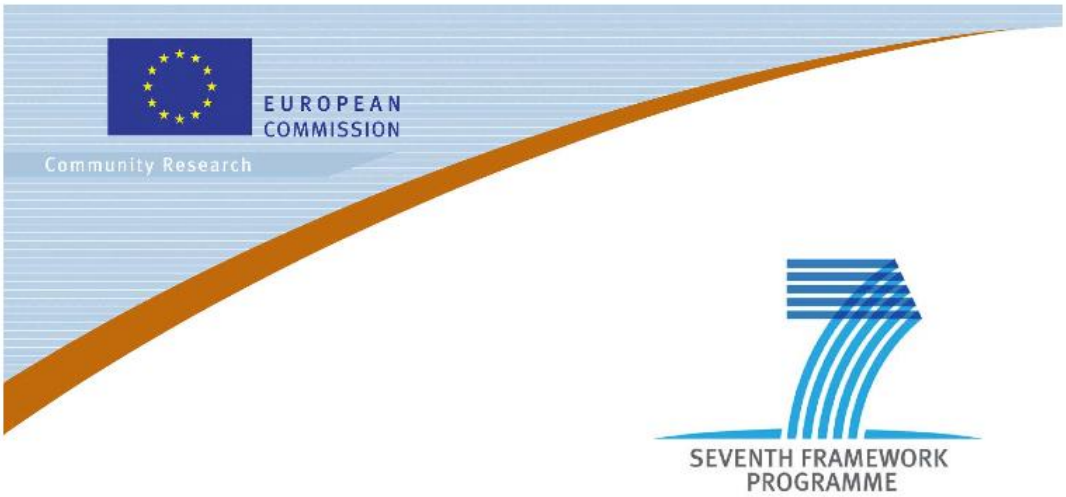


Private Public Partnership Project (PPP)

Large-scale Integrated Project (IP)

D.11.4.4: FIWARE Standardization Plan and Activities

Project acronym: FIWARE

Project full title: Future Internet Core Platform

Contract No.: 285248

Strategic Objective: FI.ICT-2011.1.7 Technology Foundation: Future Internet Core Platform

Project Document Number: ICT-2011-FI-285248-WP11-D.11.4.4

Project Document Date: 2015-02-03

Deliverable Type and Security: Public

Author: FIWARE Consortium

Contributors: FIWARE Consortium

1 Introduction

1.1 Executive Summary

This deliverable provides the final documentation of the standardization efforts taken within the FIWARE project. After a general analysis of standardization activities in FIWARE, each technical chapter presents an overview of ongoing and concluded activities in various Standards Development Organizations (SDOs). In an annex, the individual contributions and other activities are listed in a time-stamped summary for each chapter. This annex represents a snapshot that was created from a public electronic document (Wiki) which is jointly maintained and continuously updated by the FIWARE consortium.

Note that several FIWARE partners completed their parts of the project in April of 2014, before creation of this report, and we apologize if some of their work did not receive the emphasis they might have wished.

1.2 Intended Audience

As this deliverable summarizes the relationship between different FIWARE generic enablers and various standards, it is of interest to all potential users of the FIWARE platform. The lessons learned concerning the standardization process itself, and its constraints, may be of interest to individuals outside of the FIWARE consortium.

1.3 Acknowledgements

The current document has been elaborated using a number of collaborative tools, with the participation of FIWARE Working Package Leaders and Architects as well as those partners in their teams who become involved in the various standardization efforts.

1.4 Keyword list

FIWARE, PPP, Standardization, Reference Architecture, Generic Enabler, Open Specifications, I2ND, Cloud, IoT, Data/Context Management, Applications/Services Ecosystem, Delivery Framework , Security, Developers Community and Tools , ICT, Cloud Edge, Cloud Proxy.

1.5 Table of Contents

1.6 List of Figures

2 Standardization within FIWARE

2.1 Initial Stage

The aim of the FIWARE project is to create a global, practical, evolving platform for the Future Internet and for Internet of Things. Due to various socio-economic factors which will be described more below, this requires the global acceptance of open standards for various information exchange protocols and methods.

The understanding of FIWARE partners of the process of (open) standardization underwent an evolution during the course of the project. This introduction summarizes the early, middle and final stages of that understanding. The status of the actual work is covered in Section 2.

In the early stages of FIWARE, as described in the project DoW, the assumption was that the main goal of the FIWARE standardization activities should be "to ensure active contribution of specifications leading to open standardized interfaces". As a means to that end it was planned that a "thorough analysis of standardization candidates will be performed and specific steps and community-building activities will be launched", and "emphasis will be given to the adoption of specifications defined by standardization bodies and initiatives, as well as to defining particularly innovative and relevant specifications that the WP will propose for adoption by those bodies".

Since resources within the FIWARE project could not be allocated in a dedicated way for direct standardization work, it was planned that each Partner would "... utilize its network of contacts in the industry in order to reach a broad knowledge of the standardization activities and to form an interest group that provides active support".

There were a significant number of activities by consortium members towards bringing FIWARE results back to standardization bodies, but these activities were rather executed by individual members than by the consortium as a whole. Even in a case where a complete binding of an existing standard was defined by FIWARE – for OMA NGSI - there were activities by Telefonica and NEC to present the binding to OMA, but no large resources were allocated to continuous discussions with OMA about this.

Thus the FIWARE standardization work was initially conceived in terms of four stages, to (a) Monitor, (b) Influence, (c) Contribute, (d) Promote appropriate standards. The early monitoring was planned to help FIWARE be rapid and efficient in the software development, by re-using existing standards and avoiding to "reinvent the wheel". The early monitoring would also indicate which groups needed to be influenced or to receive contributions.

The work in the early stages of FIWARE resulted in a good overview of various bodies influencing Future Internet development, which has been documented on the FIWARE wiki.

2.2 Middle Stage

In the middle stage of the FIWARE project it was realized that very significant changes were occurring in the Future Internet research and in related markets, particularly the commercialization of Cloud offerings. Organizations and companies had reacted to the availability of technical solutions in the direction of Future Internet by trying to "stake out" their own areas of influence, for their technologies and/or products.

The tendency for such so-called "Balkanization" to occur has been well-described in the literature [5,6] and the logic is as follows. Every organization is aware that possessing the best technical solution does not guarantee achieving the position of a unanimously-supported global standard. In fact, everyone is aware that achieving an early, wide-spread and well-publicized deployment/acceptance of a standard or technology can be a major factor to persuade undecided users in favor of choosing it, resulting in a positive feedback towards the "early mover" [1] [2].

This leads to a "land grab" mentality whereby many companies create/join many different organizations, each standardizing a different approach, just in case one or the other standard finally becomes popular. It also results in the deliberate creation or support of "niche areas" so as to maintain a dominant position (an English proverb says, "It is better to be a big frog in a small pond, than to move into a big pond"). This has resulted in the launch of numerous organizations, as illustrated by the table below, which for brevity only shows M2M/IoT organizations, of which 2/3 arose in the last 18 months.

ORGANIZATION (O=OpenSource, S=SDO, T=Technical Forum, C= Commercial Alliance)	TYPE	START	REGION	OUTPUTS
Allseen Alliance	T	2014	America	OSS Code, Protocols, Architecture
Broadband Forum (BB-Home)	T			Protocol, Config Data Models
DLNA SmartHome Project	T	03.2014	USA	Use Cases, Guidelines
Eclipse SmartHome (OpenHAB)	O		Europe	OSS Code
ETSI SmartM2M	S			Ontology
GlobalPlatform IoT Task	T	2013	Global	
HyperCat	S		UK	S/W, Protocol, middleware, ontology
IEEE P2413 “IoT Architecture”	T	07.2014	Global	Protocols, Architecture, OSS
Industrial Internet Consortium	C	03.2014	America	Business Cases discussions
Industrie 4.0	T		Germany	Architecture, Protocols, Ontology
IoT Forum	O	06/2013	Europe	Profiles for IoT-A architectures

NIST CPS PWG (Cyber-Physical Systems Public WG)	S	06.2014	USA	Coordination of standards
OneM2M	S			
Open Interconnect Consortium	T	07.2014		Protocols, Architecture, OSS
SmartThings	O	2012	USA	Apps interwork with (many) Hubs
THREAD	C	07.2014	Global	Promote proprietary protocol based on IEEE 802.15.4 and 6lowPAN

Figure 1: List of recently-formed IoT SDOs, Fora and Alliances

The ferocity of competition between different platform standards, which can impact billions of people and services, is well described in the literature [7].

Although inefficient, the world has learned in many cases to live with such fragmentation. One approach is to develop reliable gateways/translation between each successful "community" using incompatible standards. The socio-economic conditions to achieve acceptance of multiple standards and gateways is discussed in reference [3]. The modular nature of the FIWARE platform would indeed facilitate the design of gateways to add/intact with any other FI platforms which become successful and widespread.

In the middle stage of the FIWARE project it was considered if such methods would allow FIWARE standardization and deployment to move ahead, only loosely interacting with other approaches. Remembering some history, e.g. of the growth of cellular radio networks in the USA, whereby it was initially impossible to send an SMS from one operator network to another, did not however allow for much optimism.

FIWARE partners continued seeking alignment with standardization bodies, mainly executed through monitoring activities and providing feedback from implementation of the respective standards. This approach was also applied with regard to de-facto standards like OpenStack. One particular principle applied across the different FIWARE chapters was to adopt RESTful interfaces; a reaction to their widespread usage in service-level standards from SDOs like ETSI or OMA.

FIWARE partners reacted to the proliferation of working groups and bodies active on Future Internet topics by re-considering the situation. The table shows obstacles/difficulties and various tactics which the FIWARE partners - at different times and places, with varying effort - attempted. A few of the attempts are mentioned in Section 2.

	Obstacles to success	**Counter-Tactics**
1	Genuinely different niche areas lead to the development of tightly-focused and different solutions. The advantages of adopting a more generic approach tend to be met with counter-arguments of "too high overhead" and "several of our necessary features would be lost"	(a) Show that FIWARE offers a super-set solution (b) Show that FIWARE is easy to extend
2	Need to choose appropriate SDO for FIWARE activity, from a (long) list	(a) Full analysis of all possible SDOs, with ongoing tracking of "impact on global standards" (See [4] for an analysis of the problems with this approach). (b) Partial analysis based on where FIWARE delegates have already some experience.
3	Technical superiority is not sufficient to persuade SDOs to change	(a) Offer the FIWARE ideas as an option, which might help expand the influence of the "own" specifications of the SDO. (b) Persuade the SDO of benefits, by long discussions on use cases and requirements (Note [8] provides a lot of insight into this long process).
4	Objectively, an SDO may not have capacity (time, manpower, expertise) to integrate a new/different approach. Subjectively, an SDO may suffer a kind of "mental fatigue", whereby delegates and chairpersons are unwilling to devote resources to "yet another competing idea".	Send FIWARE delegates and contributions to the SDO to (a) learn and demonstrate familiarity with the SDO procedures and existing specifications (b) illuminate the overlap between the approaches (c) do the actual work of inserting the FIWARE ideas in the SDO specifications
5	SDO does not want to adapt because it has invested time/effort/branding in a different approach	(a) FIWARE could contribute time/effort in to the normal work of the SDO, opening doors for specs from FIWARE (see above point) (b) The branding issue probably requires long-term persuasion at the highest levels (Board) of the SDO

6	A general feeling in each SDO, that to be "first to publish" is almost essential, results in a reluctance to "be distracted" by considering related-but-different proposals from external organizations.	(a) Show that adapting to FIWARE costs time initially but speeds deployment/results later
7	SDO requires code demonstrating the specification	IETF and some open-source organizations rely on "proof by running code" and FIWARE can supply this, BUT not necessarily in the same code environment as each SDO assumes. Substantial coding might be needed.
8	Overlapping of standards means that it is difficult to decide which of several similar specifications should be the focus of FIWARE activity, i.e. point (2) is not conclusive. This implies that all the points 3-7 might need to be applied not just to one chosen SDO but to multiple ones.	
9	The final barrier to global standardization is the acceptance of the specification by a significant number of users.	(a) Create/encourage an eco-system of users/developers (b) Choose a de-jure specification regime where compliance is mandatory

Figure 2: Obstacles to global standardization and some counter-tactics

2.3 Final Stage

During the final stage of the FIWARE project, early versions of the complete platform became available. FIWARE began building a community of users/developers, after extensive code had become available. Many Open Call partners were added to the project to conduct trials and hackathons [9].

At the same time, there was a developing awareness within the standardization communities, and indeed within the EC, that "coding instead of paper-ware" was a more agile and ultimately more interoperable/testable approach to (software) standardization.

This led to a change in tactics within FIWARE standardization. The approaches described in the previous section were continued to some extent, but relatively more effort was put into the coding and popularization of the code. One consideration for this change of attitude was the realization that, even if FIWARE never itself became globally successful, some of the most useful elements (APIs and protocols) would enter the open source community and become components in the next generation solutions.

The code-based approach has materialized itself in the open-source availability of nearly all Generic Enabler reference implementations in well-established open-source communities, and the presence of FIWARE in various hackathons taking place all over the world since summer 2013.

2.4 Summary

During the execution of the project, the goals of standardization work evolved. Initially the emphasis was on planning formal standardization of newly developed or changed APIs, then the emphasis shifted to the adoption of existing standards, then to "coding instead of paper ware".

All technical chapters have indeed selected a range of existing standards to be implemented by the Generic Enablers, as can be seen in the sections below. One specific standard of particular importance in this context is the OMA NGSI Context Management Framework, which was adopted by a large set of Generic Enablers from multiple FIWARE Chapters. The effect of this choice is not only compliance to an existing standard, but, more importantly, a high level of flexibility regarding FIWARE platform deployments. Components compatible with OMA NGSI can be combined in many different ways, enabling suitable system setups for a great variety of different use cases. In this sense, the NGSI API can itself be considered as a truly Generic Enabler with many implementations.

Yet another way of interaction between FIWARE and SDOs was to provide the latter with requirements on standards. This was done in the case of ETSI M2M, where the necessity for more elaborate information models than the existing black-box data containers in current M2M standards was expressed, and a work item around this requirement was founded by FIWARE consortium members (NEC, Telecom Italia, and others).

With the end of the FIWARE project, the FIWARE platform and ecosystem is aiming to become part of the standard tool chain of European Future Internet businesses. In this respect, the Generic Enablers and their APIs are targeted to become de-facto standards in everyday use by System Integrators, Cloud Providers, and Developers. The platform has proven to be usable and used in various hackathon events, and currently accelerator programs are driving SMEs to build their businesses on FIWARE.

Being a living ecosystem, the FIWARE platform will serve as a running proof-of-concept of the standards and specifications it implements. Nevertheless, it is recommendable to maintain the contact with standardization bodies in order to provide feedback & recommendation from the standards implementation and usage and try to align the further development of the standards with the actual evolution in the FIWARE implementation.

The next section reports on the status of interaction between each FIWARE Chapter and the world of standards.

3 Standardization in each FIWARE Chapter

3.1 Introduction

In this section details about the standardization activities of each particular technical FIWARE chapter are given. For each chapter, the standardization activities are grouped into the main categories (a) standards usage (b) interface definitions and standardization contributions, and (c) open-source communities addressed.

A live wiki [10] is used and continuously updated during the project, where three types of tables are used to report planned and ongoing activities:

1. **Planned Activities** for SDOs (contributions/monitoring) for each relevant FIWARE interface
2. **Responsible Persons** for each SDO activity
3. **Time-stamped Summary** of contributions/monitoring as they occur, and also a record of any known inclusions of partner or external IPR in the open standards

In addition to the chapter summaries given in this section, the appendix of this document contains a snapshot of that wiki taken at the end of the FIWARE project. Note that the wiki continues to be used by the follow-up project FI-CORE.

3.2 Applications / Services Ecosystem

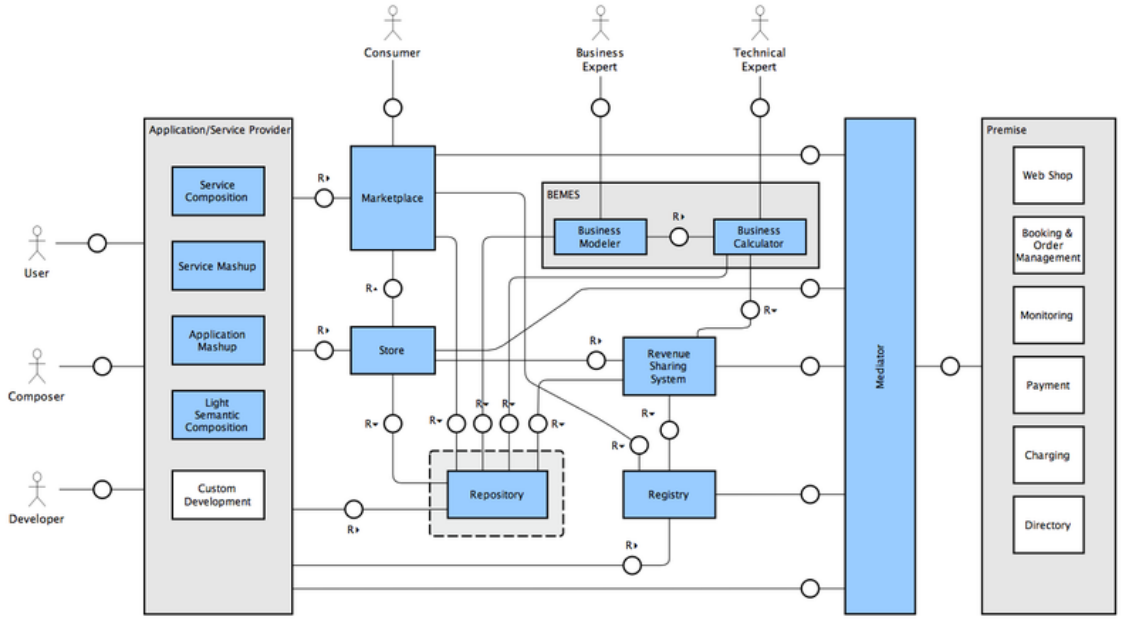


Figure 3: Applications and Services Ecosystem Architecture

The service description format is the underlying fundamental data format for most of the API. Therefore the main focus of the standardization work was on Linked USDL [11] and related APIs. Additionally, the interfaces provided by the different enablers were targeted.

The Repository Open RESTful API for accessing service descriptions is related to the Linked Data initiative [12]. Since FIWARE standardization strategy ("don't re-invent the wheel") mainly relied on using standards defined somewhere else, we only needed to monitor standardization projects, e.g. [13].

There are currently no standards activities related to the FIWARE functionality Marketplace & Store API. As a consequence, analyzing and identifying standardization organizations for potential contributions of these API specifications are aspects for future exploitation.

Standards and Specifications used by this FIWARE Chapter are:

- USDL (Store and Repository APIs are USDL- compliant)
- Adopted USDL for specification of APIs
- Contributed to USDL by providing vocabulary specifications for core, sla, pricing, legal

3.3 Cloud Hosting

3.3.1 Standards used by the Chapter

The Cloud Hosting Chapter offers Generic Enablers that comprise the foundation for designing a modern cloud hosting infrastructure suitable to develop, deploy, and manage Future Internet applications and services.

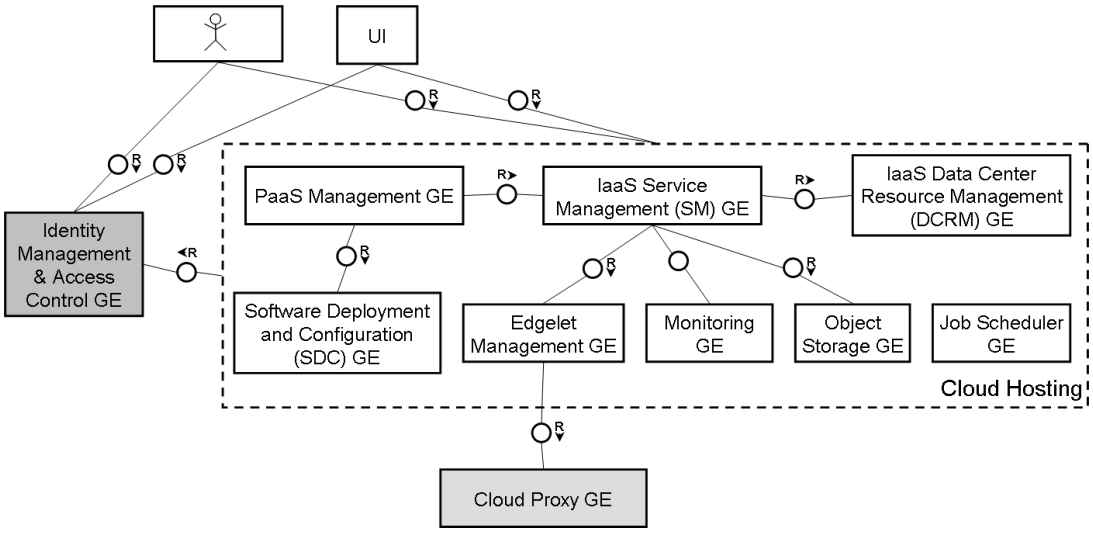


Figure 4: Cloud Hosting Architecture

The architecture comprises a set of Generic Enablers that together provide hosting capabilities of several kinds and at several levels of resource abstraction -- aiming at the needs of different applications hosted on the cloud platform.

The baseline of the Cloud Hosting architecture builds on OpenStack [14] which is itself an emerging de-facto standard for cloud computing. In consideration of both OpenStack and the FIWARE API Open Specification conventions [15], the Cloud Hosting architecture utilizes Representational State Transfer (REST) APIs for inter-component communication.

The UI component (Self Service Interfaces GE) of the architecture uses the HTML5 standard combined with a client-side MVC pattern [16] to directly access other GEs composing the architecture without requiring an interposed Web server for communication.

The FIWARE Object Storage GE extends OpenStack Swift [17] to also support the Cloud Data Management Interface (CDMI) which is a de-facto standard of the Storage Networking Industry Association.

3.3.2 Standardization contributions of the Chapter

The Cloud Hosting chapter has participated both in open source and SDO communities through its partners. In particular, the following list shows a number of different SDOs which were consulted/referenced during the specification of the following FIWARE Cloud Chapter standards:

- Open Virtualization Format (OVF), DMTF
- Open Cloud Computing Interface (OCCI), OGF
- Cloud Data Management Interface (CDMI), SNIA
- Topology and Orchestration Specification for Cloud Applications (TOSCA), OASIS
- Cloud Infrastructure Management Interface (CIMI), DMTF

Moreover, partners from the chapter actively participated in ongoing ISO SC38 deliberations through participation in the Irish National mirror group for SC38, the evolution of OGF's OCCI and the European Commission inspired ETSI Cloud Standards Coordination initiative.

3.3.2.1 *ISO/IEC JTC1/ SC 38*

Members of this work-package have continued to monitor and engage with of ISO/IEC JTC1/ SC 38 Distributed Application Platforms and Services, the Subcommittee of ISO with responsibility for Clouds standards. Both ISO/IEC 17788 Cloud Computing – Overview and Vocabulary [25] and ISO/IEC PRF 17789 Cloud Computing Reference Architecture [26] have now completed drafting and internal approvals within both ISO and ITU-T (both standards were drafted in a collaboration between the two standards organizations) and have just been published. Significant progress has also been made on drafting standards in the area of Service Level Agreement Frameworks and Technology. ISO SC38 has divided these efforts into documents covering Overview and Concepts, Metrics, and Core requirements. Cloud Hosting WP partners will continue to participate in these efforts and contribute where appropriate based on the learnings and experiences gained in projects such as FIWARE.

3.3.2.2 *OGF OCCI*

Members of the cloud hosting work-package have played a very active role in the OGF OCCI Community. Indeed one FIWARE developer (Thijs Metsch) is a co-chair of the OCCI Working Group. Learnings from FIWARE have helped mature this standard, with publication of a new version of OCCI expected in early 2015. FIWARE has directly contributed to the maintenance and enhancement of the OpenStack implementation of OCCI - the reference implementation of the Intel DCRM GE implementation.

3.3.2.3 *ETSI Cloud Standards Coordination*

Members of the cloud hosting work-package were active in the Cloud Standards Coordination working group set up by ETSI at the request of the EC as part of their Cloud Computing Strategy for Europe. FIWARE researchers edited several sections of the resulting report [27], capturing learnings and next steps based on their learnings from projects like FIWARE, and the final ETSI CSC report referred to numerous outputs from FIWARE including the draft SLAware specification for machine readable SLAs [28].

3.3.3 Open Source communities addressed

The reference implementation of most of the Cloud Chapter GEs is available as Open Source Software on GitHub and other source code hosting platforms.

Several contributions of the FIWARE Cloud Chapter partners have been accepted by the OpenStack development community and have become part of the current vanilla distribution.

Contributions span several core components, including Nova, Swift, and Cinder. For illustrative purposes, a partial list of code contributions is provided below:

- **http://stackalytics.com/?release=icehouse%2cjuno&company=ibm&metric=commits&user_id=avishay-il**
- **http://stackalytics.com/?release=icehouse%2cjuno&company=ibm&metric=commits&user_id=gilv**
- **http://stackalytics.com/?release=icehouse%2cjuno&company=ibm&metric=commits&user_id=kravchenko-pavel**

Code contributions have also been made directly to GitHub following consultations with the OpenStack Community. In particular the CDMI interface to OpenStack (the Object Storage GE) is available at https://github.com/osaddon/cdmi and the OCCI interface to OpenStack (the Intel DCRM GE implementation) is available at https://github.com/tmetsch/occi-os.

In addition to code contributions, several FIWARE members act as reviewers in the OpenStack code revision process and have been, or currently are, active contributors of blueprints for the discussion and design of new OpenStack features and components.

3.4 Internet of Things Services

3.4.1 Standards used by the Chapter

The Internet-of-Things (IoT) Chapter of FIWARE distinguishes between two main levels of information. While *Device-level information* is considered as data directly obtained from sensors, so-called *Thing-level information* relates to a higher level of abstraction. Thing-level information describes the status of real-world physical or abstract objects, whereby the particular sensors or processing units which provided the information is out of focus.

The architecture of FIWARE IoT reflects this distinction. As it can be seen in the figure below, the left-hand side of the architecture diagram contains enablers for Thing-level information processing and routing. On the IoT Gateway, the Data Handling GE is responsible for collecting and processing Thing-level information from the Protocol Adapter GE. Possibly, after processing this information, it is further routed to the IoT Backend, where the IoT Broker, Configuration Management, and Template Handler GE are responsible for aggregating Thing-level information from all Gateway instances and answering Thing-level queries on behalf of applications. The only interface of the IoT Backend towards applications or GEs outside the IoT domain is from these Generic Enablers.

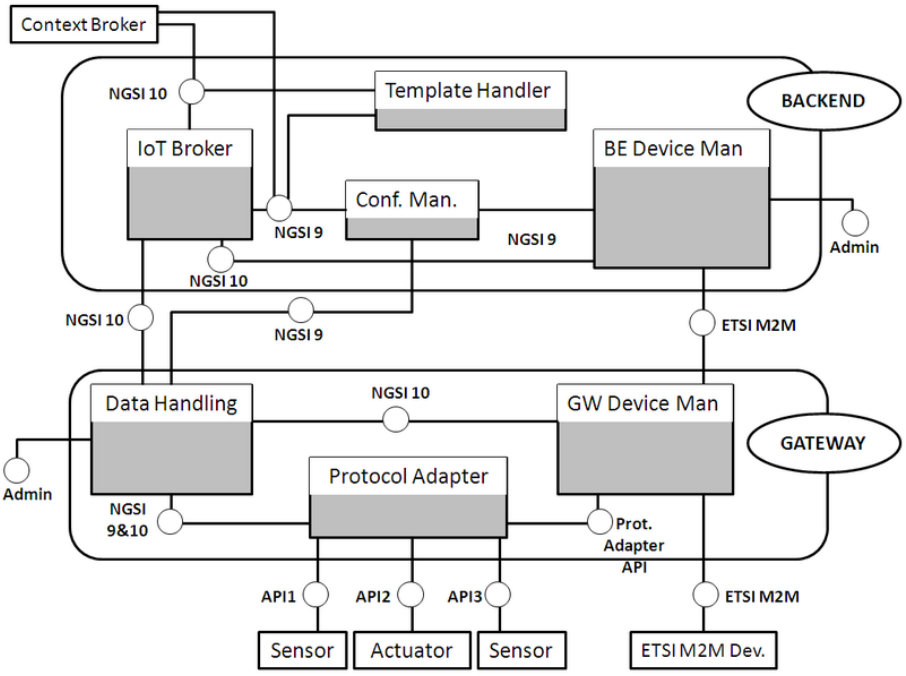


Figure 5: Architecture for Internet-of-Things, with reference points for standardization

The data model and interface between all aforementioned Generic Enablers is based on the Open Mobile Alliance standards NGSI (Next Generation Service Interface) 9/10. Abstract operation and data type definitions were provided by this standard; while FIWARE has defined a concrete binding using HTTP REST principles and xml and json message format (see next subsection).

The Generic Enablers on the right-hand side of the architecture have the role to collect and aggregate device-level information. This kind of information flows from devices to the

Gateway Device Management GE, either directly or else through the Protocol Adapter GE, depending on whether the devices are compatible to the standard used in FIWARE IoT for device-level information, ETSI M2M. The ETSI M2M standard [23] is further used for communication between the Frontend Device Management GE and its counterpart on the IoT Backend.

3.4.2 Standardization contributions of the Chapter

The FIWARE IoT Chapter has focused its standardization activities on those two standards for information exchange which are essential in the project.

As already mentioned, FIWARE IoT was a main contributor within the FIWARE project to define a RESTful binding for OMA NGSI 9 and 10. The first version of the binding was finalized within the first year of the project, and further maintained and bug-fixed thereafter. This standardization work reaches far beyond the IoT Chapter of FIWARE, as also GEs from other chapters have adopted it. Because the NGSI binding was implemented by many FIWARE enablers, various bugs and missing features could be identified and addressed.

A special requirement of the IoT Chapter which however was not addressed by NGSI is the possibility to express rules on how to translate sensor-level information into thing-level information. FIWARE IoT has therefore defined an extension of NGSI called the 'association' concept. This extension is fully backwards compatible to the existing NGSI standard.

Another requirement that has been addressed came from application developers during one of the first FIWARE events. It turned out that JSON message format is much more attractive to developers than the XML representation used in the FIWARE binding. JSON message formats were thus implemented by a number of Enablers. This format is currently documented by examples; a formal standards document has not been produced yet due to time constraints.

During the project, NGSI 9 and 10 were not actively maintained by Open Mobile Alliance. Members of the FIWARE IoT Chapter have presented the FIWARE binding to OMA at the beginning of the 3rd year of the project. The FIWARE activities have been recognized by OMA, but further steps towards making the RESTful binding an official OMA standard have not been conducted by FIWARE due to resource constraints in the standardization area.

3.4.3 Open Source communities addressed

Generic Enabler implementations or parts of it are provided via GitHub. The specific implementations are IDAS (Backend Device Management GE, partly), NEC IoT Broker (Backend IoT Broker GE), Orion Context Broker (Backend Configuration Management GE), SAP Template Handler (Backend Template Handler GE), MR CoAP Protocol Adapter (Gateway Protocol Adapter GE), IoT Discovery (Backend Configuration Management GE), EspR4FastData (Gateway Data Handling GE).

3.5 Data/Context Management

The FIWARE Data/Context Management chapter aims at providing outperforming and platform-like GEs that ease development and the provisioning of innovative applications that require management, processing and exploitation of context information as well as data streams in real-time and at massive scale. Combined with GEs coming from the Applications and Services Delivery Framework Chapters, application providers will be able to build innovative business models.

FIWARE Data/Context Management GEs enable to:

- Generate, subscribe for notifications about and query for context information from various sources.
- Model changes in context as events that can be processed to detect complex situations that will lead to generation of actions or the generation of new context information (therefore, leading to changes in context also treatable as events).
- Processing large amounts of context information in an aggregated way, using Big Data Map-Reduce techniques, in order to generate new knowledge.
- Process data streams (particularly, multimedia video streams) from different sources in order to generate new data streams as well as context information that can be further exploited.
- Process metadata that may be linked to context information, using standard semantic support technologies.
- Manage some context information, such as location information, presence, user or terminal profile, etc., in a standard way.

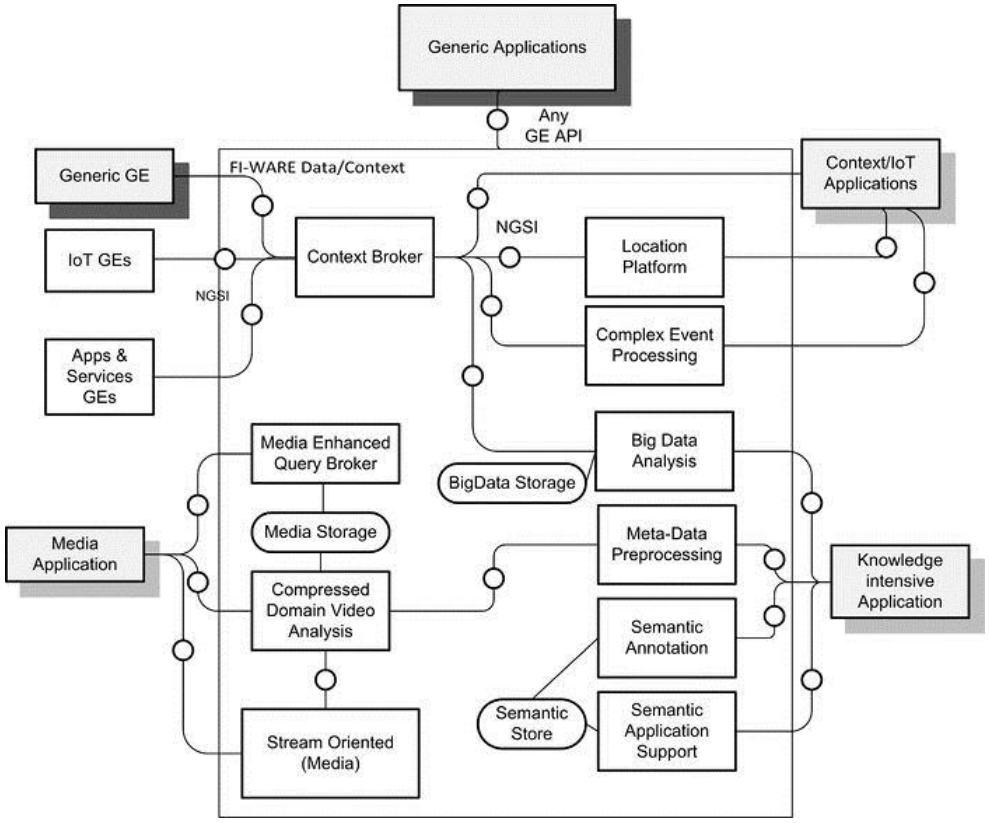


Figure 6: Data/Context Management Architecture with reference points for standardization

3.5.1 Standards used by the Chapter

Regarding standardization, there have been multiple monitoring activities, related to nearly all the Generic Enablers of the chapter, from semantics (OWL, RDF, etc.) to media (MPEG, WebRTC, etc.). A comprehensive description of those activities can be found in the FIWARE public wiki (see appendix). In particular, the most relevant standard for the Data/Context Management chapter has been NGSI, and particularly, the RESTful binding defined and implemented in two Generic Enabler implementations of the Context Broker. FIWARE NGSI allows the different GEs to communicate with each other (CEP/Proton, BigData/Cosmos, Stream Oriented/Kurento) and with GEs of other chapters. It is worth to mention that all the interaction with IoT Chapter GEs is done through NGSI, and that Wirecloud GE has been enabled to accept data from the GEs through this API.

3.5.2 Standardization contributions of the Chapter

Together with IoT Chapter members, a number of improvements to NGSI have been developed and contributed to OMA (the owner of the specification). In particular:

- RESTful binding, which has been presented and explained to OMA in July 2013.
- Proposal of JSON binding, in addition to XML, to easy the development of applications by developers, as one of the most important feedbacks received in the hackathons carried out in London Campus Party (September 2013).

3.5.3 Open Source communities addressed

An important FIWARE activity has been to release many GEs as Open Source. In some cases, important communities (in GitHub) have been established around them. In particular, the following GEs have been released as Open Source:

GEi	Owner	Repository/Community
Orion Context Broker	Telefonica I+D	https://github.com/telefonicaid/fiware-orion https://github.com/telefonicaid/fiware-connectors
Context Awareness Platform	Telecom Italia	https://forge.FIWARE.org/scmrepos/svn/data/trunk/PublishSubscribe/ContextAwarenessPlatform/PubSub_ContextBrokerGE_3.5.1_SRC.zip (not public)
Cosmos Big Data	Telefónica I+D	https://github.com/telefonicaid/fiware-cosmos-platform https://github.com/telefonicaid/fiware-cosmos-ambari
Kurento	URJC/ Naevatec	https://github.com/kurento

3.6 Interface to Networks and Devices

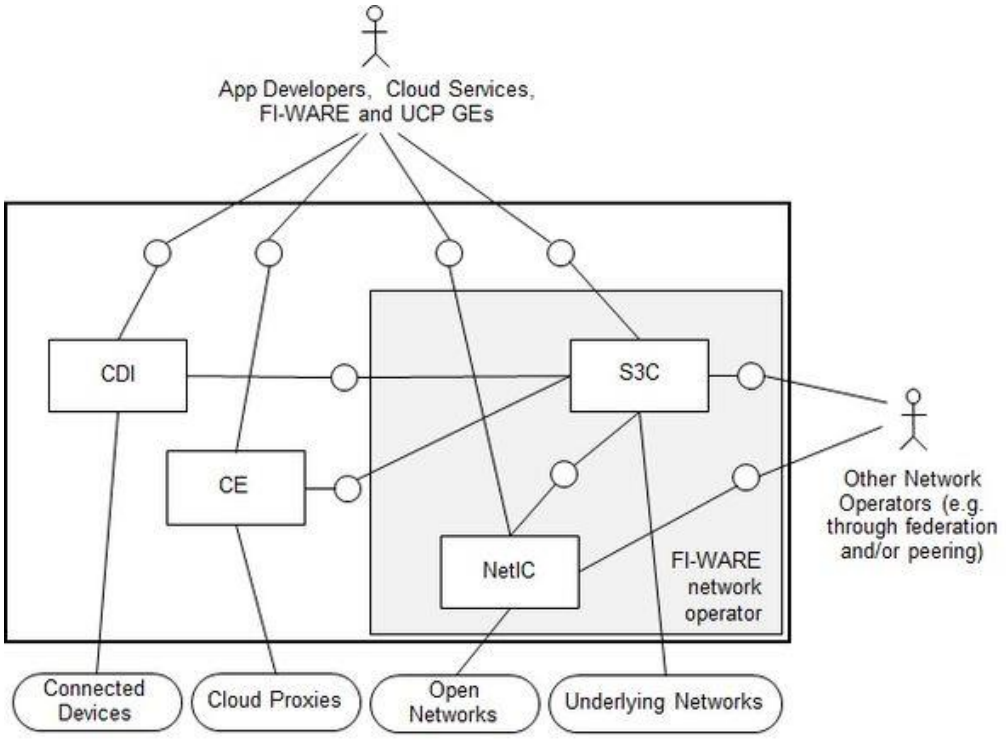


Figure 7: Architecture for Interface to Networks and Devices, with reference points for standardization

For discussion of this architecture, see [24].

3.6.1 Standards used by the Chapter

The Generic Enablers of the I2ND chapter involve different and inhomogeneous standardized interfaces, as the GEs developed cover a broad range of functionalities, managed by a variety of SDOs.

It is worth reporting that the Connected Device Interfacing GE provides a number of capabilities closely related to the W3C definitions, in particular those concerning System API and Device API Interface Working Groups. The CDI API specifications clearly mention the respective W3C API specifications they are based on.

Cloud Proxy GE largely concerns the OSGi and HGI standardization: since this is a bidirectional exchange, the details are explained in the next section.

In NetIC the OpenFlow protocol and IRTF Software Defined Networking Research Group were mainly addressed: OpenFlow has been adopted in the interfacing of NetIC, in particular for OFNIC and VNP implementations.

Finally, in S3C the main standards adopted have been those from 3GPP, IETF and GSMA. S3C is composed of many different functional features, and their specifications closely follow the evolution of such standards. For instance, the EPC OTT API provides an interface to the Evolved Packet Core defined in 3GPP, while the SMS, Telecom AS and Mediation APIs adopt the OneAPI specifications by GSMA.

3.6.2 Standardization contributions of the Chapter

One of the main links between standardization and FIWARE Interfaces to the Networks and Devices Chapter is the cloud proxy functional block. A specific implementation of an OSGi Equinox framework has been developed by Telecom Italia on board of the cloud proxy box provided by Technicolor, and installed in a dedicated container. The framework

- is based on the Oracle Java Development Kit 7 for x86 Linux, while
- the OSGi 3.6.2 Equinox implementation is profiled as requested by the HGI Open Platform 2.0 specification, with some optional services specified by Telecom Italia for its new High End Residential Routers.

The points of contact with SDOs were then mainly related to potential interactions with OSGi Alliance and HGI. But, even more than giving feedback to OSGi about the actual use of the specifications to build up the modular environment enabling the support of specific services (e.g. IoT related scenarios), attention has particularly been devoted to the cooperation with HGI, as this technical body defines a guideline for the implementation of this technical enabler on home gateways. Home Gateways (and also set top boxes) are the typical hardware boxes which are suitable to host the FIWARE cloud proxy functionalities.

The kind of interaction between FIWARE and HGI has been characterized by a two-way information flow: the FIWARE implementation took origin from the implementation of the HGi requirements in terms of choice of the Java virtual machine, OSGi services supported, needs for management of the framework. Then, after the implementation step, FIWARE communicated to HGI about the results achieved and the coherence with the overall HGI open

platform approach. Due to resource constraints, and the internal priorities of HGI activities, no direct contribution was elaborated to propose improvement to the current HGI requirements list.

It is to be pointed out that the development done exploits an open source OSGi implementation, which is Equinox based on Eclipse project.

Concerning the CDI GE, I2ND chapter planned originally the development of an OMA-DM interface, and one partner (TI) was actively contributing to the definition of the new version of specs (v2.0). However due to delays in closing the specifications this interface was not implemented in CDI. The same applied to W3C API specs, for which a proposal of extension was considered (i.e. for contacts API), but unfortunately there was not sufficient strength to promote their adoption in the working groups.

Up until cessation of activities concerning most of the implementations of NetIC GE, there were several active participations to SDOs newly established during the FIWARE lifetime. In particular, ONF was targeted, and several inputs were provided to the specification definition by FIWARE partners, including the evolution of OpenFlow protocol and, more generally, of Software Defined Networking (SDN).

3.6.3 Open Source communities addressed

Due to its nature, the OpenFlow community as well as the webinos community for CDI has been addressed by I2ND chapter development groups.

3.7 Security

3.7.1 Standards used by the Chapter

The standardization activities at the level of the Security Chapter were conducted as planned on the basis of standards identified as relevant for each group of GEs in scope of the 4 task of the Chapter.

In the figure below we highlight (using bold text and arrowed lines) on the Security Architecture where standardization effort has been directed towards interesting emerging standards. Relevant existing standards which were sufficiently mature were simply used and are not referenced in this figure.

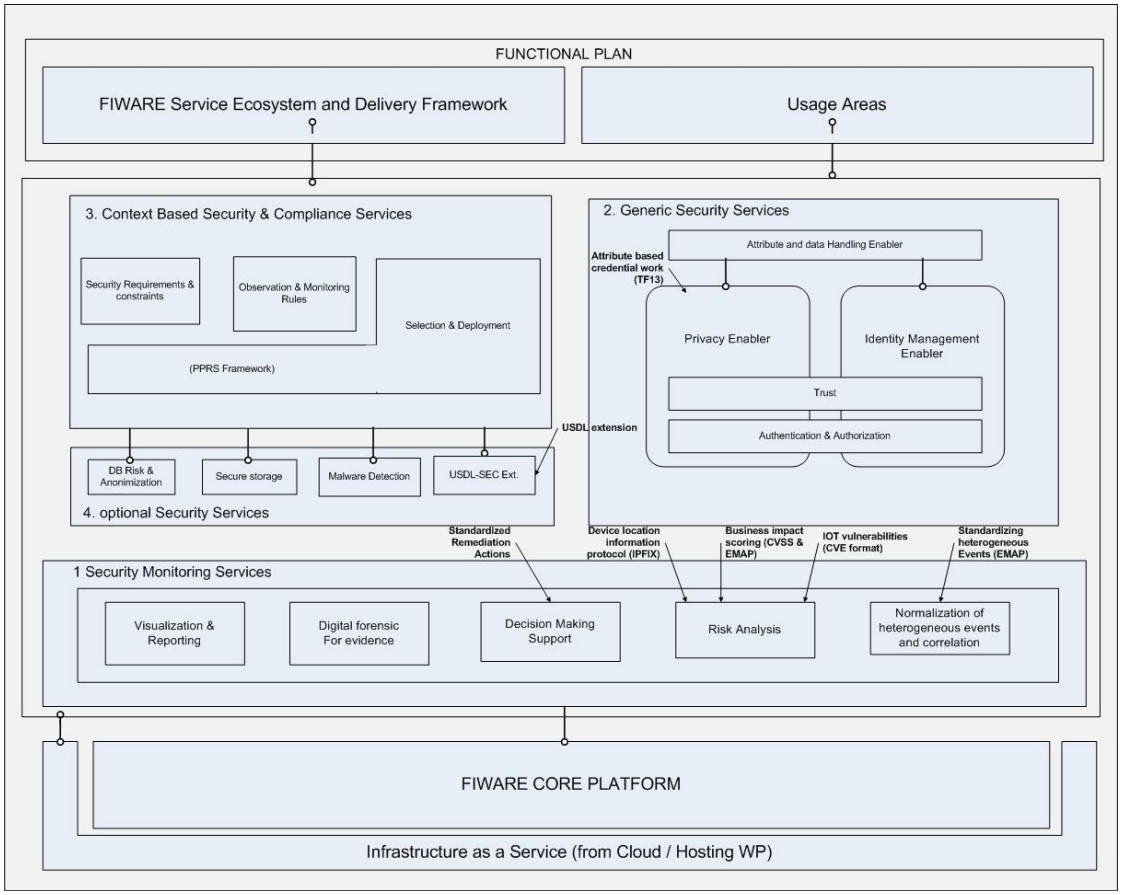


Figure 8: FIWARE Security Architecture

3.7.2 Standardization contributions of the Chapter

Hereafter we describe for each GE or group of GEs within the scope of Security Chapter the SDOs that were used, monitored and/or contributed toward.

3.7.2.1 *Security monitoring GE*

With respect to **Security monitoring GE**, de-facto standards in widespread use were monitored and incorporated so as to deliver a GE whose features are aligned with current best practice, as reported below:

- With respect to **normalization and correlation of heterogeneous events** we did investigate **Event Management Automation Protocol (EMAP) from NIST** which is a suite of interoperable specifications designed to standardize the communication of event management data. EMAP is an emerging protocol within the NIST Security Automation Program, and is a peer to similar automation protocols such as the Security Content Automation Protocol (SCAP). Where SCAP standardizes the data models of configuration and vulnerability management domains, EMAP focuses on standardizing the data models relating to event and audit management. At a high-level, the goal of EMAP is to enable standardized content, representation, exchange, correlation, searching, storing, prioritization, and auditing of event records within an organizational IT environment.

- To access information on security vulnerabilities from scanner (e.g. NESSUS) scan we rely on **Common Vulnerabilities and Exposures (CVE) from NIST** which is a dictionary of common names (i.e. CVE Identifiers) for publicly known information security vulnerabilities. We also have contacted other chapters (e.g. Cloud, IoT, etc.) to take account of their specific inputs. This is a possibility the Security Monitoring GE offers to not only deal with publicly known information but also with (domain) specific or privately known
- Risk level computation by **MulVAL attack Paths engine feature of Security Monitoring** GE, at each node of a network, is based at first step on **Common Vulnerability Scoring System (CVSS) from NIST**. The score assessment has then been extended at the path level: thus, for a given target node, each path leading to that node is given a score and the score of each path reflects the risk associated to the path as a whole. In a second step the scoring capacity has been improved so as to take account of the business impact.
- For remediation feature of Security Monitoring GE we took inspiration from the technical specification for the **Security Content Automation Protocol (SCAP Version 1.2) from NIST** for developing our Remediation App. But the added value of the Remediation app is to take into account the impact of business through the Scored Attack Paths and the opportunity to verify the impact of countermeasures thanks to the MulVal attack Paths Engine.

Overall for Security Monitoring GE we relied on US standards from National Institute of Standards and Technology (NIST) due to the lack of standards on the Cyber Security field in EU. This situation may change soon, considering that ETSI, the leading ICT standards organization, has opened recently (March 2014) a new technical committee on Cybersecurity to address the growing demands for standards in this field.

With respect to the second group of GEs focusing on Identity and Access Management, as well as Privacy, the following standards were used and activities were performed:

3.7.2.2 *Identity, Access Management and Privacy*

Identity Management GE: The identity Management Chapter focused mainly on implementation of OAuth 2.0 (from IETF OAuth WG) for each of the GE Reference Implementations. In the last steps a standard was adopted called SCIM (System for Cross-domain Identity Management). SCIM was created to simplify user management in the cloud by defining a schema for representing users and groups and also a REST API for all the necessary CRUD (Create, Read, Update, Delete) operations. The SCIM API has now been implemented in the open source version of IdM GE (i.e. KeyRock from UPM).

Access Control GE: Regarding access control GE the standard mainly monitored and used was eXtensible Access Control Markup Language (XACML) of OASIS. A number of other standards were also incorporated i.e. HTTP (IETF), SSL/TLS (IETF), X.509 (ITU-T), OAuth (IETF), JSON (IETF), JSON Web Token (IETF).

The standardization activities performed here led to an Access Control GE reference implementation compliant to XACML 2.0. Furthermore, it was undertaken to monitor XACML 3.0, which is of interest for the next release of Access Control GE (through a FIWARE follow-up project). Except for the core specification, the XACML v3.0 profiles are not yet released as

standards, therefore they are still being updated; moreover, new profiles are being worked on (working drafts) and getting momentum. For those reasons, the progress of these XACML specifications is continuously monitored.

Privacy GE: Concerning the privacy GE, the SDOs which have been supported/encouraged in connection with FIWARE work were:

- ISO/IEC JTC 1 SC 17/WG 10 on privacy-enhanced driving licenses. Preliminary work on a concrete application for credential technologies on chip cards for driver's licenses.
- ISO/IEC 18013, where use cases have been elaborated for privacy-enhanced driving licenses and concepts of such licenses.
    - Creation of a new Task Force (TF13) on privacy protection for electronic driving licenses.
    - We have finalized the documents on use cases and requirements for privacy-enhanced driver's licenses. Those documents can act as reference for future technical work on privacy-enhanced driver's licenses.
    - Distribution of document through ISO/IEC SC 17
- ISO/IEC JTC 1 SC 17/WG 4 on chip cards
    - Contributions related to privacy-enhanced authentication for chip cards related to ISO/IEC 19286. Those contributions comprise general contributions on terminology and definitions related to those of SC 17/WG 10 as well as technical contributions related to using Privacy-ABCs for chip authentication.
- ISO/IEC JTC 1 SC 27/WG 5, WG 2
    - Launching a joint study period on privacy-preserving identity management with the goal of standardizing high-level aspects related to Privacy-ABCs as well as cryptographic protocols associated with privacy-preserving credential systems.

The above efforts were done in a closely-concerted manner to facilitate the future deployment of credential-based authentication technologies through having aligned standards in different domains.

3.7.2.3 *Other major contributions to SDOs from the Security Chapter*

- **USDL-SEC** (the security extension to USDL; see W3C Incubator Activity report on USDL [11] allows for an explicit representation of a service's security features. The use of USDL-SEC has been promoted within the Chapter so as to allow security services (mainly optional security GEs) used by Context-based Security and Compliance GE to be described using USDL and its Security extension. USDL-SEC is a specification that uses Linked Data (LD) semantic web principles and technologies to interconnect security information with other descriptions and contents. USDL-SEC acts as “trait d'union” with business and functional information, thus contributing to the constitution of a comprehensive description of a service. It provides an overview of a service's security features, that can refer to a more exhaustive and fine-grained description. In this way, processes like service discovery and provisioning based on LD can make use of service's multi-faceted descriptions (comprising functional, business and security aspects), to better assist users in their decision making process.

- **IP Flow Information Export (IPFIX) Metering Process Location** was submitted to IETF, comments from the **Internet Engineering Task Force** (**IETF) IPFIX** and Internet Research Task Force (**IRTF) Network Management Research (NMR) groups** were received.

3.7.3 Open Source communities addressed

A number of Generic Enabler implementations have been provided via GitHub. This is especially the case for Privacy GE (IBM), Data Handling GE (SAP), DBA (SAP) and IdM GE KeyRock (UPM).

3.8 Advanced Middleware and Web-Based User Interfaces (MiWi)

3.8.1 Standards used by the Chapter

The Advanced Middleware and Web-Based User Interface Chapter consists of two GEs from two different but related areas:

3.8.1.1 *Advanced Middleware*

The work of the Advanced Middleware GE is mainly based on OMG (Object Management Group) Standards, but also using some Open Source Industry standards.

In the OMG our work was based on:

- OMG DDS (Data Distribution Service): DDS is the basic communication engine for the advanced middleware.
- OMG RPC over DDS: Remote Procedure Calls over DDS. This standard has been developed during the FIWARE Project, eProsima is one of the main submitters, and we delivered an RPC over DDS implementation as part of the advanced middleware
- OMG IDL (Interface Definition Language): We use this IDL spec for the advanced middleware, and the mappings IDL to C++11, and IDL to Java (also standards)
- OMG CDR: Common Data Representation: This is a standard for Data Serialization, and we provide a standalone implementation as part of the advanced middleware deliverables.
- OMG DDS Security: We use the pluggable security architecture of this standard as the basis for the advanced middleware security.

Open Source Industry-Standards used are:

- Apache Thrift IDL (Interface Definition Language): We used this specification to in the implementation of the advanced middleware KIARA component.
- JSON RPC 2.0 (JavaScript Object Notation Remote Procedure Calls) is used as a serialization protocol in the advanced middleware KIARA component.

3.8.1.2 *Advanced Web-Based User Interfaces*

The activities of the chapter with regard to the Advanced Web-Based User Interfaces are based mainly on Web Standards, first and foremost HTML5, but also including many related Web standards, such as CSS, DOM, DOM Events, Javascript, WebGL, WebCL, WebRTC, WebSockets, WebComponents, and others.

The 3D-UI-GE XML3D uses and extends HTML using a so-called polyfill approach, where a set of new apparently native HTML5 tags/elements are simulated through an implementation in Javascript. A simple inclusion of a Javascript file is sufficient for this. By design XML3D also reuses and builds many other Web standards. Examples are the DOM-Event attributes like “onclick=” or “onmouseover=”. They show exactly the same semantics and behavior on new XML3D elements as on traditional HTML5 elements. This greatly reduces the learning curve for XML3D.

The Synchronization GE uses the WebSocket protocol for communication between web clients and the server. For the server C++ implementation of the WebSocket protocol, we use the websocketpp open source library at https://github.com/zaphoyd/websocketpp which we forked at https://github.com/realXtend/websocketpp for improvements needed in REST API use. However the changes were not (yet) contributed back.

The **DaaS GE** contribution by Cyberlightning took extensive use of the omxplayer open source project (https://github.com/huceke/omxplayer) to build a display wall using raspberry PI devices. The h.264 standard video format was used for video distribution, but apart from that no specific contributions were necessary towards standardization.

The Virtual Characters GE uses the WebGL hardware-accelerated graphics rendering standard for browsers and the Three.js open source rendering library (see https://github.com/mrdoob/three.js/). We actively follow the development of Three.js but did not contribute to it so far.

The **Cloud Rendering GE** is centered around the WebRTC technology, on both the renderer and client implementations. The specifications can be found at http://w3c.github.io/webrtc-pc/. At the time WebRTC was in its infancy for general purpose use, but nowadays it is a widely used technology and all the evergreen browsers implement the technology required to utilize it. We did not participate in standardization efforts or contributed to the open source project. We used the native C library and its API as the base of the renderer from https://code.google.com/p/webrtc/.

The **2D UI/Input GE** utilized a lot of open source projects for input and for the UI part with WebComponents, but we did not need to contribute to these projects. The UI part explored the very new WebComponents technology, which is a W3C standard (http://www.w3.org/TR/components-intro/); here we did have a need to participate in the standardization efforts. The main library used was polymer, which has now progressed and is the main UI library that Google uses for both Android and the web (https://www.polymer-project.org/).

The **Interface Designer GE** did not directly use any standards, other than indirectly WebGL for the rendering (https://www.khronos.org/registry/webgl/specs/1.0/). The library itself was

made compatible with realXtend WebTundra (https://github.com/realXtend/WebTundra) and XML3D (https://github.com/xml3d/xml3d.js) client/renderer libraries.

3.8.2 Standardization contributions of the Chapter

3.8.2.1 *Advanced Middleware*

Partners of the Advanced Middleware task (EPROS, DFKI, ZHAW) are member of the OMG (Object Management Group). During the last two years EPROS (DFKI & ZHAW monitoring & voting) has been working in these standards with the following results:

- RPC over DDS Standard Final Submission: After two years, we finally agreed with the other submitters for a common standard, we have an approved joint submission and it will be released mid-2015.
- DDS Security Standard: Final Joint submission (eProsima, RTI, PrismTech); the standard has been released in June 2014.

EPROS also contributes to the MIP standards (Multilateral Interoperability Programme), an International organization of 27 countries to standardize data models and middleware for joint defense operations. eProsima is part of the Spanish delegation and works to standardize the use of WP 13 in this scenario.
Some main contributions and meetings attended are shown in the public wiki, such as the latest eProsima presentations of RPC over DDS in the OMG technical meetings.

3.8.2.2 *Advanced Web-Based User Interfaces*

The 3D-Web technology XML3D and Xflow have been originally suggested as SEs within the FI-CONTENT project (in Phase 1). They have then been promoted for usage within GEs by the FI-PPP Architecture Board, and are now part of WP13 of FI-WARE/FI-Core, where a consortium of six partners is further developing and maintaining this technology as a GE within the FIWARE.

Features to be standardised

The main features of XML3D include the definition of 3D entities (generic 3D data, geometry, shaders, animation, lights, camera, etc.) as an extension to the HTML-5 data model. This is augmented with a JavaScript (JS) implementation of the data model and its functional extensions to the HTML-5 DOM (APIs). The library “xml3d.js” implements this API and provides all the necessary functionality as a “polyfill” implementation (JS emulation of a possible future native browser implementation).

Closely connected to XML3D is Xflow, which provides a generic dataflow specification and implementation of functionality necessary for today’s highly dynamic and generic scene graphs, including animation, image processing, Augmented Reality, post processing, generic computational kernels, and related features.

A further key element related to XML3D is shade.js for the flexible and portable specification of material properties for 3D elements, the efficient transfer of assets across the Internet via BLAST, and new efficient, flexible, and reconfigurable instantiation mechanisms. Together they

have an extremely high potential for the European industry, as no such capabilities are available yet.

We are currently putting together a full specification of these technologies as a basis for possible standardization.**Current standardisation activities**

The W3C Dec3D group meets regularly to discuss all necessary topics related to preparing the standardisation. We have held courses and presentations at major events, including Siggraph, Web3D, WWW, W3C TPAC, and others. Particularly for Web3D and Siggraph conferences in August 2014, DFKI has organized workshops, tutorials, several paper presentations, and demos. We also presented our XML3D and rendering technology on the Intel booth at the large Siggraph exhibition floor this year.

Internally, we are preparing a draft for a possible submission of XML3D as a standardisation proposal. DFKI has also finished a new material model for XML3D as one of the remaining major gaps that XML3D had.

Perspective and future standardisation strategy

DFKI is currently working on the specification of the XML3D/Xflow technology, preparing a comparison to competing technology, and intends to submit this for standardisation. Similar activities are performed for the Khronos topics.

However, it is yet unclear how to cover the significant resources such a standardisation activity takes. We hope to get the support of the FI-WARE, FI-Core, FITMAN, and FI-CONTENT 2 partners for such activities.

3.8.3 Open Source communities addressed

All GEs of this Chapter are Open Source and many of them are available on Github.

- Advanced Middleware Components: https://github.com/eProsima
- 3D-UI XML3D: https://github.com/xml3d/
- In 3D-UI Three.js we work continuously with the three.js open source communities (http://threejs.org/, https://github.com/mrdoob/three.js as it is the graphics renderer in our 3D-UI deliverable
- XML3D HW-Support (Cyberlightning): Several code contributions have been made to the XML3D open source project, enabling parallel processing features in 30eseria browser applications. The work is split to support the WebCL and WebGL standards, the program code is written to work with all modern browsers supporting these standards, and a test framework is written to cover complete functionality for parallel processing features. All code contributions are distributed among the following pull request packages: (https://github.com/xml3d/xml3d.js/pull/78 https://github.com/xml3d/xml3d.js/pull/55, https://github.com/xml3d/xml3d.js/pull/49, https://github.com/xml3d/xml3d.js/pull/44, https://github.com/xml3d/xml3d.js/pull/43, https://github.com/xml3d/xml3d.js/pull/41, https://github.com/xml3d/xml3d.js/pull/33

- The **Interface Designer GE** contributions were made to WebTundra (https://github.com/realXtend/WebTundra) during the development, either directly by the GE 31eseri, or by reporting bugs that were then fixed by the WebTundra GEs developers.
- **GIS:** All changes enabling 3D content for map services were contributed to the 31eseri geoserver project and are W3DS extensions/standards. All resulting 31eseri work has been published as open source (31eseria 31eseri geoserver project, https://github.com/geoserver/geoserver/pull/517).
- **Real/Virtual Interaction:** https://github.com/Cyberlightning/WeX-RealVirtual-Backend https://github.com/Cyberlightning/WeX-RealVirtual-AndroidApp
- In the **FIWARE Demo** we did a study and research phase on the vicizities library, which is used to fetch the map tiles and buildings from open sources. We realized enhancements and bug fixes in the 31eseri library and contributed back to the 31eseri project. Our fork is https://github.com/Adminotech/vizicities, and the main pull requests are https://github.com/vizicities/vizicities/pull/97 and https://github.com/vizicities/vizicities/issues/99.

4 Conclusions & Lessons Learned

The activities from the different chapters show that standards have been (and still are) playing a role in FIWARE. In all chapters a number of standards have been used in the definition and implementation of Generic Enablers, and gaps regarding the availability of standards have been filled with own specifications. Both requirements and solutions from FIWARE were used to influence SDOs, and GE implementations served as reference implementations of standards. Outstanding examples of FIWARE standardization activities are the USDL contributions from the Applications & Services Ecosystem Chapter, the semantics work item in ETSI M2M and oneM2M by the Internet-of-Things Service Enablement Chapter, the NGSI binding defined in joint work of the Internet-of-Things Service Enablement Chapter and the Data & Context Chapter, and the Equinox gateway implementation by the Interface to the Network and Devices Chapter.

The overall approach of FIWARE is to establish a novel ecosystem of Future Internet technology enablers. Due to the involvement of major European technology and telecommunication providers, who were already extensively active in relevant standardization bodies, an additional urgent need for targeted standardization in external bodies was not felt by the majority of consortium members.

Regarding external influence on standardization, the strategy of the technical Chapters was an opportunistic one, namely, to use standards whenever they existed and were suitable, to create own APIs otherwise, and to bring own APIs back to standardization whenever this was possible without much extra effort by the existing SDO activities and links of consortium members.

The focus was more on building a community around the FIWARE platform, and the internal interoperability issues have been solved to a large extent. Making FIWARE a de-facto standard for Future Internet is on the roadmap. A careful coordination of standardization activities in SDOs will further be needed to ensure that the standardization efforts effectively contribute towards this goal. There are a therefore a number of activities of FIWARE which are top candidates to be considered for a follow-up in standardization work:

- Applications & Services Ecosystem Chapter: Identify SDO/Fora where the Marketplace & Store API might be successfully contributed
- Cross-Chapter: OMA NGSI 9 and 10 would benefit from contribution of an explicit JSON binding (currently only defined-by-example within FIWARE)
- Security Chapter: There is an opportunity to incorporated XACML v3.0, when it is completed, into a future release of Access Control GE
- Security Chapter: There is an opportunity to react to comments from IETF and IRTF about the IPFIX Metering Process Location

5 References and Bibliography

[1] "Adaptive entry strategies under dominant standards. Hybrid business models in the Open Source software industry" by Andrea Bonaccorsi, Cristina Rossi, Silvia Giannangeli (2006). See http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.3.9296

[2] "The Changing Nature of Technical Regulation in Telecom Networks" by Richard Hawkins, see http://lirne.net/resources/tr/chapter15.pdf published as Chapter 15 of "Changing Nature of Technical Regulation" (2002) a publication of LIRNE.NET, Technical University of Denmark Center for ICT (CICT)

[3] "Compatibility and Proprietary Standards: The Impact of Conversion Technologies in IT-Markets with Network Effects" by Charles Zhechao Liu, Esther Gal-Or, Chris F. Kemerer, Michael D. Smith, in Information Systems Research, Vol. 22, No. 1, March 2011, pp. 188–207. See http://www.pitt.edu/~ckemerer/compatibility-and-proprietary-standards.pdf.

[4] "Co-operation and Competition in ICT Standards Setting" by Kai Jakobs and Michael Wallbaum. Presented at: SCORE Conference 2005. See http://www.researchgate.net/publication/240642465_Scores_of_Rule-Setters_-_Co-operation_and_Competition_in_ICT_Standards_Setting .

[5] "Digital Enclosure: The Privatization of Standards and Standardization" by Timothy Schoechle, International Center for Standards Research, University of Colorado, Boulder, in "3rd IEEE Conference on Standardization and Innovation in Information Technology", Technical University of Delft, The Netherlands, October 24, 2003. See http://www.researchgate.net/publication/4047848_Digital_enclosure_the_privatization_of_standards_and_standardization

[6] "The Economics of Standards Wars" by Victor Stango, Federal Reserve Bank of Chicago, in "Review of Network Economics Vol.3, Issue 1 – March 2004". See http://citeseerx.ist.psu.edu/viewdoc/summary;jsessionid=A10C9A53216500D11BC2FAB1254A95AF?doi=10.1.1.200.2784

[7] "Platform Competition in Telecommunications" by Jeffrey Church and Neil Gandal, July 22, 2004, in "The Handbook of Telecommunications Volume 2" edited by M. Cave, S. Majumdar, and I. Vogelsang. See www.tau.ac.il/~gandal/platform.pdf

[8] "Improving the Standardization Process: From Courtship Dance to Lawyering: Working with Bulldogs and Turtles" by Michael B. Spring, 1999. See www2.sis.pitt.edu/~spring/papers/improve.pdf

[9] FIWARE Deliverable 12.4.3: Report on Campus Party Events, September 2014

[10] https://forge.fi-ware.org/plugins/mediawiki/wiki/fiware/index.php/Standardization_Activities

[11] www.**linked-usdl**.org

[12] http://linkeddata.org/

[13] http://www.w3.org/2012/ldp/charter

[14] www.openstack.org/

[15] http://forge.FIWARE.org/plugins/mediawiki/wiki/fiware/index.php/Summary_of_FIWARE_API_Open_Specifications

[16] http://en.wikipedia.org/wiki/Model%E2%80%93view%E2%80%93controller

[17] https://wiki.openstack.org/wiki/Swift

[18] http://www.dmtf.org/standards/ovf

[19] http://www.ogf.org/

[20] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=tosca

[21] http://dmtf.org/standards/cloud

[22] http://ec.europa.eu/digital-agenda/en/news/cloud-standards-coordination-final-report

[23] Sneps-Sneppe, Manfred, and Dmitry Namiot. "About M2M standards and their possible extensions." *Future Internet Communications (BCFIC), 2012 2nd Baltic Congress on*. IEEE, 2012.

[24] FIWARE Deliverable D2.3.3: FIWARE Architecture, August 2014

[25] ISO/IEC 17788:2014 - Information technology -- Cloud computing -- Overview and vocabulary, available at http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=60544

[26] ISO/IEC 17789:2014 - Information technology – Cloud computing – Reference architecture, available at http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=6045

[27] ETSI Cloud Standards Coordination Final Report, available at http://csc.etsi.org/Application/documentApp/documentinfo/?documentId=204&fromList=Y

[28] Keven T. Kearney, SLAware Service Level Agreements Specification, Version 1.0, January 2012

Appendix: FIWARE Standardization Wiki

The following pages were automatically generated from the FIWARE public wiki.

1 Standardization_Activities

You can find the content of this chapter as well in the wiki of fi-ware.

5.1 Introduction to FI-WARE Standardization

The Initial standardization plan was a very broad survey of standardization organisations and their work areas which are relevant to FI-WARE, together with a categorization of whether work in each SDO should continue to be monitored or whether additional contributions were necessary to support open standardization of FI-WARE. This page (and linked pages) is a continuously updated record of activities for standardization.

There are six project areas where, as determined in the initial plan, external standardization activities are relevant:

- Cloud Hosting
- Data Context Management
- Internet of Things
- Applications Services Ecosystem
- Security
- Networks and Devices

This set of wiki pages provides a framework and initial results for such monitoring/contributing, centered around a set of tables which can be easily updated by individuals in each topic area within the FI-WARE project. Tabular format was chosen so as to (a) keep information concise; (b) allow merging/import into databases; (c) provide visual feedback to team members of history/progress in each area.

Currently three types of tables are used:

1. **Planned Activities** for SDOs (contributions/monitoring) for each relevant FI-WARE interface
2. **Responsible Persons** for each SDO activity
3. **Timestamped Summary** of contributions/monitoring as they occur, and also a record of any known inclusions of partner or external IPR in the open standards

Examples of the tables using explanatory "content" are shown below:

Example: Planned Activities						
Date of activity	SDO as link	Exposed FI-WARE Interface	Contribute or Monitor	SDO work-item or topic to monitor/contribute	Responsible Partner(s) and Person(s)	Stds-Phase, Comment & Status
(Date is approximate. Insert word "plan" or sequence number if not yet clear)	(SDO name is used to facilitate merging all activities on all topics for this SDO)	(FIWARE I/F name allows merging all tables and filtering to see all activities on this interface)	(Monitored events should be recorded also, so team members can ask for further info)	(This is the most important human-readable part, explaining where FI-WARE will be active.)	(Names of responsible persons is important for tracking and feedback)	(Update this status for significant changes; history is seen by looking back in the table)

Example: Responsible Person(s)				
SDO	Exposed FI-WARE Interface	Responsible Partner	Responsible Person	Comment
(SDO name same as in Table 1)	(Exposed FI-WARE Interface name same as in Table 1)	(Responsible Partner organisation)	(Responsible Person)	(Comment, including official positions or editorships, etc)

Example: Timestamped Summary						
Dates	SDO or event	Contribution title and SDO ID	Exposed Interface	responsible partner	responsible person	phase/IPR/comment/status
(Date of contribution or meeting)	(SDO name is used to facilitate merging all activities on all topics for this SDO)	(Contribution title and SDO ID, with link to actual contribution)	(FIWARE I/F name allows merging all tables and filtering to see all activities on this interface)	(Responsible FI-WARE partner is for tracking)	(Names of responsible persons is important for tracking and feedback)	(Update this status for significant changes; history is seen by looking back in the table)

5.2 FI-WARE interfaces/protocols for Standardization

To make FI-WARE software and services accessible to external users, a number of references points and protocols need to be carefully defined for their use. Ideally, these "exposed" interfaces should be aligned with existing industry norms or, if that is not advisable, should be

developed into industry norms through activities of FI-WARE members in the relevant SDOs. If such collaboration is too slow, the FI-WARE exposed interfaces can of course also be openly published during the lifetime of the project, leading in the course of time and by increasing use to a so-called "de-facto standard".

Furthermore, interaction of modules within the framework of FI-WARE also requires programming interfaces and reference points for use by software developers *within* the FI-WARE platform. FI-WARE partners have benefited enormously from "prior art" in the software community and the re-use of existing standards and best-practice is highly encouraged. Accordingly, gradual changes in the specification of such interfaces within their responsible SDO also need to be monitored and FI-WARE needs to consider how/when to update the internal usage of those interfaces/protocols. This therefore requires monitoring of a number of SDO activities, without however a need to contribute.

In each of the chapters below an architecture diagram is shown (duplicated from other sections of this wiki, which are referenced) to indicate the interfaces which are candidates for standardization.

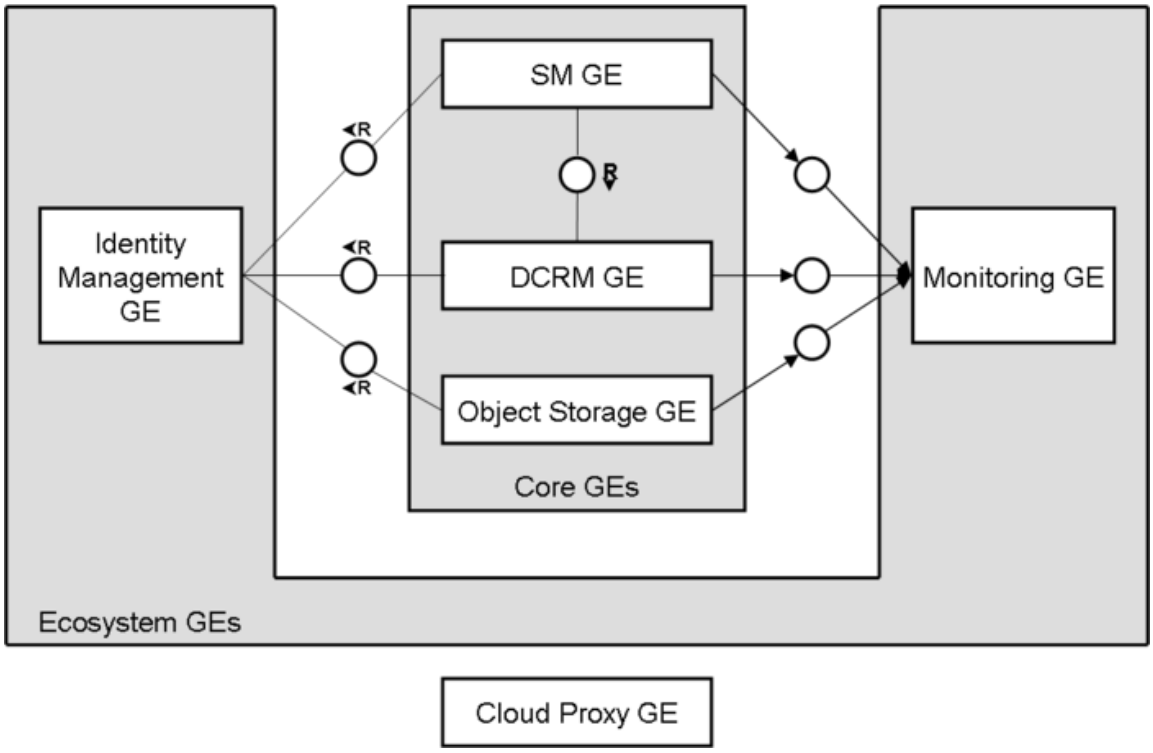
Within FI-WARE, the setting up of the correspondence of interfaces to specific SDOs is referred to as "mapping", so each of the chapters below contains the "mapping" within each FI-WARE topic area.

5.3 Mapping_Cloud_Hosting

You can find the content of this chapter as well in the wiki of fi-ware.

- Contact fiware-standardization@lists.fi-ware.eu

Figure 1: Architecture for Cloud Hosting, with reference points for standardization



For discussion of this architecture, see Cloud_Hosting_Architecture

Table 1: Planned Activities for SDOs (contributions/monitoring) for Cloud Hosting

Planned Activities for SDOs for Cloud Hosting						
Dates or ID	SDO as link	Exposed FI-WARE Interface	Contribute or Monitor	SDO work-item or topic to monitor/contribute	Responsible Partner(s) and Person(s)	Stds-Phase IPR-issues Comment & Status
1	OpenStack foundation	IaaS DataCenter Resource Management, IaaS Service Manager	Contribute	To be determined, based on evolution of corresponding GEs	TID (Fernando López), IBM (Alex Glikson)	Emerging open source project developing IaaS implementation and an API
2	SNIA	Object Storage, IaaS Service	Monitor, consider contribution in	To be determined, based on evolution of corresponding	IBM, TID	IBM and TID are involved in CDMI beyond the team working on FI-WARE

		Manager	the future	GEs		
3	OGF	IaaS DataCenter Resource Management, IaaS Service Manager	Contribute	OCCI specification updates are being drafted for JSON rendering, XML rendering and for SLA Monitoring. Feedback from GE experiences and testbed deployment already being incorporated.	Intel (Thijs Metsch, John Kennedy). TID (Fernando López)	People involved in FI-WARE on behalf of Intel are leading the OCCI work.
4	ISO JTC1/SC38	IaaS DataCenter Resource Management	Contribute	Contributions made to Cloud Vocabulary and Reference Architecture draft standards via the Irish national mirror to SC38. Learnings from FI-WARE taken on-board.	Intel (John Kennedy)	A member of the Intel FI-WARE team is on the national mirror committee for JTC1/SC38, the ISO sub-committee with responsibility for cloud standards, and insights and contributions based on GEs, the FI-WARE Interfaces and initial FI-WARE deployments are being fed back into SC38 deliberations.
5	OVF DMTF CIMI DMTF	IaaS DataCenter Resource Management, IaaS Service Manager	Contribute	To be determined, based on evolution of corresponding GEs	TID (Álvaro Polo Valdenebro), IBM (Doug Davis)	
6	TOSCA OASIS	IaaS Service Management, PaaS Management	Contribute	To be determined, based on evolution of corresponding GEs	IBM	IBM is involved in TOSCA beyond the team working on FI-WARE
7	HGI	Cloud Proxy	Monitor	To be determined	Telecom Italia, Technicolor	HGI is the "Home Gateway Initiative", the partners of this consortium (http://www.homegatewayinitiative.org) are leading operators and vendors. Its goal is to publish requirements for components for the home network, thus, it is in line with the goals of some GEs of FI-WARE (for example, the Cloud Proxy. We hope to be able to use HGI as a way to promote FI-WARE results.
8	ETSI CSC	IaaS Service Management, Object Storage, IaaS	Contribute	Contribute to ETSI Cloud Standards Coordination activities,	Intel (John Kennedy)	FI-WAREs Intel representative collated and edited several sections of the final report, with several standards contributed by FI-WARE included in the

		DataCenter Resource Management		documenting current cloud standards and specifications and identifying some conclusions for consideration by the European Commission.		report. Key observations added were called out at the Public launch of the document. Final report published November 2013.

Table 2. Responsible Persons for each SDO activity for Cloud Hosting

Responsible Persons for each SDO activity for Cloud Hosting				
SDO	Exposed FI-WARE Interface	Responsible Partner	Responsible Person	Comment
OGF	IaaS DataCenter Resource Management	Intel	Thijs Metsch, John Kennedy	Thijs is a co-founder and co-chair of the OCCI Working Group to which this interface is being contributed.
ISO	IaaS DataCenter Resource Management	Intel	John Kennedy	John is on the national mirror committee to ISO JTC1/SC38 responsible for cloud standards.
SNIA	Object Storage	IBM, Intel	Thijs Metsch (Intel), Doug Davis (IBM)	Plan to contribute feedback to future releases of the CDMI specification.
DMTF	IaaS DataCenter Resource Management, IaaS Service Manager	TID, IBM	Fernando López (TID), Alex Glikson (IBM)	Plan to monitor closely releases of the CIMI and OVF specification and possible feedback contribution to them. IBM is the co-chair of CIMI (beyond FI-WARE team).
OASIS	IaaS Service Manager, PaaS Management	IBM	Alex Glikson (IBM)	IBM is the co-chair of TOSCA (beyond FI-WARE team).
OpenStack foundation	IaaS DataCenter Resource Management, IaaS Service Manager	TID, IBM	Fernando López (TID), Alex Glikson (IBM)	Plan to contribute to OpenStack Compute API specification in order to enable reference implementation of the new features developed in FI-WARE
ETSI	IaaS DataCenter Resource Management, IaaS Service Manager, SLAware	Intel	John Kennedy, Joe Butler (Intel)	Incorporating learnings from FIWARE into output report of Cloud Standards Coordination initiative.

Table 3. Timestamped Summary of contributions/monitoring for Cloud Hosting

Timestamped Summary of contributions/monitoring fhttps://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/Mapping_Cloud_Hostingor Cloud Hosting

Dates	SDO or event	contribution title and SDO ID	Exposed Interface	Responsible partner	Responsible person	Phase/IPR/comment/status
2014-09-08	OGF	Learnings from SLAware submitted and included in draft of SLA extension for OCCI, presented at OGF42 London.	DCRM, SLAware	Intel	John Kennedy, Thijs Metsch	Draft SLA Extension for OCCI including FI-WARE contributions published September 2014. Feedback positive and community plans to incorporate into OCCI 1.2 to be circulated for Public Comment in October 2014.
2014-08-08	SNIA	Cloud Data Management Interface (CDMI) v1.1	DCRM	IBM		Formal specification
2014-06-23	DMTF	Cloud Auditing Data Federation (CADF) - Data Format and Interface Definitions Specification	DCRM	IBM	Matthew Rutkowski, Rick Cohen	DMTF standard
2014-01-03	DMTF	Open Virtualization Format (OVF) Specification	DCRM	IBM, TID	Fermín Galán Márquez, Oliver Benke	DMTF standard
2013-11-29	ETSI	Infrastructure perspective and proposed conclusions submitted and included in final report of ETSI Cloud Standards Coordination initiative.	Object Storage, DCRM, SLAware	Intel	John Kennedy	Final report published.
2013-11-25	OASIS	Topology and Orchestration Specification for Cloud Applications Version 1.0, TOSCA-v1.0-os [1]	IaaS DataCenter Resource Management, IaaS Service Manager	IBM	Simon Moser (IBM)	OASIS Standard
2013-09-18	ETSI/OGF/DMTF/SNIA and others	Presented OCCI, CDMI and SLAware efforts in FI-WARE at cloud standards plugfest.	Object Storage, DCRM, SLAware	Intel	John Kennedy	Presentation given.
2013-08-30	ISO	Contributions submitted to draft standards on cloud	Object Storage, DCRM,	Intel	John Kennedy	Contributions dispositioned by editing committee - majority accepted. Final draft

		vocabulary and cloud reference architecture.	SLAware			completed. Proceeding through ISO ratification process for final publication.
2012 Q2	SNIA	CDMI has gone to ISO	Object Storage	IBM	Doug Davis	
2013-06-27	DMTF	Profile to Enable Automated Deployment of OVF Packages version 1, DSP0265 [2]	IaaS DataCenter Resource Management, IaaS Service Manager	TID, IBM	Andreas Maier (IBM), Ron Doyle (IBM), Miguel Peñalvov (TID)	Formal specification, DMTF Standard
2013-03-18	OASIS	Topology and Orchestration Specification for Cloud Applications Version 1.0, TOSCA-v1.0-cs01 [3]	IaaS DataCenter Resource Management, IaaS Service Manager	IBM	Simon Moser (IBM)	Formal Specification
2012-06-20	DMTF	Cloud Infrastructure Management Interface (CIMI) Primer, DSP2027 [4]	IaaS DataCenter Resource Management, IaaS Service Manager	TID, IBM	Álvaro Polo (TID), Doug Davis (IBM)	Work-in-Progress version, it expires on: 2012-12-20
2012-06-13	DMTF	Cloud Infrastructure Management Interface - Common Information Model (CIMI-CIM), DSP0264 [5]	IaaS DataCenter Resource Management, IaaS Service Manager	TID, IBM	Álvaro Polo (TID), Doug Davis (IBM)	Work-in-Progress version, it expires on: 2012-10-30
2012-05-24	DMTF	Open Virtualization Format Specification, DSP0243 [6]	IaaS Service Manager	TID	Álvaro Polo	Work-in-Progress version, it expires on: 2012-12-15
November 2011	OASIS	Tosca TC was started in Oasis	IaaS Service Manager, PaaS Management	IBM	Doug Davis	
2011-08-30	ISO	OCCI incorporated into Final Report of Study Group on Cloud	IaaS DataCenter Resource Managemen	Intel	John Kennedy	Report Published

		Computing	t			

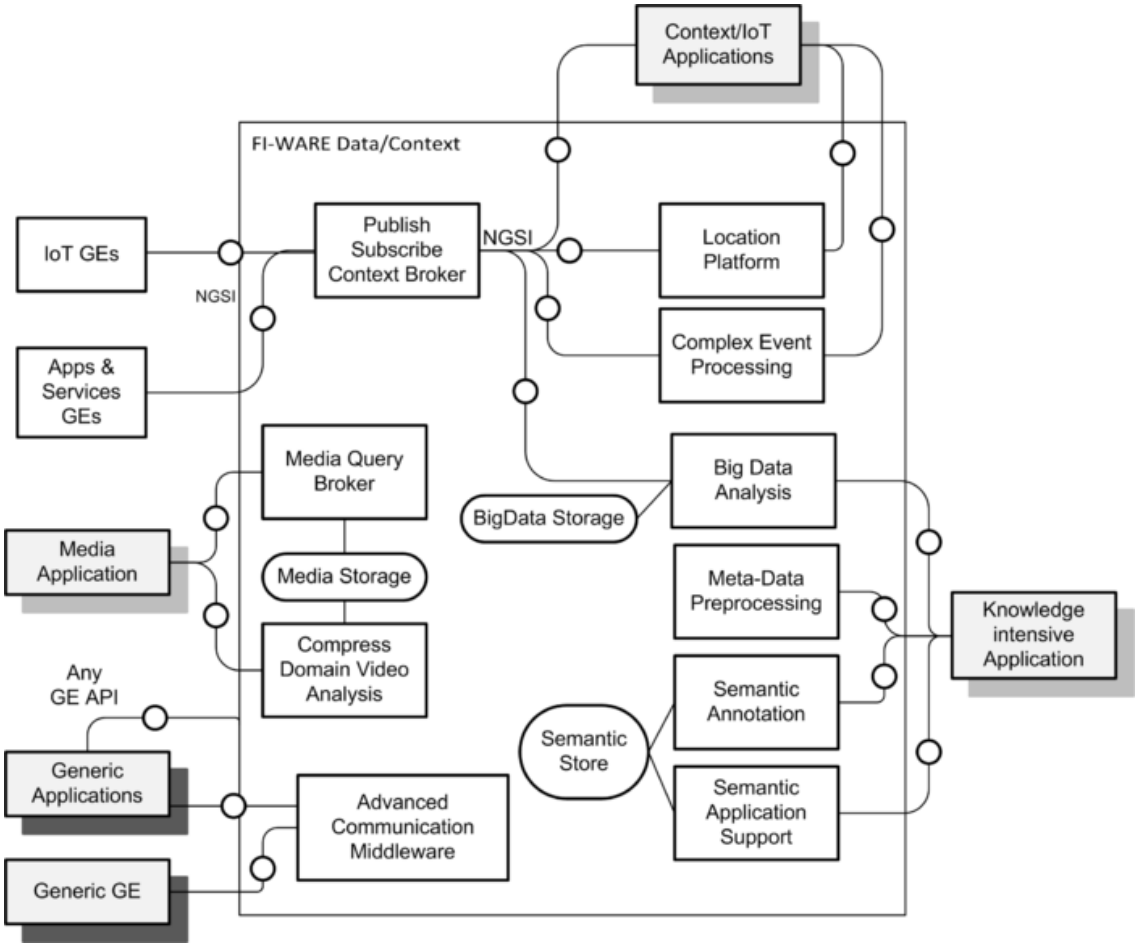
Note: the FI-WARE team will be monitoring developments in the above SDOs, both directly as well as via teams at corresponding companies directly involved in those SDOs. Specific contributions will be initiated based on the needs of the corresponding GEs -- as they evolve throughout the FI-WARE roadmap.

5.4 Mapping_Data_Context_Management

You can find the content of this chapter as well in the wiki of fi-ware.

- Contact fiware-standardization@lists.fi-ware.eu

Figure 1: Architecture for Data Context Management, with reference points for standardization



For discussion of this architecture, see [1]

Table 1: Planned Activities for SDOs (contributions/monitoring) for Data Context Management

Planned Activities for SDOs (contributions/monitoring) for Data Context Management						
Dates or ID	SDO as link	Exposed FI-WARE Interface	Contribute or Monitor	SDO work-item or topic to monitor/contribute	Responsible Partner(s) and Person(s)	Stds-Phase IPR-issues Comment & Status
Throughout the project	OMA LIF (Location Interoperability	Context Events - Location	Monitoring	MLP protocol & RESTful Terminal Location API	Tanguy Bourgault/Thales Alenia Space	First stable version of MLP and SUPL server supporting also OMA RESTful Terminal Location API.

	Forum)					
Throughout the project	ISO/IEC SC29 WG11 (MPEG) and ISO/IEC SC29 WG1 (JPEG)	Multimedia Data: Media-enhanced Query Broker (MeQB)	Monitor	MPEG Query Format (MPQF), JPSearch	Gero Bäse (SIEMENS)	Monitoring by participation at quarterly standardization meetings the advances in query languages (e.g., MPEG Query Format, JPSearch), especially their applicability for search in heterogeneous and distributed repositories.
Throughout the project	ISO/IEC SC29 WG11 (MPEG), JCT-VC	Compressed Domain Video Analysis (CDVA)	Monitor	MPEG video streams: H.264/AVC, H.265/HEVC	Peter Amon (SIEMENS)	Monitoring by participation at quarterly standardization meetings the advances in the compression of video content with respect to the respective possibility to perform compressed-domain analysis; closely monitoring the developments for High Efficiency Video Coding (HEVC), because the video compression format is likely to influence the development of future version of the FI-WARE Compressed Domain Video Analysis (CDVA) GE, for which HEVC is a good future candidate.
Throughout the project	ISO/IEC SC29 WG11 (MPEG)	Multimedia Data	Influence	Multimedia Technology	Gero Bäse (SIEMENS)	Influencing the general direction of multimedia technology in ISO/IEC MPEG by holding the position of the Head of Delegation (HoD) of Germany.
Throughout the project	ONVIF	Compressed Domain Video Analysis (CDVA)	Monitor/contribute	Open industry forum developing standards for interfaces of IP-based physical security products	Gero Bäse (SIEMENS)	Monitoring by participation and actively contributing at quarterly standardization meetings to the advances in integration and usage of standards developed in MPEG and JPEG in ONVIF specifications; standardization of the surveillance-specific additions to the metadata format, which is the output of the CDVA GE; Siemens representatives appointed as liaison officers on ONVIF and MPEG side, so standards alignment should be optimal; Siemens led the ONVIF work on interoperability analysis and, as a result, ONVIF started working

						on a new profile; Siemens proposed a FIWARE-aligned video compression technology for the new profile (based on mandates H.264/AVC).
Throughout the project	W3C	Ontologies Metadata (+ Semantic Applications Support)	Monitoring	RDF, OWL, SPARQL, Linked Data	Mauricio Ciprian/ATOS	Monitoring over different W3C channels like web page, twitter account, specific mailing list and also meeting minutes
Throughout the project	W3C	WEBRTC working group	Monitoring	WebRTC	Luis Lopez (URJC)	Monitoring, mainly through mainling lists, of the standards progress.
Throughout the project	IETF	RTCWEB working group	Monitoring	RTCWeb	Luis Lopez (URJC)	Monitoring, mainly through mainling lists, of the standards progress.

Table 2. Responsible Persons for each SDO activity for Data Context Management

Responsible Persons for each SDO activity for Data Context Management				
SDO	Exposed FI-WARE Interface	Responsible Partner	Responsible Person	Comment
OMA NGSI	Context Events	Telefonica I+D, Telecom Italia & NEC (for IoT chapter)	Fermin Galán, Boris Moltchanov & Martin Bauer (for IoT chapter)	
OMA LIF (Location Interoperability Forum)	Context Events - Location	Thales Alenia Space	Tanguy Bourgault	
ISO/IEC MPEG	Multimedia Data	Siemens	Gero Bäse and Peter Amon	
ISO/IEC JPEG	Multimedia Data, especially image metadata	Siemens	Gero Bäse	
Joint Collaborative Team on Video Coding (JCT-VC)	Multimedia Data, especially video data	Siemens	Peter Amon	
ONVIF	Multimedia Data, especially image/video and related	Siemens	Gero Bäse	

	metadata			
W3C	Ontologies Metadata (+Semantic Applications Support)	ATOS	Mauricio Ciprian	

Table 3. Timestamped Summary of contributions/monitoring for Data Context Management

Timestamped Summary of contributions/monitoring for Data Context Management						
Dates	SDO or event	Contribution title and SDO ID	Exposed Interface	Responsible partner	Responsible person	Phase/IPR/comment/status
July 2013	OMA NGSI	Context Events	OMA NGSI-9 and OMA NGSI-10 binding. Reference implementation	TID and TI (together with NEC/IoT-chapter and SAP)	Fermin Galan (TID), Boris Moltchanov (TI)	Contribution to OMA ARCH group of a document with the "mature parts" in the current FI-WARE NGSI HTTP REST binding. An introductory ppt was provided to help motivate the work. Fermín Galán (TID) wrote a pruned version of the full REST binding specification for this. Tobias Jacobs (NEC) and other NEC staff arranged the contribution. Main feedback was about required alignment with OMA REST design principles.

5.5 Mapping_Internet_of_Things

You can find the content of this chapter as well in the wiki of fi-ware.

- Contact fiware-standardization@lists.fi-ware.eu

5.5.1 Introduction to SDOs

5.5.1.1 *OMA NGSI-9/-10: Interface for Thing/Entity level information*

The OMA NGSI interface has been selected as the main interface for exchanging information and events for IoT. The OMA NGSI-9/10 data model is a core data model for FI-Ware with several components building on it. The OMA NGSI standard has reached v1.0, but is missing a REST binding, so FI-Ware has established (within the project) such a REST binding. The IoT Chapter of FIWARE has further defined an extension of NGSI to enable so-called 'Associations' that automatically translate lower-level information from Sensors to higher levels of abstraction. FI-Ware partners have introduced the REST binding to OMA, but a formal publication as an OMA standard has yet been out of scope. However, with FIWARE NGSI becoming a quasi-standard by its wide adoption throughout the European Future Internet Platform and thus extensive real-world validation, standardization within OMA is becoming increasingly attractive.

5.5.1.2 *ETSI M2M*

The second major interface identified for IoT is the ETIS M2M standard. ETSI M2M TG has achieved Release 1 and is currently working on Release 2. FI-Ware partners have identified that ETSI M2M is only looking at device information. The FI-Ware concepts of Things/Entities are not properly reflected (so far). Furthermore, ETSI M2M handles data as transparent blocks. In order to process data in a platform like FI-Ware, we need to attach syntactical and semantical information to the data. FI-Ware partner have therefore started a work item in ETSI M2M called "Semantic Support for M2M data". The goal of that activity is to ensure that upcoming versions of the standards have the necessary definitions and protocols to support semantics with M2M data. Furthermore, this enables a much more link between the ETSI M2M standard and the OMA NGSI standard.

5.5.1.3 *M2M Frontend (Gateways and Devices)*

M2M has to support a lot of different devices and gateways in the device and gateway domain. There are a large number of SDOs that are defining respective standards, e.g. the Broadband Forum, the Home Gateway Initiative, the ZigBee alliance, IETF Core, and many more. FI-Ware strategy is to at least monitor the respective standards and through contributions ensure that devices / gateways following the standards can be easily integrated into the backend system of FI-Ware.

5.5.1.4 *IoT Architectural Reference Model*

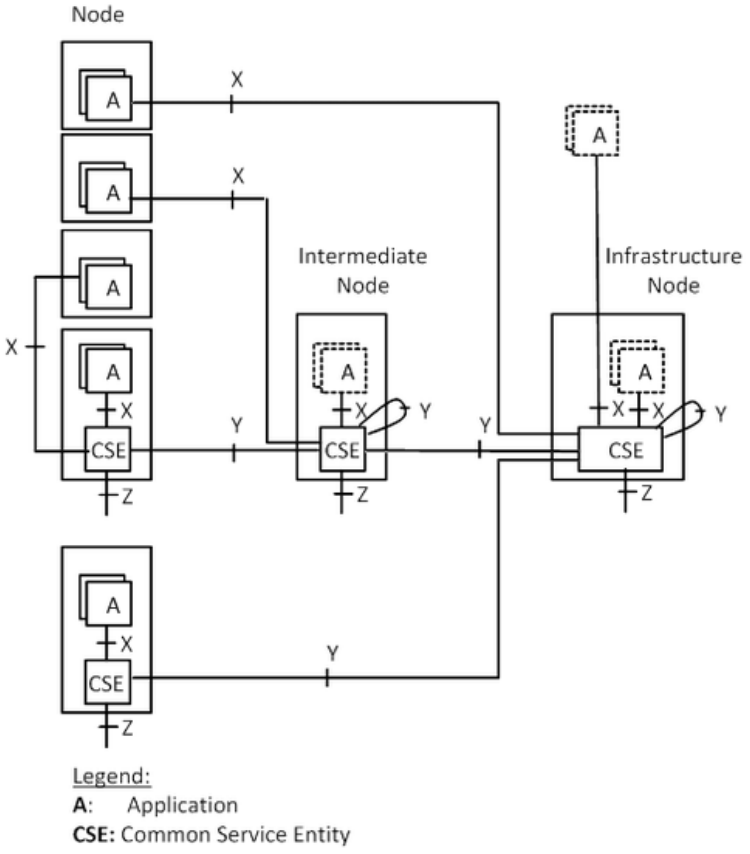
The IoT Architectural Reference Model (ARM) provides a basis for developing and analyzing IoT architectures. The ARM has been developed by the EU FP7 project Internet of Things Architecture (IoT-A) and is the basis for the IoT work in the IoT European Research Cluster (IERC). It is being handed over to the IoT Forum, a pre-standardization organization that is going to further maintain and develop the ARM. The plan is to create profiles and labels based on the ARM and the FI-WARE IoT architecture could be the basis for such a profile.

5.5.1.5 *oneM2M*

OneM2M is a partnership project, built with participation of five Standardization Bodies: ETSI, TIA, ATIS, CCSA, TTA and TTC. The consortium was officially signed in June 2011, and the first Technical Plenary meeting launched its activity in September 2012. Fi-Ware partners who are members of OneM2M are Fraunhofer FOKUS, NEC, Orange, Telecom Italia, and Telefonica.

The main objective of oneM2M, directly derived from ETSI TC M2M work, is to define interfaces and APIs of an M2M services platform, built upon devices, gateways and servers, and allowing an End to End communication chain between data's originated from the devices and related Information systems. The chosen approach (ETSI M2M originated) is network centric, REST based, i.e. devices are represented by resources. A resource Model is defined and standardized, under a tree structure, and a set of very simple commands: Create-Delete-Update-Retrieve, allows defining all possible interactions with the "real" devices and their necessary synchronization with their Models. Services are client server applications, thus http based.

A functional architecture has been defined corresponding to the following scheme:



The current status of oneM2M (updated 2013_07_01) is described into the table below, with the following highlights:

OneM2M progresses	ETSI M2M transfer
Requirements is well progressed	Almost all ETSI M2M requirements have been included and harmonized with the requirements form the other partners and members
Architecture is starting to stabilize in terms of general architecture and approach. Resource based approach has been taken.	The oneM2M approach is going in the direction of ETSI M2M (terminology is different, the concepts are the same). The API functionalities are the same. The resource based approach has been agreed on, including the resource tree (see oneM2M-ARC-2013-0287R04-High_level_Application_Programming_Interface). The identifiers are discussed to become fully compatible (see M2M-ARC-2013-0281R02-M2M_Identifiers).
Stage 3 WG3 is just started.	No oneM2M work yet.
Security	Requirements are aligned to ETSI M2M. Security studies are including ETSI M2M, but no real normative

	work started yet.
Management	Requirements are aligned to ETSI M2M. Management studies are including ETSI M2M, but no real normative work started yet. Anyhow architecture seems to go in the ETSI M2M direction. The Z interface could represent an improvement of the ETSI solution.
Interworking, abstraction and semantics	Requirements are aligned to the ETSI M2M studied solutions. No real normative work started yet.

A first release of oneM2M specifications is expected end of 2013.

Useful References:

- Public oneM2M website : http://www.onem2m.org/
- ftp://ftp.onem2m.org/Pool/: the whole set of ETSI M2M specifications made publicly available on the oneM2M ftp server.
- ETSI M2M website on the ETSI portal : http://portal.etsi.org/
- Next M2M Workshop : http://www.etsi.org/Events (6-7th November 2013)

5.5.1.6 *ITU GSI*

ITu has been working on topics related to Ubiquitous Sensor Networks as well as Internet-of-Things since a decade. Recently, a global standardisation activity for Internet-of-Things (http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx) has started. Several ITU focus groups (e.g. FG M2M, SG 2, 3, 9, 11, 13, 16, 17) are affected with lot of work being done in SG13 and SG16. Special emphasize has been put on eHealth related IoT standardisation.

5.5.1.7 *OMA Lightweight M2M*

Open Mobile Alliance is pushing for Lightweight M2M protocol that is fast becoming the global industry standard for M2M device management for the development of a fast, deployable, client-server specification to provide machine-to-machine service. Key vendors such as ARM or WirelessSierra are strongly backing this protocol which is designed to:

- Provide Device Management functionality over sensor or cellular networks
- Transfer service data from the network to devices
- Extend to meet the requirements of most any application

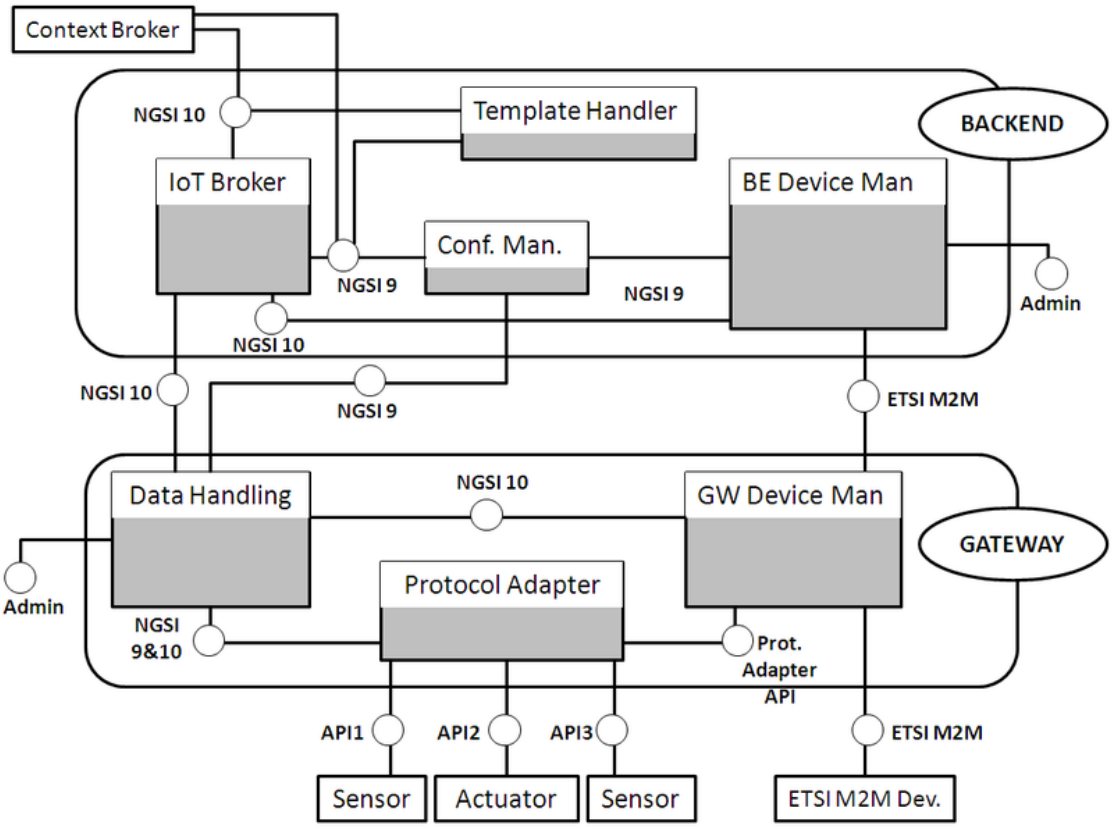
The standard defines:

- Efficient device-server communication based on IETF open Standards (CoAP and DTLS bound to UDP or SMS).

- Extensible Object and resource model for application semantics.
- Public registry of objects from OMA, other SDOs or enterprises.

5.5.2 FIWARE Activities

Figure 1: Architecture for Internet of Things, with reference points for standardization



For discussion of this architecture, see [1]

Table 1: Planned and Ongoing Activities for SDOs (contributions/monitoring) for IoT

Planned Activities for SDOs (contributions/monitoring) for IoT						
Dates or ID	SDO as link	Exposed FI-WARE Interface	Contribute or Monitor	SDO work-item or topic to monitor/contribute	Responsible Partner(s) and Person(s)	Stds-Phase IPR-issues Comment & Status
Ongoing	OMA NGSI	NGSI 9 and NGSI 10 interfaces exposed by IoT Broker, Conf. Man., BE Dev. Man., Data Hdl., GW Dev.Man.	Contribute	OMA NGSI-9 and OMA NGSI-10 binding. Reference implementation. Bug fixes and clarifications of abstract interface definitions.	Tobias Jacobs, Lindsay Frost/NEC	Binding specification finished. Implementation by several project partners and on top of several GEs. Binding presented to OMA.
Ongoing	ETSI	IoT Broker GE, Configuration	Contribute	**Work Item 1**: Members from FI-Ware have	Tobias Jacobs/NE	New work item established in ETSI M2M

	M2M	Management GE, Backend Device Management GE		continued the work item of "Semantic Support for M2M Data". This activity has the goal to include semantic support into ETSI M2M. One possible further outcome is to make the separation between thing level information and device information also a part of the ETI M2M standard. Members from FI-Ware are working together here. **Work Item 2**: Zigbee Mapping: some of the Zigbee mapping might become relevant in the future also for FI_Ware (status: monitoring, maybe contributing in the future)	C	TG. First reference use cases established. Several input documents processes. Input received from FI-Ware partners bringing the FI-Ware concept of things/entities and devices into the standard. As ETSI M2M is influencing the new oneM2M standard, the FI-WARE input will also go to oneM2M.
Ongoing	OGC	Backend Device Management GE (open specs not yet publicly released), Backend IoT Broker GE, Backend Configuration Management GE	Monitor, influence in the future	Monitoring: participated in several OGC workshops. Goal: openGIS® Standards support interoperable solutions that "geo-enable" the Web, wireless and location-based services, and mainstream IT	Juanjo Hierro/TID	N/A
Ongoing	ISO/Sensor Network Reference Architecture	IoT subsystem architecture, in general	Monitor	Read the draft specifications, monitor if there is progress, take ideas for the architecture of the IoT subsystem	N/A	N/A
Ongoing	IETF CORE	Device Management GE, Protocol Adapter GE	Monitor	Influence: Mehmet is key contributor to a number of IETF CoAP specs: Constrained Application Protocol (CoAP) (draft-ietf-core-coap-08); CoRE Link Format (draft-ietf-core-link-format-10); Group Communication	Jakob Saros/Ericsson, Jan Höller/Ericsson	key contributions

				for CoAP (draft-ietf-core-groupcomm-00); Observing Resources in CoAP (draft-ietf-core-observe-03); Blockwise transfers in CoAP (draft-ietf-core-block-07); Basic Configuration of Constrained Devices (New work proposal by Nokia)		
Ongoing	ONVIF	Device Management GE, Protocol Adapter GE	Monitor	Analysis on ONVIF by Orange, early proto implementation of an ONVIF device simulator by NSN	Laurent Artusio/Orange, Laurence Dupont/Orange	N/A
Ongoing	IETF NETCONF	Device Management GE, Protocol Adapter GE	Influence	Contributor to the NETCONF-Light protocol with TLS-binding, new work proposal: management information models for the configuration of IoT devices	N/A	N/A
Planned	ZigBee Alliance	Protocol Adapter GE	Influence	Chairing both ZigBee Gateway and Telecom Applications Profile WG	Gian Piero Fici, Telecom Italia	???
Planned	SSN-XG (Semantic Sensor Network Incubator Group)	IoT Broker GE, Configuration Management GE	Influence	SSN sensor ontology will be used and extended in defining the information model for the sensing resources in FI-WARE: ontology to describe sensors and their device, system and platform related attributes; report on semantic mark-up and to recommend methods to use ontology to describe the data available based on the existing models such as the Open Geospatial Consortium's (OGC) Sensor Web Enablement (SWE) standards	Payam Barnaghi, Tarek Elsaleh/University of Surrey	N/A

Ongoing	IoT Forum / IERC	Overall architecture	Influence	The FI-WARE architecture has been mapped to the IoT Architectural Reference Model (ARM), providing feedback to be taken into account in future versions of the ARM. Also there is the possibility of shaping one of the profiles to be developed by the IoT Forum WG according to the FI-WARE IoT architecture.	Martin Bauer/NEC	A first meeting happened in May 2013 at Future Internet Assembly to launch a common working group between IERC - Activity Chain 1 (Architecture) and Fi-Ware IoT team. It was also discussed the opportunity to have another working group between IERC-Activity Chain 4 (Semantic Interoperability). The working group AC1/Fi-Ware IoT team had a first meeting in Helsinki (June 2013 - IoT Week) to analyze convergence between the Architecture Reference Model (ARM - defined by IoT-A project) and the operational choices for implementation done by Fi-Ware. Next steps: new meeting September 2013 to analyze potential new Generic Enablers based on on-going research activities in many FP7 projects.
Planned	oneM2M	Overall architecture, Data models	Influence, Contribute	Continue the work on semantic data and abstraction that has been started in ETSI M2M, carry over the results.	Martin Bauer/NEC	What kind of sematics and abstraction will be needed in oneM2M is currently under evaluation.
Ongoing	oneM2M	Overall architecture, Interfaces	Influence, Monitor	Define interfaces of a service platform independent of the underlying network on one side, and independent of the data format on the other side, with open APIs allowing third parties to develop services in an open and interoperable services environment.	Thierry Nagellen/ Orange	Orange expectations in ETSI M2M work, was to define interfaces of a service platform independent of the underlying network on one side, and independent of the data format on the other side, with open APIs allowing third parties to develop services in an open and interoperable services environment.

						Orange is thus hoping to reuse the common set of functionalities defined by the standard as to build its own platforms, within minimizing custom design due to specific vertical needs. These requirements remain the same in oneM2M, where now worldwide telecom mobile and fixed network operators intend to enlarge their traditional activity domains towards the Internet of Things Services. Among the multiple services that will be possible to develop, using ETSI M2M then oneM2M standards, some of them are of peculiar interest: services of connectivity using various M2M Area Networks End to End secure services Trusted Data Provider Use Semantic approach and ontologies High Level descriptors and Abstracted layer definition. Openness and Interoperability
Ongoing	ITU GSI Internet-of-Things	Overall architecture, Interfaces	Monitor	ITU GSI IoT is aiming at establishing a global standard for the Internet-of-Things. ITU is working on many aspects of the system, e.g. architecture, protocols, application.	Ernö Kovacs/NEC	NEC has delegates working in ITU. Through those delegates, first contacts to monitor the ITU activities have been established.

				Especially the IoT and eHealth area is active.		
Planned	OMA Lightweight M2M	Overall specification, Object/Resources models	Monitor, Plan how to Influence/Contribute	Adopt this device DMM and representation if FIWARE. Influence definitions with our specifics.	Carlos Ralli/TID	It seems this standard is becoming a strong market trend to be considered.

Table 3. Timestamped Summary of contributions/monitoring for IoT

Timestamped Summary of contributions/monitoring for IoT						
Dates	SDO or event	Contribution title and SDO ID	Exposed Interface	Responsible partner	Responsible person	Phase/IPR/comment/status
July 2011	SSN-XG	The XG Final Report has been published, the XG is closed.	SPARQL/RDF endpoint (Configuration Management GE)	University of Surrey	Payam Barnaghi	XG Final Report, group closed.
January 2012	Agreed at M2M#18. ETSI TC M2M	Semantic support for M2M data This relates to the separation of information access between using semantic entities and device based access.	Backend Device Management GE (open specs not yet publicly released)	NEC	Martin Bauer, Tobias Jacobs	Study item. NEC is rapporteur. How to support semantic data in ETSI M2M interface is under active discussion in ETSI TC M2M. Key contributions from FI-Ware members.
20120306	ETSI M2M	M2M(12)19_033 Scope_for_TR_Study_on_Semantic_support_for_M2M_Data	(Not yet set)	NEC	Joerg Swetina	Contribute for semantic M2M
20120606	ETSI M2M	M2M(12)20_107r2 Interworking/abstraction definitions	(Not yet set)	NEC	Joerg Swetina	Contribute for semantic M2M
20120917 to	ETSI M2M#22	Monitor	(Not yet set)	NEC	Joerg Swetina	Attend to monitor

20120921						
20120924 to 20120928	M2M PP	Monitor	(Not yet set)	NEC	Joerg Swetina	Attend to monitor
20120530	M2M PP	M2M(12)20_065	(not set yet)	NEC	Joerg Swetina	Contribute Home Heater Control Use Case demonstrating need for semantics.
20120530	ETSI M2M	M2M(12)21_053	(not set yet)	NEC	Joerg Swetina	Contribute Proposal how to structure semantic information
2012-09-10	ETSI M2M	M2M(12)22_077r1	(not set yet)	NEC, Orange	Joerg Swetina	Semantic related M2M definitions
July-August 2012	OGC		(Not yet set)	TID	Juanjo Hierro	Approach OGC officials for FI-WARE membership and the common OMA/OGC work force issue
July-August 2012	Onvif		N/A	Orange	Thierry Nagellen	Approach Thales for membership options and contribution possibilities
May 2013	IoT Forum/IERC		Overall architecture	NEC	Martin Bauer, Thierry Nagellen, Carlos Ralli Ucendo	Planning of meeting at IoT Week and mapping of FI-WARE IoT architecture to Architectural Reference Model
June 2013	IoT Forum/IERC		Overall architecture	NEC	Martin Bauer, Thierry Nagellen, Carlos Ralli Ucendo	Meeting at IoT Week and discussion of the mapping between FI-WARE IoT architecture to Architectural Reference Model
July 2013	ITU	Overview ITU activities	Architecture	NEC	Ernö Kovacs,	Information exchange with ITU delegate from NEC.
July 2013	OMA	OMA-ARC-2013-0086-INP_OMA_NGSI_9_10_HTTP_REST_binding_	NGSI 9/10 interfaces	NEC, TID	Tobias Jacobs	FI-WARE NGSI binding presented to OMA, announcement of future contributions,

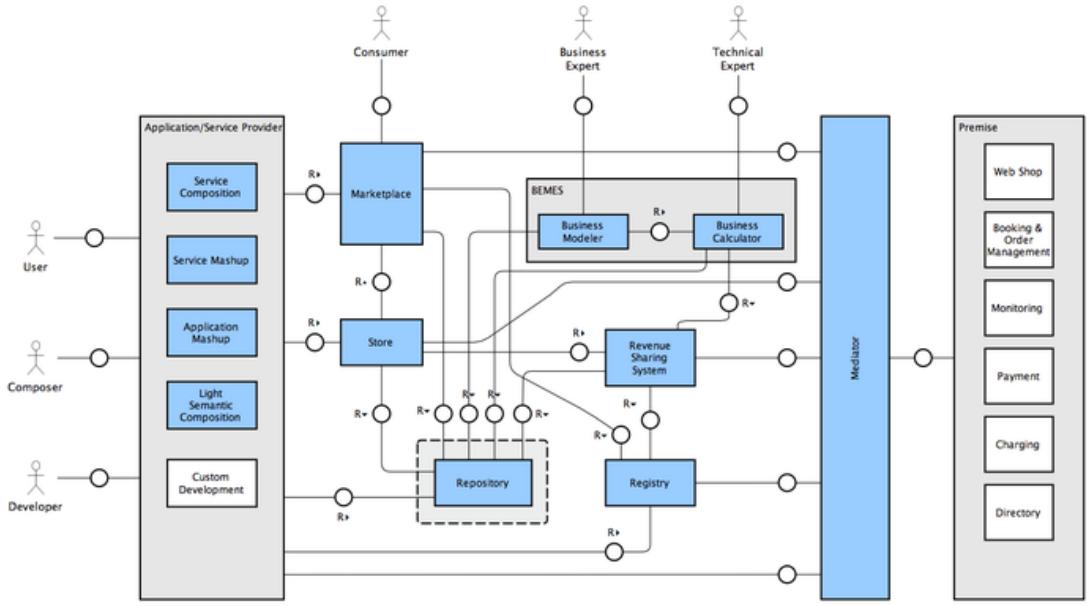
		FI_WARE				feedback received.

5.6 Mapping_Applications_Services_Ecosystem

You can find the content of this chapter as well in the wiki of fi-ware.

- Contact fiware-standardization@lists.fi-ware.eu

Figure 1: Architecture for Application & Services Ecosystem, with reference points for potential standardization



Besides the interfaces provided by the different enablers we have to look at the service description format, which is the underlying fundamental data format for most of the API. So our main focus is to work on the standardization of Linked USDL and related APIs.

The Repository Open RESTful API for accessing service descriptions is related to the Linked Data initiative. Since FI-Ware will mainly rely on the standards defined somewhere else, we will monitor standardization projects only, e.g. http://www.w3.org/2012/ldp/charter.html .

There are currently no standards activities for Marktplace & Store API. As a consequence we have to analyse and identify possible standardization organizations for potential contributions of these API specifications.

The work on Business Models and Elements has not started yet (part of the first Open Call). The APIs for these enablers will be defined in the next releases of FI-WARE. Also the appropriate standardization organizations and potential contributions will be identified later.

Table 1: Planned Activities for SDOs (contributions/monitoring) for Applications Services Ecosystem

Planned Activities for SDOs (contributions/monitoring) for Applications Services Ecosystem						
Dates or ID	SDO as link	Exposed FI-WARE Interface	Contribute or Monitor	SDO work-item or topic to monitor/contribute	Responsible Partner(s) and Person(s)	Stds-Phase IPR-issues Comment & Status
March 2013	linked-usdl.org	Repository API, Marketplace API	contribute and monitor	Vocabulary specifications for core, sla, pricing, legal	SAP, Torsten Leidig	released of version 1.0
April 2013	linked-usdl.org	Repository API, Marketplace API	contribute and monitor	API specifications for repository and marketplace	SAP, Torsten Leidig	released
April 2013	linked-usdl.org	Repository API, Marketplace API	Contribute	Create community manifest	SAP, Torsten Leidig	released
plan	linked-usdl.org	Repository API, Marketplace API	Contribute	Create Manifest and Frequently Asked Questions	SAP, Torsten Leidig	under execution
May 2013	linked-usdl.org	Repository API, Marketplace API	Contribute	Provide core repository/registry reference implementation	SAP, Torsten Leidig	released
planned	OMA	Composition	monitor	Monitoring of activitions according to Networking API, which are to be supported by the composition environment	DTAG	under execution
planned	Web Applications Working Group	Composition	monitor	Monitoring of activities according to use them for the composition environment	DTAG	Monitor activities and examine results for use in FI-WARE. Under execution
20130101 to 20130630	Linked Data Platform (LDP)	Repository	monitor	Monitoring of activities according a standard Linked	SAP	under execution

	Working Group			Data Platform and APIs		

Table 2. Responsible Persons for each SDO activity for Applications Services Ecosystem

Responsible Persons for each SDO activity for Applications Services Ecosystem				
SDO	Exposed FI-WARE Interface	Responsible Partner	Responsible Person	Comment
linked-usdl.org	Repository, Marketplace	SAP	Torsten Leidig	
W3C Web Applications Working Group	Composition	DTAG	Horst Stein	
Linked Data Platform (LDP) Working Group	Repository	SAP	Torsten Leidig	
OMA	Composition	DTAG	Horst Stein	

Table 3. Timestamped Summary of contributions/monitoring for Applications Services Ecosystem

Timestamped Summary of contributions/monitoring for Applications Services Ecosystem						
Dates	SDO or event	contribution title and SDO ID	Exposed Interface	responsible partner	responsible person	phase/IPR/comment/status
20120701 to 20130430	linked-usdl.org	USDL core vocabulary [1]	Repository API, Marketplace API	SAP	Torsten Leidig	final V1.0
20120701 to 20130530	linked-usdl.org	USDL pricing vocabulary [2]	Repository API, Marketplace API	SAP	Torsten Leidig	final V1.0
20120701 to 20130730	linked-usdl.org	USDL service level vocabulary [3]	Repository API, Marketplace API	SAP	Torsten Leidig	under negotiation
20120201 to 20120930	linked-usdl.org	Use Case Analysis	Repository API, Marketplace API	SAP	Torsten Leidig	first drafts for logistics use case and cloud use case available
20120701 to 20130630	linked-usdl.org	Stakeholder invitation	Repository API, Marketplace API	SAP	Torsten Leidig	under execution
20121101 to	linked-usdl.org	V1.0 finalization	Repository API, Marketplace API	SAP	Torsten Leidig	done

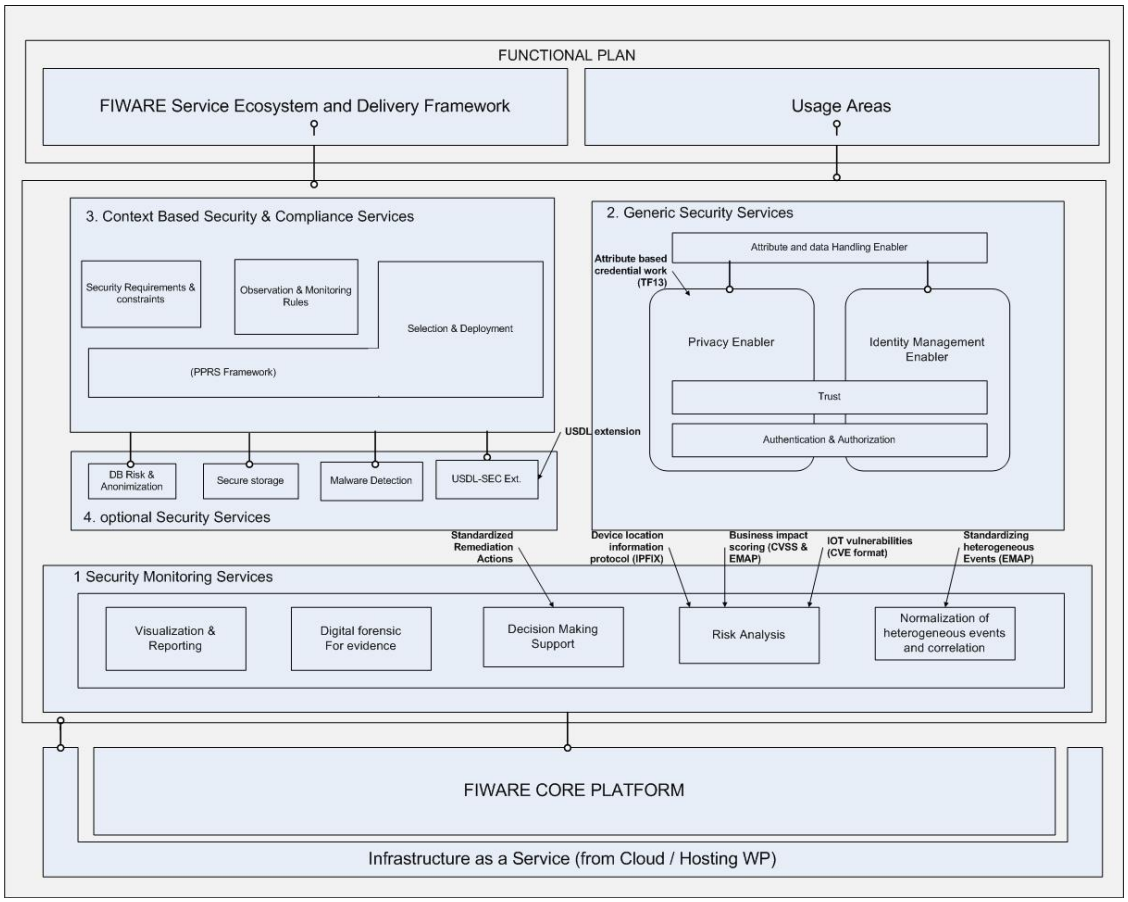
20121130						
20120930	linked-usdl.org	Linked USDL community member workshop	Repository API, Marketplace API	SAP	Torsten Leidig	done
20130201 to 20130731	linked-usdl.org	Review and change of the pricing vocabulary to include dynamic pricing models using SPIN [4]	Repository API, Marketplace API	SAP	Torsten Leidig, Jorge Cardoso, Carlos Pedricano	done
20130101 to 20130830	linked-usdl.org	Review and update of the Linked USDL Security vocabulary [5]	Repository API, Marketplace API	SAP	Francesco di Cerbo, Slim Trabelsi, Torsten Leidig	done
20130601 to 20130830	linked-usdl.org	Design of Linked USDL IPR vocabulary [6]	Repository API, Marketplace API	SAP	Torsten Leidig, Daniel Oberle	done
20130901 to 20140430	linked-usdl.org	Design of Linked USDL Core vocabulary Release 1.0 [7]	Repository API, Marketplace API	SAP	Torsten Leidig	done
20130901 to 20140430	linked-usdl.org	Design of Linked USDL IPR revision of vocabulary [8]	Marketplace API	SAP	Torsten Leidig, Jorge Cardoso	done

5.7 Mapping_Security

You can find the content of this chapter as well in the wiki of fi-ware.

- Contact fiware-standardization@lists.fi-ware.eu

Figure 1: Architecture for Security, with reference points for standardization



For discussion of this architecture, see [1]

Table 1: Planned Activities for SDOs (contributions/monitoring) for Security

Planned Activities for SDOs (contributions/monitoring) for Security						
Dates or ID	SDO as link	Exposed FI-WARE Interface	Contributor or Monitor	SDO work-item or topic to monitor/contribute	Responsible Partner(s) and Person(s)	Stds-Phase IPR-issues Comment & Status
October 3rd - 5th, 2012	8th Annual IT Security Automation Conference - Baltimore Convention Center, Baltimore Inner Harbor, MD		Monitor	Security Content Automation Protocol (SCAP)	Daniel Gidoin and Olivier Bettan	We drew inspiration from the technical specification for the security content automation protocol (SCAP Version 1.2) for developing our Remediation App. But the added value of the Remediation app is to take into account the impact of business through the Scored Attack Paths and the opportunity to verify the impact of countermeasures thanks to the MulVal attack Paths Engine.
Plan	NIST	Security Monitoring GE	Monitor	Security Content Automation Protocol	Daniel Gidoin and Olivier Bettan	Remediations are ranked according to an estimate cost composed of operational costs and impact costs (e.g. disrupted services) in an automatized process. We need a remediation base (CVE, pathes and snort rules to vulnerabilities. Otherwise we use network topology (automatically collected) to compute which firewall rules could be deployed.
Plan	NIST	Security Monitoring GE (risk analysis part)	Monitor	CVSS	Daniel Gidoin and Olivier Bettan	Initially risk level computation by MulVAL attack Paths engine, at each node of a network, is based on CVSS. In a first time, we extended the score assessment at the path level: Thus, for a given target node, each path leading to that node is given a score and the score of each path reflects the risk associated to the path as a whole. In a second time we have improved the scoring capacity again, taking account the business impact.

Plan	NIST	Security Monitoring GE (risk analysis part)	Monitor	CVE	Daniel Gidoin and Olivier Bettan	We will look to supplement the Common Vulnerabilities and Exposures (CVE) with FI-WARE IOT inputs
Plan	NIST	Security Monitoring GE (risk analysis & Normalization of heterogeneous events parts)	Monitor	Event Management Automation Protocol (EMAP)	Daniel Gidoin and Olivier Bettan	Scored paths are now mandatory for prioritizing the vulnerability impact and the remediation process.
Ongoing	ISO/IEC 18013 Information technology -- Personal identification -- ISO-compliant driving licence Part1-4	Privacy GE	Contribute	Task force (TF13)	Michael Osborne and Dieter Sommer	new Task Force on privacy protection for electronic driving licences. The task force (TF13) will look at privacy enhancing technologies for electronic driving licences. This will include the attribute based credential work that is part of the FI-WARE project.
Ongoing	IRTF NMRG IETF IPFIX	Android Flow Monitoring Optional Security Enabler	Contribute	Information Elements for IPFIX Metering Process Location - draft-irtf-nmrg-location-ipfix-01	Olivier Festor and Abdelkader Lahmadi	A third version will be submitted for the 91st IETF meeting in November, taking into account comments received during the 90th IETF/NMRG meeting in Toronto, possibly turning the draft into a NMRG working group RFC.
Done, May 2013	Linked USDL	Context-based security and compliance	Contribute	USDL-SEC	Slim Trabelsi	USDL-SEC security services description language will be defined as an extension of actual set of Linked USDL vocabularies.
Started 28/03/2014, Ongoing	ETSI Technical Committee Cyber	ETSI TC Cyber	Monitor	ETSI to develop European Standards for Cybersecurity	Pascal Bisson and Olivier Bettan	new Technical Committee on Cybersecurity. The Cyber TC will look at the development of standards in the following areas: Cybersecurity, Security of infrastructures, devices, services and protocols, Security advice, guidance and operational security requirements to users, manufacturers and network and infrastructure operators, Security tools and techniques

						to ensure security, Creation of security specifications and alignment with work done in other ETSI committees. Through its focus on Cybersecurity although not uniquely, the TC Cyber is highly relevant to follow if not to contribute what has been learnt from FI-WARE through activities on the field. Especially in scope of Task 8.1 and Security Monitoring GE.
Ongoing	OASIS XACML TC	Access Control GE	Monitor	XACML v3.0 Core Specification, Multiple Decision Profile, Core and Hierarchical RBAC Profile	Cyril Dangerville	Except for the core specification, the XACML v3.0 profiles are not yet released as standards, therefore they are still being updated; moreover, new profiles are being worked on (working drafts) and getting momentum. For those reasons, we are continuously monitoring the progress of these XACML specifications.
Done (June 2014)	SCIM 2.0	IdM Keyrock GE	Monitor	SCIM 2.0 API Specification	Álvaro Alonso	Version 2.0 of the API specification implemented and available in the current GEi
Done (2013)	OAuth2	IdM Keyrock GE	Monitor	OAuth2 Specification	Álvaro Alonso	Version 2 specification implemented and available in the current GEi

Table 2. Responsible Persons for each SDO activity for Security

Responsible Persons for each SDO activity for Security				
SDO	Exposed FI-WARE Interface	Responsible Partner	Responsible Person	Comment
NIST	Security Monitoring GE (remediation part)	Thales Communications France	Lucie Gaspard and François-Xavier Aguessy	
ISO/IEC	Privacy GE	IBM-CH	Michael Osborne and Dieter Sommer	
IETF/IRTF	Android Flow Monitoring Optional Security Enabler	Inria	Olivier Festor, Abdelkader Lahmadi and Alexandre	

			Boeglin	
Linked USDL	Context-based security and compliance GE	SAP	Slim Trabelsi	
NIST (CVSS)	Security Monitoring GE (Risk analysis part)	Thales Services SAS	Daniel Gidoin and Olivier Bettan	
NIST (CVE)	Security Monitoring GE (Risk analysis part)	Thales Services SAS	Daniel Gidoin and Olivier Bettan	
OASIS (XACML)	Access Control GE	Thales Services SAS	Cyril Dangerville	
SCIM 2.0	IdM Keyrock GE	UPM-DIT	Álvaro Alonso	
OAuth2	IdM Keyrock GE	UPM-DIT	Álvaro Alonso	

Table 3. Timestamped Summary of contributions/monitoring for Security

Timestamped Summary of contributions/monitoring for Security						
Dates	SDO or event	contribution title and SDO ID	Exposed Interface	responsible partner	responsible person	phase/IPR/comment/status
May 16, 2011	W3C	Presentation of USDL at W3C AC Rep meeting in Bilbao	Context-based security & compliance	SAP	Slim Trabelsi	use
October 27, 2011	W3C	The XG Final Report has been published, the XG is closed.	Context-based security & compliance	SAP	Slim Trabelsi	XG Final Report
October 31st - November 2nd, 2011	Security Content Automation Protocol (SCAP)	7th Annual IT Security Automation Conference - October 31st - November 2nd, 2011 - Arlington (Crystal City), VA	Security Monitoring	Thales Services SAS	Daniel Gidoin	Study of the technical specification for the security content automation protocol (SCAP Version 2 - Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930), particularly the content processing requirements and recommendations.
June 20th,	ISO/IEC	ISO/IEC 18013 -	Privacy GE	IBM-CH	Michael	to join and promote

2012		Creation of a new Task Force (TF13) on privacy protection for electronic driving licences. Meeting location: Gratkorn, Austria.			Osborne	results/ongoing activities
July 9th to July 13th 2012	Security Content Automation Protocol (SCAP)	2012 Security Automation Developer Days - MITRE Corporation Bedford, MA 01730	Security Monitoring	Thales Services SAS	Daniel Gidoin	to monitor emerging specification phase
July 31st, 2012	IETF	Information Elements for device location in IPFIX - draft-irtf-nmrg-location-ipfix-00	Android Flow Monitoring Optional Security Enabler	Inria	Alexandre Boeglin	Initial (individual) draft was submitted, not many comments were received
November 2012	ISO/IEC	ISO/IEC SC 17/WG 10 Meeting and ISO/IEC SC 17 Plenary Meeting	Privacy GE	IBM-CH	Michael Osborne	Presentation of use cases, general motivation, and potential technologies for privacy of electronic driving licenses to the TF 13 of WG 10. Discussions with the TF on how to further progress the work towards a standardization of a concrete technology.
January 2013	ISO/IEC	Joint ISO/IEC JTC 1/SC 27 and ABC4Trust Workshop on Identity Management and Privacy Standards	Privacy GE	IBM-CH	Dieter Sommer	At this event, Dieter Sommer has been invited as a panelist for discussing standardization activities related to attribute credentials. The goal of the event for our efforts was to establish informal liaisons with relevant people of other organizations, particularly ISO/IEC SC 27, WG5, and communicate our activities to those. He gave an overview of the

						activities going on in the Task Force 13 of WG 10 on privacy through using attribute credentials for electronic driving licenses to a distinguished audience. In the following discussions, also future related activities have been addressed.
February 2013	ISO/IEC	ISO/IEC SC 17/WG 10 Meeting and ISO/IEC SC 17/WG 10 TF13 Meeting	Privacy GE	IBM-CH	Michael Osborne	Discussion related to use cases for privacy in electronic driving licenses in the Task Force 13, particularly addressing the formal comments reflecting the position of one ISO member body related to privacy for electronic driving licenses. Decision on how to proceed with the working draft document towards a formal vote by the ISO member bodies.
May 2013	ISO/IEC	Complete TF13 Scope Draft and distribute it through ISO/IEC SC 17 to an international audience for feedback.	Privacy GE	IBM-CH	Michael Osborne and Dieter Sommer	The document has the following goals: • Show the complex use cases for electronic driving licences • Derive consistent privacy requirements • Survey existing privacy technologies and standardization efforts • Identify the gaps between our requirements and available technologies

						• Document the legal context in which driving licences have to operate
June 17-19, 2013	ISO/IEC	ISO/IEC JTC 1/SC 17/WG 10	Privacy GE	IBM-CH	Michael Osborne and Dieter Sommer	The use case/requirements document for enhancing privacy for Electronic Driving Licences was discussed, together with the strategy for standardisation. Active representation in the discussion included: USA, Switzerland, UK, Germany, France, Japan, Netherlands, South Africa. The primary outcome of the meeting • to refine certain sections of the document • to better distinguish between Card Holder Present and Online scenarios. • to target the SC17 Plenary in September for submission of the final document. As a direct result of our activities a new proposal for privacy technologies for Identification Cards has been submitted by SC17 Work Group 4. This work group looks at technology and standards that are relevant for all ID card types. Assuming it is accepted, this will likely be the first liaison for SC17 WG10.

July 14th, 2013	IETF	Information Elements for IPFIX Metering Process Location - draft-festor-ipfix-metering-process-location-01	Android Flow Monitoring Optional Security Enabler	Inria	Alexandre Boeglin	Second revision of (individual) draft was submitted, comments from the IETF IPFIX and IRTF NMRG groups were received.
September 30 - October 2, 2013	ISO/IEC	ISO/IEC JTC 1/SC 17/WG 10 meeting, Singapore. Privacy for the future international driving license.	Privacy GE	IBM-CH	Michael Osborne and Dieter Sommer	The goal of this meeting has been to progress our work on privacy for the future ISO/IEC electronic driving license. We have further discussed the scoping question of the effort at this meeting based on an extensive discussion on the current use case and requirements document. Active representation in the discussion included: USA, Switzerland, UK, Germany, France, Japan, Netherlands, South Africa, and Malaysia. As next steps on our side, the working group has decided that the functional requirements for the driving license setting be further detailed, taking the specifics of the ISO international driving license into account.
October 2-4, 2013	ISO/IEC	ISO/IEC JTC 1 Plenary meeting, Singapore. Privacy for the future international driving license.	Privacy GE	IBM-CH	Michael Osborne and Dieter Sommer	Our initiative was presented to the SC 17 plenary meeting, followed by a discussion in the plenary on its relations to a new privacy effort of ISO/IEC JTC 1/SC 17/WG 4 on chip cards.
January, 2014	ISO/IEC	ISO/IEC JTC 1/SC 27, Winterthur, Switzerland.	Privacy GE	IBM-CH	Dieter Sommer	Dieter Sommer met with the Swiss mirror group of ISO/IEC JTC1 SC 27 to trigger discussions related to a Joint Study Period on Privacy-ABCs in WG5 and WG2 of ISO/IEC

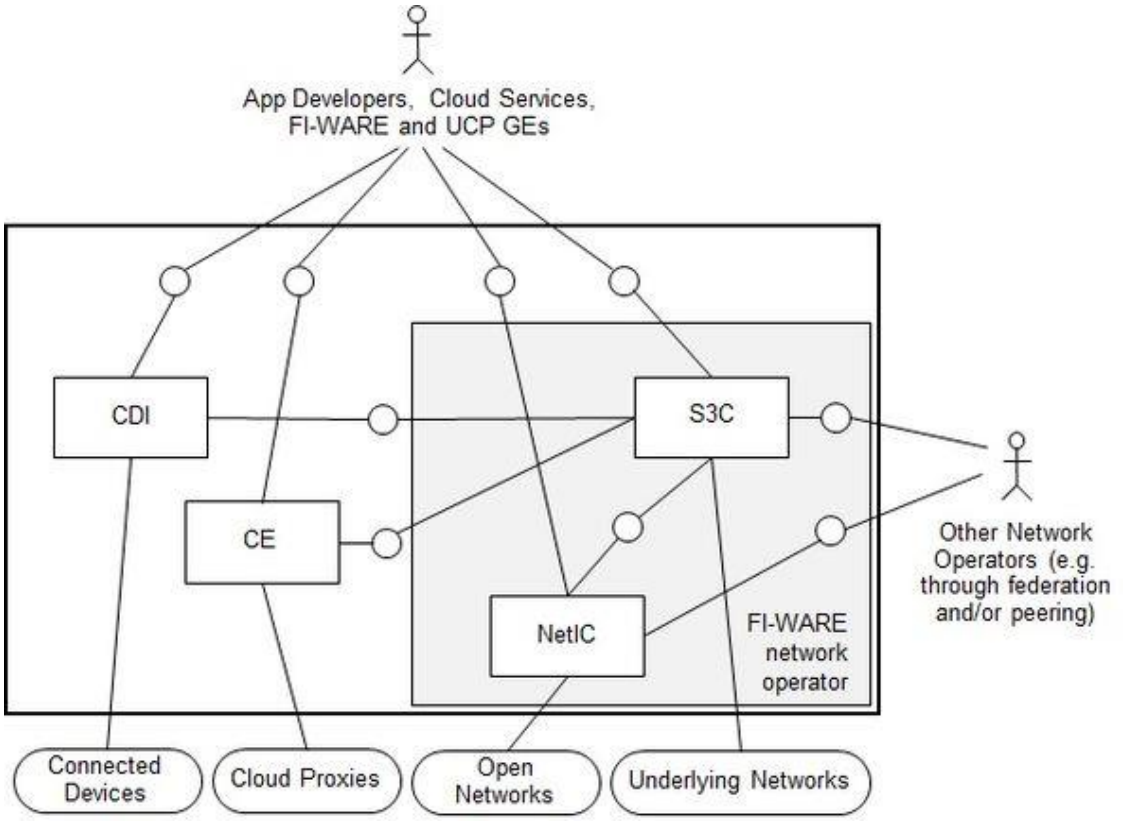
						JTC1 SC 27.
January, 2014	ISO/IEC	ISO/IEC JTC 1/SC 17/WG 4, London, UK.	Privacy GE	IBM-CH	Dieter Sommer	Dieter Sommer proposed to standardize privacy-preserving attribute based credential technology for chip cards in the new Working Group (WG) 4 effort of Subcommittee (SC) 17.
February, 2014	ISO/IEC	ISO/IEC SC 17/WG 10/TF 13, Costa Rica	Privacy GE	IBM-CH	Michael Osborne	ISO/IEC 18013, ISO/IEC SC 17/WG 10/TF 13 Meeting progressing use case and requirements documents related to privacy in the future electronic driving license.
April, 2014	ISO/IEC	ISO/IEC SC 27 working groups and Plenary meetings, Hong Kong, China	Privacy GE	IBM-CH	Dieter Sommer	Dieter Sommer proposes consideration of privacy-preserving attribute credentials for identity management.
July 21, 2014	IETF/IRTF /NMRG	Information Elements for IPFIX Metering Process Location - draft-irtf-nmrg-location-ipfix-01	Android Flow Monitoring Optional Security Enabler	Inria	Olivier Festor and Abdelkader Lahmadi	Second revision of the draft was submitted and presented during the NMRG meeting [2]. Last comments from the IRTF NMRG groups were received.

5.8 Mapping_Interface_to_Networks_and_Devices

You can find the content of this chapter as well in the wiki of fi-ware.

- Contact fiware-standardization@lists.fi-ware.eu

Figure 1: Architecture for Interface to Networks and Devices, with reference points for standardization



For discussion of this architecture, see [1]

Table 1: Planned Activities for SDOs (contributions/monitoring) for Interface to Networks and Devices

Planned Activities for SDOs (contributions/monitoring) for Interface to Networks and Devices						
Dates or ID	SDO as link	Exposed FI-WARE Interface	Contribute or Monitor	SDO work-item or topic to monitor/contribute	Responsible Partner(s) and Person(s)	Stds-Phase IPR-issues Comment & Status
Plan	W3C	CDI Device API Interface	Monitor (contribute if necessary)	Advances in Device API WG	Intel	Promotion of updates to Contacts API (done with Webinos).

Ongoing	OMA Device Management (DM) WG	Remote DM Interface of CDI	Contributing	Progressing in the specifications of OMA Device Management (DM) specifications (Next Generation).	Telecom Italia (Salvatore Scarpina)	Driving activity of WG (Chairmanship)
Ongoing	ONF (Open Networking Foundation)	NetIC southbound Interface	monitor	Extensibility WG (the WG is responsible for the "OpenFlow" specification; note that "OpenFlow Config" specification is moved to Configuration & Management WG).	NSN (Jozsef Varga)	participate at weekly conference calls
Ongoing	ONF (Open Networking Foundation)	NetIC northbound Interface	monitor (contribute if necessary)	Architecture WG (note that after assigning Northbound Interface related topics to Architecture WG, a separate NBI WG created in ONF in 2013)	NSN (Jozsef Varga)	participate at weekly conference calls "ONF SDN Architecture framework" document is published, the "SDN architecture" document is reviewed in Architecture WG and now is under ONF-wide review (to be published after that
Ongoing	ONF (Open Networking Foundation)	NetIC northbound Interface	monitor	NBI WG (formed at 2013 autumn ONF member workdays)	NSN (Jozsef Varga)	monitor mailing list (weekly conference calls are at European-unfriendly time starting at 2AM CET) Currently the use cases are defined.
Ongoing	ONF (Open Networking Foundation)	NetIC northbound Interface	monitor	Wireless and Mobile WG (formed at 2013 autumn ONF member workdays)	NSN (Jozsef Varga)	participate at weekly conference calls One of the sub-projects deals with evolved packet core (EPC) virtualization, which is important for NSN as a telecom vendor focusing on mobile broadband. It is still early phase of the work, but it is expected that the group will set requirements for the NBI (NetIC) interface to support the virtualization and deployment of SDN

						principles for EPC.
Ongoing	IRTF Software Defined Networking research group	NetIC northbound Interface	monitor	Monitor SDN (Software Driven Network / Software Defined Network) related activities in IETF/IRTF.	NSN (Jozsef Varga)	SDNRG latest activity (IETF meeting March 2014): hybrid SDN networks, incremental SDN deployment, architecture terminology, NetIDE presentation.
Ongoing	IETF Service Function Chaining working group	NetIC southbound Interface	monitor	Service chaining is a hot topic in virtualization and may have effects on the OpenFlow protocol (Note that ONF also has a L4-L7 discussion group that deals with Service chaining; 3GPP SA1 is also starting activities related to service chaining (spring 2014); ETSI NFV ISG also discussed service chaining. The monitoring of these activities is not reported, as it is done by colleagues not involved in FI-WARE, we check NSN internal reports to monitor service chaining related activities in those SDOs)	NSN (Jozsef Varga)	SFC WG latest activity (IETF meeting March 2014): use cases, encapsulation requirements, architecture.
Ongoing	IETF Interface to the Routing System working group	NetIC southbound Interface	monitor	Monitor network modelling, configuration related activities in IETF (NETConf related to the OpenFlow Config).	NSN (Jozsef Varga)	I2RS WG latest activity (IETF meeting March 2014): additional use cases, YANG models, NETConf analysis.
Ongoing	3GPP, IETF	unified S3C interface towards service providers (north)	Monitor (later Contribute)	Architecture evolution, development of a reference implementation for the support of the	in discussion DTAG	The contribution is according to the traditional "evangelisation" process of 3GPP (see figure: standardisation process). For the time being, it is

				standardisation process.		internally discussed with the respective SDO participants from DTAG, how the contribution can look like. The discussion is ongoing.
Plan	W3C	CDI Device API Interface	Monitor	Evolution of W3C System API Working Group	Intel	Monitoring System API Community Group
Ongoing	IETF ALTO WG	NetIC - Altoclient southbound interface	monitor	evolution of ALTO protocol definition	ALU-D	Currently following the evolution and accessing the documentation; future involvement under evaluation
20130620 and Ongoing	HGI (Home Gateway Initiative)	Southbound interface	monitor and liaise	Cloud proxy functionality	NEC NLE (Lindsay Frost)	Explained Cloud Proxy to HGI, invited discussions, provided FAQ. HGI members are waiting for more "how to try it" info.
20131101 to 20140430	HGI (Home Gateway Initiative)	Southbound interface	monitor	Cloud proxy vs. Open Platform 2.0	Telecom Italia (Luca Giacomello) & NEC NLE (Lindsay Frost)	Following the revision of the HGI requirements for the home gateways' execution environment and related OSGi based implementation guidelines.
20140501 to 20141031 (Ongoing)	HGI (Home Gateway Initiative)	Southbound interface	monitor	Cloud proxy as element of the HGI Smart Home architecture	Telecom Italia (Luca Giacomello) & NEC NLE (Lindsay Frost)	Following the definition of the smart home architecture OSGi based, understanding functional blocks and coherence with the cloud proxy developments.

Table 2. Responsible Persons for each SDO activity for Interface to Networks and Devices

Responsible Persons for each SDO activity for Interface to Networks and Devices				
SDO	Exposed FI-WARE Interface	Responsible Partner	Responsible Person	Comment
OMA	Remote DM Interface of CDI	Telecom Italia	Salvatore Scarpina	Chairman of OMA DM WG
ONF	Southbound interface for the VNP GE implementation (OpenFlow)	NSN	Jozsef Varga	Extensibility WG; Wireless and Mobile WG;
ONF	NetIC northbound interface	NSN	Jozsef Varga	Architecture WG; NBI

				WG;
IRTF	NetIC northbound interface	NSN	Jozsef Varga	Software Defined Networking RG
IRTF	NetIC southbound interface	NSN	Jozsef Varga	I2RS WG; SFC WG
W3C	CDI Device API Interface	Intel	Chris Woods	System API Community Group Observer
HGI	Cloud Proxy	NEC and Telecom Italia	Lindsay Frost (NEC) is SH-TF vice-chair and Luca Giacomello (TI) is HGI Chairman	HGI Smart Home TaskForce

Table 3. Timestamped Summary of contributions/monitoring for Interface to Networks and Devices

Timestamped Summary of contributions/monitoring for Interface to Networks and Devices						
Dates	SDO or event	contribution title and SDO ID	Exposed Interface	responsible partner	responsible person	phase/IPR/comment/status
20120611 to 20120615	HGI (Home Gateway Initiative)	Monitor	Cloud Edge OSGi framework support	Telecom Italia	Luca Giacomello	Evaluation of HGI SWEX specifications for adoption of latest versions in Cloud Edge
20111107	OMA Device Management (DM) WG	OMA-DM-DMNG-2011-0084R04-CR_AD_Interfaces, OMA-DM-DMNG-2011-0090R01-CR_Dictionary	Remote DM Interface of CDI	Telecom Italia	Salvatore Scarpina	Agreed
20111107 to 20111111	OMA Device Management (DM) WG	Monitor	Remote DM Interface of CDI	Telecom Italia	Salvatore Scarpina	Attended to Monitor Evolution of DM interface
20120709 to 20120713	OMA Device Management (DM) WG	Contribute	Remote DM Interface of CDI	Telecom Italia	Salvatore Scarpina	Setting workplan for DM interface evolution. Driving activity of WG (Vice-chairmanship)
20120709	OMA Device Management (DM) WG	OMA-DM-DMNG-2012-0029R01-	Remote DM Interface of	Telecom Italia	Salvatore Scarpina	Agreed

		CR_Commands_and_JSON_format	CDI			
20120709 to 20130215	OMA Device Management (DM) WG	OMA-DM-DMNG-2012-0079R01-CR_Preferred_Connection_Type, OMA-DM-DMNG-2012-0080-CR_Reason_for_connection, OMA-DM-DMNG-2013-0006R03-CR_TS_Reorganization	Remote DM Interface of CDI	Telecom Italia	Salvatore Scarpina	Monitoring on OMA-DM connection
20130217	OMA Device Management (DM) WG Budapest F2F	OMA-DM-DMNG-2013-0010R01-CR_JSON_Schema_Ref	Remote DM Interface of CDI	Telecom Italia	Salvatore Scarpina	Evolution of JSON Schema
20120301 to 20130531	OMA Device Management (DM) WG	OMA-DM-DMNG-2013-0037R01-CR_Package_3_JSON_Schema, OMA-DM-DMNG-2013-0045-CR_RD_Editorials, OMA-DM-DMNG-2013-0046-CR_AD_Editorials	Remote DM Interface of CDI	Telecom Italia	Salvatore Scarpina	Monitoring of DM interface evolution. Driving activity of WG
20130628	OMA Device Management (DM) WG Dublin F2F	OMA-DM-DMNG-2013-0047R01-CR_TS_Editorials	Remote DM Interface of CDI	Telecom Italia	Salvatore Scarpina	Agreed
20120610 to 20130709	OMA Device Management (DM) WG	OMA-DM-DMNG-2013-0052R01-CR_TS_Cleanup, OMA-DM-DMNG-2013-0053R01-CR_AlertType_Table, OMA-DM-DMNG-2013-0054R02-	Remote DM Interface of CDI	Telecom Italia	Salvatore Scarpina	Monitoring of proposals for OMA-DM Specs evolution. Driving activity of WG

		CR_Notification_JSON, OMA-DM-DMNG-2013-0055-CR_Bootstrap_from_Smartcard, OMA-DM-DMNG-2013-0056R03-CR_DM_Tree_concept, OMA-DM-DMNG-2013-0058-CR_DMAcc_GCM, OMA-DM-DMNG-2013-0059R01-CR_Bootstrap_Format, OMA-DM-DMNG-2013-0060-CR_MO_Serialization				
20120403	Extensibility WG weekly meeting	Istvan's comments on 1.3, ONF	OpenFlow (NetIC southbound interface towards Open Networks)	NSN	Istvan Kispal	Agreed
20120412	Extensibility WG weekly meeting	Circuit switching support for OpenFlow, ONF	OpenFlow (NetIC southbound interface towards Open Networks)	NSN	Istvan Kispal	Agreed
20120419	ONF member workday	Circuit switching support for OpenFlow, ONF	OpenFlow (NetIC southbound interface towards Open Networks)	NSN	Istvan Kispal	Agreed
20130415 to 20130417	Open Networking Summit	Monitor	NetIC southbound interface and OpenFlow (southboun	NSN	Istvan Kispal	Attended to participate at the different WG discussions both on OpenFlow interface and the ONF architecture

			d interface towards for VNP GEi)			
20130418	ONF member workday	Monitor	NetIC southbound interface and OpenFlow (southbound interface towards for VNP GEi)	NSN	Istvan Kispal	Attended to monitor the progress of different OpenFlow implementations and discuss future development issues
20130415 to 20130417	Open Networking Summit	Monitor	NetIC southbound interface and OpenFlow (southbound interface towards for VNP GEi)	NSN	Istvan Kispal	Attended to participate at the different WG discussions both on OpenFlow interface and the ONF architecture
20131009 to 20131011	ONF member workday	Monitor/Review	NetIC southbound interface, OpenFlow (southbound interface towards for VNP GEi), and NetIC northbound interface	NSN	Jozsef Varga	Attended to participate at the Architecture WG premeeting ("ONF SDN architecture overview" and "SDN architecture" documents scope and purpose re-definition); joint meeting among Extensibility WG and L4-L7 DG (potential service chaining requirements for OpenFlow), and several other WG discussions, including the announcement and first meeting of Wireless and Mobile WG.
20131119-20131120	ONF NBI Leadership roundtable	Monitor	NetIC northbound interface	NSN	Jozsef Varga	A two day meeting introducing activities in other SDOs that may be related to the activities of the NBI WG.
20131126	ONF architecture overview review	Review	NetIC northbound interface (SDN aspects in	NSN	Jozsef Varga	Architecture WG review of the "ONF SDN architecture overview document.

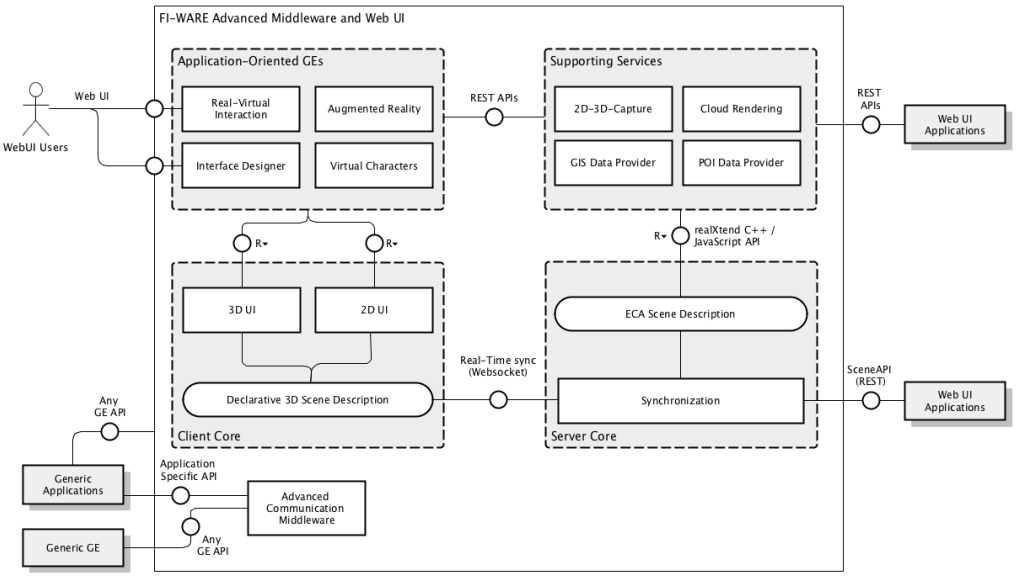
			general)			
20140303 to 20140305	Open Networking Summit	Monitor	NetIC southbound interface and OpenFlow (southbound interface towards for VNP GEi)	NSN	Jozsef Varga	Attended to participate at the different presentations on experiments with SDN and NFV deployments.
20140305 to 20140307	ONF member workday	Monitor/Review	NetIC southbound interface, OpenFlow (southbound interface towards for VNP GEi), and NetIC northbound interface	NSN	Jozsef Varga	Attended to participate at the Architecture WG premeeting ("SDN architecture" document review), several other WG discussions, and plenary meeting.
20130614	HGI member meeting	Promote FIWARE	Cloud Proxy	NEC	Lindsay Frost	Contribution SH_HGI02261.pdf introducing FIWARE Cloud Proxy
2012xxyy-20131031	IETF ALTO WG	monitor	NetIC 'altoclient' southbound interface	ALU-D	Thomas R. Banniza	following the evolution and accessing the documentation
20131025 to 20131215	HGI (Home Gateway Initiative)	Credibility test and report	Cloud Edge OSGi framework support	Telecom Italia	Luca Giacomello	Application of HGI SWEX test suite to the FI-WARE Cloud Edge implementation and possible discussion in HGI for test list adjustments (ongoing)

5.9 Mapping_Advanced_Middleware_and_Web-Based_User_Interfaces

You can find the content of this chapter as well in the wiki of fi-ware.

- Contact fiware-standardization@lists.fi-ware.eu

Figure 1: Architecture for Data Context Management, with reference points for standardization



For discussion of this architecture, see [1]

5.9.1 Introduction to SDOs

5.9.1.1 *OMG (Object Management Group)*

The Object Management Group defines enterprise integration standards for a wide range of technologies and industries. Originally aimed at standardizing distributed object-oriented systems, it now focuses on modeling (programs, systems and business processes) and model-based standards. The Advanced Middleware components are mainly based on (DDS, RPC over DDS, DDS Security, IDL, CDR) and are contributing to OMG technologies (RPC over DDS, DDS Security).

5.9.1.2 *W3C*

We are mainly aiming at the standardization of XML3D/Xflow through the W3C, which is the main standardization body for Web technology.

DFKI has already started a “W3C Community Group - Declarative 3D for the Web (Dec3D)” to prepare this standardization. This group brings together key players on the technology and market side. It evaluates which parts should or should not be part of the standard, collects applicable use cases, potential technology components, and promoted the standardization in general.

5.9.1.3 *Khronos*

Khronos is the standardization body for media APIs, including such important standards as OpenGL, OpenGL ES, OpenCL, WebGL, WebCL, and many others. To complement WebGL Khronos is currently actively standardizing a “GL Transfer Format (glTF)”. We realised recently that the current solution to asset transfers on the Internet is a complex topic (optimising for the number of connections, number of parallel connections, payload format, deserialisation and decompression performance, and other aspects) and that huge room for optimisations is still available. We have been working on an improved asset transfer format that we have already presented to Khronos as input for improvement to the current glTF proposal.

Timestamped Summary of contributions/monitoring for Advanced Middleware and Web based User Interfaces						
Dates	SDO or event	contribution title and SDO ID	Exposed Interface	responsible partner	responsible person	phase/IPR/comment/status
Ongoing	OMG	Contribute	RPC over DDS	EPROS	Jamie Martin Losa	Final joint sub-mission with RTI and PrismTech
Ongoing	OMG	Monitor	RPC over DDS	DFKI	Philipp Slusallek	Following the evolution and voting.
Ongoing	OMG	Monitor	RPC over DDS	ZHAW	Christof Marti	Following the evolution and voting.
since Project start until June 2014	OMG	Contribute	DDS Security Standard	EPROS	Jaime Martin Losa	Final Joint sub-mission with RTI and PrismTech
Since the project started	W3C	Contribute	XML3D and related technologies	DFKI	Kristian Sons	Co-chaired and driven the Declarative 3D on the Web Community Group
August 2012	Web3D, Siggraph	Contribute	XML3D and related	DFKI	Kristian Sons, Philipp Slusallek	Presentation of new technical content, ongoing

			technologies			discussions about Dec3D standards
	Web3D		XML3D and related technologies			Presentation of new technical content, ongoing discussions about Dec3D standards
August 2014	Web3D	Contribute	XML3D and related technologies	DFKI	Kristian Sons, Philipp Slusallek	Presentation of new technical content, ongoing discussions about Dec3D standards
August 2014	Khronos	Contribute	Shade.js	DFKI	Kristian Sons, Philipp Slusallek	Presentation of shade.js technology

The above table is only a short selection of our activities. We participated in several other meetings and discussion with members of various relevant standardization bodies (W3C, Khronos, etc.).