УДК 004.41

Sneps-Sneppe M.A.[1], Namiot D.E.[2]

[1] Ventspils University College Ventspils, Latvia
[2] Lomonosov Moscow State University, Moscow, Russia

ON OPEN SOURCE SMART CITY PLATFORM: HOW TO GET IT?

ABSTRACT

In this paper, we deal with the issues of standardization for smart cities. We are discussing the history of telecommunications development and the use for Smart Cities such technologies as Software-Defined Networking and Network Functions Virtualization. Further, the paper discusses the European projects for Smart Cities and urban platforms such as FIWARE and European Innovation Partnership on "Smart Cities and Communities". As a basic prototype, we consider the results and deliverables from oneM2M consortium. At the end of the paper, we provide our considerations for standardization of platforms for Smart Cities in Russia.

KEYWORDS

Internet of Things; Smart City; standard; SDN, NFV.

Шнепс-Шнеппе М.А.[1], Намиот Д.Е.[2]

[1] Вентспилский Университетский колледж, г. Вентспилс, Латвия
[2] МГУ имени М.В. Ломоносова, г. Москва, Россия

О ПЛАТФОМАХ С ОТКРЫТЫМ КОДОМ ДЛЯ УМНЫХ ГОРОДОВ: КАК ЭТОГО ДОСТИЧЬ?

АННОТАЦИЯ

В статье рассматриваются вопросы стандартизации для Умных Городов. Мы обсуждаем развитие телекоммуникаций и применение для Умных Городов программно-определяемых сетей и технологии виртуализации сетевых элементов. Далее в работе рассматриваются европейские проекты по Умным Городам и городским платформам. Как базовый прототип, мы рассматриваем разработки консорциума oneM2M. В заключительном разделе работы приводятся соображения по стандартизации платформ для Умных Городов в России.

КЛЮЧЕВЫЕ СЛОВА

Интернет Вещей; Умный Город; стандарт; SDN, NFV.

Introduction

The article discusses the development and use of standards for Smart Cities. The success in the area of Smart Cities is based on the nowadays telecommunication networks and on software industry especially. Telecommunication network architecture is undergoing a massive transformation now, primarily by Software Defined Network (SDN) and Network Functions Virtualization (NFV) technologies. But the hard question arises: is the NFV concept implementable from the software developers point of view? Efficient software-based service life cycle depends on two key factors: short time to market and deployment flexibility. Time to market can be minimized through a homogeneous software environment that enables deployment on existing network infrastructure without the need for hardware modification. SDN and NFV software seems extremely sophisticated.

The paper begins with an analysis of telecommunications, which is a bit simpler area, but much more advanced now comparing to Smart City one. Thus, we go back to telecom software history and recall some failed software projects in Section 2. In Section 3, we consider SDN and NFV basics. Section 4 is about European Innovation Partnership on "Smart Cities and Communities". Sections 5 and 6 are devoted to FIWARE and its successor AOITI as a basis for Urban Platform. In Section 7, consortium OneM2M as a Smart City prototype is looked. In the conclusion (Section 8), the authors offer their vision of development work on Smart City in Russia.

Look at the history of telecommunication

Let us start by Intelligent Network architecture developed by Bell Labs in the 1970s.

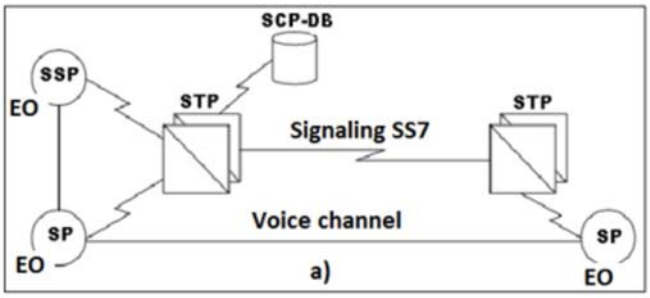

Figure 1. IN basic design

The Intelligent Network (IN) architecture is the highest achievement in the art of circuit switching (Figure 1). It allows operators to provide value-added services in addition to the standard telecom services such as PSTN, ISDN and GSM services on mobile phones. IN is used the Signaling System #7 (SS7) protocol between telephone network switching centers and other network nodes owned by network operators. The basic IN design is including:

- STP (Signaling Transfer Point),
- SSP (Service Switching Point),
- SCP-DB (Service Control Point with Database),
- Each Central Office (CO) contains Signaling Point (SP).

Figure 2 shows a case: the Advanced Intelligent Network architecture for the Defense Information Systems Network (DISN) needs. The DISN belongs to the Pentagon and is the world's largest departmental network. This is a global network. It is intended to provide communication services by transmitting different types of information (voice, data, video, and multimedia) in order to perform the efficient and secure control of the military, communications, intelligence, and electronic warfare media. Channel switching network subscribers, as well as packet switching network subscribers, can be AIN users.

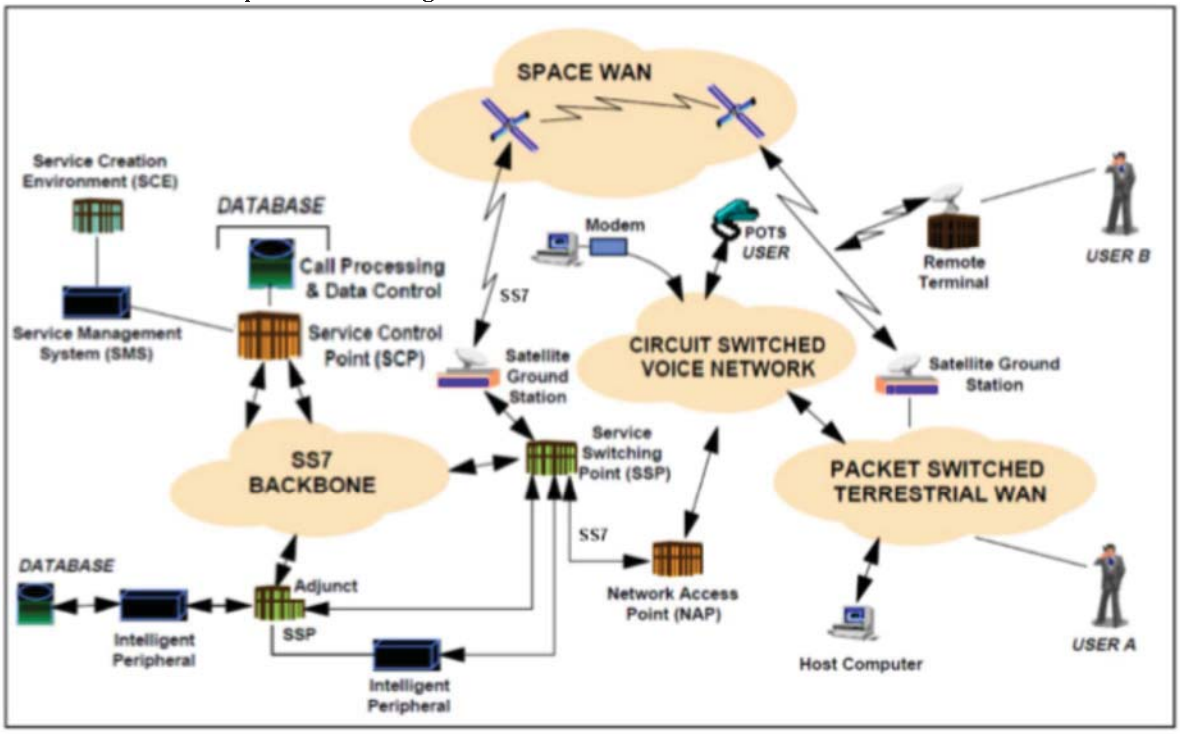

Figure 2. AIN Service Architecture in DISN

Point out the attention to the Service Creation Environment (SCE) as a standardized means for service software development. According to standards, SCE and SIB (Service Independent Block) library were invented to simplify software development and 3d parties work. There are 17 SIBs (in ITU standard) and 21 SIBs (from ETSI). In reality, telecom vendors had used up to 100 vendors specific SIBs. As a result, the AIN approach had a little success amongst software developers. The very idea failed: software developers were asked to know too many telephony details.

The next one was TINA project. TINA Consortium started its work in 1993 and planned to end in 1997. The Consortium was supported by several main actors in the telecommunication world. The aim was to define a new software architecture. According to TINA promoters, the advantages of introducing CORBA / TINA based solutions within the IN are mainly related to the possible rationalization of the service aspects (e.g., integration of service management and control), to a higher level of interoperability between applications, to the ability to extend service related capabilities, scalability of the service platform, vendor independence, etc. In general, TINA concepts had planned for use in the following IN areas:

- Service Management: The introduction of TINA in the Service Management area seems to be promising because there is a lack of standardized IN management solutions and TINA offers the ability to integrate service management and control aspects by means of common objects and protocols.
- Service Data: TINA could be useful for supporting distributed incall and outcall signaling related personal profile access, in particular for personal and terminal mobility support.
- Service Control: Access Session and Service Session mechanisms could be usefully adopted in order to provide enhanced flexibility for supporting multi-party/multi-connection capabilities.

Unfortunately, TINA concepts ended without implementation.

After then was Parlay Group (founded 1998) that specified APIs for the telephone network. Parlay project ended unsuccessfully around 2007. In 2003, the Parlay Group released a new set of web services called Parlay X. These are a much simpler set of APIs intended to be used by a larger community of developers. Unfortunately, Parlay X ended without any wide use also.

On SDN and NFV technologies

Due to IT virtualization technology consolidating, many network equipment types onto industry standard high volume servers, switches, and storage. Telecommunication network could be located in Datacentres, Network Nodes and in the end user premises, as illustrated in Figure 3. It involves the implementation of network functions in software that can run on a range of industry standard server hardware [1].

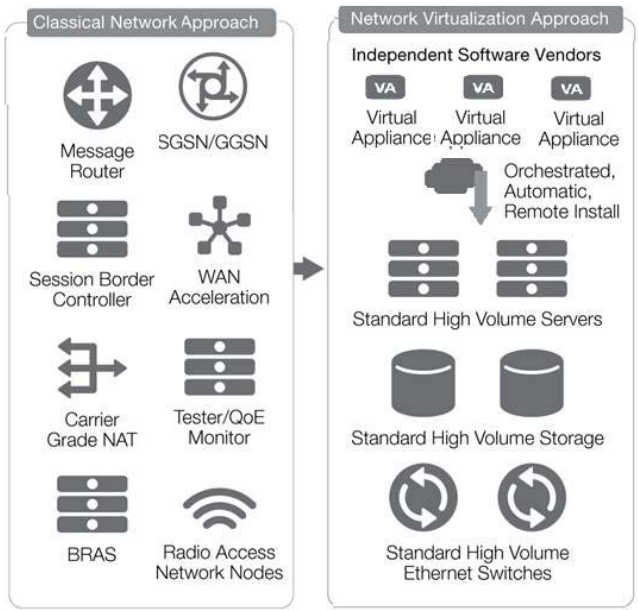

Figure 3. The ETSI vision for NFV, which relies on COTS hardware and software delivered through the cloud [1]

Now we talk about SDN as an analog to Smart City model. According to Recommendation ITU-T Y.3300, SDN is mapped to the 3-layers reference model (Figure 4). Application Control Interface (NorthBound Interface) provides an application programmatic control of abstracted network resources. Resource Control Interface (SouthBound Interface) is used to control network resources. The SDN is highly promising now for Internet services and the All-IP move at all (e.g. by using OpenFlow protocol). But it is so for SouthBound Interface part only. Meanwhile, as the NorthBound Interface issues are not solved up to now.

The key goals of the ETSI NFV Working Group are to:

- Reduce equipment costs and power consumption.
- Improve time to market.
- Enable the availability of multiple applications on a single network appliance with the multi-version and multi-tenancy capabilities.

• Encourage a more dynamic ecosystem through the development and use of software-only solutions.

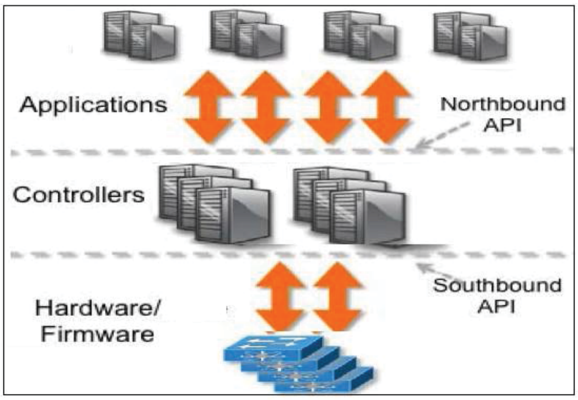

Figure 4. SDN Stack

All of these benefits can be derived from the use of commercial, off-the-shelf (COTS) hardware that can be purposed for multiple telecom-related services that currently use proprietary hardware.

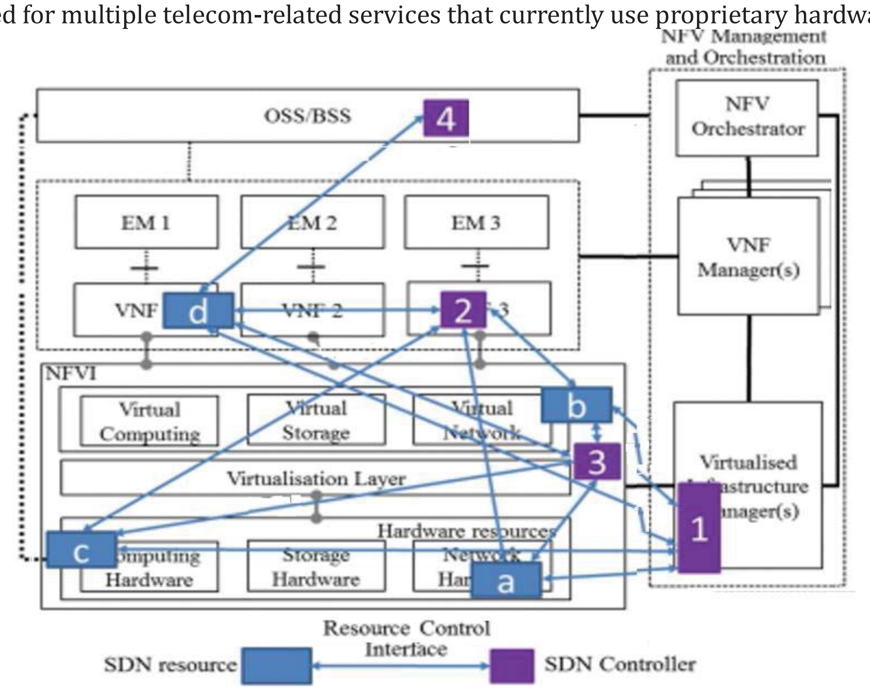

Figure 5. SDN Resource Control Interface Options in NFV

NFV is taking the software-defined networking (SDN) concept of the virtualization movement and adapting it to benefit the telecommunications application infrastructure. The major components of an NFV architectural framework are:

• Network Functions Virtualization Infrastructure (NFVI): subsystem, which encompasses Compute, Network, and Storage resources.

• Management and Orchestration: subsystem, which includes the Network Functions Virtualization Orchestrator, the Virtualized Infrastructure Manager (VIM) and Virtual Network Function Manager.

• Virtual Network Functions (VNFs): deployed in the NFVI.

What about NFV and SDN relationship, besides two above-mentioned interfaces (NorthBound and SouthBound), there is Orchestration Interface – the interface between an SDN controller and an NFV Orchestrator. It might need to pass information between the two entities, such as topology information in both directions. The same interface might be used also between an SDN application and an NFV Orchestrator.

From an SDN controller perspective, consider in more detail NorthBound Interface functions. From an NFV architectural framework perspective, the NorthBound Interface might be considered as the Application Control Interface provided by the SDN controller if that layer is embedded in the SDN controller, or it could be considered as an SDN application if it seats on top of the SDN controller. Figure 5 below shows the different combinations between the different components of SDN controller.

The similar kind of figures are given in [1] for SDN Controller/Application Orchestration, SDN

Application Control, and SDN Controller to Controller Interface Options in NFV. All these many options have to be implemented as Virtual Appliances developed by Independent Software Vendors (see Figure 3). This is the basic idea for SDN and NVF relationship!

The complexity of NFV software is in many stages more sophisticated than SDN one. Therefore the future of NFV architecture is quite doubtful.

EC Horizon 2020 and European Innovation Partnership on "Smart Cities and Communities"

Horizon 2020 is the biggest EU Research and Innovation program ever with nearly €80 billion of funding available over 7 years (2014 to 2020) – in addition to the private investment that this money will attract. One of Focus Areas is "Smart and Sustainable Cities". Each project should prove interoperability between software modules to allow an effective management of components and information flows. To ensure adaptability as new user requirements and technologies evolve, urban ICT platforms has to be based on open specifications, including the data structures and APIs (e.g. FIWARE) [2]. Urban Platform will be the main backbone for many existing sector systems (like Energy Efficient Buildings, Smart Grid, Intelligent Transport Systems, eHealth Systems) and many new applications and systems specifically designed for the City (Figure 6).

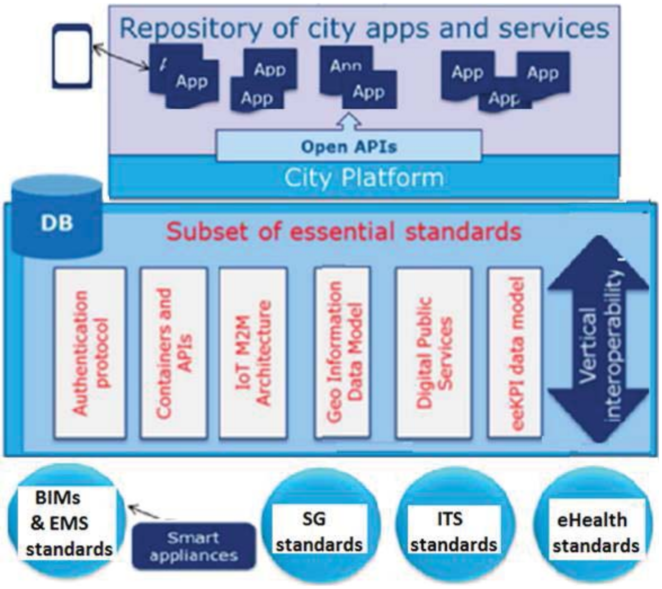

Figure 6. "Smart Cities and Communities" General vision [3]

The first infrastructures deployed in Smart Cities has been developed with proprietary or vertical solutions. Although they solve specific problems, they cause two inconveniences: on the one hand, they are hardly replicable and, on the other hand, they do not facilitate the creation of global ecosystems for entrepreneurs to develop applications and services for multiple cities (Figure 7).

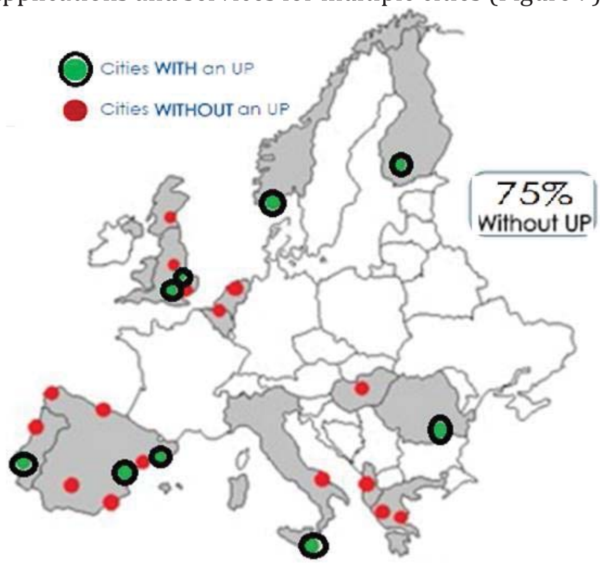

Figure 7. Smart Cities in Europe: 75% without Urban Platforms [3]

FIWARE

FIWARE is one of the biggest European initiatives in the area of Future Internet developing a set of technology standards to lower the technological barriers to the cities and its providers [4]. FIWARE is oriented to different strategic domains: Smart Cities, eHealth, Transport, Energy & Environment, AgriFood, Media & Content, Manufacturing & Logistics, and Social & Learning.

The FIWARE platform provides a set of tools and libraries known as Generic Enablers (GEs) with public and open-source specifications and interfaces. One key part of the FIWARE architecture is context management (Figure 8). Smart applications and services for cities do need information about everything happening at every moment. The management of the context information is done through a standard developed by the Open Mobile Alliance (OMA) and the NGSI. NGSI is an HTTP and REST-based technology allowing the retrieval of the information in XML and JSON formats.

Figure 8. Context information in a Smart City (bus, citizen, shop) [4]

FIWARE becomes then a fundamental pillar in the infrastructures of Smart Cities, as the different GEs build an architecture that can serve most of their needs. Among many initiatives to adopt FIWARE as Smart City platform, 75 cities from 15 countries have joined the initiative "Open & Agile Smart Cities" (Smart City Expo World Congress, 17 to 19 November 2015, Barcelona, [5]). Each Smart City platform contains many GEs as well as some specific enablers (Figure 9). In practice, the platform seems extremely complicated.

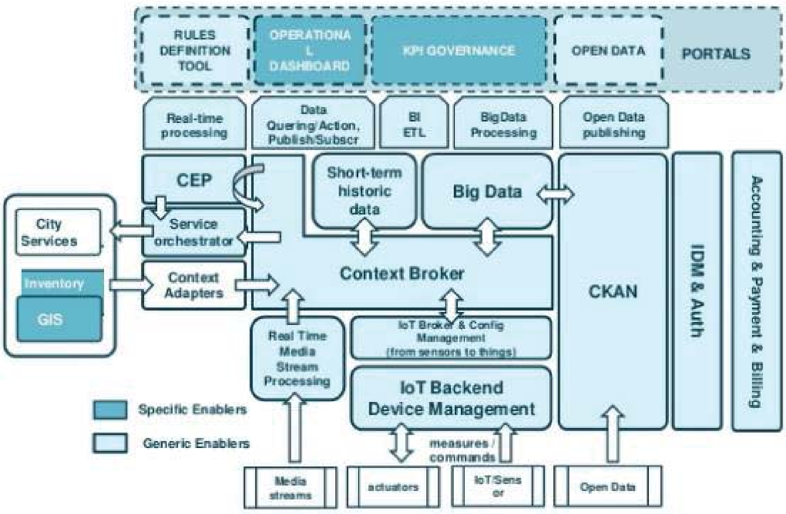

Figure 9. Target Smart City platform [4]

To provide the interoperability, Memorandum of Understanding towards open Urban Platforms for Smart Cities was issued by EC and signed in Berlin on May 21, 2015 [6]. Among others, the ambitious goals announced:

- by 2018 to create a strong EU city market for Urban Platforms
- by 2025, 300m residents of EU cities should use Urban Platform.

The question remains: how to get these goals?

Let us recall one of FIWARE critics [7]. The European Commission offers €100 million to entrepreneurs and startups from anywhere – not just Europe – to create a prototype 'smart city' application based on FIWARE. The idea is that developers use FIWARE's sandbox environment to trial their prototypes and get feedback from a smart city experts and developers that are on the platform. Now, it all sounds very laudable, but has anyone ever heard of a successful project to come out of these FIWARE competitions?

Alliance for IoT Innovation (AIOTI)

The IERC - IoT European Research Cluster – is bringing together EU funded projects with the aim of defining a common vision of IoT technology and addressing European research challenges. The European Commission has adopted on May 2015 the Digital Single Market strategy and has opened the door for large-scale proposals to improve the future of industrial development. In this context, the future activities can mobilize the important research work delivered by the IERC projects in terms of IoT technology. The launch of the Alliance for IoT Innovation (AIOTI) in order to develop and support the dialogue and interaction among the various IoT players should be seen as a signal in this direction [8].

The Alliance for Internet of Things Innovation is organized as a lean structure with 2 layers: the Board (Steering Committee) and 11 Working Groups (WGs):

WG 1: IoT European research cluster (Chaired by SINTEF)
WG 2: Innovation Ecosystems (Philips)
WG 3: IoT Standardisation (ETSI)
WG 4: Policy issues (Vodafone)
WG 5: Smart living environment for ageing well (STMicroelectronics)
WG 6: Smart farming and food security (Gradiant)

WG 7: Wearables. The "Wearables" refers to IoT solutions that integrate key technologies (e.g. nano-electronics, organic electronics, sensing, actuating, communication, low power computing, visualization and embedded software) into intelligent systems to bring new functionalities into clothes, fabrics, patches, watches and other body-mounted devices. The WG could focus their works on healthcare, well-being, safety, security and infotainment applications. (Chaired by Samsung)

WG 8: Smart cities. The "Smart Cities" working group refers to IoT solutions used by a city in order to enhance performance and wellbeing, to reduce costs and resource consumption, and to engage more effectively and actively with its citizens. Key 'smart' sectors may include transport, energy, healthcare, water, and waste.

(Chaired by Telefonica)
WG 9: Smart mobility (Bosch)
WG 10: Smart environment, smart water management (SIGFOX)
WG 11: Smart manufacturing

AIOTI is today the largest European IoT ecosystem. With 500 active members and more than 1500 high level experts split into 11 thematic working groups, during its first year, the Alliance for IoT Innovation succeeded to develop the most dynamic European Internet of Things ecosystem and to become a global influencer on IoT technology. Building on its success the AIOTI is now becoming a formal organization, which will continue to work with the European Commission on boosting the IoT innovation and deployment in Europe and beyond. The AIOTI project is a successor of FIWARE. Could it be more successful than FIWARE – it is a question.

OneM2M as a Smart City prototype

According to a recent report from McKinsey [9], up to 40 percent of the value of the Internet of Things can be enabled only with interoperability. This was the conviction behind the establishment of OneM2M, the global standards partnership for M2M and IoT service-layer standards.

OneM2M is a joint project involving eight leading ICT standards bodies across the world: ARIB (Japan), ATIS (North America), CCSA (China), ETSI (Europe), TIA (North America), TSDSI (India), TTA (Korea) and TTC (Japan). Together over 200 member companies are participating in the production and maintenance of the OneM2M standards.

Recent multi-vendor showcases and interoperability events demonstrated the wide range of applications of the technology, covering smart cities, intelligent transport, connected cars, smart metering, building automation and eHealth [10].

The OneM2M functional architecture (Figure 10) comprises three functions: Application Entity, Common Services Entity (CSE) and Underlying Network Services Entity. The basic one is the service layer: CSE includes Data Management, Device Management, M2M Service Subscription Management, Location Services and much more (Figure 11).

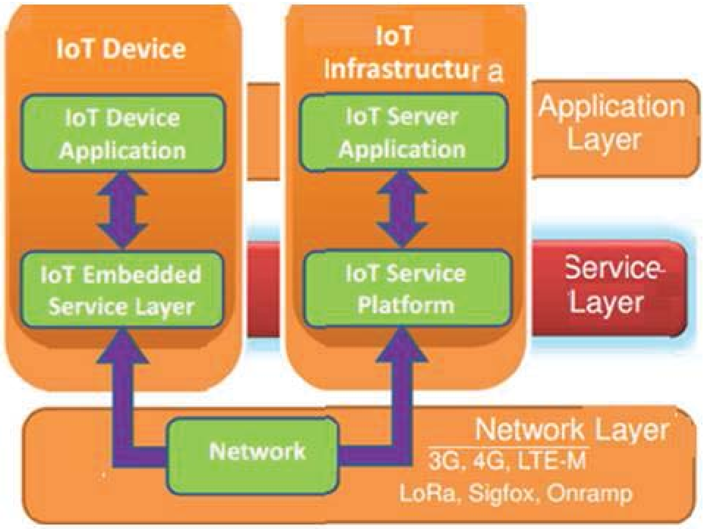

Figure 10. OneM2M Functional Architecture [11]

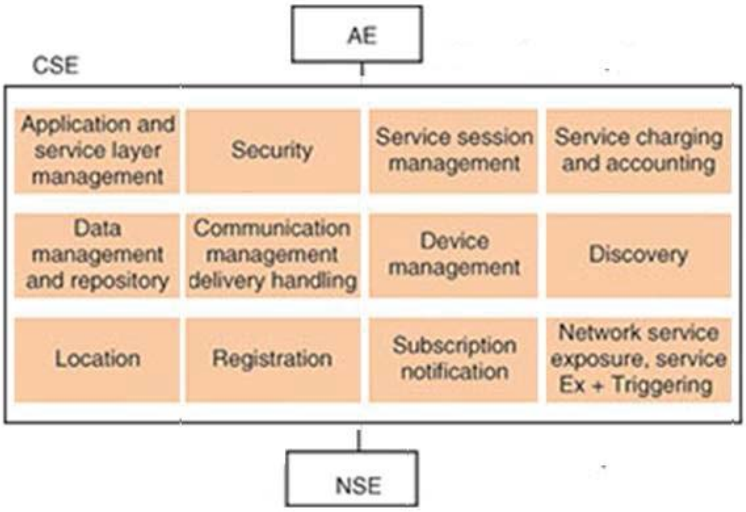

Figure 11. Common Services Functions [11]

NEC has announced [12] that it is the first company to test the new global OneM2M service layer standard in its Cloud City Operation Centre solution to enable M2M and Internet of Things device interoperability in a live smart city program. The solution bases on the FIWARE open source API-enabled platform. Using OneM2M, sensors are integrated with highly efficient local area protocols, such as the IETF's Constrained Application Protocol (CoAP), or the Message Queue Telemetry Transport (MQTT).

A few words on OneM2M critics. Speaking ahead of Mobile World Congress (Barcelona, 18 February 2016) – which will showcase the latest in mobile technology – Dr. Omar Elloumi (Nokia) said the full potential of IoT could only be realized if service providers and vendors alike look at it as a customer-centric opportunity while remaining focused on the bigger picture [13]. Without this, IoT growth will be stunted and the market will become heavily fragmented, leading to security issues and vendor lock-in.

Discussion pointed out the need to urgently increase collaboration and treat the IoT race as a marathon, rather than a sprint. The time required to create globally harmonized standards can create frustration for many companies, but this is nothing compared to the frustration consumers and industries will experience if their newly installed IoT system requires multiple controls for multiple devices and actually complicates their lifestyle or operations rather than simplifying them.

Security is another major obstacle that detailed and well-documented specifications can overcome with security functions covering identification, authentication, authorization, security association, sensitive data handling, and administration. Seamless interworking with multiple protocols, such as OMA LWM2M, OIC and AllSeen is one more area where oneM2M provides a significant value proposition to resolve the interoperability issue.

Some lessons for Russia

The article [14] aims to look for ways to solve hard Russian problems: the construction of system

112 and "Safe City" complex based on Russian hardware and software. What should we do?

The first priority is to develop unified system projects for “112” and complex "Safe city" for the whole country (primarily, the technical requirements in the information infrastructure), which implies association of Ministry of Emergency Situations and Ministry of Communications efforts and Rostelecom.

This task involves strengthening the leading role of the Ministry of Emergency Situations, as well as the revival of the leading institutes of the Ministry of Communications, in particular, the Institute ZNIIS, which weakened taken earlier in the course of privatization.

The policy of import substitution believes the use of Russian hardware and software, originally developed by the Russian safety standards, which, in turn, intends to increase Ministry of Economic Development and the Ministry of Communications to restore, in a certain sense, the functions of the former Soviet Ministry of Telecom Industry.

If we take the policy of import substitution, namely, on the development of communication networks on their own, then, in our opinion, should return to the state of knowledge achieved some 20 years ago, and to develop them further. As the reference point, we offer a system of SS7 and Intelligent Network. Given the backlog of the advanced world level, especially in the packet switching technique, which requires a strong microelectronics, should assess the prospects for channel switching, which does not require such a high speed.

To create a System 112 and the complex "Safe city" is necessary to organize training professionals able to develop regulations on communications networks with circuit-switched and packet-switched and develop hardware and software of new communication networks.

We emphasize the importance of software industry. This applies to a very painful issue for telecommunication managers about open programming interfaces (Open API). If it is an openly available set of API, you turn on many third-party developers in the development of System 112 and the complex "Safe City".

First and foremost - should be developed normative documents (standards) on the new hybrid network switching channels and packages, taking into account the latest requirements of the industrial Internet (Internet of Things and M2M communication), which is an extremely time-consuming task under the current the enthusiasm of foreign technology due to the post-Soviet period.

Smart City issues for Russia have discussed also in [15-16].

References

1 ETSI Network Functions Virtualisation – Introductory White Paper October 22-24, 2012 at the “SDN and OpenFlow World Congress”, Darmstadt-Germany. http://portal.etsi.org/NFV/NFV_White_Paper.pdf

2 Horizon 2020 Work Programme 2016 – 2017 Cross-cutting activities (Focus Areas) http://ec.europa.eu/research/participants/data/ref/h2020/wp/2016_2017/main/h2020-wp1617-focus_en.pdf

3 S. Mihaylov. Smart Cities and Communities Urban platforms. Experience from leading European cities. CONNECT, European Commission, 2015.

4 FIWARE https://www.fiware.org/2015/03/25/fiware-a-standard-open-platform-for-smart-cities/

5 Jesus Villasante. FIWARE is making cities smarter 05 January 2016 https://ec.europa.eu/digital-single-market/en/blog/fiware-making-cities-smarter

6 Towards Open Urban Platforms for Smart Cities and Communities. Memorandum of Understanding, 21 May 2015. Berlin.

7 Mike Butcher “Why Is the European Commission Spending €100M on a Pointless Hackathon?” https://techcrunch.com/2014/03/18/why-is-the-european-commission-spending-e100m-on-a-pointless-hackathon/

8 European Commission. Internet of Things Applications AIOTI. WG01 – IERC. Release 1.0. 15th October 2015.

9 Unlocking the potential of the Internet of Things. McKinsey report, 2015.

10 Ultan Mulligan, Richard Brennan, OneM2M: The Platform Standard for the Internet of Things January 5, 2016 http://sandhill.com/article/onem2m-the-platform-standard-for-the-internet-of-things/

11 OneM2M Technical Specification. TS-0001-V1.6.1 Functional Architecture, 2015-January-30.

12 OneM2M http://www.telecomtv.com/articles/m2m/nec-brings-the-onem2m-standard-to-smart-cities-12037/

13 IoT Race http://www.theinternetofthings.eu/onem2m-%E2%80%9Diot-race-marathon-not-sprint-%E2%80%93-industry-needs-urgently-increase-collaboration-warns-onem2m

14 Sneps-Sneppe M., Namiot D., Seleznev S., and Kupriyanovsky V. On system design for System-112 and the "Safe City" system // International Journal of Open Information Technologies. – 2016. – T. 4. – # 9. – S.44-63.

15 Namiot D. Umnye goroda 2016 //International Journal of Open Information Technologies. – 2016. – T. 4. – # 1. S. 1-3.

16 Namiot D., Sneps-Sneppe M. On software standards for smart cities: API or DPI //ITU Kaleidoscope Academic Conference: Living in a converged world-Impossible without standards? Proceedings of the 2014. – IEEE, 2014. – S. 169-174.

Поступила 30.09.2016

Об авторах:

Шнепс-Шнеппе Манфред Александрович, доктор технических наук, профессор Вентспилсской высшей школы; генеральный директор ООО «ЦКБ-Абаванет», manfreds.sneps@gmail.com;

Намиот Дмитрий Евгеньевич, кандидат физико-математических наук, доцент, старший научный сотрудник факультета вычислительной математики и кибернетики Московского государственного университета имени М.В. Ломоносова, dnamiot@gmail.com.