internet of Things*** – but with the specific focus on using the edge technologies addressed by CEN TC225.

There is also strong liaison status with JTC1 SC31 automatic identification and data capture techniques. CEN TC225 was in existence before this ISO committee and, on establishment of the ISO committee, handed over all its work items. The general means of operating at present is for ISO to take the lead in projects that are relevant internationally, but CEN TC225 takes the lead or sometimes works exclusively on standards relevant to Europe.

Traditionally, CEN TC225 has strong links with various European organisations that are responsible for implementing AIDC technologies. Formal liaisons currently exist with:

- ANEC – the European consumer voice in standardization.
- ECISS – European Committee for Iron and Steel Standardization.
- EDIFICE – Electronic Data Exchange Forum for Companies with interest in Computing and Electronics.
- EDMA – European Diagnostics Manufacturing Association.
- EFPIA – European Federation of Pharmaceutical Industries Association.
- EHIBCC – European Health Industry Business Communications Council.
- EUCOMED – European Confederation of Medical Devices Association.
- EUROCOMMERCE.
- GS1.
- IoT European Research Cluster (IERC).
- Odette – Organisation for Data Exchange by tele-transmission in Europe.
- UPU – Universal Postal Unit, EDI Development.

From the list of working groups and liaison organisations, it should be clear that CEN TC225 has a major role in the identification of "things" whether directly related to the Internet of Things or in legacy systems.

One of the challenges is making extensive use of legacy data systems in a way that can be suitable for the Internet. The liaison organisation GS1 has already achieved this by establishing its EPCglobal data structures. There are similar mechanisms in place for supporting legacy data. As part

of activities for the working group on the Internet of Things, these standardisation activities are being considered:

- To make some of the legacy data structures "resolvable".
- To undertake research of the identifiers developed by other CEN ICT technical committees and assess whether they are internet-ready or not.
- Work is likely to start soon on a traceability project of fish from capture at sea or farming right through the distribution chain to the retail and catering sectors.

CEN TC225 is currently in the middle of a major mandate project for the European Commission addressing RFID privacy and security aspects. There are a number of work items being developed. Some consider that this work is seen as a precursor to ensuring that privacy and security is taken into consideration for the Internet of Things.

3.11.2 Naming, Addressing and Discovery Solutions

CEN TC225 (and also JTC1 SC31) has to take a very specific approach for naming, addressing and discovery solutions. There are two fundamental pre-requisites that need to be met:

- Any scheme needs to be built on the existing legacy naming schemes.
- Any scheme suitable for the Internet of Things needs to support a long term migration from the legacy applications.

To put these points in perspective, market analysis figures from VDC Research Group for the year 2009 show that the annual market for bar code was $9.7 billion and for RFID $3.6 billion. 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, the majority of expenditure is on hardware but a combination of services and software (but not mentioned in the VDC analysis for bar code) also being quite significant.

The annual growth of the two technologies is now a little different, with 7% per annum for bar code and 14% per annum RFID. Using these figures, the current market size for bar code is $11.9 billion and $5.3 billion for RFID. The infrastructure behind such large markets has to be taken into account in any developments towards the Internet of Things.

Naming:
Many of the legacy naming systems are domain-specific. This gives rise to the potential problem of being able to distinguish between domains. One of the steps taken by ISO in its development of RFID standards was to use object identifiers to distinguish between domains and naming systems as a means to support legacy data identifiers. The new work within CEN TC225 should also help make the domain-based data elements resolvable as a complete OID structure. The GS1 EPC system has addressed naming by adding a serialised component to the existing code structure generally used for bar code. In addition, it supports some

entirely new code structures. All of these are defined in the Tag Data Standard[1] version 1.6.

It is a fallacy to assume that to achieve services associated with the Internet of Things that all bar code needs to migrate to RFID, and that all RFID needs to be serialised to the instance of a thing. One example is the use of QR Codes, or other 2D symbologies, to access particular services on the Internet. There are also many internet services supported with mobile phone Apps that work on the basis of scanning linear bar codes on food products to establish whether a particular food item is suitable or not for people with a particular allergy or health condition.

Addressing:
There are two fundamentally different aspects to addressing with the subject matter covered by CEN TC225. Individual bar codes and RFID tags are identified to their level of uniqueness considered suitable. In the case of GS1 EPC, object naming service protocol [RFC5134] is used. For some ISO related "things" the Handle system (www.handle.net) and one of its major applications the DOI (Digital Object Identifier) shows some potential (www.doi.org).

The other requirement for addressing is for communication to and from specific bar code and RFID devices. Here, the most likely long-term solution is the IPv6 address. There is a challenge within organizations where the need to migrate from Intranet IPv4 addresses has not always been recognized.

Discovery:
There are likely to be a multiplicity of discovery services given the heterogeneous nature of the "things" covered by CEN TC225, taking into account:

- The DOI system has a long-established means of supporting discovery services so any domains that use that will comply with those rules.
- Domains that opt for the Handle system will be able to use the DOI as a model to develop domain-specific semantics.
- Although GS1 has always had discovery services as part of its architecture, this standard is still in development and has not been published. However, GS1 does have specific application discovery services for certificate profiles and pedigree (for example, tracking individual packets of pharmaceutical products) exists as standards.
- There are many well-established domain-specific services already in place. For example, IATA baggage handling is able to track and trace items of luggage, with 14 million items being added on a daily basis, using existing bar code and RFID data capture. A bibliographic discovery service called WorldCat operated by OCLC[2] used by libraries currently supports just under 1.9 billion bibliographic records, with one search every second.

[1] http://www.gs1.org/gsmp/kc/epcglobal/tds/
[2] http://www.oclc.org/worldcat/

3.11.3 Migration Solution

The challenge with migration from legacy systems is the heterogeneous nature of the different applications, combined with the requirement to maintain the existing sector and organisation intranet solutions.

GS1 has "solved" some of the issues by having a migration plan from bar code to RFID, but this still lacks the significant take-up that was originally predicted during the RFID hype period about five years ago. It is also conceptually possible to use the GS1 non-serialised codes (typically represented in bar code) to migrate to some Internet of Things services.

The approach taken by ISO for migration to RFID is to use the object identifier structure to identify the domain, followed by a relative-OID that identifies the semantics of data. This is increasingly embedded in RFID standards and can even distinguish a specific sensor reading taken from an RFID tag. In the majority of cases, the application domain identifier remains associated with, but not integrated in, the OID structure. Three challenges remain:

- To make the key identifiers in legacy data systems identifiable, i.e. as part of the OID structure (as being addressed by one of the CEN TC225 work items).
- To encourage applications migrating to RFID to consider Internet of Things applications at an early stage of developing sector standards. Combined with this is the need for such sectors to address Internet of Things solutions in parallel to sector-based services. Often, the sector based services can be implemented much quicker – consider the delivery of boarding passes to print at home or to display on a mobile phone.
- Development of appropriate resolver systems – note the plural – that meet the specific security requirements of the different domains.

3.11.4 Scalability

Scalability is often considered as being a function of technology (there are examples elsewhere in this report). CEN TC225's long experience of AIDC technology over the past 22 years offers a different perspective.

For AIDC scalability is often a direct function of supply meeting demand requirements, and these are often addressed on a membership and/or subscription basis. Examples that we have already quoted justify this statement:

- GS1 is a membership organisation with a current global membership estimated at over 1.2 million businesses that generally pay an annual subscription.
- The OCLC WorldCat bibliographic database is based on membership.
- IATA's tracking of baggage handling is undertaken by its members (airports and airlines) and supported by a commercial system known as World Tracer.
- The Handle system requires the purchase of a prefix, which is domain specific and can be very low cost.

The net effect of all of this is that the network of services to support the system grows organically as required. In addition, enhancements to the system are addressed by the community and for the community.

3.11.5 Indicative Applications

These have been addresses in previous sections. It is important to understand that the applications identified above are no more than a sample. Because of the way AIDC applications are implemented, the scale continues to evolve, for example, in 1973, what is now the GS1 system had less than 100 members.

Other enablers are the development of procedures, support tools and eventually standardisation. For example, since being established in 1996, the DOI system now has 60 million registered documents, with this procedure supported by 10 registration authorities. The DOI requires supporting browsers and browser tools; this includes support by Firefox, JavaScript, and more recently by Google Chrome[3]. The DOI is now defined in ISO 26324:2012[4], achieving the accolade of an international Standard.

[3] http://www.doi.org/tools.html

[4] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43506

4. Taxonomy of Naming, Addressing and Discovery Schemes

4.1 Overview

Earlier paragraphs have provided comprehensive descriptions of the naming, addressing and discovery schemes developed by eleven (11) IERC IoT projects. The schemes are characterized by heterogeneity in terms of the mechanisms employed, the standards used, but also in terms of their maturity. The latter is due to the fact that some projects are in their early stages, while others close to the end of their lifetime. Despite this heterogeneity, one can identify commonalities between the various projects, both in terms of the addressing/discovery functionalities that they provide and in terms of the technologies (and standards) they are based on.

4.2 Taxonomy of naming and addressing schemes

The presented IERC projects adopt a variety of existing naming and addressing schemes, as illustrated in Table 1. Existing schemes in the area of naming include DNS and ONS used in conjunction with IP addresses (IPv4/IPv6) and EPC/URNs respectively, as well as URI/RDF resource descriptions used in conjunction with semantic web approaches to resource representations. However, there are also projects (e.g., ebbits), which have introduced their own naming and addressing schemes (i.e. on the basis of virtualization and custom addressing schemes).

There is a certain trade-off balance associated with the selection of existing naming/addressing schemes and the introduction of new ones. In particular, the use of existing schemes guarantees scalability and exploits the existing base of ICOs that already possess such addresses. Note that in the scope of some specific classes of IoT solutions (e.g., RFID/AutoID as addressed by CEN TC 225 and SmartAgriFood) there are already mature and extensively tested solutions. On the other hand the design of a new naming and addressing scheme holds the promise to better fulfil IoT requirements (e.g., in terms of capturing ICO classes and their relationships). Furthermore, new solutions does not suffer from the limitations of existing naming/addressing schemes (e.g., in terms of semantic richness), which were originally designed for other purposes. In several cases projects had to enhance or deviate from the capabilities of existing schemes in order to support their desired IoT functionalities (e.g., the case of the use of ONS in SmartAgriFood).

Projects / Schemes	BUTLER	ebbits	GAMBAS	iCore	IOT-A	IoT@Work	IoT.est	IoT6	OpenIoT	SmartAgriFood	CEN TC225
DNS / IPv6								X			
DNS / IPv4 & IPv6	X				X						
ONS / URNs/ EPC										X	X
DOI											X
Virtual Overlay Addresses		X									
URI/RDF (W3C SSN Compliant)			X					X	X		
URI/RDF (Other Semantic Ontologies)	X			X	X	X	X				

Table 1: Naming and Addressing schemes used/promoted by the various IERC projects contributing to AC02

Note that all projects make provision for migrating from ICOs and ICO services to the naming and addressing solutions that they propose. Most of the migration solutions include (one or more of the following):

- Some proxy/gateway solution for adapting non-compliant sensors / ICOs to the target naming and addressing system (e.g., IoT6, IoT-A, OpenIoT, GAMBAS, ebbits).
- Services (such as RESTFul APIs) for registering sensors / ICOs to the target solution (e.g., IoT@Work, ebbits, GAMBAS).
- Tools that could facilitate the sensor annotation and registration processes (e.g., ebbits, IoT@Work, OpenIoT).
- Standards (e.g., GS1 standards) that prescribe how the migration can be implemented for certain classes of identifiers.

In general, migration must be automatic (plug n' play) and effortless as possible, in order to allow for large scale applications (i.e. in terms of the number of ICOs involved).

4.3 Taxonomy of discovery schemes

Most of the IERC projects presented above implement discovery schemes for IoT resources, which are in most cases relating to the naming and addressing schemes outlined above (e.g., DNS related schemes for IP addresses, SPARQL/Semantic Schemes for RDF-compliant resources). Table 2 presents an overview of the various discovery schemes. Note that

the majority of the project promote semantic approaches based on semantically annotated resources, the use of ontologies and the use of SPARQL, as a means of supporting reasoning and boosting the intelligence of the discovery mechanisms. Among the class of the projects that adopt or promote semantic approaches, different techniques and standards are used. Some projects rely on the results of the W3C SSN group (e.g., GAMBAS, OpenIoT, IoT6) and its associated ontology, while others (e.g., ebbits, IoT@Work) create their own ontologies. Furthermore, two of the projects (i.e. SmartAgriFood, OpenIoT, GAMBAS) promote the use of LinkedData in order to enable IoT applications to link/access to other data of the LOD cloud. Also, IoT-A suggests the adoption/use of federation-based approach (based on hierarchical clustering) as means to discovering semantically annotated resources.

Projects / Schemes	BUTLER	ebbits	GAMBAS	iCore	IOT-A	IoT@Work	IoT6	OpenIoT	SmartAgriFood	CEN TC225
Attribute-based Discovery		X								
Geo-Discovery					X					
Semantic Web Approach RDF / SPARQL	X	X	X	X	X	X	X	X	X	
DNS-SD/mDNS							X			
DOI										X

Table 2: Discovery schemes used/promoted by the various IERC projects contributing to AC02

Except for the semantic based approaches, IoT-A underlines the importance of geo-discovery schemes given the importance of sensors location in the discovery process. However, geo-discovery approaches can be implemented on the basis of semantic schemes (e.g., through SPARQL and SSN). IoT6 is also exploring DNS based approaches, mainly due to its adherence to IPv6 addressing. As another example, ebbits is implementing its own discovery approach for a more unbound attribute-based discovery. However, ebbits supports also semantic discovery techniques based on SPARQL, thereby reinforcing the semantic trend which is evident in Table 2.

5. Main Issues and Outlook for Future AC02 Work

The main objective of AC02 is to provide a reference scheme for naming, addressing and discovery, along with best practices associated with the use of the proposed schemes across different application contexts. On the basis of the presented schemes, their common properties and differences, it is possible to identify some key issues that should be taken into account during the course of the development of the above-mentioned reference scheme and related best practices. These issues could guide the scope and functionalities of the target solutions and best practices.

One of these issues concerns the need and practicality of building an integrated and unified naming, addressing and discovery solution, which support all existing ICOs and IoT applications. Such a solution could possess all the desired properties of IoT applications/solutions (e.g., discovery/filtering of ICO, filtering/discovery of ICO data, support for physical and virtual entities and their relationships etc.), but would require legacy ICO systems to migrate to the solution towards global IoT applications. As an alternative to a single solution, the reference scheme of the AC02 activity could focus on the specification of a federating solution emphasizing the linking of existing naming/addressing and discovery solutions, rather than their full migration to the new unified solution. A federating solution should focus on the co-existence and interoperability of legacy and emerging solutions in the scope of IoT applications, rather than requiring their re-engineering towards adapting to a unified solution.

Along with the nature of the reference scheme (i.e. integrated or federated), the ability and feasibility of a globally accessible and available solution should be explored. A globally available solution should provide the means for migrating from existing solutions. Almost all IERC projects make provisions for migration from legacy solutions to the schemes that they introduce. Note that in most cases migration requires some additional development and deployment effort (e.g., programming/adaptation).

Another issue concerns the important of semantic approaches, notably as means to achieve semantic interoperability and enable reasoning. The taxonomy has revealed a tendency of several projects to adopt semantic web techniques as a means to injecting reasoning and intelligence to their systems. Furthermore, several projects have acknowledged the importance of reasoning on the basis of geo-location (e.g., geo-discovery approach), which however can be subsumed by the use of semantic techniques. Nevertheless, there are also projects that dispose with legacy discovery mechanisms that do not comprise semantics. The latter approach guarantees (in several cases) higher performance and compliance to legacy IoT instantiations (e.g., RFID/WSN). Hence, AC02 needs to explore the needs and merit to adopt semantics as part of its

core reference scheme. Another issue to be considered is whether the semantic part of the solution should be a mandatory part of the reference scheme.

As another consideration, there is also a need to think on whether the reference solution should deal with temporal requirements and the handling/logging of historic data about an ICO. This is a key to understanding and discovering the evolution of the ICO as it changes state (e.g., business processes, application contexts relationship with other objects etc.), which is useful in several IoT applications (e.g., traceability). Along with temporal requirements, there is also a need to consider/explore the relevant importance of different requirements (including support for mobility, ubiquitous access, interoperability, global access) for the specification of a reference naming/discovery scheme. All these requirements are important for the successful deployment of non-trivial IoT applications and should therefore be considered in the scope of the reference scheme and best practices explored in this activity chain.

The above considerations have been taken into account in order to create a relevant questionnaire (Appendix 1), which will be provided to IERC projects in order to elicit requirements associated with the reference naming, addressing and discovery scheme to be investigated in AC02 (along with relevant best practices for deploying naming/discovery IoT solutions).

6. Conclusions

This document is the first deliverable of the second activity chain (AC02) of the IERC cluster of IoT research projects. The document has been written with contributions of eleven different IoT projects, which work on various research aspects of IoT technologies, while dealing with a multitude of different applications. As the first deliverable of AC02 it includes a short (yet comprehensive) presentation of the main research directions undertaken by the contributing projects in the areas of IoT naming, addressing and discovery. Furthermore, the deliverable classifies the various addressing and discovery schemes based on a variety of criteria, including their compliance to existing and emerging standards, as well as their semantic power (i.e. based on adoption of semantic web schemes).

The taxonomy of the naming and addressing schemes used in the various projects has revealed that the majority of the projects make use of existing naming and addressing standards including URIs, EPCs/URNs, as well as IPv6 addresses. A lesser number of projects have opted for new customer naming/addressing schemes (e.g., based on custom UUID). As far as discovery is concerned, the taxonomy revealed a clear tendency towards the adoption of semantic web technologies (i.e. RDF for ICO modelling and representation, SPRQL for querying) towards intelligent discovery of IoT resources. Furthermore, geo-discovery has already been underlined as being an important feature of most discovery schemes.

Most of the projects have studied the process for migrating other sensors and ICOs to their proposed addressing and discovery infrastructures. In most cases these migration processes require additional adaptation effort, such as the implementation of proxy mechanisms for certain sensor classes, as well as the semantic enrichment/annotation of existing sensors. To alleviate this process, several all projects are providing easy to use RESTful services and associated tools.

In addition to providing a bird's eye of view on the project's IoT research on addressing and discovery, the present deliverable has also identified a set of main issues that are associated with the specification of reference scheme for IoT addressing/discovery, which is one of the future goals of the activity chain. On the basis of these issues, a questionnaire has been formulated, as a means of soliciting feedback on the relevant importance of these issues in the scope of a reference scheme. Such feedback will be useful in designing the reference scheme of the project. As part of defining such a reference scheme the possibility of integrating diverse naming and integration solutions should be explored, along with relevant interoperability solutions. Along with a reference scheme, the members of the activity chain will also strive to provide a set of best practices associated with the deployment and use of different IoT naming, addressing and discovery schemes in a variety of application contexts. These best practices are expected to reflect the projects' practical experiences from using the presented schemes in the scope of realistic IoT applications/deployments.

References

[Balakrishnan2003] H. Balakrishnan, M. Kaashoek, D. Karger, R. Morris, I. Stoica, "Looking up data in P2P systems", Communications of the ACM 46 (2) (2003) 43–48.

[Bröring11] Arne Bröring, Johannes Echterhoff, Simon Jirka, Ingo Simonis, Thomas Everding, Christoph Stasch, Steve Liang and Rob Lemmens, «New Generation Sensor Web Enablement», Sensors 2011, 11(3), 2652-2699; doi:10.3390/s110302652

[Calbimonte11] Jean-Paul Calbimonte, Hoyoung Jeung, Oscar Corcho and Karl Aberer, «Semantic Sensor Data Search in a Large-Scale Federated Sensor Network», in the Proc. of The 4th International Workshop on Semantic Sensor Networks 2011 (SSN11), 23-27 October 2011, Bonn, Germany

[Cheshire2011DNS-SD] S. Cheshire, and M. Krochmal. "DNS-Based Service Discovery", IETF Zeroconf Working Group, www.zeroconf.org/ and www.dns-sd.org/, draft-cheshire-dnsext-dns-sd.txt, 2011.

[Cheshire2011mDNS] Cheshire, S. and M. Krochmal, "Multicast DNS", draft-cheshire-dnsext-multicastdns-15 (work in progress), December 2011.

[Echterhoff10] Echterhoff, J. OGC Implementation Standard 09-001: SWE Service Model Implementation Standard; Open Geospatial Consortium: Wayland, MA, USA, 2010

[Heath11] Tom Heath and Christian Bizer (2011) Linked Data: Evolving the Web into a Global Data Space (1st edition). Synthesis Lectures on the Semantic Web: Theory and Technology, 1:1, 1-136. Morgan & Clay-pool.

[Jara2012] A. J. Jara, M. A. Zamora and A. F.Skarmeta.: GLoWBAL IPv6: An adaptive and transparent IPv6 integration in the Internet of Things, Mobile Information, IOS Press, ISSN: 1574-017x, 2012.

[Jirka09] Jirka, S.; Bröring, A.; Stasch, C. Discovery Mechanisms for the Sensor Web. Sensors 2009, 9, 2661-2681

[Karnstedt12] Marcel Karnstedt, Kai-Uwe Sattler, Manfred Hauswirth: Scalable distributed indexing and query processing over Linked Data. J. Web Sem. 10: 3-32 (2012)

[Klyne2004] G. Klyne, J. J. Carroll, "Resource Description Framework (RDF): Concepts and Abstract Syntax", 2004. http://www.w3.org/TR/rdf-concepts/.

[Montenegro2007] G. Montenegro, N. Kushalnagar, J. Hui, D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC4944, September 2007.

[Pfisterer11] Dennis Pfisterer, Kay Römer, Daniel Bimschas, Oliver Kleine, Richard Mietz, Cuong Truong, Henning Hasemann, Alexander Kröller, Max Pagel, Manfred Hauswirth, Marcel Karnstedt, Myriam Leggieri, Alexandre Passant, Ray Richardson: SPITFIRE: toward a semantic web of things. IEEE Communications Magazine 49(11): 40-48 (2011).

[Prudhommeaux2008] E. Prud'hommeaux, A. Seaborne, "SPARQL Query Language for RDF", http://www.w3.org/TR/rdf-sparql-query/, 2008.

[Renz07] J. Renz and B. Nebel. Qualitative spatial reasoning using constraint calculi. In M. Aiello, I. Pratt-Hartmann, and J. van Benthem, editors, Handbook of Spatial Logics, pages 161-215. Springer-Verlag, 2007.

[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.

[Shelby2011] CoRE Resource Directory, Internet Draft, Z. Shelby, Sensinode, S. Krco, Ericsson, June 27, 2011.

[Stoica2001] I. Stoica, R. Morris, D. Karger, M. Kaashoek, H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for internet applications", in: Proceedings of the 2001 SIGCOMM Conference, San Diego, CA, USA, August 2001, pp. 149–160.

[Taylor2011] Kerry Taylor, «Semantic Sensor Networks: The W3C SSN-XG Ontology and How to Semantically Enable Real Time Sensor Feeds», 2011. Semantic Technology Conference, June 5-9, San Francisco CA, USA

[Zamora2010] M.A. Zamora, J. Santa, A.G. Skarmeta, Integral and networked home automation solution towards indoor ambient intelligence, Pervasive Computing, 2010.

Appendix 1 – Questionnaire Feedback towards a reference addressing and discovery scheme for IoT

Please fill-in your contact details
Your Name:
Your Title:
Your Organization:
e-mail:
Phone Number (optional):
Address (optional):
Websites (optional):
FP7 IERC Project(s) that you are involved:

1. What is your role/involvement within IoT projects?

Role / Involvement	***Tick***
Integrator of IoT Systems/Applications	
Provider of IoT Solutions	
Vendor of IoT Systems/Products	
End-user of IoT Systems/Applications	
Business Analyst of IoT Solutions	
Other (Specify): _____	

2. What kind of application/solutions do you deploy:

IoT Application Domain	***Tick***
Manufacturing	
Logistics / Supply Chain Management	
Energy Management	
Smart Cities	
Retail	
Geolocation Applications	
Ambient Assisted Living	
Other (Specify): _____	

3. Which IoT addressing solution(s) do you use / deploy for your IoT Systems?

Solution/Technology	***Tick***
IPv6	
EPC/BarCode/URN	
URI/RDF	
SLP	
DOI	
Other (Specify): _____	

4. Which IoT discovery solution(s) do you use / deploy for your IoT Systems?

Solution/Technology	***Tick***
Semantic Web Solution / SPARQL	
DNS Solution	
ONS Solution	
Other (Specify): _____	

5. Which criteria do you (commonly) use/employ in order to discover IoT Resources?

Criteria	***Tick***
Sensors and Internet Connected Objects (ICO) Location	
Sensor and ICO Type/Class	
Sensor and ICO Capabilities	
Sensor and ICO Deployment (e.g., business context)	
Sensor and ICO Utility (e.g., cost, data volume)	
Other (Specify): _____	

6. Which criteria do you (commonly) use/employ in order to discover/filter IoT data?

Criteria	***Tick***
Location	
Time (temporal characteristics)	
Deployment Context / Business Context	
Other (Specify): _____	

7. A reference (blueprint) scheme for IoT addressing and discovery should:

Options	***Tick***
Comprise brand new addressing and discovery schemes (tailored to IoT applications/services)	
Be based on the federation of existing addressing and discovery schemes	
Other (Specify): _____	

8. Provide free comments on what a reference (blueprint) scheme for IoT addressing and discovery should provide:

_____

_____

_____

_____

9. Should discovery schemes for IoT resource integrate semantic capabilities?

Definitely No	Likely No	Indifferent	Yes	Definitely Yes
1	2	3	4	5

10. Grade the (relevant) importance of the scalability of the reference scheme (in terms of numbers of users, devices and their interactions):

Very Low	Low	Medium	High	Very High
1	2	3	4	5

11. Grade the (relevant) importance of the interoperability support of the reference scheme (in terms of annotation and metadata) in order to handle the heterogeneity of devices, platforms, virtual sensors etc.:

Very Low	Low	Medium	High	Very High
1	2	3	4	5

12. Grade the (relevant) importance of discovering data based on temporal requirements and constraints etc.:

Very Low	Low	Medium	High	Very High
1	2	3	4	5

13. Grade the (relevant) importance of reference scheme's support for Ubiquity/Mobility towards supporting roaming, ad-hoc access, service continuity etc.:

Very Low	Low	Medium	High	Very High
1	2	3	4	5

14. Grade the (relevant) importance of the reference scheme's support for global access/discovery of IoT resources:

Very Low	Low	Medium	High	Very High
1	2	3	4	5

15. Provide any free comments on properties/characteristics of the reference scheme:

_____

_____

_____

_____