COSMOS

Cultivate resilient smart Objects for Sustainable city applicatiOnS

Grant Agreement Nº 609043

D8.2.1 Report on roadmap and standardization activities (Year 1)

WP8: Exploitation, Dissemination, Roadmap and Standardisation

Version: 1.5

Due Date: 30/09/2014

Delivery Date: 15/02/2015

Nature: Report

Dissemination Level: Public

Lead partner: SIEMENS

Authors: Bogdan Târnaucă (Siemens), Leonard Piţu (Siemens), Panagiotis Bourelos (NTUA), Adnan Akbar (UNIS), Paula Ta-Shma (IBM), Juan Sancho (ATOS)

Internal reviewers: Francois Carrez (UNIS), Andrea Rossi (ATOS)

www.iot-cosmos.eu

SEVENTH FRAMEWORK PROGRAMME

The research leading to these results has received funding from the European Community's Seventh Framework Programme under grant agreement n° 609043

Version Control:

Version	Date	Author	Author's Organization	Changes
0.1	15/09/2014	Bogdan Târnaucă	SIEMENS	First draft of the document.
0.2	21/09/2014	David Jorquera	ATOS	Contribution to standardization activities
0.3	17/10/2014	Panagiotis Bourelos	NTUA	Adding input in chapter 2, 3.1, 4.1.4 and 4.3.1.
0.4	17/10/2014	Paula Ta-Shma	IBM	Contribution to standardization actvities
0.5	17/10/2014	Adnan Akbar	UniS	Contribution to stakeholder description and relevant organizations
0.6	05/11/2014	Bogdan Târnaucă	SIEMENS	Ready for review
0.7	05/11/2014	Francois Carrez	UniS	Reviewed document
1.0	10/11/2014	Bogdan Târnaucă	SIEMENS	Final form
RE_SUBMIT 1.1	02/02/2015	Panagiotis Bourelos	ICCS/NTUA	Revisions after the reviewer's comments. Adding content into 4.3.1 and 4.5.1
RE_SUBMIT 1.2	04/02/2015	Paula Ta-Shma	IBM	Minor addition to respond to Bogdan's comment
RE_SUBMIT 1.3	12/02/2015	Juan Sancho	ATOS	ATOS 4.5.3 update + misc. changes
RE_SUBMIT 1.4	13/02/2015	Bogdan Târnaucă	Siemens	Ready for the review
RE_SUBMIT 1.5	14/02/2015	Andrea Rossi	ATOS	Final Review

Table of Contents

1 Introduction

1.1 About this deliverable

An important goal for a project is to create acceptance among end-users and stakeholders. In order to achieve this, it is important to identify and perform standardization activities to increase the relevance and impact of the project outcome.

As a result, COSMOS plans to contribute to the most important European and International standardization organizations such as: *World Wide Web Consortium* (W3C) [W3C1], *European Telecommunications Standards Institute* (ETSI) [ETSI1], *International Organization for Standardization* (ISO) [ISO1], *International Telecommunication Union* (ITU) [ITU1], *The Internet Engineering Task Force* (IETF) [IETF1]. Experience from other projects as well as the trends in the field will be considered along with existing or proposed standards.

This document presents the activities taken in this direction and lists the foreseen steps considered in order to increase acceptance and relevance of the COSMOS project outcomes.

1.2 Document structure

The document is structured as follows. The key concepts of COSMOS, as well as the foreseen outcomes, are briefly described in Chapter 2. This is followed by a stakeholder analysis in Chapter 3 where relevant academic, industrial and standardization organizations are presented. Chapter 4 is dedicated to standardization activities and presents a number of standards to observe and consider, the contribution to open-source projects and other relevant organizations. A summary is provided in Chapter 5.

This is a public deliverable, therefore is meant to be read as a stand-alone document without prior knowledge about the project goals and proposed solution or about relevant standardization bodies and standards. As a result, some content from the projects Description of Work document is reiterated along with a brief description of the relevant standardization bodies and standards.

2 COSMOS concepts and expected outcomes

2.1 Key concepts of COSMOS

COSMOS aims at developing an IoT framework where:

- Things are able to learn based on others experiences.
- Situational knowledge acquisition and analysis mechanisms make things aware of conditions and events affecting their behavior.
- Adaptive selection approaches facilitate to manage the uncertainty and volatility introduced due to real-world dynamics.
- Decentralized management mechanisms in IoT based systems allowing applications to exploit increasing amount of interconnected things.
- Socially-enriched coordination will consider the role and participation scheme of things in and across networks.
- Management decisions and runtime adaptability will be based on things security, trust, administrative, location, relationships, information, and contextual properties.
- End-to-end security and privacy, with hardware-coded security approaches for security and privacy on storage

2.2 Foreseen outcomes

COSMOS will provide tools and mechanisms to harvest and analyse data, that lead to extended object semantics and specific property/data mappings, which can be persistently stored. Additionally the reliability and volatility of the various devices will be addressed by developing methods to dynamically link Thing attributes, so as to promote mechanisms for Thing replacement where that is deemed necessary and provide reliable identification and reputation patterns and strategies for the adaptive selection of Things.

COSMOS will also provide mechanisms for identifying similar Things, exchange relevant experiences and analyse network states. In addition, safeguarding data privacy will be accomplished, by both hardware and software approaches to security in both communication of Things as well as storage of data. As for privacy, software implemented methods will ensure the filtering of sensitive data. This will be achieved by the use of software Privelets, as developed by COSMOS.

The COSMOS approach to handling large volumes of data, which are generated by the real time applications, is to develop new mechanisms for data aggregation, interplay of computation and storage, which lead to the approaches of computation, either close to the source, or close to the storage. Also, the platform promotes the use of data filtering and data reduction. Also network inefficiencies, stemming from networking conditions and communication inefficiencies, including geographic isolation as well as ownership distribution, will be dealt with, by implementing social patterns and analysing social relationships, in order to predict Thing communication and identify critical elements, like Thing network centrality, stemming from the social characteristics analysis, in order to allow decentralized self-management of Things. Finally, mechanisms will be provided, which allow Things to react in an autonomous and predictive way.

3 Stakeholder analysis

We have identified the following categories of stakeholders relevant for both the design and development stage of the project as well as for the exploitation. Stakeholders are relevant for drawing the requirements of the COSMOS platform or acting as a reference points. They are also important since the proper positioning of the project increases the chances of a better exploitation of the results.

3.1 Research and academia stakeholders

The *Global Standards Initiative on Internet of Things* (IoT-GSI) [ITU2] promotes a unified approach in ITU-T for development of technical standards (Recommendations) enabling the Internet of Things on a global scale. ITU-T Recommendations developed under the IoT-GSI by the various ITU-T Questions - in collaboration with other standards developing organizations (SDOs) – will enable worldwide service providers to offer the wide range of services expected by this technology. IoT-GSI also aims to act as an umbrella for IoT standards development worldwide.

The *World Wide Web Consortium* (W3C) [W3C1] has initiated the *Semantic Sensor Networks Incubator Group* (SSN-XG) [SSN-XG1] to develop the *Semantic Sensor Network* (SSN) ontology which can model sensor devices, systems, processes, and observations. The Incubator Group has now transitioned into the Semantic Sensor Networks Community Group.

The OGC's *Sensor Web Enablement* (SWE) standards enable developers to make all types of sensors, transducers and sensor data repositories discoverable, accessible and useable via the Web. SWE standards are developed and maintained by OGC members who participate to the OGC Technical Committee's Sensor Web Enablement Working Group.

IEEE P2413 [P2413], would form a framework for interoperability among connected devices and related applications in home automation, industrial systems, telematics and all other sectors that are expected to use IoT in the coming years. While leaving room for differences across those industries, the standard would allow for sharing of data across IoT systems. The P2413 Working Group, doesn't want to replace existing IoT groups. Rather it aims to create a standard architecture so IoT systems for all industries can work together. So far the most advanced contributions to the P2413 group are heavily inspired from the IoT Architectural Reference Model as released by the IoT-A project; In particular Siemens is pushing their "customised" version of the ARM to this group.

3.2 Industrial stakeholders

The following sections describe the relation of COSMOS with different industrial stakeholders.

3.2.1. Service providers

Service providers are always interested in solutions, both hardware and software, which support innovative services and whose time to market is reduced. COSMOS will integrate components which will favour not only quick application development and deployment but also that of monitoring and adaptation capabilities, critical for providing high quality reliable services.

3.2.2. Device manufacturers

One of the challenges, which device manufacturers face when developing devices meant to be integrated by solution integrators, is in providing ready-to-use hardware platforms with minimum development effort. The trend is to adhere to well-known standards or to support emergent ones, in order to provide an additional selling point in comparison to their competitors. COSMOS will ease application development and hardware integration by proving facile means of exposing and using data from sensors and actuators.

Also, through the hardware coded security features COSMOS should appeal device manufactures which are interested in incorporating security features into their devices.

3.2.3. Mobile network operators

VEs are exposed using both fixed and mobile internet connections, often in harsh environments from both the traffic and accessibility perspective. Access to VE data, managing the VE network and its load on large scale deployments is only possible when the support between the network operators and COSMOS platform providers is mutual.

Network operators could also exploit the potential of developing new services for their subscribers by using COSMOS VE data exchange mechanisms. Data can be exchanged either through the message bus communication channels or through the semantically annotated REST interfaces.

3.2.4. Solution Integrators

Solution integrators are among the stakeholders who are interested in both hardware as well as software aspects of a solution. From the hardware perspective one of the things which is often considered is how software is deployed on the devices. Hardware needs to be easily deployed and configured, with minimum development effort. The same applies nowadays to software; integrators prefer off-the-shelf software packages which only require little integration effort and less development. COSMOS intendd to facilitate such integration since VEs, once deployed, should be easily used in a variety of scenarios with a minimum effort.

On the other hand, COSMOS should be aware of the requirements facing solution integrators since they are those in close relation with software developers, customers or service providers.

3.2.5. Software developers

Software developers are involved in writing the code exposing the VEs as well as integrating them into applications or other software components. It is therefore crucial that interface specifications, design patterns, and other reusable components provided by COSMOS are well described, easy to understand and to implement and , finally, that additional development effort is reduced as much as possible.

Direct feedback from software developers is needed in order to align COSMOS development with the developers' expectations.

3.3 Standardization bodies

This section describes the standardization bodies whose activities are relevant to COSMOS. It includes the descriptions and the missions of these organizations as they state them as well as the possible impact to the work performed in COSMOS or to the existing and new standards.

3.3.1. W3C

W3C is an international community that develops standards, protocols and guidelines to support the long-term growth of the Web. W3C has built several working groups to write technical reports which are used to promote the development of standards based on community consensus. These groups facilitate the exchange of innovative ideas and concepts.

COSMOS will follow the work of Semantic Web Interest Group which includes W3C Members and non-Members targeting the development of innovative Semantic Web applications based in W3C's Semantic Web technologies (RDF, OWL, SPARQL, etc.).

W3C also includes a group, Semantic Sensor Networks Incubator group (SSN-XG), the goal of which is to develop a sensor description ontology and to provide guidelines for semantic mark-up in Semantic Sensor Networks. A result of the group's work is SSN-XG, a sensor ontology that describes sensors from a device, platform and operational perspective.

3.3.2. IETF

The *Internet Engineering Task Force* (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual.

The process of creating an Internet Standard is straightforward: a specification undergoes a period of development and several iterations of review by the Internet community and revision based upon experience, is adopted as a Standard by the appropriate body and eventually published. In practice, the process is more complicated, due to (1) the difficulty of creating specifications of high technical quality; (2) the need to take into consideration the interests of all of the affected parties; (3) the importance of establishing widespread community consensus; and (4) the difficulty of evaluating the utility of a particular specification for the Internet community.

The goals of the Internet Standards Process are:

- technical excellence;
- prior implementation and testing;
- clear, concise, and easily understood documentation;
- openness and fairness; and
- timeliness.

The IETF Constrained RESTful environments (CoRE) Working Group has done the major standardization work for the REST protocol. In order to make it suitable to IoT and M2M applications, various new functionalities have been added. The core of the protocol is specified in RFC 7252 [RFC7252], important extensions are in various stages of the standardization process

Constrained Application Protocol (CoAP) is a software protocol intended to be used in very simple electronics devices that allows them to communicate interactively over the Internet. It is particularly targeting small low power sensors, switches, valves and similar components that need to be controlled or supervised remotely, through standard Internet networks. CoAP is an application layer protocol that is intended for use in resource-constrained internet devices, such as WSN nodes. CoAP is designed to easily translate to HTTP for simplified integration with the web, while also meeting specialized requirements such as multicast support, very low overhead, and simplicity. Multicast, low overhead, and simplicity are extremely important forIoT and M2M devices, which tend to be deeply embedded and have much less memory and power supply than traditional internet devices have. Therefore, efficiency is very important. CoAP can run on most devices that support UDP or a UDP analogue.

IETF CoRE - Framework for resource-oriented applications intended to run on constrained IP networks

The following IETF working groups has been identified as relevant for COSMOS:

- **roll:** Routing Over Low power and Lossy networks;
- **dice:** DTLS in Constrained Environments (DTLS stands for Datagram Transport Layer Security);
- **core:** Constrained RESTful Environments;
- **6lo:** IPv6 over Networks of Resource-constrained Nodes;
- **ace:** Authentication and Authorization for Constrained Environments;
- **homenet:** Home Networking;
- **6man:** IPv6 Maintenance (6man);
- **dnssd:** Extensions for Scalable DNS Service Discovery.

3.3.3. ITU-T

The *ITU Telecommunication Standardization Sector* (ITU-T) is one of the three sectors (divisions or units) of the *International Telecommunication Union* (ITU); it coordinates standards for telecommunications.

The following relevant groups have been identified:

- Internet of Things Global Standards Initiative (IoT-GSI);
- Joint Coordination Activity on Internet of Things (JCA-IoT);

  - networks aspects of identification of things, and ubiquitous sensor network (USN);
  - maintains list of approved IoT international standards and work in progress;

- ITU-T Study Group 17 - security of applications and services for the Internet of Things (IoT);
- ITU-T Focus Group on Smart Sustainable Cities (FG-SSC);
- Open platform for smart city stakeholders, non-governmental organizations, ICT organizations and consortia to exchange knowledge in the interests of identifying the standardized frameworks needed to support the integration of ICT services in smart cities.

3.3.4. OPC Foundation

OPC [OPC1]is the interoperability standard for the secure and reliable exchange of data in the industrial automation space and in other industries. It is platform independent and ensures the seamless flow of information among devices from multiple vendors. The OPC Foundation is responsible for the development and maintenance of this standard.

OPC technologies were created to allow information to be easily and securely exchanged between diverse platforms from multiple vendors and to allow seamless integration of those platforms without costly, time-consuming software development.

Initially, the OPC standard was restricted to the Windows operating system. As such, the acronym OPC was borne from OLE (Object Linking and Embedding) for Process Control. These specifications, which are now known as OPC Classic, have enjoyed widespread adoption across multiple industries, including manufacturing, building automation, oil and gas, renewable energy and utilities, among others.

Along with the introduction of service-oriented architectures in manufacturing systems came new challenges in security and data modelling. The OPC foundation developed the OPC UA specifications in order to address these needs; They did, at the same time, provide a feature-rich technology open-platform architecture that was future-proof, scalable and extensible.

These new OPC specifications provide a lot of similarities with the concepts and applications from the IoT field therefore COSMOS will explore the possibility to bridge these two domains (industrial and IoT oriented) in order to increase their interoperability.

3.3.5. ETSI

The *European Telecommunications Standards Institute* (ETSI), produces globally-applicable standards for *Information and Communications Technologies* (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies.

ETSI is a not-for-profit organisation which bridges manufacturers, network operators, national administrations, service providers, research bodies, user groups and consultancies. It has more than 750 ETSI member organizations drawn from 63 countries world-wide.

The organization has standardised the *Global System for Mobile communications* (GSM) cell phone system and is currently working on European telecommunication standards such as HiperLAN or TETRA.

One of ETSI's Technical Committees is TC M2M which is focused on machine-to-machine communication with limited or no human intervention. The topics of the TC include the middleware layer with various application service and specific business-processing engines for any devices capable of replying to requests for data.

COSMOS will explore the concepts and ideas proposed by TC M2M in the context of VE interactions since VEs are expected to enjoy lot of autonomy.

4 Standardization activities

4.1 Standards to observe and consider

The following sections list a number of standards which are going to be observed and considered in the development of Cosmos, besides those already mentioned. These descriptions are mainly excerpts from the publicly available descriptions and contain the key aspects which are relevant for COSMOS. The standards are highly relevant for Cosmos development and this list will be revised if needed during the project.

4.1.1. IEEE P2413 – Standard for an Architectural Framework for the IOT

The architectural framework defined in this standard will promote cross-domain interaction, aid system interoperability and functional compatibility, and further fuel the growth of the IoT market.

The adoption of a unified approach to the development of IoT systems will reduce industry fragmentation and create a critical mass of multi-stakeholder activities around the world.

This standard defines an architectural framework for the Internet of Things (IoT), including descriptions of various IoT domains, definitions of IoT domain abstractions, and identification of commonalities between different IoT domains.

As said earlier, current discussion are driven by the work achieved by the FP7 IoT-A project. Indeed COSMOS is already following the Architectural Reference Model [ARM] and related methodology.

4.1.2. ISO 37120 – Sustainable development of communities

This standard defines and establishes methodologies for a set of indicators to steer and measure the performance of city services and quality of life [ISO37120]. It follows the principles set out and can be used in conjunction with the under development standard *ISO 37101 - Sustainable development in communities - Management systems - General principles and requirements*, when published, and other strategic frameworks.

ISO 37120:2014 is applicable to any city, municipality or local government that undertakes to measure its performance in a comparable and verifiable manner, irrespective of size and location.

4.1.3. ISO 27001 - Information technology— Security techniques — Information security management systems — Requirements

An *Information Security Management System* (ISMS) is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.

ISO/IEC 27001 [ISO27001] is the best-known standard in the family providing requirements for an ISMS.

ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of an organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

4.1.4. 3GPP Machine Type Communications

The *3rd Generation Partnership Project* (3GPP) [3GPP] unites six telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TTA, TTC), known as “Organizational Partners” and provides their members with a stable environment to produce the Reports and Specifications that define 3GPP technologies.

The project covers cellular telecommunications network technologies, including radio access, the core transport network, and service capabilities - including work on codecs, security, quality of service - and thus provides complete system specifications. The specifications also provide hooks for non-radio access to the core network, and for interworking with Wi-Fi networks.

3GPP specifications and studies are contribution-driven, by member companies, in Working Groups and at the Technical Specification Group level.

The Four *Technical Specification Groups* (TSG) in 3GPP are:

- Radio Access Networks (RAN);
- Service & Systems Aspects (SA);
- Core Network & Terminals (CT);
- GSM EDGE Radio Access Networks (GERAN).

The Working Groups, within the TSGs, meet regularly and come together for their quarterly TSG Plenary meeting, where their work is presented for information, discussion and approval.

4.2 Other relevant organizations

4.2.1. IoT Forum

COSMOS is trying to comply as much as possible to the IoT Architectural Reference Model and associated methodology as far as COSMOS Architecture is concerned (as handled in WP2/Task 2.3). The IoT ARM is the main result of the FP7 EU project IoT-A. The ARM has already been adopted (or is being adopted) by many FP7 and SmartCity projects.

In the context of WP2 we will provide feedback to the Working Group “Architecture and interoperability” of the IoT Forum [IoTForum1] which has pledged sustaining and evolving the IoT ARM after the completion of the IoT-A project (late November 2013). This feedback will relate to the usability and possible improvements.

4.2.2. ECMA

The *European Computer Manufacturers Association* (ECMA) [ECMA] is an industry association founded in 1961. It is driven by industry to meet the needs of industry, generating a healthy competitive landscape based on differentiation of products and services, rather than technology models, generating confidence among vendors and users of new technology. ECMA facilitates the timely creation of a wide range of globalICT and Consumer Electronics standards, e.g. for programming languages, ECMAScript, Business Communications, Near Field Communications, High Rate Wireless Communications, Electromagnetic Compatibilty (EMC) etc.

4.2.3. OASIS

The *Organization for the advancement of Structured Information Standards* (OASIS) [OASIS] is a not-for-profit consortium that drives the development, convergence and adoption of open standards for the global information society. OASIS promotes industry consensus and produces worldwide standards for security, Internet of Things, cloud computing, energy, content technologies, emergency management and other areas. OASIS open standards offer the potential to lower cost, stimulate innovation, grow global markets, and protect the right of free choice of technology. The consortium has more than 5,000 participants representing over 600 organizations and individual members in more than 65 countries.

The *Message Queuing Telemetry Transport* (MQTT) [MQTT1] protocol is an open and lightweight publish/subscribe protocol designed specifically for M2M and mobile applications. It is useful for connections with remote locations where a small code footprint is required and/or network bandwidth is at a premium [MQTT2].

MQTT supports many features including:

- The publish/subscribe message pattern to provide one-to-many message distribution and decoupling of applications;
- A messaging transport that is agnostic to the content of the payload;
- The use of TCP/IP to provide basic network connectivity;
- Three qualities of service for message delivery:
  - "At most once", where messages are delivered according to the best efforts of the underlying TCP/IP network. Message loss or duplication can occur. This level could be used, for example, with ambient sensor data where it does not matter if an individual reading is lost as the next one will be published soon after;
  - "At least once", where messages are assured to arrive but duplicates may occur;
  - "Exactly once", where message are assured to arrive exactly once. This level could be used, for example, with billing systems where duplicate or lost messages could lead to incorrect charges being applied;
  - A small transport overhead (the fixed-length header is just 2 bytes), and protocol exchanges minimised to reduce network traffic;
  - A mechanism to notify interested parties to an abnormal disconnection of a client using the Last Will and Testament feature.

4.2.4. EPC global

EPCglobal is a joint venture between GS1 (formerly known as EAN International) and GS1 US (formerly the Uniform Code Council, Inc.). It is an organization set-up to achieve worldwide adoption and standardization of Electronic Product Code (EPC) technology.

As stated by EPCglobal [EPC1]: “EPCglobal is leading the development of industry-driven standards for the *Electronic Product Code* (EPC) to support the use of Radio Frequency Identification (RFID)” so the main focus of the group currently is to create both a worldwide standard for RFID and the use of the Internet to share data via the EPCglobal Network.

EPCglobal's board of governors includes representatives from EPCglobal, GS1, Auto-ID Labs, Cisco Systems, DHL/Exel Supply Chain, Haier Group Company, Johnson & Johnson, Kimberly-Clark Corporation, LG Electronics, Lockheed Martin Corporation, METRO AG, Novartis Pharma AG, Office of the Secretary of Defense, Procter & Gamble, Sony Corporation, The Dow Chemical Company and Wal-Mart Stores, Inc.

Although the scope of the EPCglobal is narrower than current IoT field (aiming only on RFID-based mechanisms), it might be worth monitoring EPCglobal and considering possible leverage of the standards outside the RFID domain.

4.2.5. IEEE-SA -IEEE Standards Association

The *IEEE Standards Association* (IEEE-SA) [IEEE-SA] is an organization within IEEE that develops global standards in a broad range of industries, including: power and energy, biomedical and health-care, information technology, telecommunication, transportation, nanotechnology, information assurance and many more.

IEEE-SA is a community rather than a governmental organization which is conducted by bodies which clearly do standardising work.

4.2.6. IERC - European Research Cluster

The aim of *European Research Cluster on the Internet of Things* (IERC) [IERC] is to address the large potential for IoT-based capabilities in Europe and to coordinate the convergence of ongoing activities. It has created a number of activity chains in order to favour close cooperation between the projects addressing IoT topics and to form an arena for exchange of ideas and open dialog on important research challenges. The activity chains are defined as work streams that group together partners or specific participants from partners around well-defined technical activities that will result into at least one output or delivery that will be used in addressing the IERC objectives. Following activity chain are defined within IERC:

- **AC1** - Architecture approaches and open platforms
- **AC2** - Naming and addressing schemes. Means of search and discovery
- **AC3** - IoT innovation and pilots
- **AC4** - Service openness and interoperability issues/semantic interoperability
- **AC5** - Governance, Privacy and Security issues
- **AC6** - Standardisation and pre-regulatory research
- **AC7** - Cognitive Technologies for IoT
- **AC8** - Societal Impact and Responsibility in the Context of IoT Applications

4.3 COSMOS Adherence to Standards

During year 1 of the project work on a number components has commenced, whit varying levels of development. These include the the Planner, Experience Sharing and Social Monitoring, Privelets and Data Mapper. Also work on the semantic model has been performed including that on the VE registry. A first version if the hardware cryptographic accelerator has been developed.

Whenever possible, the project team tried to design and develop these components while adhering to known and widely used standards.

The Social Monitoring component is responsible for monitoring social connections between VEs and to that end, uses a triple store with the semantic description of the numerous social relations between them. The Planner component makes use of semantic descriptions too for the technique of CBR and as such, both previously mentioned components, adhere to the RDF and OWL standards of W3C.

After researching the possibility of using an already well-established Ontology in the components of Social Monitoring and Planner, it has been found that, most probably, none of the existing Ontologies offer what the components demand. Especially for the Social Monitoring, the FOAF ontology was investigated, but could not offer solutions for social relations between VEs, as it is geared towards connections between individuals in social networks.

In fact, the decision to use semantic descriptors for these components has been strongly encouraged by the fact the key concepts of the platform, namely the VEs, are also semantically described using the same standards of representation.

In the case of the Planner, communicative connections established with the Message Bus are made using AMQP 1.0 which is a communication protocol standard (ISO/IEC 19464:2014) through the use of RabbitMQ as the technology implementing the Message Bus.

The Experience Sharing component implements communication and knowledge sharing between VEs. To this end, a RESTful implementation of this component's communication is used.

The project team is considering using JSON (open standard format ECMA-404) as the basic format for data exchange in all VE2VE and VE2Platform communications. While current implementations vary, future work is oriented to that end. Currently using JSON format are data of the Privelets component and Planner data received through the Message Bus.

Further work includes the investigation of a possible use of the JSON schema standard draft v4 (IETF), which while not yet a clear standard, is being actively monitored by NTUA, as a means to ensure data format compliance in communications. Initial implementation is being investigated for the Data Mapper.

During the first project year a hardware cryptographic accelerator has been designed and developed. The hardware cryptographic accelerator is a dedicated module integrated within the Xilinx Zynq Platform FPGA. The module is responsible for high-speed encryption and decryption of data payloads that is images taken by the bus surveillance cameras, as specified in the main use case.

The hardware cryptographic accelerator implements the functionality as per FIPS-197 [FIPS197] [http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf - FIPS PUB 197: Advanced Encryption Standard (AES)], that is a fixed key and data block length of 128bit. Both development and verification (targeted verification) tasks adhered to the FIPS-197 standard in order to ensure full compliance.

The hardware cryptographic accelerator is connected to the main system bus which is already available in the platform FPGA. The main system bus of choice is AXI (Advanced eXtensible Interface) – a complex and high performance protocol. As the cryptographic accelerator does not need such a highly complex interface the APB (Advanced Peripheral Bus) protocol was chosen as an interface. Thus a bridge between the two bus systems had to be developed. In order to provide full compliance with both interfaces, the AMBA protocol specification [AMBA] [http://www.arm.com/products/system-ip/amba-specifications.php] was used. AMBA (Advanced Microcontroller Bus Architecture), developed by ARM Holdings, is the de-facto standard in terms of hardware, inter-module, communication protocols. The standard presents both the protocol as well as basic information regarding possible hardware implementations of the proposed bus systems.

In order to test the hardware cryptographic module two sets of test vectors were used. The first test vector set was taken from FIPS-197 while the second set was generated using Crypto++ (http://www.cryptopp.com/) [Crypto]– a free but certified crypto-library.

For requirements we have used FIPS-140-1 (http://csrc.nist.gov/publications/PubsFIPS.html) [FIPS140] which specifies security requirements which must be met by production-grade hardware and software components.

4.4 Contribution to Open-Source projects

4.4.1. OpenStack Swift and Apache Spark

In April 2012, IBM joined the OpenStack open source foundation as a founding and platinum member. The IBM Haifa Research team was the first to make major IBM contributions to OpenStack by contributing a volume driver for the IBM Storwize and SVC storage systems to OpenStack's Nova and Cinder. These drivers enable clients with IBM storage products to fully participate in OpenStack deployments, and serve as a platform for future functions being developed by IBM Research. Since then the team has been very active in the OpenStack community, continuously contributing to the community, serving as core members, and participating and presenting at the OpenStack Summits.

Particularly relevant to COSMOS are two of our presentations at the OpenStack Summit in Paris in November 2014. The first presentation, “Docker Meets Swift: A Broadcaster's Experience”, presents the storlet mechanism which the IBM Haifa Research team developed for OpenStack Swift, and demonstrates how storlets can be used for media workflows and other scenarios. The storlets capability is being exploited by the COSMOS project.

The second presentation, “The Perfect Match: Apache Spark Meets Swift”, focuses on the integration between Spark and OpenStack Swift, demonstrating the advanced models for executing Spark jobs directly on Swift objects. This capability will be exploited by the COSMOS project. This work also involves our open source contributions to the Apache Spark framework which enable OpenStack Swift to be a supported Apache Spark data store.

4.5 Partner contribution to standardization activities

The following sections describe the partner contribution with regards to standardization activities, either from the observation or contribution perspective.

4.5.1. NTUA

NTUA is oriented in researching a possible extension to the FOAF social ontology that could be used as a future reference for Social IoT semantic descriptions. Provided that the semantic description is robust enough, such effort could be extended to possible standardization. Also, the means to create a CBR capable ontology are being investigated. While there is no active standard to be developed and/or enriched in this case, future work in this area could prove fruitful to new standardization efforts.

In the case of the Architecture, the IEEE P2413, which is an active standard currently developed, seems promising. NTUA will monitor the project's progress and investigate any possible alignment of COSMOS Architecture with the proposed IoT Architecture of P2413.

4.5.2. Siemens

Siemens is one of the contributors to the IEEE P2413 Working Group confirming again its strong involvement and support for the development of the IoT domain.

All standardization efforts in Siemens are coordinated by a central headquarters team. As a result there can be no direct contribution of Siemens CT to any working group.

Since IEEE P2413 just started during Cosmos first year of execution, Siemens team involved in Cosmos contacted internal contact and peer technical groups who contribute. First year activity was dedicated to identify where and how content currently based on IOT-A might be enlarged with Cosmos specific aspects.

ISO 37120 is a standard under close observation by Siemens since it is linked to activities in both the IoT as well as the infrastructure and city domain.

ISO 27001 as well is a standard under observation as any commercial solution must ensure the data security for the service providers and end customers. Security is therefore something to be considered from the lowest level of device specification and development to the highly integrated solutions which involve the interaction between devices and multiple software components and platforms.

Siemens has been strongly involved into the design of the Cosmos semantic model and related components. Existing and widely accepted ontology reuse was encouraged. Also, the results of other European projects have been applied such as those from IoT-A or IoT.est. The semantic model of Cosmos was therefore designed so that, for instance, the definition of the physical entities whose properties are exposed by VEs, is not part of the model. Instead the user can make reference to any other ontology which properly describes the physical entity.

Siemens has proposed the semantic description of the message bus topics and, since this approach presents a strong reuse potential even outside the project boundaries, it will support the dissemination of these results as well as any possible inclusion into a standard, either for message buses or as a stand-alone ontology.

4.5.3. ATOS

Having the role of a big industrial partner, ATOS is adopting and integrating a bunch of technologies in COSMOS based on their state of standardization, what provides implementation choice, flexibility, speed, agility and skills. Moreover, for those shelf-made developments, in this case the constrained-driven Complex Event Processing (CEP) engine, ATOS is following closely different standardization bodies in order to build a tool that is aligned with recognized standards.

Concerning the different technologies chosen for building up the Message Bus component, the underlying protocol for the publication/subscription of messages is the ISO/IEC 19464:2014, which is commonly known as Advanced Message Queuing Protocol (AMQP) protocol v1.0. This standard is while adopted by the community to connect hundreds of critical systems in Telecommunications, Defence, Manufacturing, Internet and Cloud Computing. In fact, relevant companies such as NASA, VMware or AT&T use it in their systems. When it comes to the CEP engine under development, AMQP is being used as the communication interface for the collection of data feeds and the publication of complex events.

In regard to event processing, ATOS has been closely following the Event Metamodel and Profile (EMP) RFP, which is a pending proposal to the Object Management Group (OMG), an international, open membership, not-for-profit technology standards consortium founded in 1989. The purpose of this RFP is well aligned with the current development state of the CEP, which treats Events as observations of state rather than actions of processes. In this direction, developing a common terminology for modelling events will help supporting interoperability among CEP engines, enable richer event classification, and facilitate identification of event patterns and anomalous conditions.

4.5.4. IBM

The role of IBM in the project concerns infrastructure such as cloud storage, therefore standardization activity concerns technologies applicable to the IoT domain although the context is more general. IBM Research – Haifa has been actively contributing to open source software communities such as OpenStack Swift and Apache Spark. At this stage of the project, these contributions have not yet involved specific standardization activities, and we currently do not forsee standardization activities related to cloud storage infrastructure for IoT workloads. On the other hand, in the data management, analytics and cloud storage infrastructure domains, we adopt open interfaces such as the OpenStack Swift REST APIs, and the Apache Spark analytics framework.

5 Summary of Actions

Wide acceptance among stakeholders is an important goal for every research and development project. This document describes the efforts taken by the project consortium in this direction and lists foreseen step (see the table below) in order to increase the relevance of the project outcomes.

Body	Action	Leading partner
IEEE	Contribution to the development of the P2413 – Standard for an Architectural Framework for the IOT standard	SIEMENS
ISO	Close observation of the ISO 37120 – Sustainable development of communities standard and of ISO 27001 - Information technology— Security techniques — Information security management systems — Requirements. Identification of relevant aspects for the Cosmos research and development activities as well as possible contributions to the standards.	SIEMENS

6 References

[W3C1]	"World Wide Web Consortium" [Online]. Available: http://www.w3.org/ [Accessed: 04-Nov-2014].
[ETSI1]	"European Telecommunications Standards Institute" [Online]. Available: http://www.etsi.org/ [Accessed: 04-Nov-2014].
[ISO1]	"International Organization for Standardization" [Online]. Available: http://www.iso.org/iso/home.html. [Accessed: 04-Nov-2014].
[ITU1]	"International Telecommunication Union" [Online]. Available: http://www.itu.int/en/Pages/default.aspx. [Accessed: 04-Nov-2014].
[IETF1]	"The Internet Engineering Task Force" [Online]. Available: https://www.ietf.org/. [Accessed: 04-Nov-2014].
[ITU2]	"Internet of Things Global Standards Initiative" [Online]. Available: http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx. [Accessed: 04-Nov-2014].
[OPC1]	"OPC Foundation – What is OPC" [Online]. Available: https://opcfoundation.org/about/what-is-opc/. [Accessed: 04-Nov-2014].
[ARM]	F. Carrez ed. , IoT- A Deliverable D1.5: "Final Architectural Reference Model for the IoT V3.0" [Online]. Available: https://dl.dropboxusercontent.com/u/23123988/D1.5%20%2020130715%20VERYFINAL.pdf. [Accessed: 04-Nov-2014].
[EPC1]	"EPCglobal" [Online] Available: http://www.gs1.org/epcglobal. [Accessed: 04-Nov-2014].
[SSN-XG1]	"W3C Semantic Sensor Network Incubator Group" [Online]. Available: http://www.w3.org/2005/Incubator/ssn/XGR-ssn-20110628/. [Accessed: 04-Nov-2014].
[P2413]	"P2413 - Standard for an Architectural Framework for the Internet of Things (IoT)" [Online]. Available:http://standards.ieee.org/develop/project/2413.html. [Accessed: 04-Nov-2014].
[RFC7252]	"The Constrained Application Protocol (CoAP)" [Online]. Available: http://tools.ietf.org/html/rfc7252. [Accessed: 04-Nov-2014].
[ISO37120]	"ISO 37120:2014 Sustainable development of communities - Indicators for city services and quality of life" [Online]. Available: http://www.iso.org/iso/catalogue_detail?csnumber=62436. [Accessed: 04-Nov-2014].

[ISO27001]	"ISO/IEC 27001 - Information security management" [Online]. Available: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm. [Accessed: 04-Nov-2014].
[IoTForum1]	"Internet of Things International Forum" [Online]. Available: http://iotforum.org/. [Accessed: 04-Nov-2014].
[3GPP]	"3GPP Machine Type Communications" [Online]. Available: http://www.3gpp.org/about-3gpp/about-3gpp. [Accessed: 04-Nov-2014].
[ECMA]	"ECMA - European Computer Manufacturers Association" [Online]. Available: http://www.ecma-international.org/. [Accessed: 04-Nov-2014].
[MQTT]	"MQTT For Sensor Networks (MQTT-SN) Protocol Specification" [Online]. Available: http://mqtt.org/new/wp-content/uploads/2009/06/MQTT-SN_spec_v1.2.pdf. [Accessed: 04-Nov-2014].
[MQTT2]	"MQTT" [Online]. Available: http://mqtt.org/. [Accessed: 12-Nov-2014].
[IEEESA]	"IEEE Standards Association" [Online]. Available: http://standards.ieee.org/. [Accessed: 04-Nov-2014].
[IERC]	"European Research Cluster on the Internet of Things" [Online]. Available: http://www.internet-of-things-research.eu/. [Accessed: 04-Nov-2014].
[FIPS197]	"FIPS PUB 197: Advanced Encryption Standard (AES)" [Online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[AMBA]	"Advanced Microcontroller Bus Architecture" [Online]. Available: http://www.arm.com/products/system-ip/amba-specifications.php
[FIPS140]	"Federal Information Processing Standards Publications" [Online]. Available: http://csrc.nist.gov/publications/PubsFIPS.html