Body of European Regulators for Electronic Communications

BEREC

BoR (17) 40

Proceedings of the BEREC expert workshop on IoT

1 February 2017, 9:00-17:30
Thon Hotel City Centre Brussels

Workshop Agenda

9:00 Opening: Preparing the revolution for the Internet of Things
Sébastien Soriano, 2017 BEREC Chair, Chairman of ARCEP

9.15 Introduction: Main messages of BEREC's IoT report
Cara Schwarz-Schilling, Co-Chair NGN EWG, BNetzA/ Francesco Sciacchitano, AGCOM

9:30 **Session 1: Privacy, network security & consumers' rights**

Chair: Peter Thornqvist, Senior Legal Advisor, PTS

Speakers:

- Clémence Scottez, Head of the Economic Sector Department, CNIL (French DPA), Article 29 Data Protection Working Party
- Dan Tofan, Expert in Network & Information Security, ENISA
- Augustin Reyna, Senior Legal Officer, BEUC
- Arthur van der Wees, Vice-Chair, AIOTI WG 4

Q&A

11:15 **Session 2: Diversity of business models & interoperability**

Chair: Jim Morrish, Co-Founder and Chief Research Officer, Machina Research

Speakers:

- Patrick Guillemin, Chairman, AIOTI WG3
- Omar Elloumi, Chair Technical Plenary, OneM2M
- Guillaume Binoche, Director of Public Affairs, Sigfox

- Robert MacDougall, Head of Enterprise Regulation, Vodafone

Q&A

13:30 **Session 3: Scarce resources (numbers and frequencies)**

Chair: Sylvain Loizeau, Head of Section Spectrum, Technology & Innovation, ARCEP

Speakers:

- Óscar Carvalho, CEPT, Coordinator of Networks & Resources Unit, ANACOM on behalf of Johannes Vallesverd, Chairman, CEPT WG NaN
- Oli Bird, Rapporteur IoT, RSPG, Ofcom
- Professor Reza Karimi, Director of Corporate Strategy, Huawei
- Stefano Nicoletti, M2M Regulatory Manager, GSMA

15:15 **Session 4: Focus on IoT industry use cases (energy & transportation)**

Chair: Vincenzo Lobianco, Director, AGCOM/Cara Schwarz-Schilling, Co-Chair NGN EWG, BNetzA

Speakers:

- Luca Lo Schiavo, Deputy Director Infrastructure regulation AEEGSI, member of CEER Distribution Systems WG
- Luciano Baratto, Regulatory Affairs, ANIGAS
- Aria Etemad, Driver Assistance and Integrated Safety, Volkswagen Group Research
- Eddy Hartog, Head of Unit Smart Mobility and Living, DG CNECT, European Commission
- Sébastien Kaiser, Head of Telecom Strategy, SNCF

Q&A

17:15 **Conclusions/Wrap up**

Dr Stephen Unger, BEREC Vice-Chair, Group Director and Executive Board Member, Ofcom

The BEREC expert workshop on the Internet of Things (IoT) took place on 1 February 2017 in Brussels.

In his **opening**, *Sebastien Soriano, Chairman of ARCEP and 2017 Chair of BEREC*, considered that IoT presents a rare opportunity to open the telecom market all over again. IoT allows the introduction of new players and business models, in a market which has reached maturity since its opening back in the 90s. This burgeoning market requires regulators to adopt a prudent approach: listening to and understanding the IoT ecosystem should be preferred over standardising it, in order to foster innovation. BEREC's IoT 2016 report is a key pillar of IoT regulation for cellular technologies, but this vision needs broadening in order to embrace the full IoT scope. Mr. Soriano considered that the main challenges to face will come from security, privacy and interoperability. BEREC needs to promote a pro-innovation regulation, which aims at empowering entrepreneurs and help them solve issues, instead of trying to come up with the solutions. IoT is a unique occasion to bring Europe back at the forefront of technology, with the help of regulators and lawmakers.

In the following **introduction** to the **BEREC Report "Enabling the Internet of Things"**, *Cara Schwarz-Schilling, Co-Chair BEREC NGN EWG and Head of Section Internet Economics, BNetzA*, and *Francesco Sciacchitano, AGCOM*, presented the main messages of this report, focusing on the topics relevant for the BEREC IoT workshop, namely privacy / network security, standards / switching and scarce resources. They welcomed that some of the conclusions of the BEREC Report are reflected in the proposal for a European Electronic Communications Code (namely the recommendations concerning a European numbering space as well as over-the-air provisioning of SIM).

Session 1 addressed issues related to **"Privacy, network security & consumers' rights"**. The chair, *Peter Thörnqvist, senior legal advisor at PTS (the Swedish NRA)*, stressed the need for interaction across different professional branches when regulatory issues related to IoT and privacy, network security and consumer protections are addressed. With IoT the growing amount of data collected in the private sphere was a new phenomenon and the question for responsibility is crucial.

Clémence Scottez, Head of the Economic Sector Department, CNIL (French DPA), Article 29 Data Protection Working Party, presented the main features of both the new General Data Protection Regulation (GDPR), and the recently proposed draft e-Privacy regulation (ePR) and addressed how they could affect the deployment of IoT services and connected things. With reference to one example involving smart meters, she emphasized that a privacy-by-design approach to define guidelines for the development of products or services using smart meters data, would increase the level of customer confidence, limiting privacy risks, giving legal assurance.

Dan Tofan, Expert in Network & Information Security, ENISA, explained why ENISA considers that IoT security matters, with reference to that no device is fully secured, and that IoT security currently seems to be limited, in most of the cases due to the lack of available resources (processing power, physical space) to incorporate "extra features" such as security. Also security by design is not yet is the norm in the industry and investments on security are limited. This can entail real physical threats with risks on health and safety. Also, there is no legal

framework for liabilities. The IoT brings “smarter” and broader attack surface. ENISA’s work on IoT and smart cybersecurity focuses on smart home, smart cities and intelligent public transport as well as smart infrastructure to help operators understand and defend from cyber threats.

Augustin Reyna, Senior Legal Officer, BEUC, illustrated through a test case including a connected doll some of the challenges for providers of such connected devices but also the risk for consumers. This case was a particular serious one since children were exposed. An investigation by the Norwegian Consumer Council showed serious privacy, consumer protection and security concerns. Apart from massive breaches of data protection law, the doll was used for advertising to children as well as product placement and hidden marketing by pre-programmes phrases endorsing commercial products. There was a considerable lack in security: no security was embedded at all, a third party could connect to the doll without having access to it, and it was very easy to “hack” and talk through the doll to the kid. These risks could have been avoided (e.g. by making physical access to the toy required, a random code printed on the toy, by requiring the user to press a button to pair). This was also a show-case for a successful cooperation between consumer agencies and consumer associations in different countries. Several toy chains as well as Amazon stopped sales, or refunds were offered. Beyond that, this case raised several outstanding policy questions. According to Mr Reyna, the case however shows that self-regulation is not sufficient.

Arthur van der Wees, Vice-Chair, AIOTI WG 4, focused on the issues of trust and responsibility for IoT devices. He pointed to the Commissions goals in their ongoing consultation on the European data economy dealing with free flow of data, data portability, accountability & liability, security & IoT trust label and personal data protection. Different categories of data needed to be adressed differently. In an environment with machines it was not clear what consent based data usage really means. It was considered crucial to balance the allocation of risk, accountability & liability for security and privacy in an IoT environment. It is a challenge to clearly allocate responsibility for the data at each stage of the data flow. He stressed that, from a cost perspective, there are sincere benefits in not having to retrofit privacy compliance and security, but instead already by design addressing needs and requirements.

In the *Q&A session* it was discussed whether certification with regard to privacy and security could be seen as solution and, if yes, who would define the rules and support them. *Mr Tofan* considered that it was more effective to focus on producers wheras *Mr Reyna* considered that consumer education could play an important part. Mr van der Wees held that preconfigured settings by producers fulfilling minimum requirements were needed. Responsibility cannot be pushed to the consumer. He also stressed that the same level of security and privacy should apply for producers from the EU and outside the EU and minimum requirements for marketing within the EU should be set. *Ms Scottez* held that certification procedures could be an effective way to prove compliance with the rules.

With regard to the question of data ownership *Mr van der Wees* held the opinion that data ownership in the digital space was “dead”. What was important is that the person has the decision on how his personal data are controlled, accessed and used. *Ms Scottez* agreed that

ownership in the legal sense was not the right concept. Focus should be on user-centric tools to empower people to have control of their data (personal information management).

Session 2 on **Diversity of business models & interoperability** was moderated by *Jim Morrish, Co-Founder and Chief Research Officer, Machina Research*.

Robert MacDougall, Head of Enterprise Regulation, Vodafone, explained the regulatory and policy context, e.g. EU Commission's Platform Communication, the proposal for a European Electronic Communications Code, Intelligent Transportation Systems and Commission consultation on Building the European data economy. He then gave a brief introduction to Vodafone and IoT activities relevant to panel objectives, e.g. IoT partnerships, innovation, platforms, related standards activity, specifying that the choice for a respective connectivity technology (e.g. 4G/4G+, 2G/3G, fixed, satellite, LPWA/NB-IoT) depends on the respective customer requirements. Mr. MacDougall gave an update on the status of over-the-air (OTA) provisioning of SIM. OTA enables switching in the IoT industry. A SIM can be remotely reprogrammed over the air so that there is no need to physically replace the SIM. However, despite early adoption in automotive, widespread market adoption of eUICC has been slower than expected. Cost of deploying eUICC and historic lack of interoperability (e.g. across SIM vendors) are hampering adoption. Envisaged next steps to address these challenges are the development of (1) a business process template within GSMA, in order to establish a transparent, traceable, predictable and scalable business process to migrate customers at end of contract, and (2) a tool to manage the switching process. Regarding the latter, discussion has started within GSMA to develop a messaging system between operators to manage the switching process based on an eUICC Proof of Concept. A long-term solution, as envisaged by Vodafone, might be a centralized switching solution operated by an independent entity.

Omar Elloumi, Chair Technical Plenary, oneM2M, introduced oneM2M as well as its design principles. oneM2M designs a software "framework", i.e. a service layer that sits between the network (3GPP, LPWA, wireline, LTN, etc.) and the applications. It provides functions that M2M applications across different industry segments commonly need (e.g. data transport, security/encryption, remote software update). It is like an operating system for the IoT but it sits both on the field devices/sensors and in servers, and it is a standard – not controlled by a single private company. oneM2M came to the conclusion that there is a need to have both network identifiers and service layer identifier and create or maintain a mapping between both during the lifecycle of the service layer subscription. The requirements that motivated this design principle are the following: (1) a device may connect through multiple access networks (wifi, 3GPP, Sigfox, etc) however data collection and exchange should be linked to the service layer identifier regardless of the access network used at a particular point in time; (2) a device may change network subscription but maintain the service layer subscription, without any disruption at the service layer. In this case, the mapping between the service layer identifier and the new network identifier (not to be confused with the network address) needs to be maintained. As a side note from a service layer perspective, number portability for M2M is not as a strong requirement as for personal communications because a network number change can be dealt with an update of the service layer identifier mapping to network identifier (or a set of).

Raoul Mallart, Vice President Imagineering, Sigfox, explained the challenges of massive IoT (low cost, global, low power, easy to use) and illustrated Sigfox' IoT activities. He then shared

Sigfox's view on how to best ensure the raise of the massive IoT market. From the day to day contacts with the market (device makers and end clients), Sigfox is observing that the IoT market has raised slower than excepted, because companies are not well prepared to integrate it in their internal functioning and have not yet developed adapted products/services to do so rather than a lack of standards on the connectivity layer. Furthermore, in Sigfox's view the different connectivity solutions currently existing on the market are in fact complimentary and not directly competing. There is room for different connectivity solutions which will address different use cases. In their opinion, the development of one single standard on the connectivity layer would have a negative effect by preventing companies to choose the most adapted solution to their specific needs. Also from an interoperability point of view, Sigfox does not see a need for a standard at the radio layer. However, a progressive global harmonisation of the frequencies dedicated to the IoT seems necessary to allow a better interoperability between devices and to allow the deployment of certain use cases which imply the worldwide mobility of a device (notably the tracking solutions). Still, Sigfox understands the risk identified by regulators and public authorities which fear that the multiplication of technologies would lead to a lack of interoperability. Interoperability is necessary to help the market grow. In this context, it is necessary to ensure interoperability (and develop standards): (1) At the network and application level: by using an optimized Internet protocol stack to help developing common IoT applications for both, devices and application servers. (2) At the data level: standardized data models could be designed.

Patrick Guillemin, Chairman, AIOTI WG 3, presented AIOTI's work on standardisations. WG3's main tasks are analysing the landscape, identifying gaps, divergences and common concerns and publishing guidance and recommendations. He gave an overview over IoT standard development organisations (SDO) and alliance landscape (both technology and marketing dimensions as well as vertical and horizontal domains) as well as over IoT open source initiatives landscape (technology and marketing dimensions). He then explained ETSI's work in support of AIOTI WG03. In 2016, ETSI has published reports on IoT standards landscaping (TR 103 375) and on IoT gap analysis (TR 103 376). ETSI report IoT standards landscaping (TR 103 375) analyses the IoT standards landscape (in total, 329 standards have been identified) and provides a list of existing standardised technology suggested for reuse by the LSPs. ETSI report on IoT gap analysis (TR 103 376) identifies technical, societal, and business gaps as a good indication of the level of maturity of standardization in a given vertical domain. Gaps are understood as (1) missing standards; missing APIs, (2) duplications requiring harmonization, and (3) missing interoperability profiles. Security & privacy gaps are classified as Societal gaps. Gaps have been identified by a survey in the IoT community, complemented by an experts' analysis. Resolution of gaps is left to the proper organisations in the IoT community.

In the *Q&A Session*, connectivity providers were asked about their view on the design principle proposed by oneM2M to separate the service layer subscription from the network subscription, which was appealing for NRAs in terms of openess.

Mr Mallart pointed to the fact that connectivity was just one element of their business model and *Mr Morrish* agreed that unhinging connectivity from service was, impossible in case of Sigfox, and staggeringly difficult for other business models. It seemed pretty impracticable in the present market.

Mr MacDougall pointed out that in the automotive sector they moved beyond connectivity and want to diversify and offer additional services.

Mr Elloumi said that there may be other models. Some energy companies have their own platform. For that case they have to work with different connectivity providers. Flexibility to switch is important for users, a business imperative and part of market demand, and the reason for operators working on eSIM. The automotive industry is one important customer group which pushes for the possibility to switch connectivity provider.

Competition in the view of *Mr McDougall* should take place between different platforms.

Session 3, moderated by *Sylvain Loizeau, Head of Section Spectrum, Technology & Innovation, ARCEP*, focused on **"Scarce resources"**. The ability to provide connectivity solutions for IoT generally relies upon the use of two types of resources: frequencies and numbers. This session was composed of four presentations.

Óscar Carvalho, CEPT, Coordinator of Networks & Resources Unit, Market Regulation dpt., ANACOM, focused on numbering issues while describing past and current CEPT works, including contributions to the ITU workflow. While M2M numbering plan management does play a key part in leveling the playing field, it could be considered as less critical to IoT than spectrum management, as M2M will remain only a small part of the total traffic. However, M2M-specific extended E.164 numbering ranges are essential to face the growing number of objects and can be addressed with national and global numbering resources. Moreover, given the inherently international nature of the market, the extra-territorial use of E.164 numbers for M2M is a key factor but also bring challenges. Finally, in order to ensure easy switching, E.212 MNC flexibility and OTA changing of SIM profiles are two possible paths that can be considered. OTA has a wider potential, but still needs to be adopted as a viable solution to all market parties. CEPT as a numbering expert group is available to cooperate in the evaluation of this matter.

Stefano Nicoletti, M2M Regulatory Manager, GSMA, went back over BEREC's "Enabling the IoT" report to highlight the advantages of OTA vis-à-vis direct MNC attributions to undertakings other than telco and indicated that the creation of a potential European numbering range for M2M would be unnecessary given that IoT is a global market. After focusing on 3GPP standard technologies and their advantages for LPWAN, he called for the adoption of a service/technology neutral framework. GSMA considers that current and future licensed mobile bands can support both IoT and personal mobile broadband services. However, harmonisation of spectrum on sufficiently large scales is vital for a global, affordable cellular IoT market.

Oli Bird, Rapporteur IoT, RSPG, Ofcom reminded the audience of the elements within the RSPG's work program addressing IoT, notably working groups on IoT and ITS, which would soon be presenting Opinions for adoption by RSPG Plenary, and the working group on 5G, which would be considering regulatory challenges and industry use cases. He presented some emerging headlines of the RSPG's view, notably that IoT is composed of a wide variety of technologies and use-cases, which in turn calls for a diversity of spectrum solutions in terms of frequency bands and authorization models. While spectrum scarcity has not restrained the growth of IoT, there is increasing demand for spectrum access, which may be met through technical harmonisation and standardisation measures, authorisation models, and

coordination between Member States in order to enable economies of scale to develop. To this end, the RSPG offers a roadmap for IoT spectrum access to enable focus on spectrum bands. There is no need for identification of frequency bands for IoT exclusively.

Reza Karimi, Director of Corporate Strategy, Huawei, expanded on spectrum matters. He proceeded to detail the pros and cons of licenced and licence-exempt spectrum as well as public and private networks for IoT. Huawei considers that NB-IoT is a powerful technology for the provision of spectrally efficient and low-cost massive M2M services and called for the EU and national administrations to work towards allowing European deployments of NB-IoT during 2017. Huawei regards licence-exempt spectrum as not ideal for safety related ITS services, due to the lack of QoS assurance. While Huawei is fully committed to enabling the coexistence of multiple technologies in license-exempt 5.9 GHz, it encourages the EC and national administrations to consider alternative authorisation models to mitigate the risk of harmful interference.

Session 4 gave a focus on "**IoT industry use cases (energy & transportation)"** and was moderated by *Vincenzo Lobianco, Director, AGCOM*, for the energy use cases and *Cara Schwarz-Schilling, BEREC Co-Chair NGN EWG and Head of Section Internet Economics, BNetzA* for the transportation use cases.

The **energy sub-session** started with two presentations of the Italian practices about the introduction of smart meters in the public utilities, respectively for electricity and gas sectors. Then the preliminary results of an analysis of the various options for the connections of smart meters were presented at the end of the session.

Luca Lo Schiavo, *Deputy Director Infrastructure regulation at the Italian Regulator for electricity, gas and water (AEEGSI), member of CEER Distribution Systems WG,* gave a presentation of the electricity smart metering experience in Italy, developed in a framework of cooperation between energy and telecom NRAs. He illustrated the deployment of electricity smart metering in Italy, started in year 2001 with the 1st generation of devices, detailing the system architecture and the benefits obtained by the industry and the customers. Mr Lo Schiavo then introduced the technical specifications of the generation 2.0 of smart meters, approved in year 2016 by AEEGSI decision n. 87. This new generation of smart meters is characterised by the introduction of a second communication channel (*chain* 2) for the real-time delivery of measured data to the end customer. In the same decision, the NRA planned the evolution towards release 2.1, whose specifications, as far as *chain 2* communication channels is concerned**,** will be drafted in collaboration with AGCOM. Concluding his speech, Mr Lo Schiavo presented the PEER (Partnership for the Enforcement of Energy Rights) initiative, launched by the Council of European energy regulators (CEER) to enhance inter-authority (cross-sectoral and cross-authority) cooperation at EU level to benefit consumers.

Luciano Baratto, Regulatory Affairs of ANIGAS –the Italian Association of the Gas Industry, presented the situation of the national gas value chain, detailing the regulated parts of the chain, which includes, inter alia, the distribution and metering. Starting from year 2007, the Italian Gas Industry was deeply involved in the implementation the AEEGSI regulation and the drafting of the technical specifications of smart meters, carried out in the UNI/CIG (Italian National Gas Standardization Body) Committee. He presented the details of specifications that, as for the communication channel, mandate 2G technology for Point to Point architecture and unlicensed based technology (WMBus) for Point to Multi Point architecture. Mr Baratto, in

the conclusion of his presentation, described how these specifications are evolving to introduce the new available M2M technologies such as NBIoT.

Vincenzo Lobianco from AGCOM, presented the preliminary results of an analysis on the various options currently in use or available a short term for the connection of smart meters to the central systems or to the end users. The analysis involved all the stakeholders: the public utility industry, meter and telecommunication equipment manufacturers, mobile service providers and tower operators offering LPWAN services, etc. The analysis was carried out in the view of the future cooperation with the AEEGSI for defining the specifications of the new release (2.1) of electricity smart meters. Nevertheless, it encompassed all public utilities, in order to check the requirements of all sectors against the characteristic and the performances of the wired and wireless solutions investigated. It emerged, from the analysis that all the alternatives at present in use and based on wired (PLC), LPWAN technologies using unlicensed bands – WMBus, LoRa, SigFox - or mobile technologies – for the time being 2G only – are meeting the current requirements of smart meters. However, considering the new requirements related to the need of increasing the consumer awareness for the resource saving and to the introduction of more advanced services in public utilities, the introduction of the new standards, like the NBIoT shall be carefully considered for the massive deployment of future proof devices, given also the long (15 years) life cycle of a smart meter.

Asked with regard to the level of cooperation and standards (overlap, joint action etc.) *Mr Lo Schiavo* replied that the situation differed at country level. In Italy CEI (the standardization national body for electrotechnical issues) is also a member of ETSI dealing with interoperability and interchangeability.

The **transportation sub-session** consisted of two presentations concerning the automotive sector and one presentation regarding the rail sector.

Eddy Hartog, Head of Unit Smart Mobility and Living, DG CNECT, European Commission, gave an overview over the EU Commission's policy on Connected and Automated driving (CAD). Stakeholders involved are the EU Commission, Member States, regions, cities and industry. The common objective is an accelerated deployment of CAD. Periodical roundtables on CAD serve to facilitate the cross-sectorial dialogue between automotive and telecommunication / IT industry. The aims are (1) to strengthen Europe's position in CAD, (2) to accelerate roll-out of increasing levels of automation in Europe, (3) enable pan-European, large-scale project on CAD, (4) facilitate alignment of roadmaps across the sectors. For a quick deployment on the ground, hybrid communication technologies might be necessary. Consensus positions are that a mix of communication technologies is required, with 5G as a front runner, that there are real spectrum needs, that data access and use, with cross-border experimentation, is necessary.

Aria Etemad, Driver Assistance and Integrated Safety, Volkswagen Group Research, explained the concept of automated driving, illustrating it with examples of Volkswagen's activities. He started explaining the different levels of driving automation, from assisted and partial automation to conditional and high automation and finally full automation. Starting from level 3, conditional driving, the driver is out of the loop. These automation levels are not yet in accordance with regulatory law, i.e. the Vienna Convention of 1968 and national road laws. There is a need for action to deal with the shared responsibilities of the driver and the system. At the example of highway scenarios, he illustrated the innovation (e.g. predictive automated

driving style, improvement of energy efficiency) and challenges (e.g. development of fault-tolerant and resilient system architecture, dealing with driver take-over situations) of automated driving. Apart from on-board sensors, automated driving is supported by cooperative ITS technologies based on ITS G5 used for robust vehicle-to-vehicle and vehicle-to-infrastructure communication as well as for developing and implementing the foreseen automated cooperative functions.

Sébastien Kaiser, Head of Telecom Strategy, SNCF, presented use cases of how SNCF makes use applications for the industrial internet to improve railway maintenance. It is expected that combining IoT with Big Data will bring major gains in safety and performance. Predictive maintenance will replace preventive maintenance. One example for the remote diagnostic of rolling stock is the maintenance of lavatories in trains using IoT sensors and LPWA networks like Sigfox and LoRaWAN. Savings of maintenance costs, increased availability for the user and reduced maintenance operation time are the major gains. Mr. Kaiser also pinpointed the lessons learned. In his experience, LPWA networks for train to ground communication are not ready yet. He raised the question what to expect from LTE-M and NB-IOT coming soon. As a second example, he presented a thermometer which is installed at the rails at critical locations. Its features are warning of abnormal temperatures in order to trigger a targeted visit. Geolocation of each sensor and autonomy of 2 years are requirements. The crucial question was how to produce the highest technology on short series in good financial conditions.

In the *Q&A session*, with regard to the different levels of automation the question was raised how to keep the attention of the driver. *Mr Etemad* replied that driver monitoring is on top of the list to see whether the driver is able to take over control again, which may take up to 10 seconds.

Again the issue of upgradability and sustainability in a long lifecycle was raised. *Mr Kaiser* replied that the lifecycle of a train was 40 years, whereas the IoT solution depends on the concrete use cases. *Mr Etemad* took the position that it depends on the amount of upgrade required. A change of system could only occur after the next lifecycle, but software upgrades were possible.

Mr Hartog pointed out that a mixed fleet of unconnected and connected vehicles will exist for many year and pose regulatory challenges. The question has to be asked to what extent the connectivity part will need to be approved along with the technical approval of the vehicle.

Asked which technologies, cellular or non-cellular, were more likely to be used, *Mr Etemad* replied that it depended on the application: For time-critical scenarios nearfield technologies (vehicle-to-vehicle) were best suited while for non-time critical applications like updating a map or infotainment LTE or similar technology would be used. *Mr Kaiser* saw application of LTE for both critical and non-critical missions.

Asked with regard the need to be able to switch connectivity provider *Mr Etemad* replied that experience in the automotive sector showed that it is always better to have more than one supplier.

In his **conclusions**, *Dr Stephen Unger, BEREC Vice-Chair, Group Director and Executive Board Member, Ofcom*, noted that IoT will be a driver for innovation in all industry sectors and

that the connectivity solutions underlying IoT services and connected devices are manifold. Dr Unger underlined that an innovation-friendly approach is a top priority of BEREC in order to create a competitive environment in the IoT sector. He welcomed that, in its proposal for a European Electronic Communications Code, the Commission has taken into account many of BEREC's suggestions put forward in the report "Enabling the Internet of Things" while stating that regarding extra-territorial use of numbers a worldwide solution is necessary. Dr Unger clarified that EU net neutrality rules are not an obstacle for the development of IoT services. Thanking the speakers and the audience, he expressed that a dialogue like today's BEREC IoT workshop is very important for a comprehensive understanding of the IoT sector and for each other's work.