An Coimisiún um
Rialáil Cumarsáide
Commission for
Communications Regulation

ComReg response to the Department of Transport consultation on connected and autonomous mobility in road transport

Response to Consultation

Reference: ComReg 21/11

Version: FINAL

Date: 11/02/2021

An Coimisiún um Rialáil Cumarsáide
Commission for Communications Regulation
1 Lárcheantar na nDugaí, Sráid na nGildeanna, BÁC 1, Éire, D01 E4X0.
One Dockland Central, Guild Street, Dublin 1, Ireland, D01 E4X0.
Teil | Tel +353 1 804 9600 Suíomh | Web www.comreg.ie

Additional Information

Approval

Legal Disclaimer

This Response to Consultation is not a binding legal document and also does not contain legal, commercial, financial, technical or other advice. The Commission for Communications Regulation is not bound by it, nor does it necessarily set out the Commission's final or definitive position on particular matters. To the extent that there might be any inconsistency between the contents of this document and the due exercise by it of its functions and powers, and the carrying out by it of its duties and the achievement of relevant objectives under law, such contents are without prejudice to the legal position of the Commission for Communications Regulation. Inappropriate reliance ought not therefore to be placed on the contents of this document.

An Coimisiún um
Rialáil Cumarsáide
Commission for
Communications Regulation

Department of Transport
Leeson Lane
Dublin 2
D02 TR60

ConnectedAutonomousMobility@transport.gov.ie.

11 February 2021

Dear Sir / Madam

Thank you for the opportunity to make this formal input to the new cross-Government national strategy which will set out the steps to be taken over the coming years to facilitate the development and deployment of connected and autonomous mobility (CAM) in Ireland.

The Commission for Communications Regulation (ComReg) is the statutory body responsible for the regulation of the electronic communications sector (telecommunications, radio communications, broadcasting transmission and premium rate services) and the postal sector.

In your consultation you define connected vehicles as those which use digital connectivity to talk to each other and to their surrounding environment. One of the key enablers will be connectivity provided by electronic communication systems (ECS) and /or electronic communication networks (ECN) to facilitate this communication.

Having taken this into account, there are four matters on which ComReg would like to contribute to the consultation that are relevant to ECS and ECN:

- the use of the radio spectrum resource;
- the use of the numbering resource;
- ensuring cybersecurity, data protection and data access; and
- the opportunities available under ComReg's Test and Trial Ireland, a wireless licensing service that encourages innovation and development of wireless communications using Ireland's radio spectrum.

1 The radio spectrum resource

It is likely that connected mobility will require the use of wireless technologies (radio equipment) which will make use of the radio spectrum resource. In Ireland, the possession and use of radio equipment is governed by the Wireless Telegraphy Act 1926, (Act No 45 of 1926), (as amended), which stipulates that an appropriate Wireless Telegraphy licence must be held, unless licence exempted.

ComReg is the authority charged with the authorisation of Wireless Telegraphy equipment in Ireland. Such an authorisation may take the form of either a licence or a licence exemption – for the avoidance of doubt there is no such thing as unlicensed use of the radio spectrum in Ireland.

In managing the radio spectrum, ComReg has set down specific rules and regulations for the possession and use of many forms of radio equipment. These regulations specify the licensing regime or exempt the radio equipment from licensing. Unlicensed or non-compliant possession or use of radio equipment is illegal, rendering offenders liable for prosecution.

The harmonised use of the radio spectrum resource is a very important matter for manufacturers as this leads to international standardisation, the use of the same spectrum bands in many parts of the world and economies of scale in manufacture. Generally, and given Irelands size and population, ComReg considers it prudent for Ireland to keep step with European spectrum harmonisation as this harmonisation is pivotal for manufacturers to achieve economies of scale. It is important to note that should a non-harmonised spectrum band be utilised it adds notable risk in the event the band chosen is subsequently harmonised for a different purpose and consequently incumbent systems are no longer prioritised or need to be moved from the band to facilitate European wide harmonised ones.

Many of the European harmonised spectrum bands have already been authorised for use in Ireland and more are currently being made available through a multi-band award process[1]. It is conceivable that this licenced spectrum might be used for connectivity in some arrangement with the respective licensees.

In 2018 the European Commission published an EU strategy for mobility of the future[2]. This strategy notes, in respect of radio spectrum, that "*The Commission will support the coexistence of different radio technologies using the 5.9 GHz spectrum band while taking into account the principles of uncompromised safety, technology neutrality and efficient spectrum use*".

In support of this statement an updated Implementing Decision[3] was published on the 7 October 2020 to harmonise the conditions for the availability and efficient use of frequency band 5 875-5 935 MHz for safety-related applications of Intelligent Transport Systems (ITS). The definitions in this Decision clearly indicate the intended use of this spectrum band for connected vehicles. In line with this Decision it is

[1] See https://www.comreg.ie/industry/radio-spectrum/spectrum-awards/proposed-multi-band-spectrum-award/
[2] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0283
[3] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32020D1426

ComReg's intention to designate this frequency band to ITS and make it available on a non-exclusive basis.

2 The numbering resource

ComReg manages Ireland's telecommunications numbering resource. To the extent that connected vehicles and devices in the CAM ecosystem utilise publicly available networks and will need numbering resources, ComReg commits to making suitable resources available to support this.

In this regard, ComReg introduced a dedicated Machine-to-Machine (M2M) number range in 2018[4], following public consultation. This was prompted in part by forecasted exponential growth of M2M connections on mobile networks and a clear trend for the 'extraterritorial' use of national numbers across the EU and internationally by M2M Service Providers e.g. in the context of cross-border road journeys. The European Electronic Communications Code[5] (EECC) also allows each Member State to have a dedicated number range for M2M services that explicitly permits extraterritorial use.

Ireland's M2M numbers have 10 subscriber digits and use the 088 prefix. This is a maximum number length of 15 digits allowed in international format (i.e. +353 88 + 10 digits) and is in line with a CEPT[6] recommendation to have M2M numbers as long as possible. This removes pressure on the existing mobile number ranges and creates a sufficient supply of numbers (10 billion) to cater for projected growth in the M2M market over the long term. The new M2M range may be used for eCall (an automatic emergency calling capability fitted in all new cars sold in the EU from 31 March 2018).[7]

Although mobile networks are evolving to all-IP networks, communications industry respondents to ComReg's 2018 consultation indicated that many M2M connections will continue to need numbers for a variety of technical and operational reasons. In the long term there remains the likelihood that IP addresses (specifically IPv6)[8] will be used for the vast majority of M2M communication[9]. However, it is expected that while the network itself could potentially function using only IP addresses, operators' operational support systems and billing systems will continue to rely on numbers for some time. Also, where connections are primarily for M2M communications, but have a requirement for occasional interpersonal communications (e.g. eCall) a telephone number would be required for that purpose. In any case, there would likely be a substantial overlap period where both IPv6 and E.164 numbers are in use. Therefore, the use of numbers for M2M communication will remain relevant for at least the next 10-15 years.

---

[4] Review of Mobile Numbering – Response to Consultation and Decision, ComReg Document 18/46, June 2018

[5] Directive 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code

[6] The European Conference of Postal and Telecommunications Administrations (CEPT) is an organization where policy makers and regulators from 48 countries across Europe collaborate to harmonise telecommunication, radio spectrum, and postal regulations to improve efficiency and co-ordination for the benefit of European society.

[7] See https://europa.eu/youreurope/citizens/travel/security-and-emergencies/emergency-assistance-vehicles-ecall/index_en.htm

[8] Internet protocol version 6 (IPv6) is developed by the Internet Engineering Task Force (IETF) for use in packet switched networks

[9] ComReg has no role in relation to the management of IP addresses. IP address resources are managed at European level by RIPE NCC (Réseaux IP Européens Network Coordination Centre), which is one of 5 regional Internet registries (RIR). It oversees the allocation and registration of Internet number resources (IPv4 addresses, IPv6 addresses and autonomous system numbers) directly to Internet service providers (ISPs) and to telecommunication organisations.

2.1 Over the Air ("OTA") Provisioning

The EECC also requires Member States to promote OTA provisioning to facilitate provider switching, with emphasis on switching between Machine-to-Machine (M2M) service providers. OTA provisioning relies on 'embedded' SIM (eSIM) technology. The automotive and transport sectors have been earlier adopters of eSIM technology and OTA provisioning for connected vehicles, freight tracking and so on.

In response to this new EECC requirement, ComReg has commissioned an expert study to support the development of a strategy for the promotion of OTA provisioning in Ireland. ComReg is one of the first National Regulatory Authorities in the EU to address the requirement. The study will consider how the potential impact of OTA provisioning could be promoted or maximised to facilitate switching in line with ComReg's statutory objectives to promote competition, to contribute to the development of the internal market, and to protect the interests of users. The study report will outline a 5-year vision for developing OTA provisioning for both consumer mobile and M2M services and a roadmap for the achievement of the vision. ComReg intends to publish the report by mid-2021.

3 Ensuring cybersecurity, data protection and data access

ComReg highlights below certain legal provisions relating to security, integrity of networks, and cybersecurity, that could be of relevance to the Department of Transport in the context of the development and deployment of connected and autonomous mobility in Ireland[10].

Section 12(2)(c)(vii) of the Communications Regulation Act 2002, as amended, provides that in so far as the objective of promotion of the interests of users within the Community is concerned, ComReg has to take all reasonable measures which are aimed at achieving this objective, including ensuring that the integrity and security of public communications networks are maintained.

Regulations 23 and 24 of the European Communities (Electronic Communications Networks and Services) (Framework) Regulations (SI 333 of 2011), which implement Articles 13a and 13b of the Framework Directive[11], place obligations on operators providing public communications networks or publicly available electronic communications services in respect of the management of the integrity and security of networks and services. Such undertakings shall take appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services. In particular, measures shall be taken to prevent and minimise the impact of security incidents on users and interconnected networks.

Regulation 23 requires an operator to notify ComReg in the event of a breach of security or loss of integrity that has a significant impact on the operation of networks

[10] Rather than ComReg commenting directly on data protection and data access issues, we consider that those issues are better placed to be commented on by the Data Protection Commission.

[11] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), as amended.

or services. Where ComReg receives such reports, it is required to inform the Minister and, where appropriate, the European Network and Information Security Agency (ENISA).

For the purpose of ensuring compliance with Regulation 23 (1), (2) and (3), ComReg may issue directions to an undertaking providing public communications networks or publicly available electronic communications services, including directions in relation to time limits for implementation.

ComReg may require an undertaking providing public communications networks or publicly available ECS to: (a) provide information needed to assess the security or integrity of their services and networks, including documented security policies, and (b) submit to a security audit to be carried out by a qualified independent body nominated by ComReg and make the results of the audit available to ComReg and to the Minister. The cost of the audit is to be borne by the undertaking.

The security provisions in the proposed **European Electronic Communications Code[12] are set out in Articles 40 and 41**. These essentially replicate the existing Articles 13a and 13b in the current Framework Directive, but with some new elements:

- Article 40 sets out in detail the relevant parameters to judge the significance of the impact of a security incident, such as the numbers of users affected, the duration of the breach, the geographical area of the breach, and the extent to which the functioning of the service is disrupted (Art. 40(2))

- ENISA shall facilitate the coordination of Member States to avoid diverging national requirements that may create security risks and barriers to the internal market. (Art. 40(1))

- Member States shall ensure that, in order to implement Article 40, the competent authorities have the power to obtain the assistance of Computer Security Incident Response Teams ('CSIRTs') designated pursuant to Article 9 of the Network and Information Systems Directive in relation to issues falling within the tasks of the CSIRTs pursuant to Annex I, point 2 of that Directive. The team will monitor developments concerning the EECC. (Art. 41(4)).

The **Directive on Security of Network and Information Systems (Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union** provides minimum standards of cyber security across the EU for private and public operators of "Essential Services" (“OESs”) and Digital Service Providers (“DSPs”). Essential Services include energy, transport, banking, financial market and digital infrastructures, while DSPs include providers of online marketplaces, cloud computing services and search engines. The NIS Directive will provide greater security for EU citizens on the reliability of digital networks. In addition, co-operation and incident-reporting between Member States will

[12] Directive 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.

increase with the establishment of the ENISA and Computer Security Incident Response Teams ("CSIRT") Networks.

The NIS Directive has been transposed by the the European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018[13].

The European Commission has adopted a proposal for a Revised NIS Directive[14].

In two parts, the **EU Cybersecurity Act** (EU Regulation 2019/881) expands the mandate of the European Union Agency for Cybersecurity (which is a new name for ENISA), it lays down ENISA's objectives and tasks; and establishes a framework for the certification of ICT products, processes and services, via European Cybersecurity Certificates. The Cybersecurity Act came into force on 27th June 2019.

The certification framework will be a one-stop shop for cybersecurity certification. It is specified that member states have 24 months following publication to abide by the provisions on National Cybersecurity Certification Authorities and Conformity Assessment Bodies. The European Commission has 12 months following publication to establish a work programme for cybersecurity certification schemes.

On 26th March 2019 the European Commission published **Recommendation 2335 on assessment of cybersecurity risk to 5G networks[15]**. The recitals are useful in recapping EU cybersecurity legislation so far.

The Recommendation identifies the actions which should be taken for (a) Member States to assess the cybersecurity risks affecting 5G networks at national level and take necessary security measures; (b) Member States and relevant Union institutions, agencies and other bodies to develop jointly a coordinated Union risk assessment that builds on the national risk assessment; (c) The Cooperation Group set up under Directive (EU) 2016/1148 (Cooperation Group) to identify a possible common set of measures to be taken to mitigate cybersecurity risks related to infrastructures underpinning the digital ecosystem, in particular 5G networks.

By 30 June 2019, Member States have to carry out a risk assessment of the 5G network infrastructure, including identifying the most sensitive elements where security breaches would have a significant negative impact.

On the basis of this national risk assessment and review and taking into account ongoing coordinated action at Union level, Member States should: (a) update the security requirements and the risk management methods applied in regard to 5G networks; (b) update the relevant obligations imposed on undertakings providing public communications networks or publicly available electronic communications services pursuant to Articles 13a and 13b of Directive 2002/21/EC; (c) attach conditions to the general authorisation concerning the security of public networks against unauthorised access and ask for commitments from the undertakings

[13] http://www.irishstatutebook.ie/eli/2018/si/360/made/en
[14] https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union
[15] See here- https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks

participating in any upcoming procedures for granting rights of use for radio frequencies in 5G bands as regards compliance with security requirements for networks pursuant to Directive 2002/20/EC; (d) apply other preventive measures aimed at mitigating potential cybersecurity risks.

The work of the Cooperation Group should identify best practices measures applied at national level - on the basis of these national best practices, a toolbox of appropriate, effective and proportionate possible risk management measures to mitigate the identified cybersecurity risks at national and Union level should be agreed by 31 December 2019, for advising the Commission on developing minimum common requirements to further ensure a high level of cybersecurity of 5G networks across the Union. The toolbox should include: (a) an inventory of the types of security risks that can affect the cybersecurity of 5G networks (e.g. supply chain risk, software vulnerability risk, access control risk, risks arising from the legal and policy framework to which suppliers of information and communications technologies equipment may be subject in third countries); and (b) a set of possible mitigating measures (e.g. third-party certification for hardware, software or services, formal hardware and software tests or conformity checks, processes to ensure access controls exist and are enforced, identifying products, services or suppliers that are considered potentially not secure, etc.). These measures should address every type of security risk identified in one or more Member States following the risk assessment.

Once European cybersecurity certification schemes relevant for 5G networks are developed, Member States should adopt, in compliance with Union law, national technical regulations providing for mandatory certification of information and communications technologies products, services or systems covered by these schemes.

Member States, together with the Commission, should identify the conditions concerning the security of public networks against unauthorised access to be attached to the general authorisation and security requirements for networks for the purposes of asking commitments from the undertakings participating in procedures for granting rights of use of spectrum in 5G bands pursuant to Directive 2002/20/EC.

Member States should cooperate with the Commission to develop specific security requirements that could apply in the context of public procurement related to 5G networks. This should include mandatory requirements to implement cybersecurity certification schemes in public procurement insofar as such schemes are not yet binding for all suppliers and operators.

Member States should cooperate with the Commission to assess the effects of this Recommendation by 1 October 2020, with a view to determine appropriate ways forward. This assessment should take into account the outcome of the coordinated Union risk assessment and the Union toolbox.

On 16th December 2020 the European Commission proposed a **Directive on the Resilience of Critical Entities**[16]. With this proposal, the Commission intends to

[16] https://ec.europa.eu/home-affairs/news/commission-proposes-new-directive-enhance-resilience-critical-entities-providing-essential_en

create an all-hazards framework to support Member States in ensuring that critical entities are able to prevent, resist, absorb and recover from disruptive incidents, no matter if they are caused by natural hazards, accidents, terrorism, insider threats, or public health emergencies like the one the world faces today. The proposal, which covers ten sectors, namely energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, public administration and space[17].

4 Test & Trial Ireland

Test & Trial Ireland is a wireless licensing service provided by ComReg to encourage innovation and development of wireless communications using Ireland's radio spectrum. On the edge of Europe, Ireland offers an environment with low radio interference potential and access to a large range of radio frequencies for research and development through Test & Trial Ireland.

Operating within the EU, Ireland has a high availability of clean radio spectrum given its low military use and location in Europe with only one land border. In principle, any spectrum band that is not in use can be made available for testing and trialling of technologies, systems and services that require access to the radio spectrum.

Test & Trial Ireland helps wireless research and development in Ireland by enabling users to:

- confirm viability prior to commercial rollout;
- utilise pioneering new technology;
- benefit from a low-cost testing environment to enable innovation;
- test wireless blueprints for export to global markets;
- showcase inventive research; and
- trial wireless products for European and/or global markets.

Test & Trial Ireland may be of relevance to the national CAM strategy when it comes time to evaluate or compare different technologies and/or systems.

Test & Trial Ireland has been used by many businesses and for a variety of use cases. Further information and contact details can be found at www.testandtrial.ie .

5 Future engagement

If there are specific needs in relation to CAM, Ireland may need to bring these to International and European fora to ensure that they are taken into account. In respect of spectrum and numbering the Department of the Environment, Climate and Communications (DECC) and ComReg are the Irish representatives at these fora.

[17] The European Commission adopted the European Critical Infrastructure (ECI) Directive in 2008, which applies to the energy and transport sectors.

ComReg will also contribute to international working groups (primarily those of BEREC and CEPT) that seek to address any remaining issues that impede the provision of pan-European and global connectivity solutions for the automotive and other sectors.

ComReg is mindful that many aspects of modern society require the use of the radio spectrum resource. ComReg takes effort to maintain a watchful eye on a number of developing markets to determine when it is appropriate to release new spectrum bands, exempt bands from licensing or to take other actions to facilitate the use of ECS/ECN by these markets. For example, following the publication of Project Ireland 2040[18] it was determined that smart grids would be required to ensure smart operation of the power system , ensure energy efficiency, and enable maximisation of the exiting power grid. To provide connectivity for smart grids ComReg prepared, consulted on, and then held a competitive award for the 400 MHz band[19] for use by smart grids. The same spectrum is ideal to manage electric vehicle charging points which might form part of any smart grid.

To manage its work ComReg consults on and publishes Strategy Statements covering three separate areas of its remit. There is a Strategy Statement on the Electronic Communications Sector, a Strategy Statement on Radio Spectrum and a Strategy on Postal Regulation. Each of these helps determine what areas ComReg will focus its attention on and the engagement of stakeholders is very important to help shape our strategies and determine what future work we will be undertaking.

We look forward to engaging with DoT on CAM so that any specific requirements from this new market can be taken into account in our work.

Please do not hesitate to contact me if I can be of further assistance.

Yours sincerely

George Merrigan

Director

Market Framework Division

Commission for Communications Regulation

[18] Project Ireland 2040 - National Planning Framework http://npf.ie/wp-content/uploads/Project-Ireland-2040-NPF.pdf

[19] See https://www.comreg.ie/publication/results-of-the-400-mhz-band-spectrum-award