Deliverable D5.5
Third report on communication, marketing and standardisation

Project name	5G Enablers for Network and System Security and Resilience	
Short name	5G-ENSURE	
Grant agreement	671562	
Call	H2020-ICT-2014-2	
Delivery date	30-05-2017	
Dissemination Level:	Public	
Lead beneficiary	Trust-IT	Stephanie Parker, s.parker@trust-itservices.com
Authors	Trust-IT: Stephanie Parker, Silvana Muscella, Benedetta Romani, Caterina Piagentini Telecom Italia: Luciana Costa and Paolo de Lutiis	

European Commission

5G PPP

Executive summary

5G is considered to be one of the most transformative technologies, playing a crucial part in the digital single market and its objectives to revitalise the European economy. A multi-stakeholder dialogue on the European and global levels bringing consensus on early standardisation on 5G security represents a very important milestone as 5G developments get under way.

The mission of 5G-ENSURE to become the reference project on 5G security, places emphasis on timely contributions to standardisation under WP5, which also commits to raising considerable awareness around the projects outputs to a diverse set of stakeholders. Joint activities and knowledge exchange across the 5G PPP also form an important goal of the project.

This third report covers the results achieved for communication, marketing and standardisation as core activities within WP5 in the period **November 2016** to **April 2017** and provides a plan for the final six months of 5G-ENSURE (May to October 2017). It provides an updated, in-depth assessment on the current 5G security standardisation landscape, highlighting opportunities for 5G-ENSURE engagement. It then goes on to present measurable impacts in terms of standardisation; dissemination of results, collaborations with the 5G PPP and overall visibility; community building indicating key growth areas and concrete examples. The report includes overall progress on core KPIs and a consideration of qualitative metrics reflecting overall impact in an evolving landscape.

The plan covering the period from **May** to **October 2017** provides current activities foreseen for disseminating 5G-ENSURE final outputs, joint 5G PPP activities, stakeholder engagement at future events, 5G-ENSURE webinars, promotional activities and newsletters. Important activities in this regard include the open consultation (trust in 5G networks and 5G security) and the 2nd International Workshop in June 2017 during ETSI Security Week.

An updated version of the deliverable will be provided in late October to ensure stakeholders are aware of the full impacts achieved in relation to the project's final findings and outputs. This is particularly important as engagement with strategic synergies, such as NIST, ITU-T, 5G Infrastructure Association, are extended and/or newly created in alignment with the EC's priorities on ICT standardisation. 5G-ENSURE is ensuring dedicated effort is allocated to ensure the most fruitful exchanges for the benefit of 5G PPP also as it moves towards Phase 2. The updated version of the deliverable will be added to this version in Annex 2.

Foreword

5G-ENSURE belongs to the first group of EU-funded projects which collaboratively develop 5G under the umbrella of the 5G Infrastructure Public Private Partnership (5G PPP) in the Horizon 2020 Programme. The overall goal of 5G-ENSURE is to deliver strategic impact across technology and business enablement and standardisation by realising a vision for a secure, resilient and viable 5G network. The project covers research & innovation - from technical solutions (5G security architecture and test bed with 5G security enablers) to market validation and stakeholders engagement - spanning various application domains.

D5.3 is the Second Report on Communication, Marketing and Standardisation covering the period May to October 2016 with plans for the period November 2016 to April 2016 provided with partner "sign-off". The results build on D5.2 – First Report on communication, marketing and standardisation, which documentedthe impact of related activities for the period November 2015 to April 2016 and set out plans for the period (May to October 2016, as per the Description of Action.

Disclaimer

Copyright notice

Contents

Tables

Figures

Abbreviations

3GPP	3rd Generation Partnership Project
5G PPP	5G Infrastructure Public Private Partnership
ETSI	European Telecommunications Standards Institute
ICT	Information and Communication Technologies
IETF	Internet Engineering Task Force
ITU	International Telecommunication Union
KPI	Key Performance Indicator in relation to 5G-ENSURE
MFCN	Mobile and Fixed Communications Networks
mMTC	Massive Machine Type Communication
ONF	Open Networking Foundation
NFV	Network Virtualisation Function
NIST	National Institute of Standards and Technology
SDN	Software Defined Network
SMARTER	New Services and Markets Technology Enablers

1. Introduction

The transformation of the global economy into a digital economy affects all industries and service sectors. Europe's competitiveness and productivity crucially depend on its ability to generate, scale-up and effectively harness digital innovations across all sectors of the economy, including Europe's traditional strengths such as vehicle manufacturing, automation, machine equipment and financial services. The European Digital Single Market strategy is designed to make Europe's role in the in the global digital economy a key priority.

5G is considered to be one of the five building block technologies for Europe's DSM. 5G communication networks enable seamless global communication between different kinds of 'nodes', connecting data, vehicles and other objects, smart sensors or voice. 5G is expected to become the essential global infrastructure for communication.

Given its global nature, and the connections it makes between ICT and non-ICT sectors, 5G critically depends on standards to ensure interoperability and security, privacy and data protection. Standardisation is also key for SMEs to scale up and reach larger markets in the global marketplace. The European Commission 5G Action Plan defines the steps for EU wide deployment of 5G networks beyond 2020, which will leverage take up of 5G standards.

Standardisation is a key requirement for new technologies like Massive Machine Type Communication (mMTC), infrastructure virtualisation (SDN, NFV), and network resource sharing, also in the face of growing cyber threats and the increasing need to defend national and European critical infrastructure through cyber security. These technologies introduce or allow for more stakeholders with more complex trust relationships, and lead to new security and resilience requirements along with new opportunities to implement extensive and accurate security solutions.

The overall goal of 5G-ENSURE is to deliver strategic technology and business impacts and drive standardisation by realising a vision for a secure, resilient and viable 5G network under the umbrella of the 5G Infrastructure Public Private Partnership (5G PPP) in the Horizon 2020 Programme. The project covers research and innovation on a 5G reference security architecture, a set of 5G security and privacy enablers and a test-bed, as well as market validation and stakeholder engagement at EU and global levels. In addition, 5G-ENSURE works collaboratively with the other projects funded in phase one of the 5G PPP, primarily through its contributions to various work groups such as security, pre-standardisation and architecture to share knowledge and to the COMMS group to help maximise visibility and engagement.

Work package 5, **Dissemination, Standardisation and Exploitation,** brings these elements into one place with the objective of promoting the 5G-ENSURE project, its results and its collaborations as widely and effectively as possible to all relevant stakeholders. To achieve this objective, WP5 focuses on:

- Monitoring standardisation activities directly related to the 5G-ENSURE research topics, ensuring the overall viability and coherence of the project results.
- Participating in and contributing to standardisation bodies, such as the 3GPP and ETSI, with two international standardisation workshops planned.

- Ensuring international visibility of the project, particularly by engaging in a multi-stakeholder dialogue on security, privacy and standardisation, recently highlighted at CeBIT20161. Disseminating the outcomes of the project's work to the 5G PPP projects and all the relevant stakeholders identified through a collaborative process, and by building an overall strategy for the exploitation of results. This strategy will take 5G-ENSURE results to all interested parties from relevant scientific areas, business and market verticals, cultural, legal/regulatory authorities.
- Performing a market assessment for each security enabler oriented to better understand the key players, market barriers and opportunities.

1.1 Scope and Purpose

Work package 5 supports all the other WPs in spreading information about the project with the goal of increasing its visibility and impacts. Actions include updating the 5G PPP projects about deliverables available on the website and 5G-ENSURE activities of interest to them.

The work package is articulated into four tasks:

T5.1 – Standardisation, where the strategic goal is to influence the most relevant standardisation bodies early on and map research topics to related standardisation efforts.
T5.2 – Marketing and Communication, where the strategic goal is the creation and timely delivery of the most effective messages to all major stakeholders, including practical guidance and tools on security and privacy in 5G.
T5.3 – Stakeholder Involvement and 5G Security Community Development, where the strategic goal is to define and implement an engagement plan with priority on building a 5G-security-aware community and a strengthened 5G PPP.
T5.4 – Market Analysis and Exploitation, where the strategic goal is to support a ready to use test-bed service for the 5G security community and facilitate industrial partners in new product rollout.

WP5 interacts with the other WPs within the project as follows:

- WP2 – informing on the most appropriate timing for a submission to the standard, sharing and agreeing on the potential contributions once the project achieves preliminary results.
- WP3 – providing input related to market demand in terms of the 5G security enablers, potential barriers and opportunities to drive and prioritise WP3 activities.
- WP4 – in terms of the vision for the 5G security test bed and operational plan, analysing potential sustainability models.

The purpose of D5.5 is to report on the actions performed during the period from November 2016 to April 2017. As such it sets out to detail its on-going analysis of the 5G security standardisation landscape, while also measuring impact in terms of concrete contributions and collaborations, dissemination of results and overall visibility, as well as community building to ensure 5G-ENSURE is widely broadcast to all major stakeholders.
Progress to date is used as the basis for planning actions for the final six months of the project (May to October 2017) as the project delivers its final outputs and ensure they are communicated and disseminated

[1] http://5gensure.eu/news/industry-panel-cebit-2016-calls-collaboration-5g-security-and-privacy.

with the highest possible impact. An updated version of this deliverable will be made available at the end of October to demonstrate how this has been achieved. It will be added in Annex 2.

1.2 Main Achievements

The figure below, http://5gensure.eu/project-vision, provides a visual representation of the main achievements of 5G-ENSURE at the present time. The image covers the main technical achievements, that is, the security and privacy enablers, the test-bed and reference security architecture. Main outcomes to date of the extensive collaboration with the other projects within the 5G PPP, as well as key impacts for standardisation, press coverage and community growth.

Figure 1: 5G-ENSURE Achievements so far

1.3 Structure of this report

Section 2 - Communication Strategy, summarising goals for communications and marketing, standardisation, stakeholder engagement and measurable impacts (KPIs and qualitative metrics).

Section 3 - Updated analysis of the current standardisation landscape, identifying relevant standardisation activities and opportunities for 5G-ENSURE.

Section 4 – Measurable impacts for project contributions to 5G Security Standardisation.

Section 5 –Measurable impacts for the dissemination of 5G-ENSURE results achieved so far, collaborative work with other projects within the 5G PPP and overall visibility of the project.

Section 6 – Measurable impacts for community building, with a detailed analysis of LinkedIn connections and Twitter, indicating key growth areas.

Section 7 – Plans and targets for the next six months of the project.

2. Communication Strategy

In the context of 5G-ENSURE, we define communication as a regular flow of activities planned to promote and raise public awareness on the security aspects of future 5G network, and to increase to the widest possible audience, beyond the project's stakeholder community, an understanding of how technology innovations may contribute to advancement in security. These activities span creating web content, populating social media channels, producing press articles, promoting the 5G PPP activities (e.g. events and work groups), and building a community around 5G-ENSURE.
Dissemination mostly refers to technical work leading to project results and outputs and the exploitation thereof, promoting them to specific target groups (the stakeholder community) both during and after the project according to the innovation management processes defined in the Grant Agreement. Related activities include technical papers (including open access publications), presentations, including standardisation efforts, F2F business meetings and the analysis of market conditions.

Standardisation plays a central role in 5G-ENSURE for spreading the technical results of the project in target SDOs and having an impact on the ongoing standardisation effort in the field of 5G security and privacy characteristics of next-generation networks, promoting industry-wide consensus in general and more specifically through two international workshops.

5G-ENSURE communication activities strategy follow the SMART approach (specific, measurable, achievable, realistic, targeted and timed):

1. The use of several communications channels such as events, online instruments (project site, newsletters), media (press releases, advertisements), publications (leaflets, poster) and other promotional material. The project team is also active on social media like Twitter and Linkedin.
2. The use of targeted messages for each audience with the goal of increased public awareness of the project, and to keep the community informed about the latest project achievements and to facilitate understanding to groups outside the project.
3. Communicating activities at the right time following the project's information availability and time plan.
4. The monitoring of communication effectiveness by measuring the impact achieved.

The purpose of the key performance indicators (KPIs) is twofold:

- Ensure a continuous stream of activities around the project and
- Evaluate the impact of effort spent on a particular activity. The KPIs also serve as a driver for staying up-to-speed on developments in the 5G landscape.

2.1 Goals for Communications and Marketing

The 5G-ENSURE communication strategy is aimed at maximising the visibility and awareness of the project, and support the dissemination and exploitation of its results and outputs. The communication strategy defines the graphic identity and branding of 5G-ENSURE, as well as the communication toolbox as the means for engaging the different stakeholders targeted, including joint activities with the 5G PPP.

Specific goals of year two are:

- Increment promotional activities and ensure the dissemination of results achieved by the project, such as the security reference architecture, the security and privacy enablers and the test-bed receive high visibility in relevant forums.
- Engage with the telecom and IT media, social media influencers, and project corporations to help boost visibility and therefore impact.
- Extend the 5G-ENSURE community, ensuring high relevance and regular engagement, including timely communications on project outputs and presence at EU and international events.
- Play a key role in fostering and facilitating greater stakeholder engagement within the 5G PPP and beyond, sharing advice and providing concrete examples of achievable impact at the programme level.

2.2 Goals for Standardisation

Goal of the standardisation work in 5G-ENSURE, during the first year, has been mainly to take part at the security discussions and activities which have been carried in the main SDOs, with the objective to take part of the 5G security pre-standardisation work, from the start. With this objective in mind, the effort has been spent in transferring the knowledge gained on security. This has permitted to bring several of the security and privacy requirements which have been identified by the analysis of representative, even if not exhaustive, use cases for security and privacy. In the second year of the project the goal of standardisation work is mainly devoted to bring some of the innovative solutions, defined within the project as enablers for security and privacy, within the targetted working groups, and to take also part at the evaluation of the different proposals under discussion, in terms of adherence to the security and privacy requirements/principles.

In the second year, the ambition is extended beyond 5G-ENSURE, to reach a level of agreement also with others 5G PPP Phase 1 projects. In this context, the plan is to take advantage of the co-operation work on 5G security conducted by phase 1 projects involved within the Security Work Group and to carry on in the engagement with the Pre-standardization WG. Here the main effort is devoted in sharing the contributions prepared for the attending meetings, e.g. 3GPP SA3, and the initiatives of common interest for 5G standardisation. Activities also include engagement with the Advisory Board members, where knowledge exchange also feeds into international conferences, the end 5G-ENSURE International Workshop and liaison at global level.

Specific goals of the standardisation plan for this second year are to:

- Contribute to standardisation to identify gaps in the security and privacy requirements already provided as part of the pre-standardisation work.
- Provide contributions to the security and privacy issues selected as priority for phase 1 standardisation, by identifying security enablers pecified from the project which can be proposed as solution for addressing these issues. This draws on the work in WP3 where a first set of 5G Security enablers has already released as achievement of the first year and getting complemented, in this second year, with additional features as well as new solutions (D3.6). Interface with the 5G PPP for the submission of joint standards contributions.
- Engage in international exchanges on standardisation, in particular extending the interaction with NIST in the US and the ITU-T, sharing insights on 5G security and privacy priorities.

- Promote outcomes within the 5G community, the IT and telecommunications media, particularly the roadmaps from the two international workshops.

2.4 Primary and Secondary Stakeholder Targets

Stakeholder mapping is a common activity across the 5G PPP to allow easy comparisons between peer projects spanning radio and core network technologies. A distinction is drawn between primary stakeholders, corresponding to the largest part of the project's community, and secondary, which are mostly channels that are used to reach primary stakeholders, that is, telecom, IT and business media channels.

2.4.1 Primary stakeholders for 5G-ENSURE

Primary stakeholders for 5G-ENSURE are:

- **5G industry** within and beyond the 5G PPP, spanning connectivity providers, large and small companies (SMEs), manufacturers, and supply chain companies. Industry groups and business associations can play a key role in reaching these companies.
- **Standardisation organisations (e.g. SSOs, SDOs)** and related international industry associations that can spped up time to reach consensus, as well as regulators and policy makers for sharing timely 5G-ENSURE analyses of relevant 5G security standardisation.
- **Phase 1 projects in the 5G PPP**, covering radio and network technologies, the Euro5G CSA and the work groups within the 5G PPP.

2.4.2 Secondary stakeholders for 5G-ENSURE

5G-ENSURE targets secondary stakeholders for:

- Increasing understanding of 5G across all major beneficiaries, from citizens to public and private sector organisations. This may include policy priorities and actions taken by the EC and EU member states.
- Raising awareness of the importance of security and privacy among the general public in building trust and fostering best practices.
- Maximise the visibility of 5G-ENSURE.

Sample targets include:

- **Telecom media channels** important for reaching 5G industry stakeholders, e.g. TelecomTV, Inside5G, Mobile World, Telecoms.com, Total Telecom, Telecom News, Fierce Wireless Europe,
- **IT and business media channels**, e.g. Computer Weekly, TechTarget, TechTalk, Inside Tech Europe, CloudPro, The Register, ITProPortal, SourceSecurity.com, IT Security Portal, Tech radar. For SMEs: Business Insider, Business Matters, Talk Business Magazine, European CEO, Small Business Magazine.

2.5 Measurable Impacts

5G-ENSURE plans its activities on communication, marketing and standardisation using a monthly **check list** shared with partners on the project wiki. Four major colour-coded categories are used to indicate the main

focus of the activities: communications and community; standardisation (liaison and engagement with security experts); joint 5G PPP activities and dissemination of outputs and reports. Details of each activity are given in this report, indicating any interconnections across the four categories.

2.5.1 Key Performance Indicators

WP5 uses both quantitative and qualitative metrics to gauge the relevance and impact of its activities in WP5. We use two straightforward processes for defining and measuring an initial core set of key performance indicators (KPIs) for four complementary activities: communications and community building, including stakeholder engagement; standardisation related activities; joint 5G PPP activities and the dissemination of outputs.

- A flash report is used to define and measure the KPIs, comparing the delta with the end-of-project KPI targets over the entire project lifecycle measured on a quarterly basis.
- A check list with all planned and completed actions updated on a monthly basis.

Both documents are shared with the consortium.

The table below shows current progress on the initial core set of KPIs for WP5 up to April 2017.

Table 1: KPIs for WP5 Core Activities

Communication & community	Standardisation	Joint 5G-PPP activities			Dissemination of outputs	
5G-ENSURE - Community KPIs						
KPI	Target EoP	Delta	Total to date	November 2015 - April 2016	May-October 2016	November 2016 - April 2017
Twitter followers	500	+4	504	164	154	182
LinkedIn Connections	650	+160	810	2	462	338
Community DB for LinkedIn	900	13	887	210	355	322
PR/media content	4	0	4	2	1	1
Media coverage & visibility	15	+19	34	9	4	21
LinkedIn Updates	36	+4	40	0	12	28
Events - standardisation/5G security (excl. project workshops)	6	0	6	2	2	2
Events - 5G-PPP Joint activities (incl. Project workshops)	8	1	7	2	2	3
Publications to disseminate technical results	12	2	10	2	4	4
Technical conferences	8	+2	10	1	4	5
Publications: joint 5G-PPP	2	+4	6	1	2	3
2nd Open Consultation on 5G security (starting May 2017)	60					

Our commitment to an “ambitious set of KPIs” has been the right direction to take for 5G security, privacy and trust, where it is essential to ensure proper understanding of top-priority challenges as the basis for consensus building.

5G-ENSURE has achieved its community and stakeholder engagement targets, surpassing many of the targets set, such as for LinkedIn. The target set for project visibility through press activities has also been surpassed in terms of press clippings generated. Community building has achieved increased reach in term of geographies, with more countries covered internationally, also also in terms of business outreach, with a higher number of SMEs and representatives from the telecom industry, as well as a growing number of key representatives in standards organisations.

Future steps: This means that 5G-ENSURE can now focus on quality engagement and drive consensus on its standardisation activities and ensure outputs are widely broadcast. To this end, we will increase our focus on content for the website, Twitter and LinkedIn, ensuring a more SEO-driven approach to web content and in drawing attention to major outputs, with videos and demos highlighted on a new home page design.

2.5.2 Qualitative Metrics

WP5 has also implemented a set of qualitative aspects to measure the relevance of media activities, technical publications, workshop organisation and external events, and the standardisation roadmap.

QM1*: Readership of media channels where 5G-ENSURE is visible, analysing professions, geographies.* 5G-ENSURE partners have been encouraged to establish good relations with the media, especially telecom and cyber security journalists, whether from business or research. This approach has proved to be fruitful with 21 press clippings generated in the period covered by D5.5. thanks to discussions with journalists at Black Hat Europe and the Mobile World Congress. 5G-ENSURE has also extended its connections with the media on LinkedIn and especially Twitter with direct engagements on project-related outputs.

QM2*: Readership of journals where technical articles are published, such as reputation, readership and geographies.* New research has been visible at top conferences and have been highly visible at peer conferences in EU and globally. Achievements include best paper selected for MOST 2017, driving IEEE workshop series on security in NFV and SDN.

QM3*: Workshops – Matching actual participants with the stakeholder targets.* The 2nd Workshop, From Research to Standardisation, takes place within ETSI Security Week, ensuring relevant stakeholders are guaranteed and also increasing visibility and recognition. The initial target of 43 participants has already been reached at the time of writing this report with plans underway to increase promotional activities.

QM4*: Workshops – gauging consensus of participants and the level of interest, e.g. passive and active supporters; passive and active opponents; fence-sitters.* Collaboration with NIST and ITU-T are good benchmarks for evaluating the value of R&I and standardisation within 5G-ENSURE. The current project community is another demonstration of its relevance with over 500 representatives from industry, including SMEs, and good representation of sensior specialist in target standardisation organisations.

QM5*: External events, assessing the audiences actually reached at commercial and technical events, influential participants, new contacts and main takeaways.* 5G-ENSURE has played an active role within the 5G PPP and several of its work groups. Promotional activities have ensure good visibility already for EuCNC and top engagements on the Technology Board workshop last February. The community has several large and influential members (as reported below) and has received support on social media from several partners, notably Ericsson and Nokia.

QM6*: Standardisation roadmap (2 iterations) – quality of contributions, types of endorsements, as well as circulation and visibility.* The 5G-ENSURE standardisation plan was very well received by the community, helping to bring in a good number of senior specialists and positive comments generally.

3. Current Standardisation Landscape

Main Takeaways

- As expected, 3GPP started the specification for phase 1 in March 2017 (finalisation foreseen by the mid of 2018). First security specification TS 33.501 could be ready by the end of 2017.
- 3GPP and ETSI TC Cyber confirmed as main targets for the project: 15 direct contributions presented since the beginning 2016, most of them agreed. Additional contributions planned to be presented during the last 6 month of the project
- Analysis of the 5G standardisation landscape submitted to ITU-T SG 17. ITU-T confirmed

it has not yet started specific activities on 5G security.
- Analysis also submitted to the EC to ensure timely updates are made available with respect to the EC's ICT standardisation priorities.
- NIST confirmed its interest in 5G-ENSURE project enablers and research results, in particular: Fine-grained Authorisation Enabler, Privacy, Federative Auth+ID, IoT/Group-based authentication
- ETSI recognises 5G-ENSURE as one of main 5G Security actors and includes the 2nd International 5G-ENSURE workshop in the official ETSI Security Week 2017 agenda.
- New synergy established with 5G Infrastructure Association (Secretariat General)

3.1 Industry and Policy Contexts

The EC communication on ICT Standardisation Priorities for the Digital Single Market published in April 2016, is of particular importance to 5G-ENSURE with its focus on early 5G standardisation activities. The Communication is a priority policy action aimed at supporting Europe's role in the global digital economy

5G communication networks is one of the DSM technology building blocks along with cloud computing, the Internet of Things (IoT), (big) data technologies, and cyber security. 5G is expected to become the essential global infrastructure for communication. Given its global nature, and the connections it creates between ICT and non-ICT sectors, 5G critically depends on standards to ensure interoperability, security, privacy and data protection. The EC's 5G Action Plan for EU wide deployment of 5G networks beyond 2020 will leverage the uptake of 5G standards.

From an economic perspective, standards and the way they are implemented will make one of the most meaningful contributions to the 5G PPP programme, helping pull different technologies under one umbrella as 5G becomes even more reliant on standards, due to the expected broad impact on the networked society.

Infrastructure networks are increasingly strategic infrastructures in modern society, and that will be even more evident in the near future with new 5G networks. Moreover, due to the critical nature of the information transported by networks, Telcos face some of the most severe threats. Security standardisation has an important role to play in the future development of 5G. In the domain of Information and Communication Technologies (ICT), standards are particularly important because they are focused on interconnection and interoperability. Standards allow the existence of open markets for both: the final customers, who want to use different services from different providers, and the providers themselves, in order to use different products from different suppliers to reduce costs and achieve time to market. Moreover also Privacy aspects deserve special and dedicated attention, as stressed by the EU with specific the Privacy Mandates (e.g. M/530) and the recent General Data Protection Regulation (GDPR).

Lack of timely technical solutions may endanger the growth of 5G-enabled products and services and may put at risk privacy and liberty of citizens. Network and systems security are fundamental elements of the economic growth that 5G will bring through improved services, higher data rates, new interfaces, and new business models. Yet progress on standardisation of 4G/LTE has been hindered because of the difficulty in creating consensus on fundamental architectural issues related to security, e.g. the placement of the user data encryption.

In order to minimise exposure to risks, the objective of 5G-ENSURE project's standardisation activities is to drive the specification of new networks in such a way that security is built in from the design phases and

not appended later as an add-on feature. The strategy is to provide relevant SDOs with a set of security and privacy requirements derived from the threat analysis of 5G use cases so that they are received in time and may be used to build the new 5G security architecture. Taking into account a set of security, privacy and liability issues and addressing them directly in the standardisation and regulation processes will ensure a 5G network which is "Secure by Design".

At the 5G PPP programme level, 5G-ENSURE will make a concerted effort to build consensus and transfer knowledge across the 5G PPP, including pre-standardisation consensus, its leadership of the Security WG established in March 2016 and other relevant WGs.

3.2 Snapshot of relevant Standards Organisations and Industry Associations

As 5G will impact a vast number of new technologies, many standards bodies will be involved in standardisation efforts. From a 5G-ENSURE perspective, the most relevant standards bodies are:

3GPP- 3rd Generation partnership project [24]**:** the main organisation for creating standards in mobile communications. Its current 5G standardisation time plan currently spans 2016-2019 and is aimed at gradually realising the full 5G capabilities in three consecutive releases. 3GPP has been confirmed as the main relevant standardisation group for the specification of the 5G and in particular for its security aspects, as emerged by the 1st 5G-ENSURE International Workshop, the 1st Open Consultation and the experienced gained during the first year of activities of the project. 5G-ENSURE has contribuited since the beginning of the official activities on 5G Security of the Group, by supporting the creation and the elaboration of the Study Item TR33.899, and recently supporting the new Technical Specification on 5G Security that will lead the first normative phase of the group.

ETSI – European Telecommunications Standards Institute [25]**:** produces globally applicable standards for Information & Communications Technologies including fixed, mobile, radio, broadcast, internet, aeronautical and other areas. The ETSI Industry Specification Group for Network Functions Virtualization (ETSI ISG NFV) will play the main role to standardise the infrastructure aspects of 5G networks, that will be more and more virtualised and softwarised. Moreover, ETSI TC CYBER, the Technical Commeetee dedicated to the cybersecurity, will coordinate all the security aspects carried-on within each TC operating under the ETSI umbrella. In particular the TC CYBER is working on Privacy and LI aspects and other strategic topics related to the security of the ICT. Also TC CYBER has been identified as one of the most relevant group by the 5G-ENSURE project, in particular because of its horizzontal view (not related to a specific technology) on cyber security.

ITU-T - The ITU Telecommunication Standardisation Sector [26]: coordinates standards for telecommunications (as one of the three sectors of the International Telecommunication Union. Its Focus Group on network aspects of ITM-2020 (International Mobile Telecommunication system) was established in May 2015 to analyse how emerging 5G technologies will interact in future networks as a preliminary study into the networking innovations required to support the development of 5G systems. In December 2015, the Focus Group (FG) received an extension to its lifetime and with a new ToR in order to engage also open-source communities. The group follows an intensive work plan to complete its study prior to the first Study Group 13 meeting in study period 2017-2020. The FG, althouth considering Security of primary importance, has not addressed security topics directly neither during its lifetime extension.

The ITU's Radio Communication Sector (ITU-R) has completed "Vision" for "5G" mobile broadband connected society in September 2015. The horizon for the future of mobile technology is considered instrumental in setting the agenda for the the World RadioCommunication Conference 2019.

GSM Association [27] and **NGMN Alliance** [28]: GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 250 companies in the broader mobile ecosystem. The NGMN Alliance mission is to expand the communications experience by providing a truly integrated and cohesively managed delivery platform that brings affordable mobile broadband services to the end user with a particular focus on 5G while accelerating the development of LTE-Advanced and its ecosystem. Although not official SDOs, GSMA and NGMN will also play an important role as drivers for the 5G specifications across the industry.

3.2.1 Opportunities for 5G-ENSURE

5G-ENSURE draws on the representation of consortium partners and its Advisory Board in relevant standards bodies. The main focus of the current phase of the project is on monitoring on-going activities and on identifying the specific groups where security is addressed. In Table 2 are reported the actions which have been started within 3GPP where the project search results can be proposed for possible standardisation actions. Also ETSI TC CYBER has been targeted with specific contributions related to the privacy protection in the mobile context.

Table 2: Short term 5G-ENSURE opportunity

SDO Group		Partners Involved	5G-ENSURE opportunity
Short Term			
3GPP	RAN	TIIT	Investigation of the access security requirements in RAN.
	SA3	EAB TIIT NOKIA	Study on Security Aspects of the Next Generation System (TR 33.899)
ETSI	TC CYBER	TIIT	TR 103 304, *Personally Identifiable Information (PII) Protection in mobile and cloud services* TS 103 458, Application of Attribute-Based Encryption (ABE) for data protection on smart devices, cloud and mobile services DTS/CYBER-0025 (Provisional Identifier) “Attribute Based Encryption for Attribute Based Access Control” STF-529 (Specialist Task Force) Attribute Based Encryption - Common protocol for data access control for Cloud, Mobile and IoT

We are still evaluating the opportunity to contribute also in other SDOs based on the representation of consortium partners, although at the present time such possibility has not yet identified

The following sections provide an update of the current plan standardisation landscape for 5G with particular reference to the main target organisations for 5G-ENSURE standardisation efforts wihin the 5G PPP and beyond.

3.3 3GPP

The 3rd Generation Partnership Project (3GPP) is a unit of seven telecommunications standards development organisations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA and TTC).

3GPP has three Technical Specification Groups (TSGs):

1. Radio Access Networks (RAN) [29] - a technology that connects individual devices to other parts of a network through radio connections.
2. Service & Systems Aspects (SA) [30] – architecture and capabilities of systems.
3. Core Network & Terminals (CT) [31].

The former GERAN TSG has been closed and incorporated as a WG under the RAN umbrella. The previous activities ongoing withing GERAN have been recently moved to the new RAN6 group (Legacy RAN radio and protocol). Moreover it is woth mentioning that the CT WG2 (focus on Terminals Capability) have been closed, whereas the CT WG5 (focus on OPen Service Access, OSA) has been and transferred in 2008 to Open Mobile Alliance (OMA).Given the scope of the 5G-ENSURE project, the most relevant TGS is the SA, with particular attention to the SA3 (Security) whereas RAN and CT can be considered less relevant. Hence the present document will focus on SA1 (Architecture), SA2 (Architecture) and SA3 (Security) and with less emphasys also on RAN TGS. CT has not been considered a possible target. Each TSG has Working Groups that are responsible for developing reports and specifications, which define the Cellular Phone System. These groups are showed below.

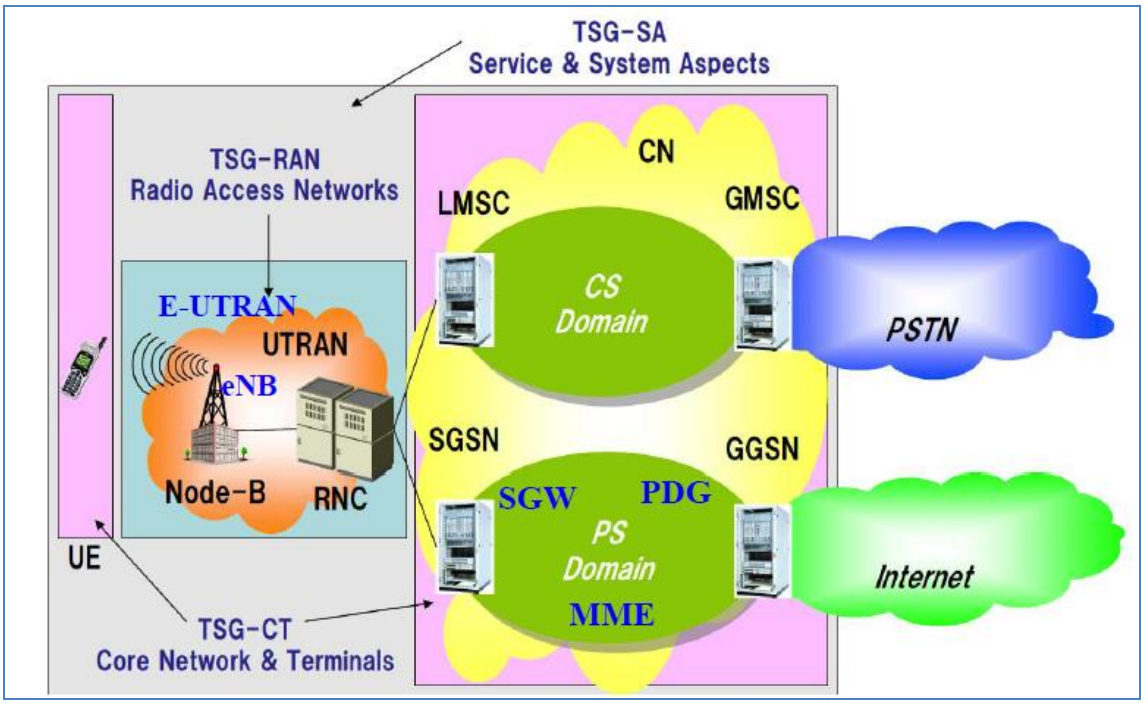
Figure 2: Main 3GPP Groups

Project Co-ordination Group (PCG)

TSG RAN Radio Access Network	**TSG SA** Service & Systems Aspects	**TSG CT** Core Network & Terminals
RAN WG1 Radio Layer 1 spec	SA WG1 Services	CT WG1 MM/CC/SM (Iu)
RAN WG2 Radio Layer 2 spec Radio Layer 3 RR spec	SA WG2 Architecture	CT WG3 Interworking with external networks
RAN WG3 Iub spec, Iur spec, Iu spec UTRAN O&M requirements	SA WG3 Security	CT WG4 MAP/GTP/BCH/SS
RAN WG4 Radio Performance Protocol aspects	SA WG4 Codec	CT WG6 Smart Card Application Aspects
RAN WG5 Mobile Terminal Conformance Testing	SA WG5 Telecom Management	
RAN WG6 Legacy RAN radio and protocol	SA WG6 Mission-critical applications	

The scope of each TSG groups is reported in the figure below.

Figure 3: Scope of the TSG



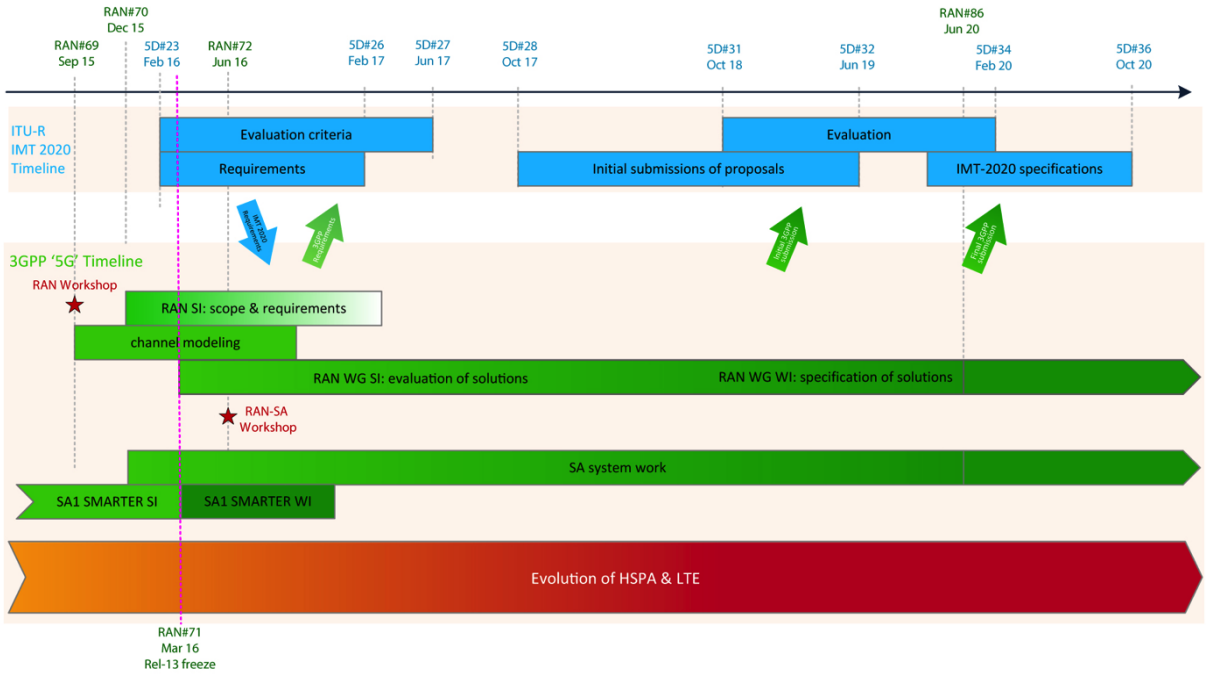
In March 2015, 3GPP endorsed a tentative timeline for the standardisation of next generation cellular technology, also known as "5G". This section briefly summarises some of the key milestones and how the work is expected to proceed in 3GPP working groups.

During the RAN & SA plenary meetings #67 (Shanghai, 9-13 March 2015), 3GPP discussed and endorsed the main 5G milestones. The following high level milestones were agreed to comply with the ITU-R IMT-2020 process constraints:

- **2016/2017**: submission of 3GPP requirements to ITU-R.
- **2018**: submission of 3GPP 5G solution to ITU-R for evaluation (i.e. "does it satisfy ITU-R requirements for 5G?").
- **December 2019**: submission of final 3GPP 5G specs to ITU-R.

Consequently, the following initial 3GPP 5G timeline was agreed, as illustrated below.

Figure 4: Initial 3GPP 5G Timeline



The 5G normative phases have started officially in March 2017 with the Release 15:

- Phase 1 (Rel-15) to be completed by June 2018 addresses the more urgent subset for commercial deployments
- Phase 2 (Rel-16) to be completed by March 2020 IMT 2020 submission, addresses all identified use cases & requirements

3.3.1 Radio technologies (RAN)

There are three emerging high level use cases for Next Generation Radio Technology (also from IMT 2020 discussion):

- Enhanced Mobile Broadband.
- Massive Machine Type Communications.
- Ultra-reliable and Low Latency Communications.

There is a wide agreement that the Next Generation Radio Technology should be able to support a variety of new services such as **Automotive, Health, Energy, and Manufacturing**.

Some of these services are being described by SA1 in the SMARTER project.

From the radio point of view, the consensus has been built around the need for a new, non-backward compatible, radio as part of Next Generation Radio Technology while LTE evolution will continue in parallel. For this purpose, RAN work is based on:

1. Channel modelling for bands above 6 GHz. The study item (SI) on "channel modelling for spectrum above 6 GHz (TR 38.900)" has been approved in September 2016 and its results are available since the RAN#72 meeting (June 2016). According to this SI:

- In the first part of the SI, RAN has identified the status and expectations on high frequencies (e.g. spectrum allocation, scenarios of interest, measurements, etc).
- Then the SI has developed a channel model(s) for frequencies above 6 GHz up to 100 GHz (from Q1 2016). Anyway it is important to note that the document is a 'living' document, i.e. it is permanently updated and presented to TSG-RAN meetings.

2. Scenarios and requirements for next generation radio technology. RAN has started the SI in December 2015 (REL-14 v1.0.0 was approved by email after RAN #73 in October 2016 as TR 38.913). According to this SI description:

- RAN will develop scenarios and key requirements of the new radio technology. These requirements will drive the design of the new RAT (in parallel to ongoing LTE evolution). The bulk of the requirements should be agreed in the first six months of the RAN discussion to guide the design of the new radio in the WGs. The RAN study may remain formally open until the corresponding ITU-R task is closed (for this reason, RAN SI is shown as a fading block in the timeline diagram).
- RAN will import the relevant IMT 2020 requirements and add its own requirements. These requirements are used by the ITU-R AH to drive the IMT 2020 submission to ITU-R (which may include LTE).

3. Radio solutions.

- In March 2016, RAN approved a Study Item (TR38.801) for RAN WGs to evaluate technology solutions for next generation radio. The deliverable has been approved during RAN#75 in March 2017.

Some of the security issues analysed by 5G-ENSURE project can impact on the 5G radio definition. For this reason it is worth spending part of 5G-ENSURE effort on monitoring the RAN WGs. In fact the current version of the TR 38.913 (V14, published during October 2016) already contains some high level security requirements proposals to take into consideration for the design of the radio access. In particular the deliverable contains the clause 10.12 (Security and Privacy related requirement relevant for Radio Access) with the following text:

The RAN design for the Next Generation Radio Access Technologies shall ensure support for integrity and confidentiality protection of radio signalling messages, including messages between RAN and Core network nodes.

The RAN design for the Next Generation Radio Access Technologies shall ensure the ability to support integrity and confidentiality protection of user plane messages, including messages between RAN and Core network nodes, with the use of such security to be configurable during security set-up.

The RAN design for the Next Generation Radio Access Technologies shall ensure support for the allocation and use of identities to provide user privacy, e.g. reduce the need for sending any permanent identities in the clear.

The RAN design for the Next Generation Radio Access Technologies shall ensure the efficient establishment of RAN security mechanisms.

The RAN design for the Next Generation Radio Access Technologies shall ensure resilience against jamming.

NOTE: Security and Privacy-related system requirements are reflected in 3GPP TR 33.899 [32]. This TR includes security areas on "RAN security" and "Privacy security", which is a possible source of security and privacy related requirements for the Radio Access.

- During the RAN#74 meeting in Vienna (December 2016), the 3GPP came to consensus on 5G terminology. The new 5G physical layer will be officially named, “NR” for new radio and the new 5G core network will be called, “5G CN”. A connection between NR and 5G CN will be named “NG”. At the same plenary meeting, 3GPP agreed to a work plan proposal (RP-170741) for the first 3GPP 5G New Radio (NR) specification that will be part of Release 15 – the global 5G standard. It has been agreed to accelerate the 5G NR schedule by introducing an intermediate milestone for an early completion of a variant called Non-Standalone (NSA) 5G NR (*EPC core & LTE anchor*). Hence there will be two releases:Intermediate Stage 3 completion for Non-Standalone 5G-NR (at RAN#78, December 2017)
- Stage 3 completion for Standalone 5G-NR (at RAN#80, mid 2018).

3.3.2 Service & Architecture Requirements (SA1)

In March 2015, the SA approved the first official 3GPP Study Item (SI) related to 5G development. The name of the SI is “New Services and Markets Technology Enablers”, a.k.a. SMARTER [33] (http://www.3gpp.org/DynaReport/22891.htm).

SMARTER is the SA WG1 project used to:

- Collect and develop high-level use cases
- Identify the related high-level potential requirements to enable 5G.

The Study Item aims to identify the market segments and verticals (e.g. Automotive, Healthcare, Manufacturing, Energy) and their requirements as the focus for 3GPP and that cannot be met with current LTE/EPS (Evolved Packet System) state of the technology. To this end, the 3GPP collects contributions from all the external organisations working on the 5G concept (e.g. NGMN, 5G Americas [34], Chinese IMT-2020 (5G) Promotion Association [35], ITU-R WP5Ds, 5G Forum [36], Republic of Korea).

The SMARTER work has been organised so that a subset of distinct work items (WI) and study items (SI) with clearly focused objectives are executed in each phase of the work.

As a first phase, several 5G use cases covering various scenarios have been developed and the related high-level potential requirements have been identified. Use cases with common characteristics have been grouped together and documented in SMARTER (TR 22.891). Starting from this TR, the next steps involve the selection of a few, e.g. 3-4, use cases (or groups of use cases with common characteristics) for which new individual building block study items have started. The scope is to further develop the selected use cases and their potential requirements, and capture desired system requirements and capabilities that apply across the different verticals.

A review and consolidation of the resulting requirements will be performed on completed study items, and will close phase 1 of SMARTER. Of course each phase of SMARTER needs to be compatible and consistent with the previous Phase. The original target was March 2016, with the intention of subsequently starting normative work on study items. At the end of 2015, beginning of 2016, SA1 has already started on a set of specialised Study Items dedicated to analysing in detail specific scenarios, and finalise all of them by the end of June 2016. The current list of the derived SIs is the following:

- SMARTER-CRIC, dedicated to the analysis of the Critical Communications.
- SMARTER-eMMB, for the enhanced Mobile Broadband.
- SMARTER-NEO, for Network Operations.

- SMARTER-mIoT, massive Internet of Things.

All four were approved at the 3GPP SA#72 (Busan 15-17 June 2016) meeting, and contextually 3GPP SA1 started the consolidation of the four Technical Reports into a single Technical Specification (TS 22.261, Service requirements for next generation new services and markets) with normative Stage 1 requirements for next generation mobile telecommunications, guiding the work of the Stage 2 and Stage 3 groups in 3GPP. In March 2017 (during SA#75) the version 2.0.0 of the TS 22.261 were approved. The document compiles requirements that define a 5G system in order to support new deployment scenarios to address diverse market segments. The main characteristics include:

- Support for multiple access technologies.
- Scalable and customisable network.
- Advanced KPIs (e.g., availability, latency, reliability, user experienced data rates, area traffic capacity).
- Flexibility and programmability (e.g., network slicing, diverse mobility management).
- Resource efficiency (both user plane and control plane).
- Seamless mobility in densely populated and heterogeneous environment.
- Support for real time and non-real time multimedia services and applications with advanced QoE.
- Interoperability with legacy 3GPP systems.
- Multi-network connectivity and service delivery across operators.
- 3GPP access network selection.
- eV2X aspects.
- Flexible broadcast/multicast.
- Higher-accuracy positioning.

Other Working Groups can use the four original SMARTER Technical Reports, and in particular the content of the TS.22.261, as input for their studies in this area.

New use cases may be added to the SMARTER TR during the ongoing work. They can be included at the earliest in the next open Phase (selection of a few use case).

The most relevant crucial points of the 5G, partly already addressed also by NGMN, are related to:

- The concept of Slicing was introduced, as already emerged during NGMN 5G activity. A slice is composed of a collection of logical network functions that supports the communication service requirements of particular use case(s). It should be possible to direct terminals to slices in a way that fulfils operator needs, e.g. based on subscription or terminal type. The network slicing primarily targets a partition of the Core Network, but it is not excluded that the RAN may need specific functionality to support multiple slices or even partitioning of resources for different network slices.
- The need for very low latency for scenarios of: Indoor Mobile broadband, On-demand Networking, Virtual presence, Connectivity for drones, Industrial and Localised Real-time Control, Tactile Internet, Natural disaster.

- Coexistence with legacy systems is considered a key requirement. In order to support the different use cases and business models with their varying demands, it is expected that the 5G system will include one or more 5G RAT(s) optimised for different market segments. The support of co-existence of new 5G RAT(s) and an E-UTRAN would cater for a sound migration path. However, seamless handover between the 5G RAT(s) and GERAN or UTRAN is not required.
- The secure storage for subscriber identity and network access credentials has been discussed, proving to be the most controversial issue. Different opinions have emerged between the A proposal of maintaining the dedicated physical secured and tamper resistant entity (UICC) controlled and managed by mobile operator, and the a proposal of adding something new at least to address low complexity devices market and use cases.

  The SMARTER work has been used within 5G-ENSURE project as an input for collecting the use cases having security and privacy impacts resulting in the delivery of D2.1 deliverable [http://www.5gensure.eu/deliverables].

3.3.3 System Aspects (SA2)

The study on potential new 5G architectures started in December 2015 (as part of Release 14). The SI dedicated to the 5G aspects is the TR23.799 (short name NextGen) “Study on Architecture for Next Generation System” with the objective of designing the system architecture for the next generation mobile network. Within SA2 group, regular meetings and discussions are held to discuss the progress of this study item. The TR 23.799 has been finalized at the end of 2016 as V 14.0.0.

The security aspects, initially not part of the objectives , have been now included. In fact the title of the study Item has been canged into “Study on Architecture and Security for next Generation System”. Since the Security parts are in charge of the SA3. SA2 has now started two new technical specifications (normative phase) whose delivery has foreseen by the end of 2017:

- System Architecture for the 5G System (TS 23.501)
- Procedures for the 5G System (System Flows) (TS 23.502)

SA2 will have a critical role in reconciling Service requirements (SA1) and Radio-specific requirements (RAN), with the objective of making sure that there will be a coherent and consistent architecture/system.

3.3.4 Security Aspects (SA3)

SA3 is the main target group for the standardisation actions within the 5G-ENSURE project because it address technical issues very much in line with the project expected outcomes and a strong commitment on this body of a 5G-ENSURE partner. In fact SA WG3 is responsible for security and privacy in 3GPP systems, determining the security and privacy requirements, and specifying the security architectures and protocols. The term of reference of SA3 declares:

“*SA WG3 has the overall responsibility for security and privacy in 3GPP systems. The WG will perform analysis of potential threats to these systems. Based on the threat analysis, the WG will determine the security and privacy requirements for 3GPP systems, and specify the security architectures and protocols*.”

In particular, during the SA3#82 meeting in February 2016 the opening of a new SI dedicated to the security aspects of the 5G was agreed. Such a SI (TR 33.899), strictly related to the on-going work in SA1 (Smarter), SA2 and RAN, has been called “Study on Architecture and Security for Next Generation System”.

The SA3 objective is to study preliminary threats, requirements and solutions for the security of next generation mobile networks. Work is expected work to include:

- Collection, analysis and further investigation of potential security threats and requirements for the next generation systems, based on the work of 3GPP Working Groups.
- Investigation of the security architecture and access security in co-operation with SA2, RAN2 and RAN3.

The TR 33.899 has been proposed to capture the output of this study. The rapporteur of this SI is Vesa Torvinen from Ericsson. The security threats and requirements, and the security architecture may additionally include standalone security topics that SA3 sees as crucial. While these topics may not be covered by the security work described above, they will not be in conflict with requirements from other 3GPP WGs. It is part of the study to determine whether such topics need to be dealt with, and, if so, what they are.

At the present time the TR 33.899 cointains the following Security areas:

1. Security architecture deals with architectural aspects of the security for NextGen system.
2. Authentication deals with authentication framework, identifiers, and credentials, authentication methods.
3. Security context and key management deals with security aspects related to management of security context and security keys.
4. RAN security deals with the security for Next Generation radio interface and radio access network.
5. Security within NG-UE deals with the security of sensitive data handled within the NG-UE.
6. Authorisation deals with both, authorization of the UE to access the network and authorization of the network to serve the UE.
7. Subscription privacy deals with various aspects related to the protection of subscribers’ personal information, e.g. identifiers, location, data, etc.
8. Network slicing security covers security aspects related to the network slicing concept such as service access, network function sharing and isolation.
9. Relay security deals with security of the NextGen connectivity over relays.
10. Network domain security deals with security of the signalling protocols in the network domain such as authentication, integrity, and availability.
11. Security visibility and configurability deals with presentation of security information to a user of a UE, and management of security configuration by a user or a UE.
12. Credential provisioning deals with security aspects of provisioning 3GPP credential(s) on equipment that will access the NextGen system.
13. Interworking and migration deals with security aspects related to the interworking and migration scenarios between radio technologies and possible core network concepts.
14. Small data deals with massive number of IoT UEs that usually send small amounts of data sporadically and also moves around.
15. Broadcast/Multicast security deals with security for broadcast services that will be used in verticals, for example MCPTT, Critical Communication, V2X, and massive MTC.
16. Management Security deals with security related to management plane and deployment scenarios.
17. Cryptographic algorithms deal with cryptographic algorithms to be used for security mechanisms and protocols within Next Generation System.

The complete or partial conclusions of this study (the latest version, not yet approved, contains more then 400 pages and no specific conclusions) will form the basis for the normative work and/or for any further

study. As expected, the normative part has started officially in march 2017 with the approval of the Work Item aimed to deliver the Technical Specification TS 33.501 “Security architecture and procedures for 5G System” that will contain the normative aspect related to the 5G Security and the rapporteur of this WI is Alf Ziggerminer from NTT. The first consolidated results are expected by the end of 2017.

For such reasons, SA3 is actually the main target for the standardisation action of the project, where it is possible to propose for standardisation many of the research topics results achieved during the lifetime of the 5G-ENSURE, although at the present time most of the project effort has been dedicated to the Privacy aspecs.

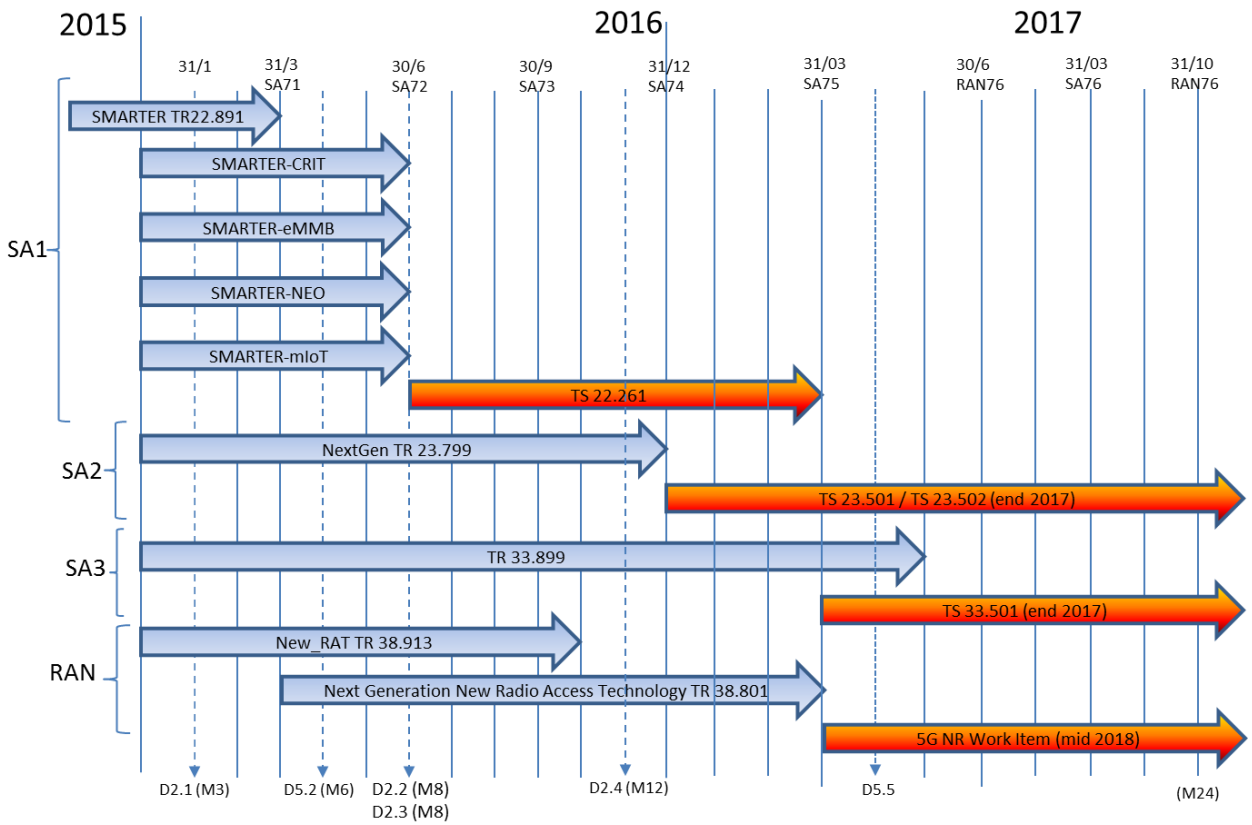
3.3.5 5G-ENSURE opportunities in 3GPP

Following the on-going work in 3GPP, potential contributions from 5G-ENSURE can be:

- Within SA1 as part of the study item started for the first selected use cases, further develop these use cases and their potential requirements. The TS 22.261 should be evaluated if the first set of selected use cases have a mapping with the use cases defined within the project.
- Within SA2, it is important to take into consideration the evolution of the TR 23.799 and its successors TS 23.501 and TS 23.502, since the architecture of 5G as defined by 3GPP will have a huge impact on the security aspects under definition within 5G-ENSURE. The objective is to make sure that the 5G-ENSURE security architecture will be coherent and consistent with the SA2 architecture/system. It is, however, important to note that the security aspects will be forwarded directly by SA2 to SA3. Such an aspect confirm that SA2 and SA3 will work aligned and the project effort can be focused on the SA3 works. As expected the specification works started in March 2017.
- RAN also has to be taken into consideration. The current version of TR 39.913 (release 14) already covers security albeit in a very high level of detail. It is expected that all the security related matter will be analysed by SA3 as also mentioned explicitly in the TR 33.899
- Finally SA3, the 3GPP security group, with its SI on the Security Aspects of the Next Generation System (TR 33.899) that until now has been actually the main target for 5G-ENSURE, and the recent TS 33.501 dedicated to the normative works. All the main results of the project obtained during 2016 (D2.1 on use cases, D2.2 on Trust model and D2.3 on security requirements) and the preliminary results achieved in the field of Security architecture (WP2) and Security Enablers (WP3) can be proposed for evaluation by the security experts in SA3, during both: the finalization of the TR33.899 (finalization initially expected during SA3#86 in 2017, the meeting held in Sophia Antipolis, and then postponed to the meeting SA3#87 in Slovenia), and the just started specification works aimed to deliver the TS 33.501 “Security architecture and procedures for 5G System” by the end of 2017.

The following GANTT chart illustrates the main 3GPP action plan for 5G as monitored since the beginning of the 5G-ENSURE project in 2015 to April 2017 (deadline for the deliverable D5.5) and the forecast to the end of 2017. The blue arrows are related to the study items dedicated to 5G, whereas the red arrows are related to the normative phases .

Figure 5: 3GPP GANTT 1 – Updated april 2017



3.4 ETSI

5G will impact a vast number of new technologies that will need standardisation, including against growing threats to ICT-centric organisations. There is increased interest in defending national and European critical infrastructures through cyber security. To cope with the complexity of the security and privacy aspects, ETSI has set up a reference group to create security standards and coordinate security matters across the ETSI work areas.

3.4.1 TC CYBER

ETSI TC CYBER Technical Committee was established by ETSI in 2014 to address the growing demand in the area of cyber security standardisation. The Cyber security technical committee (TC CYBER) works closely with relevant stakeholders within and outside ETSI to collect, identify and specify requirements and thus develop appropriate standards to increase the privacy and security of organisations and citizens across Europe.

The activities of TC CYBER include the development of standards in the following areas:

- Cyber security.
- 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.

TC CYBER acts as the ETSI centre of expertise in cyber security, in addition to the specific standardisation tasks it will perform. These aspects can facilitate the possible action within the ETSI scope. Responsibilities of TC CYBER (from the ToR) include:

- Advise other ETSI TCs and ISGs on the development of Cyber Security requirements.
- Develop and maintain the Standards, Specifications and other deliverables to support the development and implementation of Cyber Security standardisation within ETSI.
- Identify gaps where existing standards do not fulfil the requirements and provide specifications and standards to fill these gaps, without duplication of work in other ETSI committees and partnership projects.

Although TC Cyber has not yet started a dedicated Work item on 5G security, it has been naturally selected as the target group for the results of 5G-ENSURE reseach on Privacy. In fact, TC CYBER is active in the field of privacy aspects and also security requirements for visualised environmentsand during the CYBER#8 meeting, the following sentence has been introduced in the ToR to better describe the activities of the group: “Provision of security mechanisms to protect privacy”. Formal approval of the latest version of the ToR has been approved in early 2017.

Among the various Work Items created by the TC, the following are of particular interest for 5G-ENSURE:

- TR 103 304 “PII Protection and Retention”. The document contains a collection of use cases and an analysis of the threats, risk and vulnerabilities related to the protection of Personally Identifiable Information (or PII). The deliverable has been agreed and published with a new title: “Personally Identifiable Information (PII). Protection in mobile and cloud services”. The new title has been proposed by the project 5G-ENSURE, together with a description of the rational of such a change. In particular now the deliverable takes into account also the mobile scenario (i.e. “5G”) with the description of the use case related to the protection of the IMSI taken form the D2.3.
- TR 103 370 “Practical introductory guide to privacy”. The document presents the basics for privacy management, key definitions, status of standardisation (existing and future work) in ISO, CEN/CENELEC, ETSI and finally a practical guide on how to introduce Privacy management in equipment, services and solutions. The aim is to introduce terms and definitions and set up the scene of existing standards, although it is technically impossible to have definitions and principles which are in line with all legal frameworks. The document can be considered as an input for M/530 (Privacy). The document will be published by the end of 2017.
- TS 103 485 “Mechanisms for privacy assurance and verification”. The document provides technical means, building on on-going work in TC CYBER that enable assurance of privacy and verification of said assurance. The document will address Identity Management with respect to privacy. There is no significant progress for this work item and the schedule was reviewed. The TB approval has been confirmed to be September 2017.
- TS 103 486 “Identity management and naming schema protection mechanisms”. The intent of this work item is to identify means to protect identity (as distinct from privacy) in order to alleviate some of the resultant threats. The work item will detail the mechanisms to protect such data in the general case and link to specific use cases in NFV, the PLMN domain, and the wider Internet of Things domain to ensure that the widest scope of protection can be

defined. There is no significant progress for this work item and the schedule was reviewed. The TB approval has been confirmed to be September 2017.

- TS 103 487 “Baseline security requirements regarding sensitive functions for NFV and related platforms”. The document defines security baseline requirements for sensitive functions including Lawful Interception (LI) and Data Retention (RD) in an NFV hardware/platform environment. The deliverable has been published in April 2016.
- TS 103 458 “Application of Attribute-Based Encryption (ABE) for data protection on smart devices, cloud and mobile services”. During the CYBER#7 meeting in Sopia Antipolis (June 2017) the new WI hass been approved with the support of Telecom Italia. This WI specifies an application of ABE to implement ABAC for specific environments where access to data has to be given to multiple parties and under different conditions. The work item will describe the ABE encryption and decryption mechanisms, the boundary conditions relating to the underlying cryptography, the key distribution protocols and any related architectural aspect. Three main use cases will be addressed: Cloud, Mobile, IoT. The 5G-ENSURE project results will feed into the mobile part. The objective is to provide user identity protection preventivg disclousure to unauthorised entities. During the CYBER#8 meeting (Sorrenti Italy) a specific liaison has been officially sent by the TC CYBER to the 3GPP, informing SA3 about the new activities and asking for support. The TB approval has been proposed to be June 2018.
- DTS/CYBER-0025 (Provisional identifier) “Attribute Based Encryption for Attribute Based Access Control”. This WI specifies standard features needed to use ABE as ABAC. It specifies a protocol including the following features: - Interactions between the principal, the service provider, the authority releasing attributed - The policy schema for data access control - Key, policy, and attribute distribution - Key, policy, and attribute expiration and revocation - Definition of what subset of ABAC (XACML) may be mapped into the protocol -Definition of semantics for a basic set of attributes to ensure interoperability - Identification of additional attributes required by the protocol that would require an extension to traditional ABAC (e.g. an extension to XACML) - Mapping the protocol to a standard Public Key Infrastructure X.509 (PKIX) - Mapping the protocol to a standard assertion protocol (SAML) - Definition of new protocol bindings when existing bindings do not cover the deployment scenario (e.g. a CoAP binding for the IoT case) The deliverable will cover both the Ciphertext-Policy (CP-ABE) and Key-Policy (KP-ABE) variants of Attribute-Based Encryption. The TB approval has been proposed to be early 2018.

Moreover in the scope of Privacy and Protection of PII by using ABE mechanisms, Telecom Italia has sponsored the creation of a Specialist Task Force, the STF-529 “Attribute Based Encryption - Common protocol for data access control for Cloud, Mobile and IoT”. The proposed STF is tasked to provide an ETSI Technical Specification to define a protocol for ABE addressing the following key elements:

- Definition of interactions between the actors and stakeholders (e.g. principal, the service provider, the authority releasing attributes).
- Standardisation of a naming scheme for attributes.
- Standardisation of an access policy schema.
- Definition of a standard set of mechanisms to distribute and revoke attributes and policies using certificates in a standard public key infrastructure (PKIX).

- Mapping to a standard assertion mechanism (SAML) and to a standard Attribute Based Access Control language (XACML).
- Bindings to transport protocols when existing standards do not cover the foreseen use cases.

An STF is Specialist Task Force, a team of highly skilled experts, brought together to perform specific technical work under the direction of one of our technical committees, the TC CYBER in this case. This committee is ultimately responsible for approving the standards produced by the STF. STFs are used by ETSI to accelerate the standardization process in areas of strategic importance and in response to urgent market needs.

3.4.2 ETSI ISG NFV

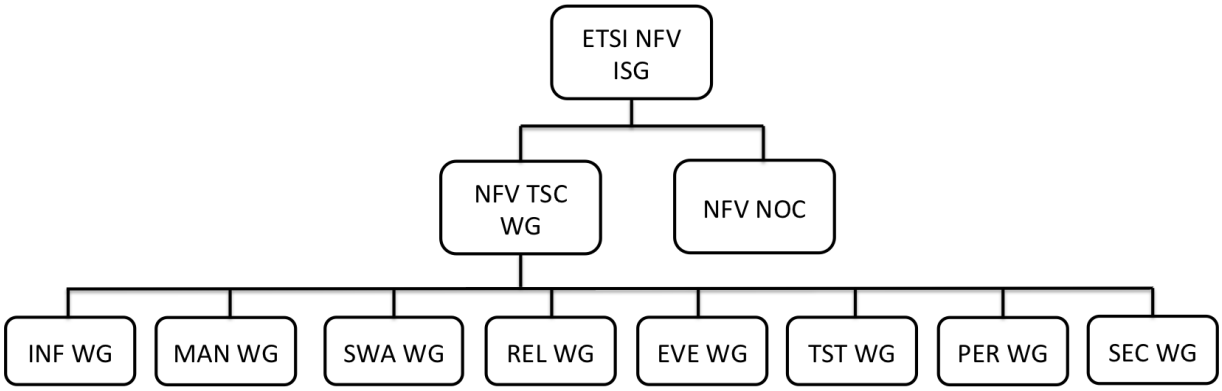
ETSI Industry Specification Group (ISG) for NFV is the home for developing requirements and specifications for NFV and has been given an additional two-year mandate chaired by Diego Lopez (Telefonica), who is also a member of the 5G-ENSURE Advisory Board. In 2012, the leading telecommunications network operators decided that ETSI ISG would be the place for facilitating the industry's transformation and development of an open, interoperable, ecosystem as well as for sharing the experiences of NFV development and early implementation. Over the past 3 years, ETSI ISG NFV membership has grown and currently includes over 270 individual companies including 38 of the world's major service providers as well as representatives from both telecoms and IT vendors. Many 5G-ENSURE partners are involved in ETSI ISG NFV, such as ORANGE, Telecom italia, NEC, Ericsson.

The main goal in forming ETSI ISG NFV was to produce the technical specifications to enable the development of an open, interoperable, commercial ecosystem based on virtualised network functions. The ETSI ISG NFV maintains core NFV documentation, including an architectural framework and associated technical requirements, as well as liaison relationships with other specialist SDOs and industry alliances contributing technology or applying NFV concepts within their specialisations. In order to do so there are several working groups (WG) formed under ETSI ISG NFV. These are as follows:

- NFV TSC : Technical Steering Committee.
- NFV NOC: Network Operators' Council.
- NFV INF : Interfaces and Architecture Working Group.
- NFV REL : Reliability and Availability Working Group.
- NFV SWA: Software Architecture Working Group.
- NFV MAN : Management and Orchestration Working Group.
- NFV TST : Testing, Experimentation and Open Source Working Group.
- NFV EVE : Evolution and Ecosystem Working Group.
- NFV SEC : NFV Security Working Group.
- NFV PER : Performance and Portability Working Group.

To manage such a large body with different WGs, the ETSI ISG NFV established an operational structure as depicted in the figure below.

Figure 6: ETSI ISG NFV operational structure



We focus on the NFV SEC WG activity as the most interesting working group from a 5G-ENSURE perspective.

3.4.2.1 ETSI NFV SEC WG

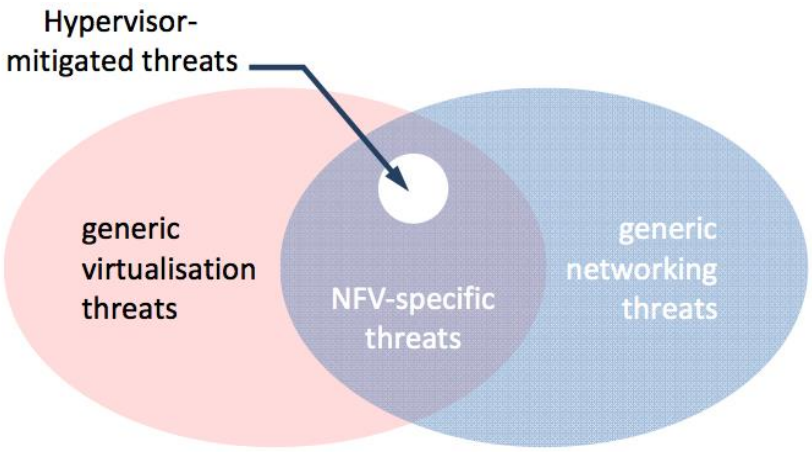
ETSI NFV SEC is the working group (WG) responsible for technical specification that spans multiple WGs. The SEC WG is responsible for security considerations throughout the NFV platform. In order to achieve such a goal, NFV SEC WG is working on many different topics, ranging from defining a problem statement, defining the threat landscape, identifying potential areas for security vulnerabilities, hardening requirements, NFV specific use of security functionalities, etc. among others. The main responsibilities of this WG are as follows:

- Proactively and reactively reviewing all new work items (WIs) for likely security impacts.
- Analysing threats to security in virtualised environments and deriving service and security requirements.
- Identifying and specifying best practice in areas of security for NFV environments.
- Investigating security enhancements for NFV.
- Addressing the tension between service function and privacy; and the impact of trends such as opportunistic encryption.
- Contributing to the security aspects of NFV demonstrators / proofs of concept.
- Work with external security experts and accreditation institutions to highlight the importance of NFV and encourage involvement.

Threat Landscape

The figure below highlights the threat landscape for NFV deployments. The left hand side of the figure depicts the threats that are generated by using the virtualisation technology in general. Since NFV uses virtualisation at its core, the traditional virtualisation threats are also a concern for NFV deployments. At the same time, virtualisation mitigates some of the threats that are currently possible in physical device scenario. The right-hand side of the figure shows the generic networking threats. However, NFV SEC WG is mostly interested in threats that are specifically related to NFV when the virtualisation threats and traditional networking threats are combined. This is due to the fact that the generic virtualisation threats and the generic networking threats are already currently known and may be the solutions/best practices are readily available. However, the threats that are emerging by combining these two landscapes are quite new and require further study.

Figure 7: Visualisation of the NFV threat surface [source: ETSI GS NFV-SEC 001]



Areas of Concern

After analysing the key security issues submitted by the participants in the first ETSI NFV ISG meeting, NFV SEC WG has compiled the main areas of concern grouped into 10 domains:

1. Topology Validation & Enforcement.
2. Availability of Management Support Infrastructure.
3. Secured Boot.
4. Secure crash.
5. Performance isolation.
6. User/Tenant Authentication, Authorisation and Accounting.
7. Authenticated Time Service.
8. Private Keys within Cloned Images.
9. Back-Doors via Virtualised Test & Monitoring Functions.
10. Multi-Administrator Isolation.

Current reports

The current suite of NFV SEC WG publications are publicly available for use as a reference point, and include:

- ETSI GS NFV-SEC 001: Problem Statement.
- ETSI GS NFV-SEC 002: Cataloguing security features in management software.
- ETSI GS NFV-SEC 003: Security and Trust Guidance.
- ETSI GS NFV-SEC 004: Privacy and Regulation; Report on Lawful Interception implications.
- ETSI GS NFV-SEC 006: Security & Regulation report.
- ETSI GS NFV-SEC 009: Report on use cases and technical approaches for multi-layer host administration.
- ETSI GS NFV-SEC 010: Retained Data Report.
- ETSI GS NFV-SEC 012: Architecture for sensitive components – Specification.
- ETSI GS NFV-SEC 013: Security management & monitoring specification.

Along with these published reports, there are several work-in-progress drafts that are also available for public review:

- ETSI GS NFV-SEC 005: Certificate management report.
- ETSI GS NFV-SEC 007: NFV Attestation report.
- ETSI GS NFV-SEC 011: Lawful Interception Architecture Report.
- ETSI GS NFV-SEC 014: MANO Security Specification.

Active Work

Currently, SEC has active work ongoing on the following topics:

- Security work for MANO. This includes threat analysis for the components of MANO, for the internal interfaces and the external interfaces. The outcome of this work are requirements that mitigate the identified threats
- Security aspects of multi-layer host administration.
- SEC is also preparing work items for continuing work on certificate management, security management and monitoring, attestation and LI.

3.4.3 5G-ENSURE opportunities in ETSI

Within the ETSI TC Cyber given the number of WIs related to privacy, clearly that topic is one of the main interests for the group.

As anticipated in the previous reports, since the CYBER#6 meeting (February 2016) the 5G-ENSURE project planned to open, or at least to contribute to, a specific work item dedicated to analyse the privacy aspects in the 5G scenarios. Concrete actions has been carried on by extending a previous TR (the TR103.304) to the mobile scenario, by sponsoring the approval of the new Technical Specification TS103.458 during CYBER#7 (June 2016) and finally by supportin the creation of the STF-529 and the related objectives. Hence it is expected that significant part of the project effort in 2017 dedicated to standardisation activities will be spent to elaborate contributions for that deliverables (to be noted that the dealine of the Work Item and STF are foreseen beyond the end of the project activities).

ETSI ISG NFV: following the work performed in ETSI ISG NFV SEC, there are many potential areas for contribution. Since most of the technical reports are currently under development, timely contributions would have an impact towards further development of this technology in the right direction.

3.5 5G Time Line for ITU (IMT 2020)

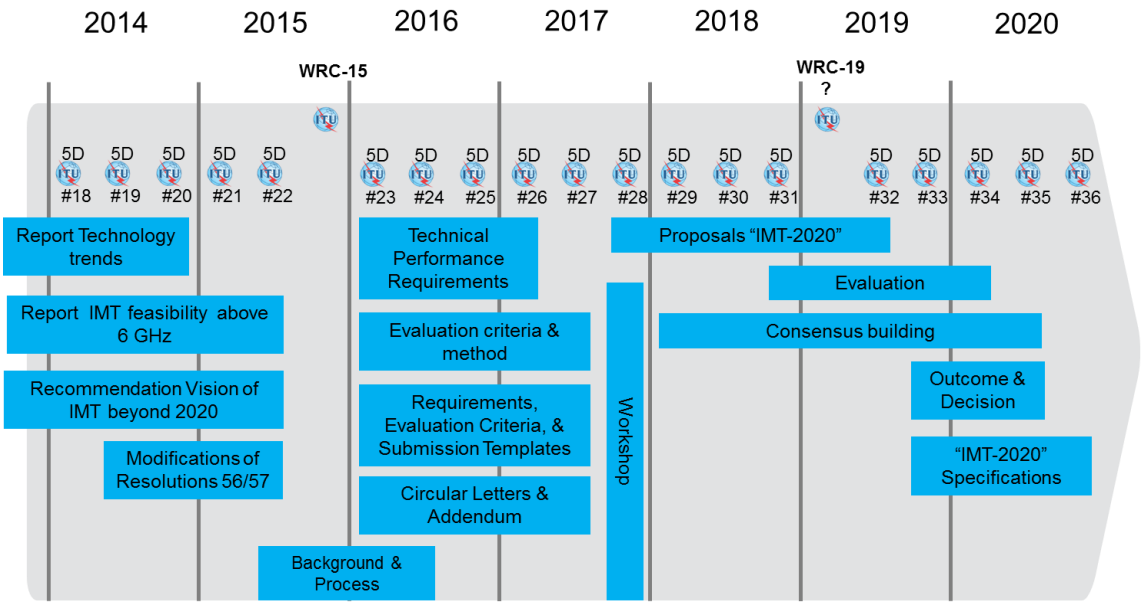
3GPP is committed to submitting a candidate technology to the IMT 2020 process triggered by ITU-R according to the two following submission deadlines:

1. Initial technology submission by ITU-R WP5D meeting #32, June 2019.
2. Detailed specification submission by ITU-R WP5D meeting #36, October 2020.

For deadline 2, 3GPP has decided to submit the final specifications at the ITU-R WP5D meeting in February 2020, based on functionally frozen specs available in December 2019. This early submission will allow enough time for the transposition of the specifications by the Organisational Partners of 3GPP prior to their own submissions into the IMT 2020 process before October 2020.

RAN ITU-R Ad-Hoc Group is selected to maintain the relationship between 3GPP and ITU-R (i.e. verify timing and coordinate submissions of 3GPP documents to ITU-R).

Figure 8: 5G Time Line for ITU [Source: 3GPP RP-150483]



3.5.1 ITU *Focus Group* -IMT2020

The network study group is within the purview of ITU's Standardisation Sector (ITU-T), an ITU bureau, which is expected to parallel the 5G standardisation work of ITU-R (ITU's Radio Communication Sector). While ITU-R is briefed with coordinating international standardisation of "IMT-2020" RAN systems, ITU-T has a similar role on the wireline side, looking at standardisation requirements of wireline networks to support 5G RANs.

The work to be carried out by ITU-T on the network aspects will be an important complement to the activities undertaken by ITU-R in developing the radio interface standards for IMT-2020.

The Focus Group on network aspects of IMT-2020 was established in May 2015 to analyse how emerging 5G technologies will interact in future networks as a preliminary study into the networking innovations required to support the development of 5G systems The original plan was to finalise the work by the end of 2015. The group took an ecosystem view of 5G research of development and published the analysis in a Report [37] to its parent group, ITU-T Study Group 13 [38]. Due to the short and fixed duration of the first period of the Focus Group, security aspects have not been addressed.

In December 2015, the Focus Group received an extension to its lifetime to the end of 2016 and now it has been officially terminated. The latest Terms of Reference called for the group to engage open-source communities, influencing and taking advantage of their work by introducing them to the challenges that telecoms players must overcome in the development of the 5G ecosystem. Specific tasks and areas of work included:

- Explore demonstrations or prototyping with other groups, notably the open-source community.
- Enhance aspects of network softwarisation and information-centric networking.
- Continue to refine and develop the IMT-2020 network architecture.

- Continue to study fixed-mobile convergence.
- Continue to study network slicing for the fronthaul/backhaul network.
- Continue to define new traffic models and associated aspects of QoS and operations, administration and management applicable to IMT-2020 networks.

ITU-T standardisation activity based on the findings of the Focus Group will prioritise the alignment of 5G deliverables with those of ITU-R, ensuring that standardisation work on the network aspects of 5G is informed by the progression of its radio-transmission systems.

The Focus Group was not not particularly interested in security aspects, and that has also been confirmed during the lates 5G-ENSURE Workshop in Sophia Antipolis and during an official interview held at the beginning of 2017. The only document produced at the end of 2015, the "Report on Standards Gap Analysis", reports the following sentence:

This focus group has looked at the following wireline aspects of IMT-2020 and has studied each in some detail and produced detailed gaps related to each subject. Due to the short and fixed duration of the Focus Group, there will be some areas, one example is security, which not have been addressed. This should also be considered when formulating possible new work on standardisation topics

Hence the group, even if it can be considered to be of interest for the project research topics (given its activities on e.g. Network Softwarization), has not been considered one of the main target for the 5G-ENSURE project.

At the end of 2016 the FG released the following 9 deliverables (draft Recommendations and Technical Reports) to ITU-T Study Group 13:

- Draft Terms and definitions for IMT-2020 in ITU-T (O-040).
- Draft Technical Report: Application of network softwarisation to IMT-2020 (O-041).
- Draft Recommendation: Requirements of IMT-2020 from network perspective (O-042).
- Draft Recommendation: Framework for IMT-2020 network architecture (O-043).
- Draft Recommendation: Requirements of IMT-2020 fixed mobile convergence (O-044).
- Draft Technical Report: Unified network integrated cloud for fixed mobile convergence (O-045).
- Draft Recommendation: IMT-2020 network management requirements (O-046).
- Draft Recommendation: Network management framework for IMT-2020 (O-047).
- Draft Technical Report: Application of information centric networking to IMT-2020 (O-048).

3.6 IETF

The Internet Engineering Task Force (IETF) [39] is the standards body that specifies the basic communication protocols to be used in the Internet. The mission of IETF today is to improve the technology so the Internet meets new and future expectations on communication networks.

In recent years, the IETF has worked on a new version of the HTTP protocol. The new version is called HTTP/2, and it provides performance improvements by means of a binary representation of the commands. Other improvements include header field compression and support of multiple exchanges on the same connection. HTTP/2, published as IETF RFC 7540 (May 2015) [40].

On the security side, the HTTP/2 RFC states that TLS version 1.2 or a higher version must be used for HTTP/2 over TLS. The new phase of work also focuses on opportunistic encryption for HTTP. This proposal

makes it possible to run HTTP over TLS and encrypt the communication, without requiring strong server authentication (17 March 2016) [41].

The IETF is also updating the TLS protocol (the latest draft is for TLS is v 1.3, 21 March 2016 [42]). One of the main goals of the new version is to encrypt as much as possible of the handshake messages to reduce the amount of data available to attackers. Another major goal is to reduce the handshake to one round-trip. TLS 1.3 will also update the profiles to address known weaknesses in CBC block cipher modes and RC4.

A new working group has been formed in IETF: the QUIC WG [43]. The aim of the WG is to create a UDP based protocol that would minimize connection establishment, reduce overall latency, support stream multiplexing and multipath communication. For security, the goal is to use TLS 1.3 to protect the QUIC communication.

The Internet of Things (IoT) is one of the areas where IETF has been dedicating a considerable amount of effort. Whilst HTTP can be used for IoT devices, a new lighter weight version of the protocol has been defined for Constrained Devices. That protocol is called “The Constrained Application Protocol (CoAP)”, which is specified in RFC 7252. CoAP is based on the same Representational State Transfer (REST) architecture and provides a generic request/response interaction model similar to the Hyper-Text Transfer Protocol (HTTP). However, unlike HTTP, messages in CoAP are exchanged asynchronously over the unreliable datagram-oriented transport such as UDP with optional reliability.

Datagram Transport Layer Security (DTLS) provides communications privacy for datagram protocols and is based on the standard Transport Layer Security (TLS) protocol that is used widely on the Internet. The CoAP base specification provides a description of how DTLS can be used for securing CoAP. It proposes three different modes for using DTLS, namely: Presharedkey mode (where nodes have per-provisioned keys for initiating a DTLS session with another node), Raw-PublicKey mode (where nodes have an asymmetric-key pair(s) but no certificates to verify the ownership) and Certificate mode (where public keys are signed in certificates by a certification authority). In addition, IETF has also specified an implementation profile for TLS version 1.2 and DTLS version 1.2 that offers communications security for resource-constrained nodes that are part of IoT. The CoAP specification also provides an alternative approach for securing communication with Internet Protocol Security (IPSec). It argues that many constrained devices already have support for link layer encryption in hardware which can be used to make IPSec a viable option in such networks. There is work ongoing in this area with the standardisation of header compression for IPSec [44].

There are also other communication security issues associated with resource-constrained IoT devices that sleep during their lifecycle to save energy. Such IoT devices cannot afford to stay online for large amounts of time to be polled data or support computationally intensive security protocols. To ensure data integrity, authenticity and confidentiality in such devices, the cryptographic protection measures need to be applied directly to the application-layer message objects. This method of communication security is also referred to as “object security”. Relevant drafts are listed in the Reference section.

Access control mechanisms are a necessary and crucial design element to any application's security. Therefore, it is not surprising that IETF is also investigating how web-based access control and authorisation solutions can be applied to resource-constrained devices that are part of the IoT. It is currently defining an authorisation and access control framework for resource-constrained nodes based on the OAuth 2.0 framework, which is currently the de-facto standard for authorisation on the web.

Work is currently ongoing on a draft about “Practical Considerations and Implementation Experiences in Securing Smart Object Networks”. This drafts discusses how to use and implement cryptographic

mechanisms in constrained devices. The current draft[53] has been adopted as a working group document by the LWIG WG.

There is also work ongoing on an EAP method for bootstrapping security for devices with restricted user interfaces and no pre-configured authentication credentials. A draft, Nimble out-of-band authentication for EAP (EAP-NOOB) [45], has been submitted to IETF.

3.6.1 5G-ENSURE opportunities in IETF

In the context of the Internet of Things, a potential contribution to IETF is input to the Authentication and Authorization for Constrained Environments (ACE) working group, which is currently working on adapting OAuth 2.0 to constrained environments. Our input will take in consideration the solution envisioned in the Fine-grained authorization enabler, which relies on OAuth/CWT/COSE mechanisms and 5G credentials to provide secure access control in RCD with minimal communication and low computational overhead. This work aligns well with the current IETF work and could therefore be a valuable contribution to the standardisation process.

3.7 IEEE

IEEE [46] has recently initiated the formation of some projects related to privacy in IEEE protocols. Specifically the creation of project "P802E - Recommended Practice for Privacy Considerations for IEEE 802 Technologies" [47] which is intended to draw up recommendation documents on Privacy in IEEE 802. This group was formed as a result of an IEEE Project Authorisation Request (PAR) from the IEEE 802 EC Privacy Recommendation Study Group. The University of Oxford has been involved with IEEE Privacy activities since it was part of the initial presentations at an IEEE 802 plenary tutorial on Pervasive Surveillance of the Internet, which led to the formation of the IEEE 802 EC Privacy Recommendation Study Group. The IEEE privacy study group to coordinated some MAC randomisation trials at recent IETF meetings in Hawaii (IETF91), and Berlin (IETF92), and at one IEEE 802 standards meeting.

IEEE 5G Initiative has set up research and study groups on cloud-based mobile core, radio analytics, channel modelling, tactile internet, next-generation fronthaul interface. The special interest groups (SIGs) focus on: mmWave, end-to-end security, edge cloud, tactile internet, resilience, end-to-end latency, mobility, network architecture, gigabit service enablement, sensing. 5G-ENSURE has had an initial interaction with Dutta Ashutosh, co-chair of the initiative and also a member of the project's community.

3.7.1 5G-ENSURE opportunities in IEEE

As part of the 5G-ENSURE project, work has continued on P802E project activities by participating in teleconferences and contributing to the working documents. At the present time there are no specific opportunities for direct contributions for the 5G-ENSURE results.

3.8 ONF

The Open Networking Foundation (ONF) tackles the most important issues related to Software-Defined Networking (SDN), collaborating with the world's leading experts on SDN and the OpenFlow™ Standard regarding SDN concepts, frameworks, architecture, and standards.

At the present time there are no specific opportunities for direct contributions for the 5G-ENSURE results.

3.9 NIST

NIST (Network Information Security & Technology) is a non-regulatory federal agency within the U.S. Department of Commerce. The mission of NIST is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security. Relevant to 5G-ENSURE is the Computer Security Division (CSD), responsible for developing standards, guidelines, tests, and metrics for protection of non-national security federal information systems. NIST standards and guidelines are developed in an open, transparent, and collaborative manner that enlists broad expertise from around the world. In February 2014, NIST issued the Framework for Improving Critical Infrastructure Cybersecurity. The Framework, created through collaboration between industry and government, consists of standards, guidelines, and practices to promote the protection of critical infrastructure. Its approach helps owners and operators of critical infrastructure to manage cybersecurity-related risk.

3.9.1 5G-ENSURE opportunities in NIST

During the first period of the project a call has been organized with NIST representatives working within the Computer Security Division. The call objective was to share information on NIST activities on 5G and to share insights on 5G-ENSURE project with the aim of identifying potential synergies. Currently, NIST is not involved in security activities specifically related to 5G. The Wireless Networks Division of NIST is working on three emerging technologies to enable 5G which are Massive Multi-user MIMO, Millimeter-wave Communication Systems, and Ultra-dense Networks.

Specific opportunities for international cooperation directly related to 5G-ENSURE have been identified within NIST.

Some of the NIST standards have been identified as relevant for specific project enablers by the partners of the consortium and a map between the enablers and relevant security standards have been produced and shared with the people of the Computer Security Division. Collaboration with NIST has been expected to increase in this second year. As a follow up of the previous discussions and shared information about 5G-ENSURE enablers and standards map, additional standards has been suggested by NIST to be investigated since relevant for the project enablers. In particular NIST has showed the interest in learning more about some specific enablers such as IoT and Privacy Enhanced Identity Protection.

To enable deeper discussion on the enablers of interest, an extended call was organized with NIST in late April 2017. Five NIST representatives and 9 partners attended the call, chaired by technical coordinator Pascal Bisson.

4 of the 5G-ENSURE enablers have been presented in more details to NIST.

- Privacy Enhanced Identity Protection (Telecom Italia).
- Device identifier(s) privacy/ (University of Oxford).
- Fine-grained Authorisation Enabler (Thales).
- IoT/Group-based authentication (SICS).

Several questions were raised to better understand the solutions and how they integrate/interact with the current network procedures.

NIST recognised the value of the solutions also from the technical point of view. Interaction with NIST will continue in terms of an exchange of view on any enabler features, specifications and underlying standards. A physical side-meeting will be organised between 5G-ENSURE and NIST people during ETSI Security Week

in June to discuss enablers of interest continued in R1 but also the new ones in R2. These actions will help in promoting the European 5G security research companying NIST.

3.10 NGMN P1 WS1 5G Security

The NGMN Alliance is a mobile operators-driven global partnership that develops and promotes operator requirements to meet mobile-broadband users' needs and expectations.

Since September 2016, it is a global partnership of 28 leading mobile operators as members, 44 leading technology vendors as contributors, and 27 universities or research institutes as advisors. It drives global harmonisation and convergence of industrial standards and initiatives, by working on requirement levels and providing guidance to SDOs for standards development.

The NGMN Alliance has been focusing on 5G since 2015 and has established its intended role in 5G development.

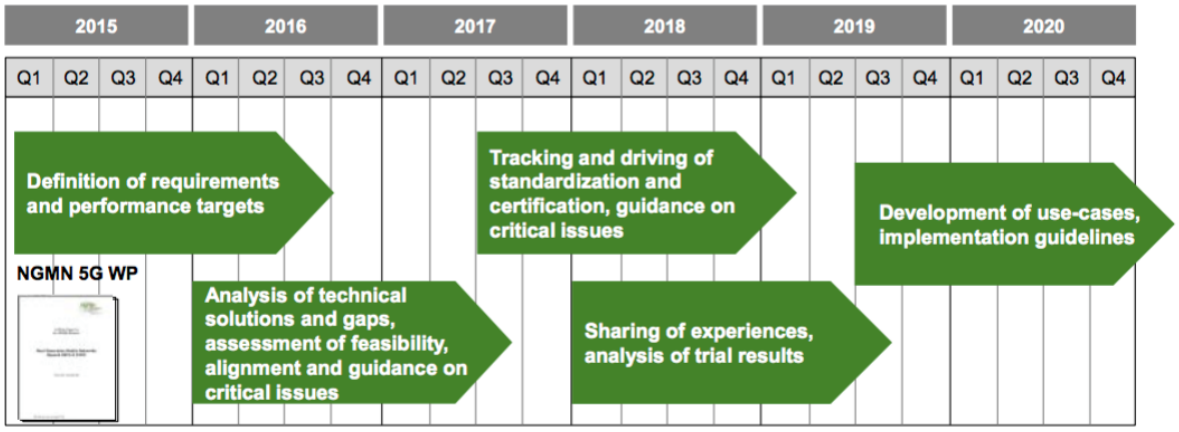


Figure 9: NGMN Role in 5G Development

Published in February 2015, the well-received NGMN 5G White Paper [48], focuses on consolidated 5G end-to-end operator requirements to satisfy customer needs and to drive a successful ecosystem for the markets in 2020 and beyond:

> "5G is an end-to-end ecosystem to enable a fully mobile and connected society. It empowers value creation towards customers and partners, through existing and emerging use cases, delivered with consistent experience, and enabled by sustainable business models."

During the June 2015 Forum and Board meetings, the NGMN Alliance set up a 5G Work Programme to support 5G-related standardisation, building on the NGMN 5G White Paper. Its project teams will produce deliverables to share with all relevant industry-organisations, SDOs and research groups on

- 5G requirements and design principles.
- Analysis of potential 5G solutions.
- Assessment of future use cases and business models.

Figure 10: NGMN 5G Work Programme

In particular, 5G security matters are addressed by the 5G Security group within P1 (Project 1) "Requirements & Architecture" WS1 (Work Stream 1) "Architecture". The 5G Security group started as part of the NGMN 5G Work Programme established in June 2015 to support 5G-related standardisation. The group has been led by Orange and co-led by Vodafone. It concluded its mission and ceased its operation in August 2016, after having produced totally four deliverables and sent them via NGMN liaison to 3GPP as input to SA3 and SA2. These deliverables provide high-level 5G security considerations and recommendations, while avoiding specific solutions, with an objective of helping SDOs to develop 5G specifications with proper security measures.

The first deliverable is the document "Security Considerations for Virtualisation in 5G", which is 5G-relevant but not 5G specific. In particular, it highlights the importance of trustworthiness of VNFs and virtualisation platforms, security of their interactions, and auditing of their activities.

The second deliverable is the document "5G Security Recommendations Package #1", which focuses on better protection of the access network as well as the security risks of DoS attacks in the 5G context.

The third deliverable is the document "5G Security Recommendations Package #2: Network Slicing". It highlights the security threats associated with the network slicing concept in 5G, although the concept is still subject to clarification of its eventual architecture and functional capabilities.

The fourth, and last, deliverable is the document "5G Security Recommendations Package #3: Mobile Edge Computing / Low Latency / Consistent User Experience". It focuses on the security risks arising from the support of mobile-edge and low-latency applications in 5G. It also highlights the security challenges in providing consistent user experience across all kinds of radio access in a 3GPP network. In particular, it suggests that the low latency targets need to be reviewed carefully for the envisaged 5G low-latency applications, because they may impose undesirable compromise on the security measures.

In its last meeting, the NGMN Board agreed to establish a Security Competence Team (SCT) within NGMN.

The set-up of the future security work (based on the SCT) will not be structured like a project (i.e. milestone-based delivery) but as a permanent/standing group of experts in NGMN with the tasks

a) to support other work-streams on Security-related questions.
b) to work on specific Security-items in case identified.

The objective of the SCT might not only be the delivery of an agreed consensus view on a specific topic (i.e. finalisation of a White Paper) but could also be just an open discussion and analysis of certain issues.

Hence, one of the immediate first tasks of the team will be to discuss and to review existing proposed security topics and issues, and to decide which and how items should be addressed.

3.10.1 5G-ENSURE opportunities in NGMN

The work of NGMN P1 WS1 5G Security group has concluded last year. The findings has been delivered to 3GPP SA3 and SA2, as part of the documents produced in which most of the 5G-ENSURE project partners has been contributed Thhe insights from the deliverables have also be leveraged by 5G-ENSURE project in developing 5G security enablers.

In the next period SCT could be another opportunity to bring the project's knowledge and results gained in 5G security. The plan is to monitor it as part of 5G-ENSURE standardisation work.

3.11 GSM ASSOCIATION

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with almost 300 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai and the Mobile 360 Series conferences.

3.11.1 Fraud and Security Architecture Group (FSAG)

Recently, several discussions within the GSMA FSAG group have focused on Customer Privacy issues in mobile network. At the FSAG#36 meeting in London at the end of June 2016, Fabian van den Broek, Radboud University of Nijmegen and Shafiul Alam, Royal Holloway - University of London both presented possible approaches that could improve user privacy over the air interface. Both researchers agreed to produce a common description of their individual proposals to detect IMSI catchers. This contribution was presented during the regular FSAG conference call (17th October 2016). It described possible system enhancements to 3G and 4G networks that reduce the privacy impact of IMSI catchers without requiring any changes to the serving networks or to the mobile phones. In both the enhancements, changeable (temporary) IMSIs are used to help protect privacy; therefore, attacks which obtain an IMSI (i.e. IMSI catching) will only obtain a changing identity, which is of lesser value due to its temporary nature. The analysis was used to brief other GSMA working groups and to serve as the basis to propose possible solutions for the SA3 study item.

Piers O'Hanlon and Ravi Borgaonkar, Computer Science Department, University of Oxford presented a work on "WiFi-based IMSI Catcher" to the GSMA's Fraud and Security Architecture Group (FSAG) conference call (26 septmber 16). They discovered two issues that can result in the exposure of the IMSI on WiFi networks. They effectively enable the creation of a low-cost WiFi-based IMSI catcher (which may be created using the appropriate software on a WiFi enabled laptop/mobile). They enable an attacker to track targets devices by their IMSI (even when out of mobile/cellular coverage and regardless of whether WiFi MAC randomisation is used). The results of this work is in part related to the activities conducted within the 5G-ENSURE project in the context of privacy issue in 5G network.

3.11.2 5G-ENSURE opportunities in GSMA

The GSMA is not a standards body but its remit as an industry association can help influence the specification of 5G, by building consensus among specific mobile operator interests in scope of the 5G-ENSURE project.

The recent discussions within the FSAG GSMA showed that the attention to the customer privacy issues in the current and next generation network is growing and that some reaserchers are working to identify possible and feasible solutions. 5G-ENSURE has exploited this opportunity by reporting on the work performed in the privacy context. During the GSMA FSAG#43 meeting on 6-7 December in Bonn, the Privacy Enhanced Identity Protection Enabler, developed in 5G-ENSURE, has been presented. The solution has taken lot of interest and valuable feedback have been received.

The plan is to continue to follow the discussions within this group and also to provide update on the next enhancements which will be relased on privacy topics.

4 Measurable Impacts for 5G Security Standardisation

Main Takeaways

- 5G-ENSURE provides some requirements for 5G privacy to 3GPP SA3 study work on 5G Security.
- Two of the 5G-ENSURE enablers proposed to 3GPP SA3 now under discussion and evaluation.
- The 5G-ENSURE Standardisation Plan has been well received by the community, increasing interest in related activities. This is a good basis for future discussions at the 2nd International workshop and beyond.

4.1 5G-ENSURE Standardisation Plan

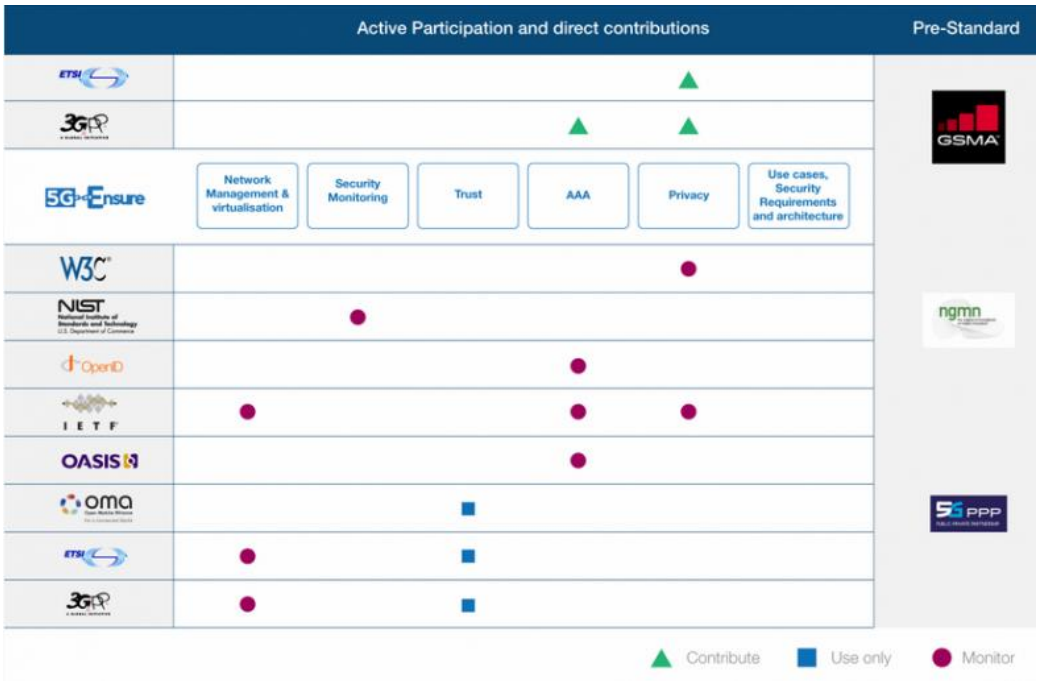
The Task 5.1 (Standardization) maintains and updates the Standardisation plan of the project following the evolution of the project research topics and the standardirzation ecosystem.

The following picture describes the current 5G-ENSURE standardisation plan. The 5G-ENSURE Standardisation Plan is aimed at ensuring contributions to 5G standardisation are both timely and targeted, with partners pursuing an industry-led approach and by down-streaming relevant research results into the standardisation process. The 5G security standardisation plan focuses on:

- Contributions to the most relevant standards bodies, particularly 3GPP and ETSI.
- Monitoring of on-going studies on 5G standardisation.

The ultimate goal is help create some kind of harmonisation within the standardisation ecosystem. 5G-ENSURE has also undertaken actions with other standards bodies to share project results of interest. The on-going collaboration with NIST is one example of this.

Figure 11: 5G-ENSURE Standardisation plan



4.2 Contributions to target SDOs

The following lists all the contributions prepared by the project members and submitted to the standardisation meetings.

Standardisation Organisation	Title of Contribution	Meeting detail	Short link to document
3GPP SA3	Study on Architecture and Security for Next Generation System	SA3#821-5 February 2016	http://ow.ly/N4bk30agl2z
3GPP RAN	pCR on Section "Security and Privacy" of TR38.913 - Requirements on user identity	RAN#71 March 7 - 10, 2016	http://ow.ly/ju9l30agl5m
3GPP RAN	pCR on Section "Security and Privacy" of TR38.913 - Requirements on security visibility	RAN#71 March 7 - 10, 2016	http://ow.ly/lheD30agl8i
3GPP RAN	pCR on Section "Security and Privacy related requirement relevant for Radio Access" of TR38.913 – Requirements on radio signaling messages	RAN#71 March 7 - 10, 2016	http://ow.ly/mZJn30aglbY
3GPP SA3	pCR - New security area for subscriber privacy	SA3#83 9-13/05/2016	http://ow.ly/MeUs30aglUB
3GPP-SA3	pCR - New key issue for subscriber identifier protection	SA3#83 9-13/05/2016	http://ow.ly/QqLA30agmuh
3GPP-SA3	pCR to draft-TR 33.899 on New security area for AAA	SA3#83 9-13/05/2016	http://ow.ly/PxTu30agnaS

3GPP-SA3	pCR to draft-TR 33.899 on Core Network Control Plane Security	SA3#83 9-13/05/2016	http://ow.ly/1Vh930ago3T
3GPP-SA3	pCR to draft-TR 33.899 on New security area for network virtualization security	SA3#83 9-13/05/2016	http://ow.ly/4IkR30agokp
3GPP-SA3	pCR to draft-TR 33.899 on Radio Access Network security	SA3#83 9-13/05/2016	http://ow.ly/7xsg30agotn
ETSI-TC-CYBER	Access control mechanisms and policy rules for PII protection on smart devices, cloud and mobile services	CYBER#7 15-17 June	http://ow.ly/hnWQ30agoDP
ETSI-TC-CYBER	PII Protection in mobile and cloud services	CYBER#7 15-17 June	http://ow.ly/ZzpC30agoMI
3GPP-SA3	Enhancing the concealment of permanent or long-term subscriber identifier	SA3#84 25.-29.07.2016	http://ow.ly/glH130agoRu
3GPP-SA3	Deletion of key issue #7.1 on subscriber identifier privacy	SA3#84 25.-29.07.2016	http://ow.ly/VZmH30agoVB
3GPP-SA3	New privacy key issue on transmitting permanent subscriber identifiers only when needed	SA3#84 25.-29.07.2016	http://ow.ly/fkPU30agoYD

Please note that the 3GPP documents are public, whereas the ETSI working documents are for ETSI members only.

4.3 Contribution to ITU-T and EC

Following an exchange with ITU-T, 5G-ENSURE identified an opportunity to contribute to Study Group 17 (Security) with the aim of filling the knowledge gaps identified.

The 5G-ENSURE analysis covers:

- Analysis of the current standardisation landscape.
- Groups and activities with particular reference to 3GPP and ETSI.
- Opportunities for 5G-ENSURE, especially in the ETSI activities.
- 5G-ENSURE Standardisation Plan.
- 5G-ENSURE Outputs: security and privacy enablers; reference security architecture; test-bed; and trust model.

The analysis was also sent to Unit E1 – DG CONNECT.

4.4 5G PPP Pre-standardisation Work Group

The aim of the WG is to identify standardization and regulatory bodies to align with (e.g. ETSI, 3GPP, IEEE and other relevant standards bodies) and to develop a roadmap of relevant standardization and regulatory topics for 5G. Moreover, one of the main task of the group, is to keep traces of the direct contributions made by H2020 funded projects in order to evaluate the real impact of on the standardisation of 5G. Unfortunately, as discussed and agreed during various 5G-PPP Pre-Standardisation WG calls, it is very difficult to assess the real impact of the direct (and indirect) contributions. In fact:

- Usually a contribution that is treated can easily be revised many times, merged with other documents, etc. before a final outcome is known. Documents by that time may have changed beyond recognition. Sometimes some revisions aim simply to correct a spelling mistake.
- On the other hand, discussion documents generally get 'Noted' regardless of what impact they have had. Listing the official outcome of documents as per 3GPP meeting minutes often does not reflect the impact a document has had. If we base how the contribution was used on input other than the meeting minutes, it becomes a source for arguments on what the impact really was.
- An exception could be to indicate whether documents were 'not handled'. But even there, you can have different interpretations. E.g. was it not handled because the document did not address one of the agenda items for the meeting, or was it not handled because there were more documents on the agenda than time permitted to handle. In the first case impact is almost zero, in the second case the document is likely to have been read by meeting attendants and taken into consideration.

Anyway the collaboration with the 5G-PPP Pre-Standardization WG has **allowed** 5G-ENSURE project to to share with the other H2020 funded project**s** the list and the status of the direct contributions presented, **provide** information about standardi**s**ation topics and events and participate **in** the elaboration of whitepaper**s** and workshops proposals**.**

5 Measurable Impacts for Dissemination of Results and Outputs

Main Takeaways

- Key role in 1st of a series of IEEE workshops on security in SDN and NFV.
- Original research on theory and applications of information security at peer-reviewed conference.
- High interest and 20 press clippings generated from Black Hat Europe, increasing awareness of mobile privacy issues.
- High levels of collaboration with the 5G PPP and its groups, including 3 white papers in the period covered. High visibility of common 5G PPP activities further demonstrating this.
- High visibility of 5G-ENSURE 5G test-bed at trade fairs as key to supporting its sustainability.
- Timely updates on 5G-ENSURE outputs shared across all stakeholder groups through in-house newsletters and social media.

5.1 Technical Achievements, Scientific Conferences and Publications

5.1.1 Impacts for 5G-ENSURE Outputs

5G-ENSURE makes regular updates on the project's website, on social media and LinkedIn, as well as through its newsletters. Updates are also shared during the monthly 5G PPP COMMS Group calls and published on www.5g-ppp.eu as relevant. All these activities combine to provide important additional visibility and are expected to increase considerably in the last 6 months of the project. The organisation of the 2nd International Workshop within ETSI Security Week also provides additional external visibility of the project.

Table 3: 5G-ENSURE Outputs

Website Update	Related Link and related visibility
5G-ENSURE enablers (April 2017)	http://5gensure.eu/security-enablers 482 views with over 160 additional views via March 2017 newsletter (542).
5G-ENSURE Standardisation Plan (December 2016)	http://5gensure.eu/standardisation-5g 884 views with over 300 additional views via LinkedIn after sharing the plan (1184)
5G-ENSURE reference security architecture (November 2016)	http://5gensure.eu/5g-ensure-architecture 1089 views
Publications and deliverables (periodical updates)	http://5gensure.eu/deliverables and http://5gensure.eu/publications 2,670 views
Service Suite and test-bed	http://5gensure.eu/5g-ensure-testbed

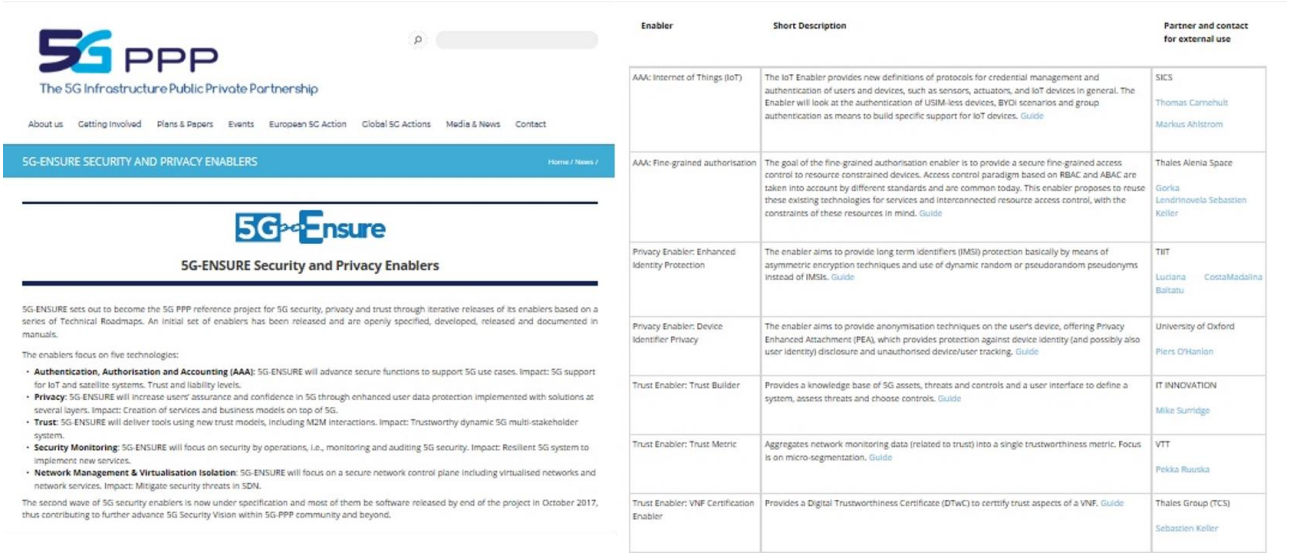
	634 views
About	http://5gensure.eu/project-vision 1215 views

The figure below is one example of external interest in the 5G-ENSURE Technical Roadmap for the enablers, leading to future F2F enagement at the 2nd International Workshop.

Figure 12: Testimonial on 5G-ENSURE Enablers

The next figure shows an example of visibility of outputs on the 5G PPP.

Figure 13: Sample of Visibility on 5G PPP



5.1.2 Scientific Conferences

The tables below show the main impacts of 5G-ENSURE at international technical conferences and related publications.

Table 4: Impact of Black Hat Europe

Event	Black Hat Europe 2016
Date and Venue	3-4 November 2016 in London.
Focus	Technical event series on global information security.
Stakeholder category/ies	Professionals and researchers for deeply technical hands-on sessions and discussions.
5G-ENSURE role and outcomes	University of Oxford presentation and demo of WiFi-based IMSI Catcher, WiFi-IMSI-Catcher-BH.3-4Nov16.pdf. Partners: Piers O'Hanlon and Ravishankar Borgaonkar
Web links	http://5gensure.eu/events/oxford-university-presents-wifi-based-imsi-catcher-black-hat-europe
Impact	Interviews with journalists generated 20 clippings in EU and international online magazines for business and IT security. Black Hat were among the top social media engagements, highlighting both the talk and some of the press coverage. This press coverage plays a key role in raising awareness of privacy issues in mobile networks and devices among a wider public. Press coverage: http://5gensure.eu/press-coverage/wifi-based-imsi-catcherAn interview with Piers O'Hanlon published as a LinkedIn blog post was also important in raising awareness of these issues, while also offering an opportunity to promote the work of the University of Oxford within 5G-ENSURE. The full list of clippings are included in Annex 1. LinkedIn post: https://www.linkedin.com/pulse/privacy-issues-mobile-networks-interview-piers-ohanlon-network

Table 5: Impact of 1st IEEE Workshop on NFV and SDN

Event	1st International Workshop on Security in NFV-SDN (SNS2016) IEEE
Date and Venue	7 November, Palo Alto, U.S. Co-located with the 2nd IEEE Conference on Network Function Virtualization & Software Defined Networks (IEEE NFV-SDN'2016)
Focus	Insights into 5G security research and standardisation activities, discussing the 5G security challenges and opportunities. Putting into perspective the emerging and promising Software Defined Security,
Stakeholder category/ies	Industry representatives and researchers working on SDN/NFV, and security.
5G-ENSURE role	The workshop featured 6 selected workshops and 2 invited keynotes (Nokia, Thales) with 40 participants, which is more than expected for a first workshop (the conference was attended by around 200 participants with a 25% acceptance rate).

	Good levels of exchange and keynotes well received. Nokia played an active role in the discussions on virtualisation and softwarisation in mobile networks. Nokia also highlighted the focus of 5G-ENSURE and its outputs, such as the security and privacy enablers, the security architecture and standardisation efforts. Partner: Linas Maknavicius (Nokia), chairing SNS'2016 intro - Cover slide.pdf; SNS'2016 workshop Program Presenters.pdf; SNS'2016 Keynote1 - 5G Virtualization Security Challenges - Nokia.pdf
Web links	http://5gensure.eu/events/1st-international-workshop-security-nfv-sdn-sns2016
Impact	Insights on the role of NFV and SDN in transforming the telecommunications industry. Sharing of new knowledge on security and technical challenges, as well as the benefits gained, such as faster time to roll out new services, scalability and performance. The success of the event helped pave the way for a 2nd workshop in conjunction with the 3rd IEEE Conference on Network Softwarisation (IEEE NetSoft 2017) in July 2017. Event announcement: http://5gensure.eu/events/second-international-workshop-security-nfv-sdn-july-2017-call-papers

Table 6: Impact of National Security and Resilience Conference

Event	National Security and Resilience Conference 2016
Date and Venue	09 November 2016, London, UK
Focus	UK conference on security and trust in the digital economy.
Stakeholder category/ies	Government and industry
5G-ENSURE role and outcomes	IT Innovation gave a talk on trust and security modelling, including the Trust Builder from 5G-ENSURE. The updated flier was also distributed.
Web link	http://www.nsr-conference.co.uk/
Impact	The conference was particularly timely in terms of the publication of the UK's Cyber Security Strategy 2016-2021, a 5-year action plan based on an in-depth review of the previous strategy period (2011-2015 with annual updates). Of particular interest is the new emphasis on mobile networks as one of the most important critical infrastuctures in cyber space. The strategy highlights the importance of implementing strong cyber security strategies and risk management techniques within the industry. This is a promising topic for discussion also for the 2nd International Workshop during the ETSI Security Week in June.

Table 7: Impact of Ericsson Annual Security Day

Event	Ericsson Annual Security Day

Date and Venue	5 October 2016
Focus	Provide selected employees with an update on the security risk landscape and encourage a cyber security culture within the organisation.
Stakeholder category/ies	5G researchers
5G-ENSURE role	The event featured a 5G-ENSURE poster and discussions on the project. Ericsson took the opportunity to share insights into collaborative research on 5G security, and the new approaches it requires. 5G-ENSURE shared key features of the in-house event on social media as a best practice for other organisations to adopt.
Web link	https://www.ericsson.com/research-blog/security/5g-security-unlike-anything-youve-seen/
Impact	This is a yearly recurring event which usually gathers around 100-150 Ericsson people working with security, and one that should be replicated in EU to build a cyber security culture right across the organisation. It constitutes a good practice in view of efforts by ENISA and others to build a cyber security culture in EU organisations, http://www.5gensure.eu/news/ericsson-5g-security

Table 8: Impact of HITS Workshop on future mobile services

Event	HITS Workshop on future mobile services
Date and Venue	19–20 October
Focus	HITS, the High Quality Networked Services in a Mobile World research project, held its annual workshop during which researchers and participating representatives from business gathered to present ongoing research and to discuss the further development of the project.
Stakeholder category/ies	5G stakeholders from industry and researcher
5G-ENSURE role	Mats Näslund from Ericsson gave a talk promoting 5G-ENSURE results, with a particular focus on 5G security challenges and the approach adopted by the project. The talk was promoted on Twitter and Linkedin.
Web link	https://www.kau.se/en/cs/news/workshop-future-mobile-services
Impact	The LinkedIn post received a lot of attention within this professional network, demonstrating interest to community members.

Table 9: Impact of 19th Annual International Conference on Information Security and Cryptology

Event	19th Annual International Conference on Information Security and Cryptology

Date and Venue	30 November – 2 December 2016, KIISC (Korean Institute of Information Security and Cryptology)and NSR (National Security Research Institute), Korea
Focus	Original research on theory and applications of information security.
Stakeholder category/ies	Researchers from academia and industry working on information security.
5G-ENSURE role	SICS paper entitled: A Secure Group-Based AKA Protocol for Machine-Type Communications. Authors: Rosario Giustolisi, Christian Gehrmann, Markus Ahlström, Simon Holmberg.
Web link	http://www.icisc.org/icisc/asp/cfp.html
Impact	Excellent forum for disseminating new research in the field.

5.1.3 Publications in top-tier journals

The table below shows the impact of 5G-ENSURE dissemination of research findings through publication in top-tier journals. All publications are available at: http://5gensure.eu/publications.

Table 10: 5G-ENSURE Publications in Top Tier Journals

Paper Title	Authors	Journals/conference proceedings
TruSDN: Bootstrapping Trust in Cloud Network Infrastructure	Nicolae Paladi and Christian Gehrmann 5G-ENSURE partner: SICS	In Proc. of the 12th EAI International Conference on Security and Privacy in Communication Networks (SECURECOMM 2016).
White Rabbit in Mobile: Effect of Unsecured Clock Source in Smartphones	Shinjo Park, Altaf Shaik, Ravishankar Borgaonkar, and Jean-Pierre Seifert 5G-ENSURE partner: Ravishankar Borgaonkar, University of Oxford	6th Annual ACM CCS 2016 Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM).
Analysis of Trusted Execution Environment usage in Samsung KNOX	Ahmad Atamli-Reineh, Ravishankar Borgaonkar, Ranjbar A. Balisane, Giuseppe Petracca, Andrew Martin 5G-ENSURE partner: Ravishankar Borgaonkar, Andrew Martin	In Proc. of the Workshop on System Software for Trusted Execution (SysTEX 2016)
Runtime Verification of Temporal Properties over Out-of-order Data Streams. The paper describes the underlying theory and algorithms of one of the Task 3.5 enablers.	David Basin, Felix Klaedtke, and Eugen Zalinescu.	Computer Aided Verification (CAV).

5.1.4 Showcases at Trade Fairs

5.1.4.1 9th International Forum on Cyber Security

Table 11: Impact of 9th International Cyber Security Forum (FIC2017)

Event	9th International Cyber Security Forum (FIC2017)
Date and Venue	24-25 January , Lille (France)
Focus	Research and innovation in cybersecurity more focused, this year, to the uses enabled by the digital transformation where more intelligent is requested to meet the challenges of an increasingly connected world.
Stakeholder category/ies	5000 IT professionals, Industry, Universities and innovative SME.
5G-ENSURE role and outcomes	b-com exhibition stand showcased 5G-ENSURE results and its 5G Test-Bed specifically created within the project and set-up to satisfy the needs and requirements of the security enablers developed. The test bed envisions what a 5G network could be at a small scale. A new, marketing-facing flier was produced with b-com for distribution at the event. The flier focuses mainly on the 5G test-bed that was presented there.
Web links	https://www.forum-fic.com/site/GB/Forum/2017_Program,C59984,I60520.htm?KM_Session=d93fa1622498dd3f653b73cff62d6616%20%E2%80%8B
Impact	5G-ENSURE conducted an interview with b-com prior to the event and published it as an article on LinkedIn. b-com received good visibility on the social media channels and also worked in synergy by sharing updates and photos during the event.

Table : Impact of 9th International Cyber Security Forum (FIC2017)

5.1.4.2 Mobile World Congress 2017

Table 12: Impact of Mobile World Congress 2017 (MWC17)

Event	Mobile World Congress 2017 (MWC17)
Date and Venue	27-02 March, Barcelona
Focus	5G and IoT and cloud. Lot of exhibition and a number of use cases were on showcase at MWC17, ranging from health services to IoT-enabled camera drones, location services to smart lighting, fitness to augmented reality/virtual reality (AR/VR), smart factories to autonomous cars.
Stakeholder category/ies	Trade Fair: Industries, SMEs, mobile operators, vendors
5G-ENSURE role and outcomes	**5G-ENSURE** contribution to 5G PPP Vision WG paper presented at MWC'17 getting inputs from the Security WG white paper content. 5G-ENSURE was represented through the **B-COM** stand, circulating the flier on the 5G test-bed, the 5G PPP white paper inserted in a specially-designed folder by 5G-ENSURE.

Web links	https://www.mobileworldcongress.com/start-here/agenda/ https://www.mobileworldcongress.com/exhibitor/b-com/ https://5g-ppp.eu/5gia_event_at_mwc2017/.
Impact	5G-ENSURE news piece on partner takeaways from MWC17: http://5gensure.eu/news/5g-ensure-takeaways-mobile-world-congress-2017 Journalists from TechNative captured groundbreaking research from our French SME partner in a Q&A with Michel Corriou, Networks and Security director. The article highlights b<>com's focus on certain key 5G technologies like SDN, cloudification, and the convergence of radio access networks. Through the involvement of investor-members, the company is at the crossroads of issues raised by academic research and needs expressed by industry. b<>com promoted the 5G-ENSURE 5G test bed, enablers and security-by-design approach during the event, and also supported the distribution of the new 5G PPP White Paper "Innovations for new Business Opportunities". Social Media Coverage: top engagement with 5G Americas Latin America, 5G Americas Brasil, EUBra-BIG SEA and RedeRNP. On the policy front, MWC17 attracted attention from Roberto Viola (Director General at DG Connect), the Digital Single Market and EC Net Technologies while tweets on b<>com were shared by Startup Europe and Networld 2020 SME. Top engagement also with the Mobile World Congress. The article also featured in the March newsletter, with a round-up published also as an article on LinkedIn.

5.2 Collaboration and Showcases with 5G PPP

5.2.1 5G PPP Workshops and Meetings

Table 13: Impact of Global 5G

Event	Global 5G
Date and Venue	9-10 November 2016, Rome
Focus	The conference agenda features high-level policy and industry keynotes with plenty of opportunities to debate key topics spanning spectrum, standards and deployment of 5G. The event in particular covers the main results of European 5G-PPP projects.
Stakeholder category/ies	5G stakeholders from industry, research, standards bodies and policy makers from around the globe to define actions to key to enabling the so-called 5G EcoSphere.
5G-ENSURE role	5G-ENSURE hosted an exhibition stand featuring a TIIT demo on privacy, a new 5G-ENSURE video, an updated flier on the main project outputs, a new flier on 5G security standardisation, and an updated poster. The 5G-ENSURE technical coordinator, Pascal Bisson, attended the 5G PPP Technology Board meeting, where he presented the 5G-ENSURE “golden nuggets”: enablers, test-bed and security architecture, which was co-produced by the

	Consortium in October 2016. The 5G PPP Annual Journal with an introduction from Gunther Oettinger was also distributed during Global 5G. The journal provides an update on 5G PPP projects' achievements, including 5G-ENSURE.
Web link	http://5gensure.eu/events/5g-ensure-showcase-second-global-5g-event
Impact	5G-ENSURE gained new insights into the security challenges for Industry 4.0 verticals, international initiatives on 5G, and work within the 5G PPP (research, industry, cross-project activities). 5G-ENSURE interacted with stakeholders from industry, the US Federal Communications Commission (FCC), and peer projects to discuss future steps.

5.3.2 5G PPP Cross-project workshop

Table 14: Impact of Cross-Project Workshop

Event	Cross-Project Workshop organised by METIS-II.
Date and Venue	6-7 February 2017, Athens
Focus	The workshop brought together most of the 5G PPP phase 1 projects. The agenda featured overall RAN Design and Architecture, Network Slicing, Security, Air Interface Design, Complexity, Performance and use cases. Presentations and discussions looked into scenarios and evaluations of the 5G system and 5G Architecture. Participants also discussed overall progress of 5G PPP phase 1 projects, which shared their understanding of how 5G fits together, with the aim of aligning project perspectives at the European joint programme level.
Stakeholder category/ies	5G PPP peer projects, including representatives from research and industry. EC policy makers.
5G-ENSURE role	5G-ENSURE technical coordinator, Pascal Bisson (Thales) chaired the session on security and also presented the main findings and outputs of the project. 5G-ENSURE chaired the Security Session. The discussion with also representatives from CHARISMA, METIS-II, and SUPERFLUIDITY focused on major security issues in 5G and the way these 5G PPP projects are addressing them. 5G-ENSURE presentation was used to raise awareness among other projects on assets developed (Golden nuggets). Presentation was overall very welcome/appreciated. 5G-ENSURE promoted the event as part of a joint action within the 5G PPP COMMS Group, both on the project website and via the social media channels.
Web link	http://5gensure.eu/events/5g-ppp-cross-project-workshop-6-7-february-2017-athens
IMPACT	Very good level of participation most of the 5G-PPP Projects Phase 1 were there and represented (some with 2-3 representatives). 5G-ENSURE published an outcomes news piece on the project website, highlighting the main discussion points and outcomes. The news piece also featured in the March 2017 of the 5G-

	ENSURE newsletter. http://5gensure.eu/news/technical-outcomes-5g-ppp-cross-project-workshop

5.4 Contributions to 5G PPP Work Groups

5.4.1 Knowledge Sharing and Consensus Building

Security is a transversal matter impacting many domains and this why 5G-ENSURE is active in more 5G-PPP WG. As part of its co-operation with 5G-PPP, 5G-ENSURE has contributed to many of the whitepapers produced within the followed WGs, in order to provide its security perspective.

Within the 5G PPP Work Groups, 5G-ENSURE has so far targeted the following WGs:

- Security WG as chair (Thales, Orange)
- Pre-standardisation WG (TIIT).
- Architecture WG (Ericsson).
- Vision and social challenges (IT Innovation).
- 5GPPP Network Management & Quality of Service Working Group (NEC).
- 5G-PPP Cross-project use cases WG (Nokia).
- COMMS Group (Trust-IT).

Information and updates on these WGs are available on the project website: http://5gensure.eu/5G PPP-wgs. The table below provides a summary of the outcomes achieved so far.

Table 15: 5G-ENSURE Contributions to 5G PPP Groups

5G PPP SECURITY WORK GROUP	
Co-chairs: Jean-Philippe Wary, Orange and Pascal Bisson, Thales	5G-ENSURE leads the WG on 5G security within the 5G PPP. **Objectives**: Bring together the projects within the 5G PPP that have a common interest in the development and progression of topics related to security. Ensure, to as great an extent as possible, that the projects are working in a complementary manner towards consistent goals, exchanging ideas, minimising the duplication of effort, contributing to relevant standards, and, where possible, co-operating on the development of compatible components, demonstrators, the exchange of data, results and the interworking of communication layers, where applicable. Members: Membership is open to any project with a primary focus on security in scope with the WG's ToR. Current members include: 5G-ENSURE, 5G NORMA, SPEED-5G, 5GEX, CHARISMA, CogNet, SELFNET, Virtuwind, SeSAME. **Outcomes**:

	Q2 2016: Contributions to 5G-ENSURE public consultation on 5G security; sharing of 5G-ENSURE results to encourage re-use and sharing of newly acquired expertise within the 5G PPP. Plans Q4 2016: the WG has worked to the "*5G-PPP Phase 1 Security Landscape*". The paper that will be publicly released in April, describes the 5G-PPP Security Landscape of Phase 1 projects, i.e. what is in scope and covered by 5G-PPP Phase 1 Projects from the specific viewpoint of 5G Security. Objective of this whitepaper is to present the way 5G security has been addressed by providing the rational but also to pave the way forward for Phase 2 Projects, for them to leverage on the achievements resulting from the previous phase. A proposal for workshop "5G Security: Phase 1 landscape and foreseen evolutions" has been submitted at EuCNC17 and accepted. **Future steps:** WG Security workshop organization at EUCNC17 and also organization of the 5G SEC WG Physical Meeting. Objective is also to have on-board new Phase II Projects interested and to ensure overall sustainability of the SEC WG (transfering the chair and co-chair – while staying involved as Phase I project)
5G PPP PRE-STANDARDISATION WORK GROUP	
Chair: Olav Queseth, Ericsson	**Objectives**: Identify standardisation and regulatory bodies to align with e.g. ETSI, 3GPP, IEEE and other relevant standards bodies, & ITU-R (incl. WPs) and WRC (including e.g. ECC PT1). Develop a roadmap of relevant standardisation and regulatory topics for 5G: evaluate existing roadmaps at international level and propose own roadmap for 5G being aligned at international level. Influence pre-standardisation on 5G and related R&D: potentially propose where topics should be standardised; influence timing on R&D work programs (e.g. EC WPs). **5G-ENSURE inputs**: Q1 2016: Sharing of project's vision and activities. Contributions to the message on standardisation at MWC2016 (February) by drawing attention to security and privacy aspects. Q2 2016: WG coordinator active participation at 5G-ENSURE 1st International Workshop on 5G Security Standardisation, bearing testimony to valuable contributions, including use cases covering very diverse security requirements in 5G networks. Q2 2017: Elaboration of a new whitepaper aimed to describer the impact of the H2020 funded project on the 5G Specification during the phase 1. The

	document will be ready in June 2017 during the EuCNC conference in Finland. **Future steps**: sharing of hands-on technical results and updates on contributions to standardisation efforts. Contribution to WG Roadmap and alignment of 5G-ENSURE roadmap for security standardisation.
5G PPP ARCHITECTURE WORK GROUP	
Chair: Simone Redana, Nokia	**Objectives**: Serve as a common platform to facilitate the discussion between 5G PPP projects developing architectural concepts and components. Foster the discussions on the basis of the KPIs described in the 5G PPP contract. Facilitate consensus building on the 5G architecture. **5G-ENSURE inputs**: Q2-3 2016: Contribution to the 5G PPP White Paper "View on 5G Architecture" (final version, July 2016). **Future Steps:** A set of workshops being planned to allow projects to show updates to their architectures. 5G-ENSURE has requested slot on April 10
5G PPP VISION & SOCIETAL CHALLENGES WORK GROUP	
Jean-Sebastian Bedo, Orange	Develop a consensus in Europe on 5G systems / infrastructures / services, Identify vertical application domains which would benefit from 5G (views of other sectors on 5G requirements) and associated challenges, **5G-ENSURE inputs**: The need for a well-defined but also flexible trust model, enabling but not enforcing a very flexible approach to use network slicing within and between domains, and even slicing of slices to support agile and complex business relationships within vertical sectors The need for security to be maintained and demonstrated while seeking other improvements in agility, scalability and performance, some of which may be easier to achieve by removing or bypassing security features. The WG has released a paper “5G Innovations for New Business Opportunities” presented and distributed at MWC’17. 5G-ENSURE has led a chapter on ‘A Secure and Trustworthy Network’ and has also contributed to the chapter on ‘A Resilient and Reliable Network’. **Future steps:** many of the goals of Vision WG are met: • the survey and analysis of verticals opportunities • input for the Phase II call based on that • the white paper explaining the significance of Phase I achievements

	Two areas identified that may become the focus in the next 6 months: • capturing additional challenges from Phase II projects • analysing sustainable business models and value chains Now reviewing/revising the Terms of Reference
5GPPP Network Management & Quality of Service Working Group	
Felix Klaedtke, NEC	**5G-ENSURE inputs**: 5G-ENSURE has contributed to the security session of the "*Cognitive Network Management for 5G"* whitepaper. The paper introduces the vision of cognitive network management based on the 5G requirements and solutions, as well as analyse the challenges. The novelties for network management in 5G are presented, including autonomicity, NFV, SDN, network slicing, architectures and security. **Future steps:** a proposal for workshop at the EuCNC workshop has been submitted
COMMS Group	
Stephanie Parker, Trust-IT	Active participation in monthly conference calls (since October 2016) to discuss main activities within the projects and define how to support joint promotional activities. On behalf of 5G-ENSURE, Trust-IT has provided benefits of being active on social media with concrete examples, offering tips on how to engage online. Trust-IT has also provided guidance on press releases and generally been one of the most active members of the group. Since the start of calls, every project within phase 1 of the 5G PPP have set up social media accounts and most of them have become more actively engaged. 5G-ENSURE has been a driver behind the setting-up of the LinkedIn Group, to which it makes min. 2 contributions/month.

5.4.2 White Papers

5G-ENSURE has made contributions to several 5G PPP white papers through its active participation in several 5G PPP Work Groups. The contributions have been widely promoted through project channels, including LinkedIn and Twitter.

- Innovations and New Business Opportunities, http://5gensure.eu/news/5g-ppp-white-paper-innovations-new-business-opportunities
- Cognitive Network Management, http://5gensure.eu/news/5g-ppp-white-paper-cognitive-network-management-5g

The Security WG, chaired by 5G-ENSURE, has produced a white paper on Phase 1 Security Landscape with 45 contributing authors from nine 5G PPP projects. Key findings in the white paper will be part of the

discussions at the EuCNC 2017 workshop. The booklet will be graphically designed and circulation during EuCNC, and widely promoted to the community.

5.4.3 5G PPP Technology Board

5G-ENSURE has contributed to the TB paper submitted at the EuCNC 2017.

The paper Leading Innovations Towards 5G: "*Europe's Perspective in 5G Infrastructure Public-Private Partnership (5G-PPP)*" introduces the PPP programmatic perspectives and focuses on TB PPP Phase 1 Golden Nuggets. The technological and architectural innovations, researched and developed by 5G-PPP Phase 1 projects, are presented with also the innovative areas such as 5G system design and evaluation, novel air interfaces, network management, virtualization and service deployment aspects as well as the security. The main contribution from 5G-ENSURE relates to the *5G Networks Security and Integrity* golden nuggets through the main achievements in the context of 5G Security Architecture, 5G Security enablers and 5G Security Testbed.

The paper has also been registered in Edas under the Wireless and Optical Networks (WON) track.

5.5 Visibility of 5G-ENSURE

5.5.1 Press Coverage

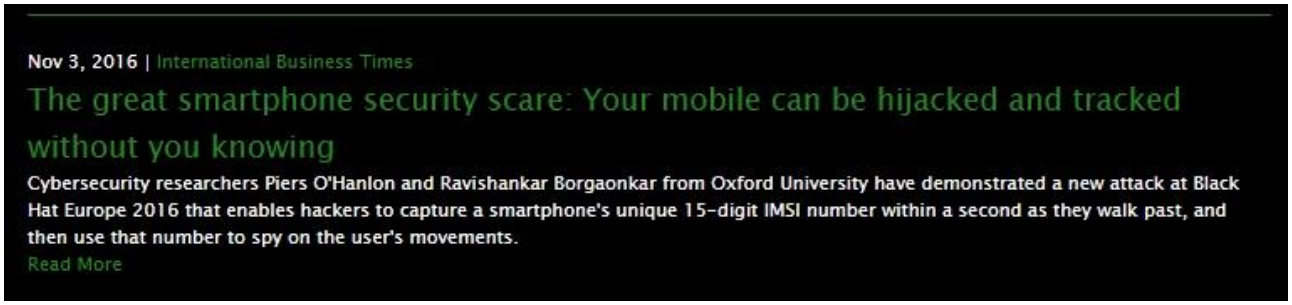
November 2016

The University of Oxford (Piers O'Hanlon and Ravishankar Borgaonkar) presented their research on International Mobile Subscriber Identity-catcher (IMSI-catcher), a telephone eavesdropping device used for intercepting mobile phone traffic and tracking location data of mobile phone users at Black Hat Europe, 1-4 November in London.

The presentation, WiFi-based IMSI Catcher, received a lot of attention on Twitter and on the conference website. Interviews with journalists from online IT and business media generated 20 press clippings, http://5gensure.eu/press-coverage/wifi-based-imsi-catcher, reported in Annex 1. The conference organisers also highlighted the press coverage, https://www.blackhat.com/html/press.html.

To highlight the importance of the research, 5G-ENSURE published an interview with Piers O'Hanlon as a LinkedIn blog post (60 clicks), https://www.linkedin.com/pulse/privacy-issues-mobile-networks-interview-piers-ohanlon-network.

Figure 14: Black Hat Europe 2016



March-April 2017

The b<>com stand at MWC17 received attention from journalists at TechNative, which captured the groundbreaking research from our French SME partner in a Q&A with Michel Corriou, Networks and Security director. The article highlights b<>com's focus on certain key 5G technologies like SDN,

cloudification, and the convergence of radio access networks, https://www.technative.io/mwc-qa-bcoms-networks-and-security-director-michel-corriou/.

Figure 15: TechNative coverage of b-com at MWC17

The article was top Tweet in March 2017.

Figure 16: Top Tweet March 2017

French journal "L'Usine Nouvelle", a famous weekly on manufacturing, industry and innovation, a reference among French media also published an article on b<>com, with a long part dedicated to 5G-ENSURE, including the interview with Michel Corriou.

5.5.2 Overall Visibility and Impact on Social Media and Professional Networks

November 2016

Global 5G received the most coverage in November 2016, both the 5G-ENSURE booth and key discussions on security and privacy associated with 5G and the Industrial Internet of Things.

Figure 17: Top Tweet and Mention November 2016

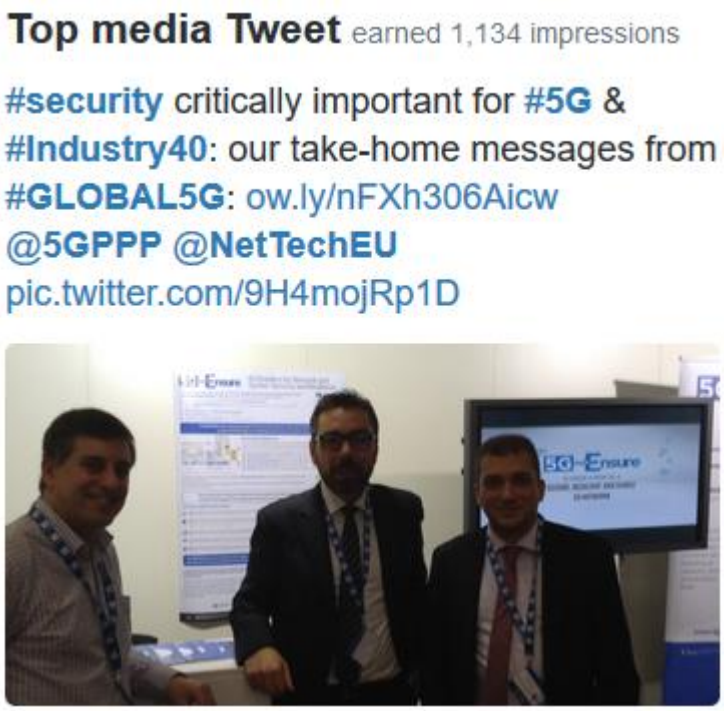
5G-ENSURE Twitter activities during Global 5G and throughout December helped draw attention to international developments on 5G, including 5G needs in Brazil (e.g. remote access, enhanced broadband, ultra-reliable mMTC); future scenarios at Olympic Summer Games 2020 in Japan and 5G capabilities at Olympic Winter Games 2018 in South Korea. The post-event takeaways news piece and Tweets highlighted the critical role of security in 5G.

December 2016

5G-ENSURE visibility at Global 5G continued in December 2016 along with insights into international developments and promotion of the project's standardisation plan, and the b<>com stand at the 9th International Forum on Cyber Security (FIC 2017). The plan received over 400 views on LinkedIn and helped spontaneously recruit over 15 specialists from target standardisation organisations.

The Top Tweet shows 5G-ENSURE engagement with peer project CHARISMA at Global 5G.

Figure 18: Top Media Tweet December 2016



The box below shows some of the top tweets in December 2016.

Telecoms industry expertise key for successful #IIoT says @wef representative in @TelecomTV interview: ow.ly/wrEX307kJrA	1,933 impressions
1 of our **#SME** partners **@IRT_BCom** is showcasing **@5GEnsure** test bed & achievements so far at **#FIC2017** 24-25 Jan ow.ly/dOrB307isY8 pic.twitter.com/iHtIndxLKN	1, 590 impressions
Here's our current #5G pre-standardisation plan for #security & #privacy within the @5GPP. @3GPPLive @ETSI_STANDARDS @GSMA @NGMN_Alliance pic.twitter.com/YyNU7pncBG	1,295 impressions
EU-Japan co-operation on #5G starts w/ 5G!Pagoda coordinated by @AaltoUniversity & @UTokyo_News_en ow.ly/ntec307i55O	1,181 impressions

January 2017

Most of the visibility in January 2017 revolved around the b<>com stand at FIC 2017, where the 5G test-bed was one of the key features with dedicated promotional designed and circulated. The stand also featured in the b<>com newsletter and project newsletter. An interview was made with Michel Corriou and published as a LinkedIn blog post in the run-up to the event (86 clicks), https://www.linkedin.com/pulse/5g-ensure-5g-test-bed-interview-michel-corriou-b-com-5gensure-network.

Figure 19: b-com Visibility at FIC2017

The box below provides examples of Twitter activities with particular reference to FIC2017, where engagement with the regional cyber security cluster (@ExcellenceCyber) was also important in increasing visibility. The new 5G-ENSURE Roadmap for the enablers also received visibility, as did activities on the 5G PPP.

#FIC2017 Lots to see at @IRT_BCom Stand B20 on #network security, #5G testbed, #SDN, #CyberSecurity demos @FIC_fr https://www.forum-fic.com/ pic.twitter.com/YcVVpxABxT	1,463 impressions
Interview w/ Michel Corriou, @IRT_BCom on #5G testbed, #security & #privacy enablers, #cloud & #devops http://ow.ly/FX3G308iN7H @5GPPP pic.twitter.com/zMGCnDsR97	1,408 impressions
#FIC2017 @centralesupelec partnership showcase at @FIC_en @FIC_fr: @Inria_Rennes @DGA @IRT_BCom @IMTAtlantique @ExcellenceCyber @cyberwiser pic.twitter.com/l1ah3CpFwu	1,648 impressions Total: 4,515
Our updated technical roadmap for #5G security enablers is now available to advance vision in @5GPPP & beyond, ow.ly/5Ndi308wWzN pic.twitter.com/Rd3a5KWnvd	1,337 impressions
#5G innovations from @5GPPP projects: @mmMAGIC_5GPPP @metis2020 @5GPPPCogNet @5GNorma @H2020_COHERENT @sonataNFV http://ow.ly/6FCr3089c6P pic.twitter.com/SqMrDMapgp	1,920 impressions

February 2017

Twitter activities in February 2017 were important for promoting the 5G PPP Technology Board meeting in Athens, MWC17 and EuCNC. Promotion of EuCNC attracted well over 4,000 impressions and MWC over 2,000, including visibility of the 5G PPP joint programme activities.

The Technlogy Board Meeting was the Top Media Tweet of the month.

Figure 20: Top Media Tweet February 2017

Sample of Tweets for EuCNC 2017: Don't forget deadline for @EuCNC 2017 workshops, papers, sessions ends next Monday 20 Feb. @5GPPP @FANTASTIC5G @charisma5G @metis2020 pic.twitter.com/yS6LG1TbxI	Total impressions: 4,067
5G Infrastructure Association at #mwc17 #5G Action Plan: from Research to Trials 28-02 14:00 - 15:30 Press Conference Room 1 Media Village pic.twitter.com/4wUu9CxOkP	I,110 impressions
Great to see @5GPPP projects together next week in Athens to share insights & priorites for #5G @metis2020 @mmMAGIC_5GPPP @FANTASTIC5G https://twitter.com/charisma5G/status/826748220349018112 …	Announcement: 1,527 impressions Live from event: 1,364 impressions

March 2017

This was a key month for visibility on Twitter with an average of 1,000 impressions/day. 5G-ENSURE worked closely with the 5G PPP COMMS Group to ensure high visibility of the 5G PPP activities during the Mobile World Congress, particularly the annual Media & Analyst Event "5G Action Plan - From Research to Trials" hosted by the 5G Infrastructure Association (5G IA) and distribution of the Vision Work Group White paper from the b<>com stand.

Top Tweet was on the election of new 3GPP RAN Chair, the promotion of which was also supported by NOKIA and attracted 3,127 impressions.

Figure 21: Top Media Tweet March 2017

5G-ENSURE March newsletter: Our latest newsletter reports on @5GPPP project progress on #5G #security & #MWC17. Sign up here: 5gensure.eu/newsletter-sub… Our news round-up for March 2017 is out. @5GPPP cross-project WS report; #mwc17 partner takeaways & new white paper, ow.ly/3urL30amo6p	Total impressions: 2,599 (1,277 + 1,362)
MWC17 press coverage: #mwc17 Q&A w/ Michel Corriou, @IRT_BCom on quest to innovate for the common good by @TechNativeLive @TechNative ow.ly/mpDs309vnx0 pic.twitter.com/lQrzVV2FiO Thanks to @TechNative & @Domhalps for coverage of our #SME partner, @IRT_BCom - great job https://twitter.com/Domhalps/status/837640688904851458	Total impressions: 5,424
Promotion of 5G IA and 5G PPP: #mwc17: White paper on "5G Innovations for Business" is available at the @IRT_BCom Stand F17 in Hall 8 @5GPPP @NetTechEU @DSMeu pic.twitter.com/oOObZabpSV Crucial steps twds stronger international #IoT & #5G collaboration w/ the Euro/Brasil #5GPPP signature at #mwc17 w/ @AIOTI_EU @abincbr pic.twitter.com/S2AYJTrOFN	1,548 impressions 1,4012 impressions
Promotion of our workshop with CHARISMA: What impact will widespread adoption of #nfv #Sdn have on network security? A key topic at 2nd Int'l WS SNS2017 http://ow.ly/SdKF309I66A pic.twitter.com/RHqgI5nr80	1,692 impressions

The post-event takeaway news piece on MWC17, http://5gensure.eu/news/5g-ensure-takeaways-mobile-world-congress-2017, highlights also the impact on social media:

Top engagement with 5G Americas Latin America, 5G Americas Brasil, EUBra-BIG SEA and RedeRNP. On the policy front, we attracted attention from Roberto Viola (Director General at DG Connect), the Digital Single Market and EC Net Technologies while our tweets on b<>com were shared by Startup Europe and Networld 2020 SME, and the Mobile World Congress event Twitter.

Figure 22: Sample of Visibility during MWC17

April 2017: Trust Model Survey and EuCNC workshop

The 5G-ENSURE Survey on Human Trust and Network-related Threats has received visibility across policy, media and consumer groups through promotion on the project website and that of the 5G PPP, http://5gensure.eu/news/5g-ensure-survey-human-trust-and-network-related-threats and https://5g-ppp.eu/5g-ensure-survey-human-trust-and-network-related-threats/, with 202 views on LinkedIn.

Re-tweets include:

- NetTechEU (Unit E1 - DG CONNECT), 4294 followers
- CnectCloud (Unit E2 - DG CONNECT), 2193 followers
- TechNativeLive, 33.7K followers; TechNative, 46.1K followers; Dominic Halpin (co-founder of TechNative), 17.6K followers
- London Networker (mobile/network consumers), 12K followers
- 5G PPP and some peer project, e.g. Sonata.

Figure 23: Visibility of Trust Survey on Twitter

5G-ENSURE enablers: We are delivering on our roadmap for #5G #security & #privacy enablers: 5gensure.eu/security-enabl… @NetTechEU @5GPPP @HardenStance	1,163
EuCNC Workshop: Our WS at @EuCNC on 12 June: #5G Security - Phase 1 landscape and foreseen evolutions ow.ly/dO9J30aW82S @5GPPP @NetTechEU pic.twitter.com/xEm9rgotSI	855
2nd International Workshop: Our 2nd International Workshop: From Research to Standardisation is part of ETSI Security Week, ow.ly/3xbg30bcaS9 @NetTechEU @5GPPP	680
5G PPP White Paper: New white paper on Cognitive Network Management for #5G #nfv #SDN network slicing, #Security ow.ly/xI0A30avwJh @NetTechEU @5GPPP	1,537

5.5.3 Newsletters and Communications Material

The 5G-ENSURE newsletters aim to keep the 5G PPP and wider community abreast of key activities and outputs from the project. We present below the newsletters circulated.

For the December newsletter, an inforgraphic on the main achievements in 2016 was prepared, designed and circulated. The infographic provides a snapshot of the 5G enablers, the security architecture, the 5G test-bed, the standardisation activities and key findings from the open consultation. It also shines the spotlight on 5G communications and community, as well as joint activities with the 5G PPP.

Key features of the newsletter circulated in December, February and April are shown in the figures below. The March newsletter was also published as an article “News Round-up”, where the biggest audience was from London, UK and Germany. It was shared with shared with 30 young researchers at Buffalo based on LinkedIn interest prompts.

Figure 24: December Newsletter

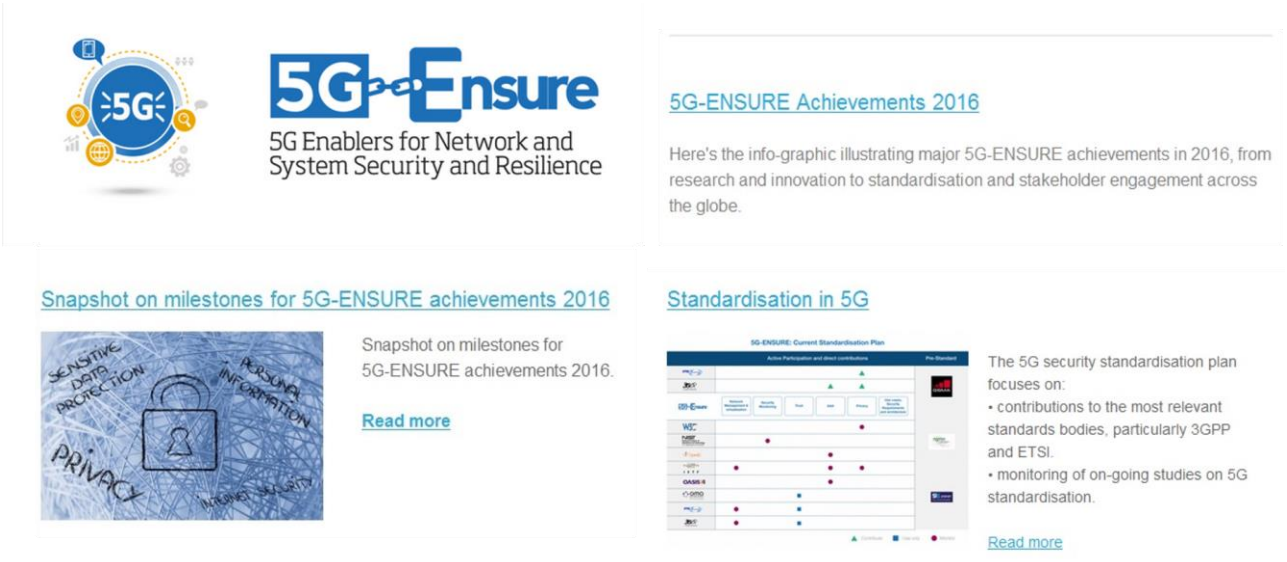


Figure 25: Newsletter February 2017

Figure 26: Newsletter April 2017

5G-ENSURE designed a new brochure on standardisation for circulation at Global 5G. This brochure has been updated with inputs from ITU-T. The brochure provides the basis for the 5G-ENSURE Roadmap on 5G security standardisation and complements the promotion of the project's standards plan, http://5gensure.eu/standardisation-5g, which has been widely broadcast across stakeholders involved in the most relevant standardisation organisation.

The brochure will be updated to reflect the findings of the open consultation and the main takeaways from the 2nd International Workshop in June 2017 during ETSI Security Week.

Figure 27: New 5G-ENSURE Standardisation Brochure

Promotion of the workshop, From Research to Standardisation, takes place in concert with ETSI and includes the use of co-branded banners for the website, Twitter and LinkedIn. ETSI has promoted the workshop through its monthly newsletters. 5G-ENSURE has also produced a Save-the-Date postcard for circulation at MWC2017 via the b<>com stand.

Figure 28: Save the Date Postcard for 2nd International Workshop

6. Measurable Impacts for Community Building and Networking

Main Takeaways – Direct engagement with stakeholders has been key to building a vibrant global community around project focus

- 5G-ENSURE has recruited an average of 80/month new connections on LinkedIn since July 2016.
- Industry represents the largest portion of this community (61%) with the largest growth coming from SMEs, from 62 to 136 small companies joining 5G-ENSURE.
- 5G-ENSURE has achieved excellent representation of specialists from target standards organisations, including
- 5G-ENSURE Twitter is an international community spanning 49 countries worldwide with an average of 27 new followers/month. Active members are from key hotspots in both mature and transition markets.

6.1 5G-ENSURE Community

6.1.1. LinkedIn Network

5G-ENSURE has a LinkedIn community of **810 LinkedIn connections**, with an **average of 80 new members a month** since July 2016 recruited through a continuous flow of insightful information on this professional network encouraging organic growth.

The following groups represent 61% of the 5G-ENSURE professional network are are the organisations that will be benefit most from standardisation, with many contributing to the development thereof:

- 5G Industry (connectivity providers, manufacturers, SMEs):
    - Operators: 118 (up from 60 representatives).
    - Manufacturers: 153 (up from 90 representatives).
    - Professional roles in the above include heads of standardisation/technology standards, OSS mobile network standards specialists, RAN operational teams, wireless standardisation specialists, standards strategists etc.
- SMEs and micro businesses: 136 (up from 62), more than doubled.
- Large companies (vertical industries): 84 (up from 65).

Good growth has also been achieved for leading representatives and decision making in European Standards Organisations and global Standards Development Organisations. The promotion of the project's Standards Plan has played a key role in achieving organic growth.

- ESOs and SDOs: 48 (up from 28 representative), with the highest growth coming from new 3GPP and ETSI connections and a higher number of organisations covered, as indicated in the table below.

The increased number of Industry and SME associations along side sector/thematic groups is also important for increasing visibility through a multiplier effect, including greater international reach.

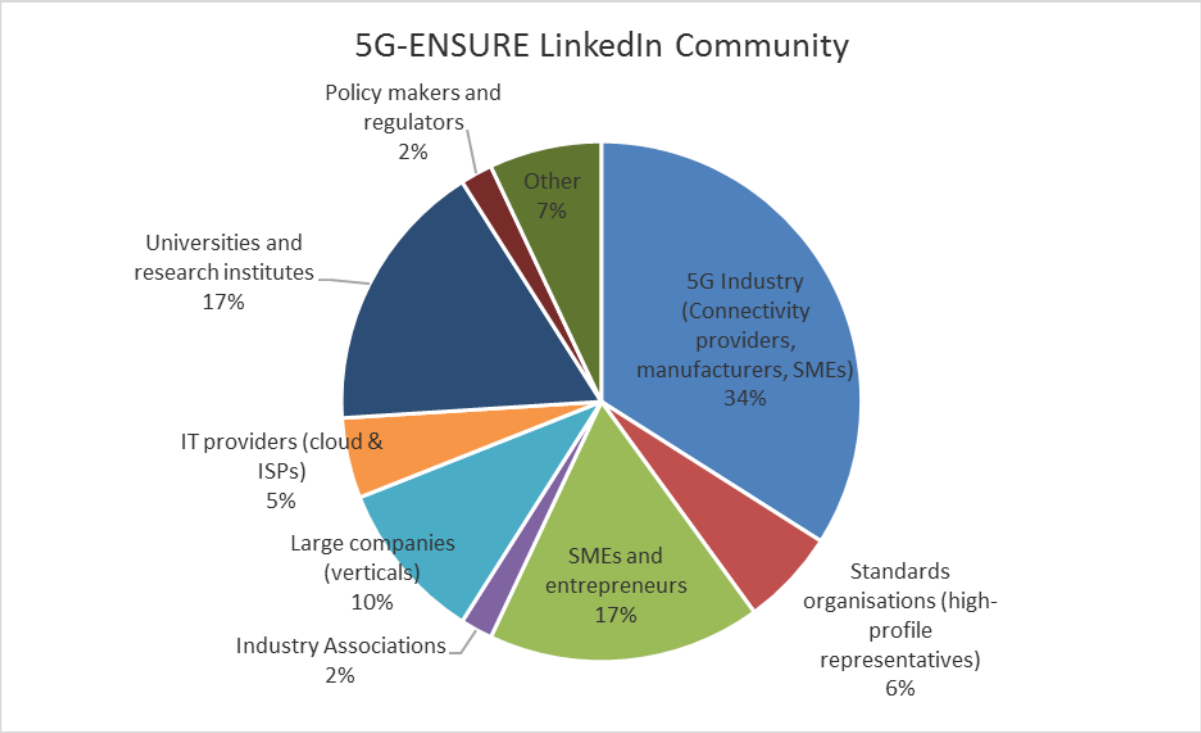
- Industry Groups (including ICT clusters): 20

Other groups within the network:

- IT providers (cloud, internet service providers): 40 (up from 23 representatives).
- Universities and research institutes: 137 (up from 80 representatives).
- Policy and regulators: 19 newly recruited.
- Other: 5G PPP peer projects, self-employed, trainers, consultants, not specified.

The figure below shows the percentage break down of the 5G-ENSURE LinkedIn Community with regard to primary and secondary stakeholders:

Figure 29: LinkedIn Community



The table below provides a sample of community members from both the primary and secondary stakeholder categories.

Table 16: Sample of LinkedIn Connections

PRIMARY STAKEHOLDERS (including representatives from 5G PPP phase 1 projects	
5G telecommunications industry	AT: A1 Telekom Austria AG; BE: KPN BASE, Proximus/Belgacom, Orange Belgium; DE: Vodafone Germany; Deutsche Telecom, T-Systems International GmbH; ES: Telefonica, Parlem; FR: France Telecom/Orange, Bouygues Telecom, Com4Innov; Orange Labs; GR: OTE/COSMOTE, Intracom Telecom; IT: TIM/Telecom Italia; LU: Tango S.A (Proximus); NL: Vodafone Ziggo Netherlands, T-Mobile Nederland; SE: Ålands Telefonandelslag; SL: Telekon Slovenia; UK: Vodafone UK. CH: Swisscom; Monaco Telecom; NO: Telenoir. Brazil: Oi S.A; China: China Telecom; India: Jio; Japan: NTT DOCOMO; KDDI Corporation; South Korea: SK Telecom; Vietnam: Viettel Network Technologies Center - Viettel Group; US: Verizon & Verizon Wireless, Liberty Global, T-Systems. Suppliers/manufacturers: Cisco Systems, Ericsson, Huawei Technologies European Research Center, Nokia, Qualcomm, Samsung Electronics.

Industry 4.0, IIoT, & SMEs and Vertical Industries	**Companies** – SMEs and large companies include supply chain providers, hi-tech companies and vertical industries. **SMEs**: 3IF - Internet of Things and Industrial Internet Future (Industry 4.0), 5G UP, EICT GmbH, EnvOps, Green Communications, Incelligent, InnoRoute, InterDigital Communications, IS-Wireless, Lime Micosystems, OTREMA, Montimage, Nextworks, naudit High Performance Computing and Networking, PRISMA Telecom Testing, RESEIWE A/S, Rohde & Schwarz, SETECS, SpinalCom (fog middleware), TerUsus. **Vertical industries**: Aerospace: AIRBUS; Automotive: Daimler, DEXMA Tech, FIAT Research Centre,Toyota, Volkswagen, Volvo, Robert Bosch GmbH (SME supplier); Electrical/Electronic Manufacturing: ABB; Financial services and FinTech: Banca d'Italia, BNP Paribas Fortis, Lloyds Banking Group, Pagero (SME), Square (SME), Strategic FinTech (SME), Credit Agricole Bank Poland S.A. Gaming, entertainment: Sony EU & Sony China, Technicolor; Healthcare: Philips; Hi-tech engineering: Dyson; Smart Cities: Accenture, DFRC (SME), Ubiwhere (SME); Transport: Comesvil, Gemalto; Utilities: ABB, Tatung Czech, tec ICT (SME).
Standards Bodies - sample	ETSI: 13+ leading representatives and decision makers, e.g. TC CYBER Vice Chair; ETSI NFV ISG Chair; ETSI NFV ISG Vice-Chair; ETSI SCP; TC RRS (Reconfigurable Radio Systems) WG 1 Chair; Director of Technical Strategy, ETSI Standardization Projects; ETSI CTO; ETSI Board Member and IPR committee chair. 3GPP: 12+ leading representatives in, e.g.: 3GPP TSG SA Chairman; 3GPP TSG SA Vice Chairman; 3GPP RAN Standards Strategist; 3GPP SA2 Vice Chairman; Chairman 3GPP SA3; 3GPP RAN Chairman; 3GPP TSG RAN Vice-Chair; 3GPP Ran1 delegate; 3GPP RAN working group 1 Chairman; Chairman of 3GPP SA6. 3GPP SA3. AIOTI WG03: Chair (ETSI); high level architecture leader. IEEE: 7 leading representatives, e.g. Chair of IEEE Tactile Internet Sub-Committee; IEEE Sensors Council; IEEE 1914 WG Chief Editor; IEEE IoT Initiative Chair scenario track; IEEE 5G Initiative Co-chair; IEEE Privacy. IETF: Chair; CCAMP Working Group Co-Chair; ACE Group Chair. Leading representatives and members in the ITU SG17 (Security) and SG20 (IoT); Kantara Initiative; Open Mobile Alliance - Vice-Chairman of Communications Group (COM WG); Open Networking Foundation.
Industry Groups	**EU-based**: EIT Digital (Directors/Co-location Managers - France, Italy & Netherlands), EUROCITIES, Digital Catapult (Personal Data and Trust), EuroCloud Germany, Irish Internet Association, Connected Smart Cities Network (EU founded), EERA - The European Energy Research Alliance, DIMECC Oy, European Privacy Association, Cap Digital, DIGITAL EUROPE - Technology Regulation & Policy Group company representative, Finnet Association, European Cyber Security Organisation (ECSO). **International**: GSMA Latin America; GSMA - Head of Networks; 5G Americas - Head of Latin America; NGMN; Wireless World Research Forum; World Economic Forum; The Khronos Group (U.S.); Taiwan-Japan Industrial Collaboration Promotion Office (TJPO), Ministry of Economic Affairs; OSGi Alliance.
5G PPP projects	Coordinators and representatives from: EURO5G, 5GEX, CHARISMA, mmMAGIC, SELFNET, SPEED 5G, 5G-Crosshaul, Sonata and international 5G project: 5G!PAGODA. (EU-JP) and PICASSO (EU-U.S.).

SECONDARY STAKEHOLDERS
Policy - EC: Thibaut KLEINER, Head of Cabinet of @GOettingerEU; European Commission, Programme & Policy Officer - Smart Mobility, Connected and Automated Driving, Electromobility; European Commission - DG CONNECT - Innovation and Starts-Up Unit, Head of Sector ICT Standardisation. **EU Regulars and governments**: Ofcom and IP Networks & Digital Media, HM Cabinet Office (UK); Ministere de l'Economie et des Finances, European and international spectrum harmonization adviser at DGE (FR); SFR Spectrum Policy Manager; Flemish Government (Vlaamse Overheid) (BE); OFCOM - Swiss Telecom Regulator (CH). **CERTS/CSIRTS/national cyber security centres**: Andalucia CERT, national cyber centre (DK).
Universities & research institutes : Aarhus University (IoT), Aalto University, BISDN at Berlin Institute for Software Defined Networks, CTTC, HHI Fraunhofer, Iowa State University, King's College London, KTH, Peking University, Technical University of Madrid, TELECOM SudParis, Trinity College Dublin, Universidad de Murcia, University of Oxford, University of Southampton, University of Surrey 5G Innovation Centre, Federal University of Ceará, Brazil, 5G Lab (DE).
EU and International initiatives: European Cyber Security Organisation (ECSO); GDPR Awareness Coalition;

6.1.2. 5G-ENSURE Twitter Followers

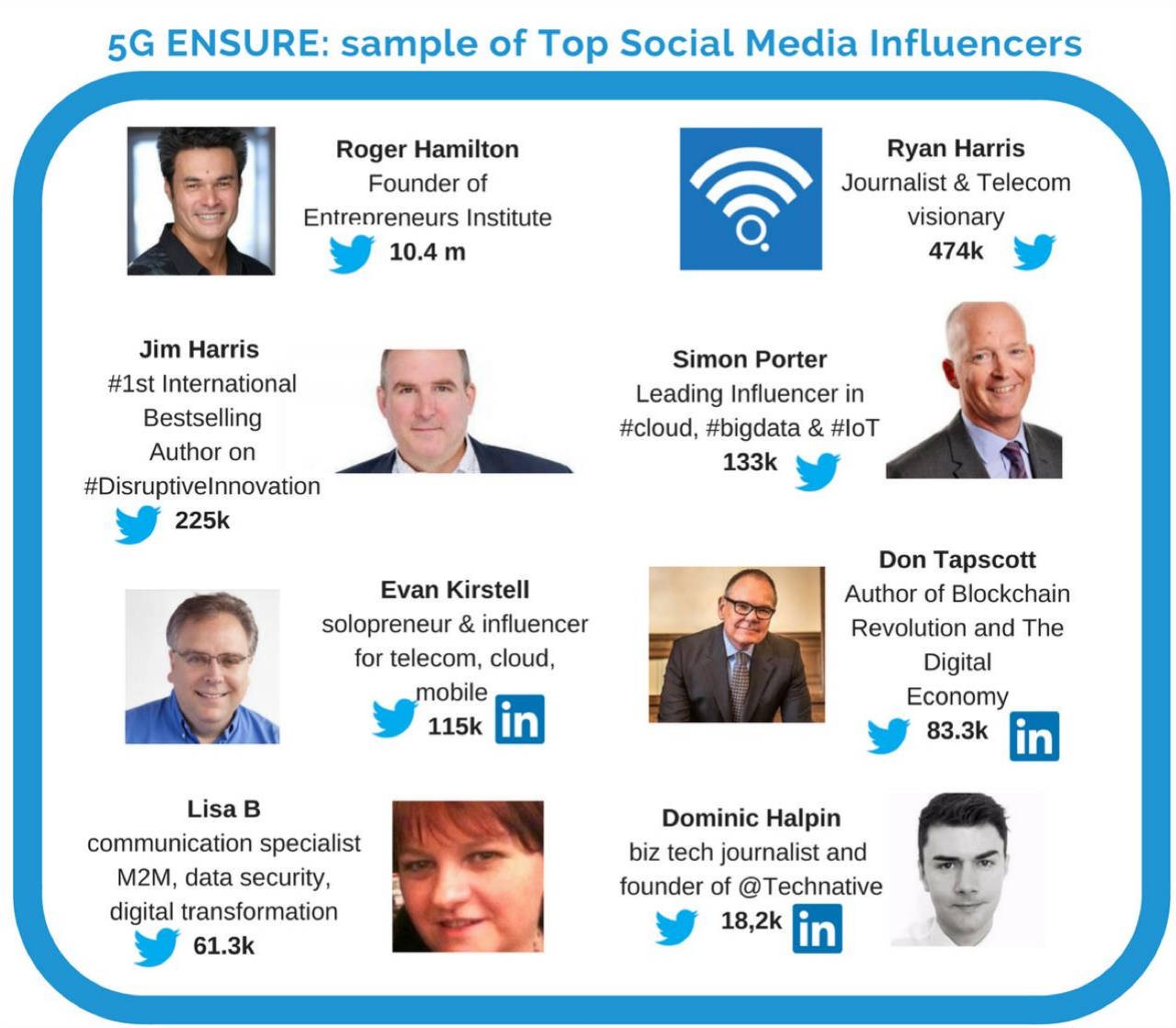
5G-ENSURE has extended its followers to 504 from 318 reported in D5.3., with an average of 27 new followers a month. The geographical coverage of 49 countries is showed in the figure below.

Figure 30: Geographical Coverage on Twitter

Top ten countries are UK (19%), U.S. (10%), Belgium (8%), France (7%), Finland (6.4%), Spain (5.2%). Italy (4.8%), Germany (3.6%), India (3.6%) and Brazil (3.2%). Top cities include capital cities and ICT hubs (London, Madrid, Bangalore, Rio de Janeiro, Turin, Boston, Chicago, Barcelona, Brussels, Dubai, Tokyo).

The figure below shows a snapshot of top social media influencers that 5G-ENSURE has recruited through its regular engagement on Twitter. The influencers include two authors of digital transformations.

Figure 31: Sample of Social Media Influencers



6.1.3 5G-ENSURE Impact on Social Media

The use of twitter in 5G-ENSURE is an important part of the communications strategy, designed to raise awareness of 5G-ENSURE activities and outputs, engage with primary and secondary stakeholders, and share results across the 5G PPP. Six twitter metrics are used to gauge impact of twitter campaigns, e.g. tweets, followers (identifying top followers each month), following, impressions (number of times users are served a tweet in a given timeline, search results or from twitter profile), profile visits (number of times profile page visited), mentions (number of times @5GEnsure is mentioned in tweets). Some of these metrics are also used to benchmark performance against peer projects, e.g. tweets, followers, likes and lists.

The table below shows monthly twitter performance based on the metrics used and overall achievements.

Table 17: Impact on Twitter

Overall Performance since November 2015	
Tweets	*999*
Followers	*504*
Following	*261*
Total impressions	*621,778*
Total profile visits	*9,557*
April 2017	
Number of tweets	*29 – accounting for EU holiday break*
Number of profile visits	*405*
Tweet Impressions	*18,900*
New followers	*14*
Top follower	*DBmaestro (DevOps), 9,754 followers*
Mentions	*7*
March 2017	
Number of tweets	*42*
Number of profile visits	*584*
Tweet Impressions	*31,600*
New followers	*38*
Top follower	*Roger James Hamilton, Founder of Entrepreneurs Institute, 1.09M followers*
Mentions	*16*
Febraury 2017	
Number of tweets	*56*
Number of profile visits	*584*
Tweet Impressions	*38,100*
New followers	*31*
Top follower	*Jim Harris, author of Disruptive Innovation, 221,000 followers*
Mentions	*15*

January 2017	
Number of tweets	*50*
Number of profile visits	*801*
Tweet Impressions	*31,500*
New followers	*34*
Top follower	*Simon Porter, leaing influencer for cloud, big data and IoT, 133K followers*
Mentions	*11*
December 2016	
Number of tweets	*25 – accounting for EU holiday break*
Number of profile visits	*552*
Tweet Impressions	*17,800*
New followers	*32*
Mentions	*10*
November 2016	
Number of tweets	*63*
Number of profile visits	*773*
Tweet Impressions	*31,600*
New followers	*28*
Mentions	*30*

7 Plans and Targets for Next six Months

7.1 Primary and Secondary Stakeholder and Engagement Plan

7.2.1 Engagement Plan for Primary Stakeholders

Table 18: Primary Stakeholder Engagement Plan

5G Industry: vendors/manufacturers, telecom operators, including representatives involved in the 5G standardisation process within key standards bodies for 5G. This group also includes **SMEs** and start-ups with an interest in early 5G developments, verticals with future 5G use cases prioritising security and privacy. Increasing attention to industry verticals, covering (but not limited to) healthcare, manufacturing, financial services, gaming/media, automotive where an increasing numbers of players are involved (e.g. Automotive: Car manufacturers, mobile and telecom operators, academia, network and technology providers (chipset makers); Services (insurance, driver assistance, security on content delivery); Smart cities; Satellite-based communications, as well as industry regulators). **Industry Engagement Plan** Engagement through community development on **LinkedIn** as an important professional network, T**witter** and at different types of **events** targeting industry and experts involved in standardisation, and the media. 5G-ENSURE also reaches out to communication specialists and 5G professionals within partner organisations to build momentum around 5G-ENSURE. Engagement aims to raise awareness of security, privacy and trust as central to the uptake of 5G, targeting also employees working on security within vendor and telecom corporations. The annual Ericsson Security Day (200 employees targeted) and SICS Open House events are just two examples of awareness-raising. Help drive consensus around the 5G-ENSURE approach across primary stakeholders from 5G industry and target standardisation organisations. **SME Engagement Plan** Engagement with SMEs focuses on tailoring messages on 5G to people less familiar with 5G concepts while highlighting the importance of security and privacy in building trust. Engagement takes place through LinkedIn, market research/telecom media, as well as business associations and developer platforms, e.g. DIGITALEUROPE and its trade associations for reaching SMEs, ensuring the business community is well prepared to leverage the opportunities of 5G in terms of new vertical use cases and new supply chain roles. Communications to these audiences are focused on ensuring the business benefits of 5G are understandable.
Standards bodies: 3GPP, ETSI, ITU, IETF, IEEE Privacy and the IEEE5G Initiative, which are also key targets within the 5G PPP phase 1 projects. 5G-ENSURE specifically targets the 3GPP SA3 and ETSI CYBER as the most relevant groups addressing 5G security and privacy challenges with contributions from the project, while monitoring and using other relevant standards. The GSM Association and its Fraud and Security Group (FASG) and the alliance for Next Generation

Mobile Networks (NGMN).

Regulators targeted: ITU, Working Party 5D – IMT systems (WP5D) [4], ECC, ECC Project Team 1 [5] (ECC PT1) responsible for implementing the WAPECS concept (the new European flexible approach based on technology and service neutral regulation) for Mobile and Fixed Communications Networks (MFCN).

Policy makers targeted: European Commission (policy leaders: 5G, Digital Single Market, Cyber security framework, privacy and data protection laws), EC Net Technologies, ENISA [6], national and European legislators.

Engagement Plan

Meetings and conference calls are the primary channel used to contribute and monitor relevant 5G standardisation efforts. Other important channels are LinkedIn and twitter as part of the project's community development.

The engagement plan for 5G policy makers includes participation at 5G PPP events, such as the 2nd 5G-ENSURE International Workshop and the workshop organised by the Security Work Group during EuCNC 2017.

5G PPP Phase 1 Projects: including industry and research stakeholders, and relevant international initiatives as primary 5G stakeholders, where 5G-ENSURE engages at multiple levels.

Drivers for engagement: encourage uptake of relevant 5G-ENSURE outputs, such as the security and privacy enablers and the test-bed, build consensus on the project's standardisation efforts, and contribute to a harmonised and coherent approach to 5G in Europe.

Euro-5G: Coordination and support action acting as the reference point for joint 5G PPP activities at the programme level. Coordination through a dedicated mailing list.

Radio technology projects: 5G-XHaul, 5G-NORMA, COHERENT, FANTASTIC-5G, Flex5Gware, METIS-II, mmMAGIC, CHARISMA, SPEED-5G.

Network technology projects: 5G-Crosshaul, 5GEx, CogNet, SESAME, SELFNET, SONATA, Superfluidity, VirtuWind.

Engagement Plan: Euro5G

Channel for disseminating the results of 5G-ENSURE and promoting activities (e.g. events, public consultation).

Participation in the 5G PPP COMMS Group aimed at facilitating stakeholder engagement across phase 1 projects, including joint dissemination and promotion of Work Group activities.

Joint publications, e.g. the 5G Annual Forum.

Joint events and exhibition stands, such as EuCNC.

Engagement Plan: 5G PPP Phase 1 Projects

Chairing of the 5G Work Group on Security and defining outputs such as white papers.

Contributions to other WGs, detailed above:

- Pre-Standardisation WG for timely contributions to standards bodies (e.g. ETSI, 3GPP). Prioritising timely contributions to standardisation and sharing knowledge across the 5G PPP

and relevant Work Groups. 5G-ENSURE chairs the Security WG within the 5G PPP.

- Architecture, Vision and Societal Challenges, Network management, QoS and Security Work Group, SDN / NDF Work Group, 5G-PPP cross-project collaboration.
- SME WG by participating in SME engagement in general and of benefits for 5G-ENSURE partners belonging to this category. Contribute to increased visibility of opportunities and thresholds for the 5G PPP programme in future calls.

Organisation of joint events and publications, to which 5G-ENSURE can contribute.

Sharing and promoting technical and non-technical outputs across the 5G PPP, the European Commission, the 5G-Infrastructure Association, related projects from EUREKA, and related national initiatives.

Promotion of joint publications, e.g. 5G PPP WG white papers.

Contributions to public consultation on 5G security and the 5G-ENSURE Roadmap on Security Standardisation.

7.2.2 Engagement Plan for Secondary Stakeholders

Telecom Media: Engagement Plan

Raise awareness about 5G-ENSURE outcomes through media channels and journalists. Promote the key value proposition of 5G-ENSURE and how the project can impact verticals.

Production and circulation of press releases, opinion pieces/expert interviews.

Insight Briefs: industry panel discussions, including the importance of global collaboration of common challenges.

Social media posts on major industry insights/updates, partner achievements to encourage a relay across the channels.

IT and Business Media: Engagement Plan

Social media engagement to monitor coverage of 5G and retweeting or commenting on articles.

Informative press releases on 5G business benefits, potentially including interviews with 5G champions.

Highlight the need for 5G security and privacy through concrete examples and comprehensible to average readers.

7.3 Standardisation

7.3.1 Meetings scheduled

The following table summarises the meetings of the main standards bodies relevant for 5G security and in view of the current focus on 3GPP SA3 and ETSI TC CYBER. In the past, the SA3 meetings in Santa Cruz (November 2016) and Sophia Antipolis (February 2017) have been decisive for the definition of the plan on 5G Security (conclusion of the study phases and beginning of the normative phases). Now SA3 will have to

take into consideration the outcomes of SA1 (requirements), SA2 (Architecture) and SA3-LI (Lawful Interception) on 5G specifications produced so far, with a new plan to be defined for 2017 (not yet ready at time of writing). In particular, the current version of the TR 33.899 will be finalised during the SA3#87 meeting in Slovenia. Regarding ETSI, it is expected that the work on the definition of the technical measures to protect privacy in mobile environments started during the meeting in Sophia Antipolis (February 2017) will be finalised during the first half of 2018, beyond the end of the 5G-ENSURE project.

Table 19: Meeting Schedule of main Standards Bodies for 5G Security

3GPPSA3#65-LI	25 - 28 Apr 2017	US
3GPPSA3#65-LI	25 - 28 Apr 2017	West Palm Beach, Florida
3GPPSA1#78	8 - 12 May 2017	Oporto
3GPPSA2#121	15 - 19 May 2017	Hangzhou
3GPPSA3#87	15 - 19 May 2017	Ljubljana
NFV#18-F2F-Sophia Antipolis	16 - 19 May 2017	Sophia Antipolis
CYBER#10	31 May - 2 Jun 2017	Sophia Antipolis
3GPPRAN#76	5 - 8 Jun 2017	West Palm Beach, Florida
3GPPSA#76	7 - 9 Jun 2017	West Palm Beach, Florida
Security Week - Standards and Legislation	12 Jun 2017	Sophia Antipolis
Security Week - eIDAS	13 Jun 2017	Sophia Antipolis
Security Week - NFV Tutorial	13 Jun 2017	Sophia Antipolis
Security Week - NFV Security	14 Jun 2017	Sophia Antipolis
Security Week - eDelivery	14 Jun 2017	Sophia Antipolis
Security Week - 5G Security	15 Jun 2017	Sophia Antipolis
WORKSHOP-Security Week - 5G ENSURE	16 Jun 2017	Sophia Antipolis
3GPPSA2#122	26 - 30 Jun 2017	San Jose Del Cabo
3GPPSA3#66-LI	25 - 28 Jul 2017	Ljubljana
3GPPSA3#88	7 - 11 Aug 2017	CN
3GPPSA2#122-Bis	21 - 25 Aug 2017	Sophia Antipolis
3GPPSA1#79	21 - 25 Aug 2017	China (TBD)
3GPPRAN#77	11 - 14 Sep 2017	Sapporo
NFV#19-F2F-Denver	12 - 15 Sep 2017	Denver
3GPPSA#77	13 - 15 Sep 2017	Sapporo

CYBER#11	25 - 27 Sep 2017	Sophia Antipolis
3GPPSA3#66-LI Bis	27 - 29 Sep 2017	Sophia Antipolis
3GPPSA3#88-Bis (Adhoc on 5G)	9 - 13 Oct 2017	Singapore
3GPPSA2#123	23 - 27 Oct 2017	Ljubljana

7.3.2 From Research to Standardisation - 2nd International Workshop

5G-ENSURE has started the organization of the second International workshop that this year will be part of the ETSI Security Week 2017 program.

The ETSI Security week is a very attractive international event and a good opportunity to meet with key security experts and to network, share, influence and learn about the issues and advancements in security.

The detailed program of the ETSI Security week is available at http://www.etsi.org/etsi-security-week-2017.

In particular the following sessions will focus the discussion on more topics of interest for the project where the expectation is to receive valuable inputs:

- *Standards & Legislation:* the focus is on standards for industry sector to understand their needs in terms of standards, best practices, certification, labels and also to have a view on how industry is implementing products complying with the recent European cybersecurity legislation (e.g. GDPR, NIS Directive). The expectation is to complement the findings of 5G-ENSURE open consultation where many questions are related to standard needs for industry.
- *NFV Security Tutorial*: this session will introduce and cover security considerations specific to virtualized and NFV environments. Virtualization and network management is one of the security area in scope of the project and it will be useful to listen the discussion on issues with the establishment of trust in a multi-layer and multi-administrator environments.
- *NFV Security Workshop:* an entire day of the ETSI security week will have a sharp focus on the NFV security dedicating the discussion on the NFV security problems, challenges, opportunities and proving a view on the state of the art development of security solutions. It will be relevant for the project to understand the approach taken considering that some security enablers have also been released by 5G-ENSURE.
- *5G Security workshop:* one of the objective of this event is to give an update of what is happening on 5G security standards, the 5G security requirements from Verticals and business (non-technical) and 5G security research on-going on 5G security and several projects. The workshop is organized the day before 5G-ENSURE providing a good link for continuing discussion on 5G security and for presenting the mains achievements of the project.

5G-ENSURE workshop "**2st 5G-ENSURE INTERNATIONAL WORKSHOP FROM RESEARCH TO STANDARDIZATION**" will be held at the 16 of June 2017.

The objective is to report the progress and technical achievements in 5G privacy and security after one year from the first workshop. In particular the scope is to transfer the vision, the concepts and the enablers matured and released for 5G network and system security as a background for the standardization work as well as for the future research phase.

The workshop is organized in two sessions.

- The first one is more technical. It gives a view on the trust and liability model between the new actors and business models expected in 5G networks and also on the risk methodology defined for the risk evaluation from which are derived the mitigation recommendations and the security requirements. The focus is also on the 5G security architecture defined as a reference for 5G networks and also agreed as a vision in the 5G-PPP Security working group between most 5G-PPP Phase I projects. Furthermore the session provides a deep overview on a number of key enabling technologies related to Privacy-enhancing technologies and Network Management and Virtualisation Isolation. Videos are planned in support to facilitate the understanding as well as to demonstrate the solution.
- The second session focus on the influence the project has in the context of standardization also its engagement with 5G-PPP through the creation of the Security working group. In this context valuable is the presence of SA3 chairm man to get the status and latest timeline of 3GPP work in the security matter. Finally the first findings of the open consultation on "*What else needs to be done on 5G Security?*" are reported to stimulate the discussion in the final panel.

Table 20: Latest Agenda for 2nd International Workshop

Time Slot	Workshop Feature
08:45-09:15	Workshop Registration
09:15 - 11:00	5G-Ensure Achievements **5G-ENSURE Project overview** (*Luciana Costa - TIM*) **Trust Model for 5G** *(Mike Surridge, IT-INNOVATION)* **Risk Model** *(Linas Maknavicius, Nokia)* **5G Security Architecture** *(Alireza Ranjbar, Ericsson)* **Security enablers for 5G network:** • **Privacy enablers: Enhanced Identity Protection** (Baltatu Madalina, TIM) • **Network Management and Virtualization Isolation Security** (Felix Klaedtke, NEC) • **Bootstrapping Trust in virtualized network environments** (Nicolae Paladi, SICS)
11:00	Coffee Break and networking
11:30 - 12:45	Security: the work of standardization and 5G-PPP Cooperation ***Results from the open consultation on "what else needs to be done on 5G Security?"*** (Luciana Costa -TIM) 5G-ENSURE Standardization Plan *(Paolo De Lutiis -TIM)* 5G Security: Phase 1 landscape *(Jean Philippe Wary - Orange)* 3GPP 5G Security Work *(Anand R. Prasad, NEC)* IoT Scenarios and Standardisation *(Giovanni Bartolomeo, University of Rome)*
12:45 - 13:30	International panel on 5G Security way forward *What work needs to be done over the next few years towards the integration and uptake of 5G security solutions as we move towards the launch of the first commercial 5G networks?* International security experts and 5G-ENSURE advisory board members will discuss priority actions for standardisation, security and cooperation key to building consensus.
13:30	Networking Lunch and Refreshments

7.3.3 Open Consultation 2017 - "What else needs to be done on 5G Security?"

5G-ENSURE project has worked to drive the 5G Security Vision to get it shared and agreed within 5G-PPP and beyond. The first Open Consultation on 5G Security has been a step towards this direction, by consulting stakeholders, including other 5G-PPP Projects, on the areas of security and privacy challenges and priorities. The outcomes have been shared and used as part of this type of cooperation among the 5G-PPP projects, that has gained momentum within the 5G-PPP Security WG created on behalf 5G-ENSURE in March 2016. The Security Landscape whitepaper released in April 2017, is the result of one year of concerted effort that carried to build consensus and common positions across 5G-PPP project on the priority areas for 5G security selected from the finding of the first open consulation. In the meantime the work of 5G-ENSURE project went beyond the 5G-PPP community with the engagement in international exchanges with standardisation, for example with NIST in the US sharing insights in the area of security innovations and with ITU-T in discussing on security standards gap analysis.

Also this second year, 5G-ENSURE is conducting an open consultation to continue the activity of relations with the main 5G stackholders, disclosing its security vision and encouraging in providing answers with the objective to have that vision complemented. The main objective of this second consultation is to take stock of the progress of work on security aspects of future networks after more one year. For this the project is seeking the views on the work that has been done by 5G-PPP project and beyond, in particular to:

- Evaluate the usefulness of the results coming from 5G-PPP funded projects and beyond, including their ability to influence the 5G specification work.
- Report on 5G security perspective (mainly industry driven) and get it complemented from the perspectives of others stockholders (e.g. regulator and policy makers, SME, business verticals, etc..)
- Identify the security aspects which have not yet been addressed or which have been only partially covered to understanding the main barriers on progressing on them and how they can impact on the 5G adoption if not solved in time.
- Understand and establish the way forward for future 5G Security work by identifying what else needs to be done on 5G security.

The open consultation will be opened in May. The first findings will be presented during the second 5G-ENSURE workshop that will be part of the ETSI Security Week program, in Sophia Antipolis, France on 16 June 2017 to stimulate and encourage discussion with international experts I security.
The plan is anyway to collect answers until September.
The Open Cpnsultation is available at:

7.3.4 Synergies on Security and Standardisation

5G-ENSURE is actively pursuing its

7.4 5G PPP Joint Programme

7.4.1 5G Security Work Group

The findings of the whitepaper "*5G-PPP Phase 1 Security Landscape*" released by the WG will be presented within the Security WG Workshop "5G Security: Phase 1 landscape and foreseen evolutions" at EuCNC17 event.

7.4.2 Pre-Standards Work Group

The WG is planning a document "*Summary for Phase 1*" to be published in time for the EuCNC 17 event. Scope of this paper is to report on the work that 5G-PPP Phase 1 projects have done about standardisation to measure the total impact on 5G specifications. This is another importante initiave where 5G-ENSURE intends to contribute by reporting on the actions performed.

7.4.3 Euro-5G: Annual Journal

The project will publish in Q3 2017 the second edition of its *European 5G Annual Journal*. This issue of the Journal will be produced in collaboration with the H2020 projects to extract their exceptional achievements and to present them in the best possible way for broad public, but also presenting technical programme achievements on high-level for wide spectrum of researchers and managers.

This represents a significant opportunity to disseminate the activities of the project. 5G-ENSURE will contribute by reporting the goals of the project, the major achievements/innovations during the second year and KPIs (Key Performance Indicators).

7.4.4 5G Networks: a European Vision Book

The book 5G Networks: an European Vision is an initiative that comes from Rui Luis Aguiar (Universidade de Aveiro/Instituto de Telecomunicações Head of Networks and Multimedia), Jean Sebastien Bedo (Head of Networks Foresight and Strategy, Orange Labs Research), David Kennedy (Director Eurescom GmbH) and Bernard Barani (European Commission DG-Connect).

The objective is on one hand, to bring together in a single book a review of the technical concepts explored inside the funded EU Phase 1 projects. On the other hand, the aim is to make this book a reference for the novel researchers that will be engaged in this next phase, and a simple-to-read overview of the work already done.

The book is structured to present a snapshot of the future 5G networks, with a strong emphasis on the European Vision. The book will contain an overall view of the multiple aspects that will be required for the realization of the future networks, presenting state-of-the-art developments from different projects. The first part of the book will set the stage for understanding the 5G ideas and concepts. The second part of the book will be a comprehensive set of chapters addressing different technologies required for building 5G networks. Finally, the third part of the book will contain some discussion on future paths for the 5G networks.

5G-ENSURE has lead the Security chapter of the book. This chapter is mainly devoted to work engaged on 5G Security within 5G-PPP Phase 1. Starting from areas of major concerns for 5G Security (namely IAM, Trust, Privacy, Security Monitoring and Network Management and virtualization) it reports on security requirements derived from innovative use cases collected and which were used to drive the 5G Security Vision. The 5G Security Technical Roadmap initiated in support of Vision accomplishment is then introduced detailing security enablers in scope both in terms of product vision and features planned. The 5G Security architecture presentation follows and shows strong anchorage in true standardization efforts also encompassing enablers covered and beyond. To complete the picture, the 5G Security tested which was setup to get installed/deployed and so integrated 5G security enablers once implemented is advertised together with procedures attached. The chapter ends by reporting on joint work engaged across 5G-PPP Projects mainly through 5G-PPP Security WG led by 5G-ENSURE Project since the spearhead on field. It also

stresses additional actions under way (e.g. joint demos, new enabler accommodation) and shows overall sustainability of the work through successive Phase of the 5G-PPP.

The plan is for the book to be available for the mid of June.

7.5 Joint Events and Dissemination of Results

7.5.1 5G-ENSURE Workshop: Security WG

Security WG Workshop "*5G Security: Phase 1 landscape and foreseen evolutions*" will be held on 12 June at EuCNC 17 event in Oulu, Finland . The proposal has been presented by 5G-ENSURE on behalf of 5G PPP Security WG.

The workshop builds on the work conducted on 5G Security by the 5G PPP Security WG created and coordinated by the 5G- ENSURE project (5G Enablers for network and system security and resilience https://5g-ppp.eu/5g-ensure/), one of the 5G-PPP projects from the European Union's Horizon 2020 research and innovation programme.

The purpose of the workshop is threefold:

- Present the 5G Security Landscape whitepaper, as result of the exchange and collaborative work conducted with other 5G PPP Phase 1 projects active or interested in the security field (CHARISMA, SELFNET, 5G- NORMA, SONATA, 5G-Ex, SPEED-5G, COGNET, SESAME, VIRTUWIND, SUPERFLUIDITY, METIS II). The whitepaper has a focus on areas of shared topics (e.g. 5G Security architecture, 5G Privacy, Trust, Security monitoring and management, Slicing/Virtualisation, Standardisation) which have been clearly identified, by the 5G-PPP projects involved, as priority areas for 5G, and for which a common position has been established. The findings can provide a reference point for driving future work on 5G security.
- Open a discussion with other relevant stakeholders to complement the findings coming from the Landscape whitepaper on 5G security with their perspectives. The aim is to discuss the ways forward for 5G security, covering perspectives from political to economic, social and technological, by establishing links between all the domains which are in some way impacted by 5G security.
- Provide the necessary guidance to future projects to continue to advance 5G Security in the right direction while taking advantages not only of findings but also assets coming from Phase 1 projects and manifested through collective work achieved within 5G-PPP Security WG that would help to strengthen cross-project fertilisation.

The workshop is organized under the theme security in the track "NET - Networking", but the technical topics address all the EuCNC tracks.

It will be an half-day workshop structured to have:

- Presentation of the findings of "5G Security Landscape" whitepaper on behalf of the 5G-PPP Security WG
- Keynote with one or two invited speakers
- Panel on "5G Security Perspectives" aiming to bring together representatives of large industry, vertical domains (e.g. Industry 4.0, Energy, Automotive, …), legislation/regulation, large organization such as Interpol of NATO, cyber security institution (e.g. ECSO) or government. Looking at the different perspectives the panel aims to identify security gaps between current industry/agency security practices and the focus of 5G-PPP Phase 1 projects on 5G Security.

The following channels will be used to promote the event:

- Announcement Banner for website, Twitter and LinkedIn with invites to register for EuCNC, which can be shared across the 5G PPP projects through the 5G PPP COMMS Group.
- Social media campaign (led by 5G-ENSURE) to be conducted with the 5G PPP COMMS Group with LinkedIn blog posts and announcements across selected LinkedIn 5G-related Groups:
    - Promotion via the 5G PPP COMMS Group and Technical Board Mailing Lists
- Specific event promotion on 5G-ENSURE and CHARISMA project websites, also on 5G PPP and peer projects

Dissemination of outcomes of the workshop include:

- Post-event executive summary for circulation also at Net Futures 2017
- Short interviews with selected speakers/panellists for promotion on the project website and social media

Newsletter on the main outcomes from the "5G Security Perspectives" panel that highlights the commonalities and the gaps on which to work.

7.5.2 5G Enablers for Network and System Security and Resilience Demo Stand

The EuCNC17 event has been selected as a best opportunity for demonstrating the project results.

5th generation mobile networks will enable new kinds of mobile applications and business opportunities by supporting higher capacities and lower latencies as well as by separating infrastructure from virtual network operators. However, along with the new technologies and business opportunities come new security threats and trust issues that 5G developers must address, in addition to the legacy security threats.

5G-ENSURE has worked until now for a secure, resilient and viable 5G network. The project has specified and developed a set of innovative solutions in the areas recognized as topmost priorities for 5GPPP & 5G Security: AAA, Privacy, Trust, Security Monitoring and Network management & virtualization isolation. The second wave of 5G security enablers and their software release is planned by end of August 2017. In addition a 5G test-bed has been created to provide an environment where the developed security enablers can be easily integrated, deployed and tested. The enablers are linked to major building blocks of the 5G Security Architecture early defined and under consolidation as a reference for future networked ecosystems to enable entirely new business opportunities.

Objective of the EuCNC exhibition is to show some of the results coming from the 5G-ENSURE project, particularly several of the security enablers which have already been developed (so coming from the first release). The aim is to demonstrate the security enhancements these enablers provide individually, through their's advances capabilities/features, but also showcase, the added value they could have collectively (i.e. working in cooperation, with regards to enhancements in access control, privacy, trust, as well as network management and virtualization security).

The exhibition will also be an opportunity to describe how the 5G-ENSURE test-bed (with remote nodes in Rennes, France, and Oulu, Finland) enables the development and testing of complex end-to-end, multi-domain, multi-operator 5G oriented security scenarios.

The demonstration will show 5G security solutions from several project partners (VTT, Telecom Italia, NEC, SICS and Thales) and a geographically distributed 5G test-bed.

The following technologies will be demonstrated:

- Micro-segmentation - i.e. software defined networking based approach for network function virtualization. The technology enables isolation of different 5G applications and user organizations from each other. Consequently, security can be customized based on clients' specific needs.
- Internet of Things - this security enabler provides important new features to the existing AKA protocol that is directly aimed at enabling IoT. It will be demonstrate the capability of a novel group-based AKA protocol that makes the simultaneous authentication of groups of IoT devices much more efficient.

- Security monitoring and trust metrics - the demonstrated monitoring approaches include policy compliance checking and anomaly detection in 5G micro-segments. This combined with real-time trust metric evaluation demonstrates how 1) service providers and end-users can be made more aware of 5G connections trustworthiness and 2) how 5G network can be made more self-resilient.
- Privacy enhancements - the enabler prevents tracking of mobile users by hiding user identifiers. The demonstration will show the privacy enhancement in EAP-AKA through the user identifiers (IMSI) encryption and how its adoption provides evidence of identity trust that can be used to calculate a trust metric value for 5G systems.
- VNF Certification - the enabler certifies trustworthy implementation of the VNF and exposes their characteristics through a Digital Trustworthiness Certificate. The demonstration will show the certificate creation.

As part of the demonstration two scenarios will be also reproduced "factory's video monitoring" and "remote control of an IoT home heating system". It will show privacy and DoS attacks against these applications (in '3G/4G environments') with the objective to provide concreate cases where the adoption and integration of the described enablers allow to address these threats.

7.5.3 Stakeholder Engagement at Events

7.5.3.1 Conferences and Workshops

Table 21: SICS Open House

Event Title: SICS Open House on 17 May 2017 in Sweden	
RISE_SICS is hosting its annual Open House on 17 May to showcase its research and innovation to businesses and large companies. Key partnerships will be in the spotlight, including 5G-ENSURE will a poster presentation and distribution of project fliers.	Swedish businesses, large companies and 5G industry.

Table 22: MOST 2017

Event Title: Mobile Security Technologies (MoST) 2017 on 27 May 2017 in San Jose, CA (U.S.) **Co-located event**: IEEE Symposium on Security and Privacy Oxford have also been invited to Black Hat USA and co-located meeting with GSMA Device Security Group	
University of Oxford: paper presentation, "Mobile subscriber WiFi privacy", has been selected to receive the Best Paper Award by the MOST 2017 Program Committee.	Researchers, practitioners, policy makers, and hardware and software developers of mobile systems to explore the latest understanding and advances in the security and privacy for mobile devices, applications, and systems.
Weblinks: http://5gensure.eu/events/5g-ensure-paper-ieee-mobile-security-technologies-most-2017 http://www.ieee-security.org/TC/SPW2017/MoST/	

5G-ENSURE has identified other potential events for disseminating its results, including possible showcase events. For the latter, 5G-ENSURE is considering engagement with its standards synergies, its Advisory Board and continued F2F interaction with the 5G PPP Security WG. Journalists have also been identified to support media outreach should this prove a feasible option.

Table 23: Potential Events for 5G-ENSURE

Event	Date & Venue
Global 5G	24-25 May, Japan https://5g-ppp.eu/wp-content/uploads/2016/11/The-3rd-Global-5G-Event-in-Tokyo-Japan.pdf
IEEE ICC 2017-4th International Workshop on 5G Architecture (5G-NORMA)	25 May, Paris http://icc2017.ieee-icc.org/workshop/5garch-2017-4th-international-workshop-5g-architecture
Net Futures	28-29 June, Brussels
2ND International Workshop on Security in NFV-SDN (SNS 2017)	3 July, Bologna, **5G-ENSURE & CHARISMA**
Helsinki 5G Week, 18-21 September	**IEEE CSCN 2017 collocated with the IEEE 5G-IoT Summit Helsinki** **5G PPP,** http://www.helsinki5gweek.org/
IEEE NFV-SDN 2017, 6-8 November	http://nfvsdn2017.ieee-nfvsdn.org/

8. Conclusions and Next Steps

8.1 5G Security Standardisation Landscape

The 5G-ENSURE analysis of the 5G security standardisation confirms that 3GPP and ETSI TC Cyber as the main targets for the project: 15 direct contributions presented since the beginning 2016, most of them agreed. Additional contributions are planned and will be presented during the last 6 months of the project.

- NIST has confirmed its interest in 5G-ENSURE project enablers and research results, in particular: Fine-grained Authorisation Enabler, Privacy, Federative Auth+ID, IoT/Group-based authentication. Due to the positive outcomes, activities have increased and also include planned F2F interactions as opportunities to showcase the project's R&I.
- ETSI has recognised 5G-ENSURE as one of main 5G Security actors and includes the 2nd International 5G-ENSURE workshop in the official ETSI Security Week 2017 agenda.

5G-ENSURE has also engaged with stakeholders to identify new synergies and knowledge exchanges:

- 5G-ENSURE has interacted with ITU-T to agree on an interview investigating current studies on 5G security. This exchange has led to the dedicated analysis of the 5G standardisation landscape submitted to ITU-T SG 17. ITU-T confirmed it has not yet started specific activities on 5G security. Interactions are continuing both on the 5G security analysis and the open consultation 2017, identifying also opportunities for F2F interactions.
- The above analysis has also been submitted to the EC to ensure timely updates are made available with respect to the EC's ICT standardisation priorities.
- A new synergy has been established with 5G Infrastructure Association (Secretariat General) as part of the EU drive towards greater participation in standardisation. An initial meeting is taking place during EuCNC to share the project's experiences and define future steps.

Contributions:

- 5G-ENSURE has provides several requirements for 5G privacy to 3GPP SA3 study work on 5G Security.
- Two of the 5G-ENSURE enablers have been proposed to 3GPP SA3 and are now under discussion and evaluation.
- The 5G-ENSURE Standardisation Plan has been well received by the community, increasing interest in related activities. This is a good basis for future discussions at the 2nd International workshop and beyond.

8.1.1 Summary of Next Steps

- Share findings of the open consultation during the 2nd International Workshop and subsequently through dedicated blog posts, relevant events, with the 5G PPP community, ITU-T, NIST and the 5G IA.
- Provide an Executive Summary of the 2nd International Workshop to be widely broadcast amongst the project's community, relevant events, with the 5G PPP community, ITU-T, NIST and the 5G IA.
- Produce and circulate a media article on how research findings can make valuable contributions to standardisation, including ETSI channels.

8.2 Dissemination of results, 5G PPP Collaboration and Visibility

5G-ENSURE is an active contributor to the 5G PPP, chairing the Security WG, which is poised to deliver its white paper on phase 1 security landscape. 5G-ENSURE also participates is several other WGs and has contributed to other white papers that have been published in early 2017. The project is also active in the COMMS Group, providing guidance on communications and stakeholder engagement, including the media.

5G-ENSURE continues to target top-tier journals and renowned conferences as venues for disseminating its research results, for example, on privacy issues and theory and applications of information security. The presentation at Black Hat Europe generated 20 press clippings, helping to increase awareness. 5G-ENSIRE has also played a key role in the IEEE workshop series on security in SDN and NFV, with the 2nd edition planned for July 2017.

Partners have also ensured high visibility of the 5G test-bed at trade fairs as key to supporting its sustainability and offering an SME partner new media channels for its work.

Finally, timely updates on 5G-ENSURE outputs shared across all stakeholder groups through in-house newsletters and social media.

8.2.1 Summary of Next Steps

- Widely disseminate the Security WG white paper at events such as EuCNC, 2nd International Workshop, amongst the 5G PPP community and stakeholders.
- Intensify dissemination of all project outputs as they become available across communities and media channels.
- Provide and promote insightful reports from future events.

8.3 Stakeholder Engagement

Direct engagement with stakeholders has been key to building a vibrant global community around 5G security, privacy, trust and standardisation. 5G-ENSURE has recruited an average of 80/month new connections on LinkedIn since July 2016. 5G industry represents the largest portion of this community as important for building consensus. 5G-ENSURE has also achieved excellent representation of specialists from target standards organisations. The largest growth has come from SMEs with an increase from 62 to 136 small companies joining 5G-ENSURE during the period covered.

5G-ENSURE Twitter is an international community spanning 49 countries worldwide with an average of 27 new followers/month since the start of the project. Active members are from key hotspots in both mature and transition markets. This community also includes social media influencers, with whom engagement will grow as outputs become available.

8.3.1 Summary of Next Steps

- Analyse the SEO for the 5G-ENSURE website to ensure it reflects the project's outputs and make any necessary improvements to home page and key sections, including more dynamic formats.
- Intensify activities on Twitter and LinkedIn to ensure traffic is driven directly to major outcomes and outputs.
- Design and promote dynamic content and visuals, including videos on outputs, highlighting unique selling points.
- Ensure overall messaging is geared towards the exploitation plans, both collectively and individually.
- Keep the community abreast of updates with regular newsletters.

8.4 Update to D5.5

At the end of the funding lifecycle, 5G-ENSURE will produce an updated version of this deliverable to cover all major activities and resulting impacts. This update will ensure that all stakeholder are aware of the results achieved, including the 5G-ENSURE community, the 5G PPP, the IA, the EC and target standardisation organisations.

Each major outcome will be accompanied by a high-impact visual and/or video to help convey the message clearly and concisely.

Annex 1 – Press Clippings and Visibility

Major research findings on the research conducted by the University of Oxford were presented and demonstrated by Piers O'Hanlon and Ravishankar Borgaonk at the Black Hat Europe security conference in early November 2016: WiFi-based IMSI Catcher, leading to considerable press coverage. Visibility will help to flag privacy issues at the highest levels and ensure they are swiftly addressed.

Press clippings:

The Register: Build your own IMSI slurping, phone stalking stingray-lite box, using bog-standard Wi-Fi, http://www.theregister.co.uk/2016/11/03/wifi_imsi_catcher/.

Network World: The great smartphone security scare: Your mobile can be hijacked and tracked without you knowing!, http://www.networkworld.com/article/3138468/security/mobile-subscriber-identity-numbers-can-be-exposed-over-wi-fi.html.

PC World: Mobile subscriber identity numbers can be exposed over Wi-Fi, http://www.pcworld.com/article/3138472/security/mobile-subscriber-identity-numbers-can-be-exposed-over-wi-fi.html.

SC Magazine: Black Hat EU: researchers remind that IMSI catchers still a threat, http://www.scmagazineuk.com/blackhat-eu-researchers-remind-that-imsi-catchers-still-a-threat/article/570453/.

International Business Times: The great smartphone security scare: Your mobile can be hijacked and tracked without you knowing!, http://www.ibtimes.co.uk/great-smartphone-security-scare-your-mobile-can-be-hijacked-tracked-without-you-knowing-1589716.

Best Security Search: Cell phones can be traced via Wi-Fi, http://bestsecuritysearch.com/cell-phones-can-easily-traced-via-wifi/.

The Intercept: Hackers and law enforcement could hijack Wi-Fi connections to track cellphones, ttps://theintercept.com/2016/11/07/hackers-and-law-enforcement-could-hijack-wifi-connections-to-track-cellphones/.

The Hacker News: Wi-Fi can be turned into IMSI Catcher to track cell phone users everywhere, http://thehackernews.com/2016/11/imsi-track-cellphone.html

Bitshacker: Wi-Fi can be turned into IMSI Catcher to track cell phone users, http://bitshacker.com/2016/11/04/wi-fi-can-turn-imsi-catcher-track-cell-phone-users/

Naked Security: Who needs a stingray when Wi-Fi can do the job?, https://nakedsecurity.sophos.com/2016/11/08/who-needs-a-stingray-when-wi-fi-can-do-the-job/

01 Net.com (French): Comment le Wi-Fi des opérateurs mobiles permet de pister les abonnés, http://www.01net.com/actualites/comment-le-wi-fi-des-operateurs-mobiles-permet-de-pister-les-abonnes-1055430.html.

Computer World (Hungarian): Ellophatók a mobil előfizetők azonosítói wifin keresztül, http://computerworld.hu/computerworld/ellophatok-a-mobil-elofizetok-azonositoi-wifin-keresztul.html.

Version (Danish): Mobilbrugeres ID-nummer kan opfanges fra almindeligt wifiudstyr, https://www.version2.dk/artikel/forskere-forvandler-almindeligt-wifi-prisvenlig-imsi-catcher-1020909.

Intelligence Online: Fake Wi-Fi hotspot replaces IMSI catcher, https://www.intelligenceonline.com/corporate-intelligence_terabytes/2016/11/09/fake-wi-fi-hotspot-replaces-imsi-catcher,108188976-ART.

TechWorm: Cell Phone Users can be tracked easily using just WiFi and here's how, http://www.techworm.net/2016/11/cell-phone-users-can-tracked-easily-using-just-wifi-heres.html.

XaKep: WiFi IMSI-Catcher, https://xakep.ru/2016/11/04/wi-fi-imsi-catcher/.

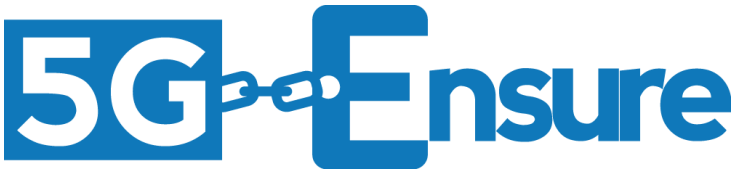
SecNews: Πώς μπορείτε να εντοπίσετε εύκολα χρήστες κινητών μέσω WiFi (Greek), https://secnews.gr/150196/%CF%80%CF%8E%CF%82-%CE%BC%CF%80%CE%BF%CF%81%CE%B5%CE%AF%CF%84%CE%B5-%CE%B5%CE%BD%CF%84%CE%BF%CF%80%CE%AF%CF%83%CE%B5%CF%84%CE%B5-wifi/.

The Tech News: Learn Tracking Cell Phones Using WiFi Connection, http://thetechnews.com/2016/11/12/learn-tracking-cell-phones-using-wi-fi-connection/.

Univers Free Box: Deux chercheurs dénoncent le Wi-Fi opérateur qui piste les abonnés (French), http://www.universfreebox.com/article/37017/Deux-chercheurs-denoncent-le-Wi-Fi-operateur-qui-piste-les-abonnes.

Autobild: Si usas WIFI publico, ten cuidado con esto, http://www.autobild.es/noticias/si-usas-wifi-publico-ten-cuidado-con-esto-304613.

Annex 2 – Extension to Deliverable D5.5 "Final report on communication, marketing and standardisation Press Clippings and Visibility"



Extension to Deliverable D5.5
Final report on communication, marketing and standardisation

Project name	5G Enablers for Network and System Security and Resilience	
Short name	5G-ENSURE	
Grant agreement	671562	
Call	H2020-ICT-2014-2	
Delivery date	20.11.2017	
Dissemination Level:	Public	
Lead beneficiary	Trust-IT	Stephanie Parker, s.parker@trust-itservices.com
Authors	Trust-IT: Stephanie Parker, Silvana Muscella Telecom Italia: Luciana Costa and Paolo de Lutiis All partners have contributed through focused activities, coordination and reporting of impacts.	

Executive summary

5G is considered to be one of the most transformative technologies, playing a crucial part in the digital single market and its objectives to revitalise the European economy. A multi-stakeholder dialogue on the European and global levels bringing consensus on early standardisation on 5G security represents a very important milestone as 5G developments get under way.

The mission of 5G-ENSURE to become the reference project on 5G security, places emphasis on timely contributions to standardisation under WP5, which also commits to raising considerable awareness around the projects outputs to a diverse set of stakeholders. Joint activities and knowledge exchange across the 5G PPP also form an important goal of the project.

This document is an extended version of D5.5 (April 2017) with regard to the communication, marketing and standardisation undertaken by 5G-ENSURE in the period May to October 2017. It presents the overall impact achieved through pre-defined KPIs and qualitative metrics to demonstrate relevance for the targeted stakeholders. It reports on the dissemination of project results and findings through peer-reviewed papers and presentation at technical events, including external coverage achieved. It covers project showcases through demos and presentations at events across Europe, as well as collaborative work within the 5G PPP joint programme, spanning Work Group publications and workshops while providing the basis for sustainable collaboration.

Another example of sustainable work comes from participation in global 5G security standardisation, reporting on the latest contributions, takeaways from the 2nd international workshop during ETSI Security Week, findings from the 2nd open consultation, and insights from NIST. Actions undertaken provide the foundations for future contributions to 5G security.

Central to sustainable actions is the strong, global community developed over the project life cycle and its continuous growth. This document details community members forming part of the 5G ecosystem, showing the value of professional networks like LinkedIn in conveying key messages in an interactive and informative way, as well as impacts through engagement on Twitter as another global communications channel.

Finally, it provides a plan for post-project communications marketing to ensure full coverage of project outcomes and assets moving forward.

Foreword

5G-ENSURE belongs to the first group of EU-funded projects which collaboratively develop 5G under the umbrella of the 5G Infrastructure Public Private Partnership (5G PPP) in the Horizon 2020 Programme. The overall goal of 5G-ENSURE is to deliver strategic impact across technology and business enablement and standardisation by realising a vision for a secure, resilient and viable 5G network. The project covers research & innovation - from technical solutions (5G security architecture and test bed with 5G security enablers) to market validation and stakeholders engagement - spanning various application domains.

D5.5 extension reports on the last Communication, Marketing and Standardisation activities covering the period May to October 2017 acording to the plan in D5.5 – Second Report on communication, marketing and standardisation. The report provides an overview of a consolidated community around 5G and 5G security and privacy issues, spanning the professional LinkedIn network, liaison with standardisation organisations and impacts on social media channel, Twitter. In addition, it reports on overall stakeholder engagement and visibility of 5G-ENSURE, as a means to quantify and qualify its contributions to the 5G PPP and provide a foundation for exploitation where reputation and trust play a key contributing role. The document also provides a post-project plan to ensure results are broadcast as widely as possible

Disclaimer

Copyright notice

Table of Contents

Abbreviations

3GPP	3rd Generation Partnership Project
5G PPP	5G Infrastructure Public Private Partnership
ETSI	European Telecommunications Standards Institute
ICT	Information and Communication Technologies
IETF	Internet Engineering Task Force
ITU	International Telecommunication Union
KPI	Key Performance Indicator in relation to 5G-ENSURE
MFCN	Mobile and Fixed Communications Networks
mMTC	Massive Machine Type Communication
ONF	Open Networking Foundation
NFV	Network Virtualisation Function
NIST	National Institute of Standards and Technology
SDN	Software Defined Network
SMARTER	New Services and Markets Technology Enablers

1. Introduction

1.1 Scope and Purpose

The purpose of *D5.5 Extension* is to report on the actions performed during the period from May to October 2017 and impacts achieved, with the aim of supporting the exploitations plans defined in D5.6.
This document takes stock of the overall impacts and defines plans for the next few months to ensure all outputs and assets are fully covered and broadcast to 5G-ENSURE stakeholders.
It reports on the dissemination of research findings and technical developments, spanning papers, presentations and demos at external events, as well as collaboration with the 5G PPP, including contributions to work groups and joint publications. It summarises the main achievements with respect to 5G security standardisation, the 2nd International Workshop during ETSI Security Week and the main findings of the Open Consultation 2017.
It provides a detailed overview of a consolidated community around 5G and 5G security and privacy issues, spanning the professional LinkedIn network, liaison with standardisation organisations and impacts on social media channel, Twitter. In addition, it reports on overall stakeholder engagement and visibility of 5G-ENSURE, as a means to quantify and qualify its contributions to the 5G PPP and provide a foundation for exploitation where reputation and trust play a key contributing role. To this end, the document also provides a post-project plan to ensure results are broadcast as widely as possible.

1.2 Structure of the Report

The report is structured as:

Section 2 – summarises the objectives, primary and secondary stakeholders. It provides a snapshot of the quantitative metrics (key performance indicators) used as drivers in achieving tangible impacts for 5G-ENSURE. It also provides a qualitative assessment of activities and results, with the aim of demonstrating the relevance and value of the work undertaken in WP5 in support of the technical WPs 2-4.

Section 3 – reports on the main dissemination actions that have taken place in the period between May and October 2017 through papers, technical conferences and demo presentations. This section also covers the main activities undertaken as part of the 5G PPP Joint Programme, showing the different ways in which 5G-ENSURE has contributed to events, work groups and joint publications, including actions to sustain collaboration on 5G security.

Section 4 – focuses on 5G-ENSURE contributions to early 5G security standardisation through direct (individual and joint) contributions to the most relevant standardisation organisations, such as the 3GPP and ETSI. It also documents direct engagement through the 2nd International Workshop, including liaison with members of the Advisory Board and NIST. Finally, it offers insights on the Open Consultation, which has taken place during the period covered by D5.5 Extension.

Section 5 – details the final results for community building through professional and social networks, and overall stakeholder engagement as part of regular activities undertaken by WP5. The overall goal is to show how 5G-ENSURE has attracted interest among its primary and secondary stakeholders to inform and educate them on important security and privacy issues in 5G, foster best practices and showcase results.

Section 6 – summarises the main conclusions and sets out plans for the forthcoming period to ensure all major outputs are broadcast as widely as possible.

Section 7 – comprises annexes covering a complete overview of papers and conferences, an overview of contributions to the 5G PPP programme, contribution to 5G security standardisation, an analysis of the 2nd open consultation and overview of social media and press coverage.

2. Objectives and Stakeholders

5G will only succeed if we all focus on security, privacy & trust, Adrian Scrase, CTO at ETSI and 3GPP

2.1 Main Objectives

The work package is articulated into four tasks, with the following objectives and core activities:

T5.1 – Standardisation, where the strategic goal is to influence the most relevant standardisation organisations early on and map research topics to related standardisation efforts.

- *5G-ENSURE has conducted an in-depth analysis of on-going and planned standardisation efforts related to 5G security since the beginning of the project.*
- *5G-ENSURE has organised 2 international workshops (2016, 2017) to present its work on 5G security and contributions to related standardisation.*
- *5G-ENSURE has conducted two annual open consultations to collect feedback from stakeholders on the directions undertaken and open issues.*

T5.2 – Marketing and Communication, where the strategic goal is the creation and timely delivery of the most effective messages to all major stakeholders, including practical guidance and tools on security and privacy in 5G.

- *5G-ENSURE has designed and developed a website as a central communication tool for its activities and outputs. Branding has been designed around the overall project identity and also to reflect its contributions to the 5G PPP. Collaterals have been regularly updated.*
- *Core messages on the importance of security and privacy, 5G-ENSURE value proposition in driving 5G security and standardisation have been central to achieving WP5 objectives since the very outset.*

T5.3 – Stakeholder Involvement and 5G Security Community Development, where the strategic goal is to define and implement an engagement plan with priority on building a 5G-security-aware community and a strengthened 5G PPP.

- *5G-ENSURE has engaged stakeholders through multiple channels and formats, using professional networks (LinkedIn), social media (Twitter) for regular interactions, raising awareness on security, sharing insights and collaborative work, showcasing results.*
- *5G-ENSURE has disseminated its research findings through targeted journals and conferences in both the EU, U.S. and Australia. All public deliverables have been promoted through 5G PPP channels. In the second year, particular emphasis has been given to demos and dissemination of project assets.*
- *External events, project workshops and trade fairs/exhibtions have been used as key forums for extending outreach to 5G stakeholders from the supply side, SMEs, and standards specialists.*

T5.4 – Market Analysis and Exploitation, where the strategic goal is to support a ready to use test-bed service for the 5G security community and facilitate industrial partners in new product rollout.

- *5G-ENSURE has regularly scanned the landscape for emerging trends and insights on 5G market opportunities in relation to security, and potential revenue streams. The analysis has been extended in year 2 as more information has become available/updated.*
- *5G-ENSURE has provided iterative templates to capture the value proposition and exploitation strategies (collective and individual) for both D5.4 and D5.6, guiding partners towards a collective understanding of objectives.*
- *5G-ENSURE has facilitated partners in adopting the Market and Technology Readiness Levels (MTRL) methodology to combine technology maturity with go-to-market strategy.*

2.2 Primary and Secondary Stakeholders

Primary stakeholders also relate to the 5G-ENSURE joint and individual exploitation plans. The main stakeholders are **5G ecosystem** comprising industry and standardisation organisations:

- **Supply side organisations**, within and beyond the 5G PPP, spanning connectivity providers, suppliers, supply chain companies, including SMEs.
- **Vertical industries** (both large companies and SMEs), such as automotive, energy, factories of the future, healthcare, hi-tech manufacturing, media and entertainment.
    - Industry associations with the potential to speed up the time to reach consensus on priority security and privacy issues, including issues like fraud and identity theft.
- **Phase 1 and Phase 2 projects in the 5G PPP and** national projects covering radio and network technologies, the Euro5G CSA and the work groups within the 5G PPP.
    - Projects contributing to 5G PPP WGs, primarily the Security, Pre-Standardisation, Architecture, Vision and Societal Challenges, Network Management and Quality of Service, and in Q42017, the SME WG.
    - SME innovators, including members of the 5G PPP SME WG (Networld2020 SME).
    - 5G PPP coordination and support actions to increase outreach and visibility.

Secondary stakeholders mostly refer to channels (media, industry/multiplier associations) that help relay communications across their networks and helping to increase understanding of 5G amongst the targeted stakeholders. Specific channels are also targeted to raise awareness of security and privacy and how their role in building trust and confidence. Lastly, these channels can help maximise visibility of 5G-ENSURE, including brand recognition.

- **Telecom media channels** important for reaching 5G industry stakeholders, e.g. TelecomTV, Inside5G, Mobile World, Telecoms.com, Total Telecom, Telecom News, Fierce Wireless Europe,
- **IT and business media channels**, e.g. Computer Weekly, TechTarget, TechTalk, Inside Tech Europe, CloudPro, The Register, ITProPortal, SourceSecurity.com, IT Security Portal, Tech radar. For SMEs: Business Insider, Business Matters, Talk Business Magazine, European CEO, Small Business Magazine.
- **Linked In groups**, e.g. 3GPP & 3GPP 5G Standards, 5G Networld2020 SME WG, IEEE 5G Initiative, 5G PPP, Global Suppliers Association, Wire Communications & Mobile Networks, Software Defined Networks, Information Security Community, Cyber Security Forum Initiative (CSFI), Privacy Professionals, IoT Tech (general and news/events), IEEE IoT.

- Regulators and policy decision makers for the timely sharing of security and privacy issues.

2.3 Main Outputs and Assets

The table below shows the main outputs for each technical WP as an indication of how WP5 has coordinated its activities.

Table 24: Overview of Outputs and Assets

WP2	Golden Nugget for the 5G PPP: - Security Architecture with consensus within the 5G PPP. **Views on the website**: 1702
WP3	Golden Nugget for the 5G PPP: - Security and Privacy enablers with detailed exploitations plans and exemplary business model. 25 enablers with 23 as software releases and 2 as open specifications with maturity levels between 3 and 6, and commercial readiness levels between 3 and 4. The enablers have been presented to international technical constituencies, 5G PPP peer projects (phase 1 and 2), as well as to NIST for feedback on the implementation of sufficiently mature standards and as frontrunners in the context of 5G and related standardisation. **Views on website**: 1500
WP4	Golden Nugget for the 5G PPP: - The 5G Test-Bed with a sustainability plan defined through a business model. The test-bed has been promoted at cyber security and mobile network events. **Views on website**: 759
Other outputs	5G Trust Model. Use cases, risk assessments, Risk Model. Contributions to relevant standardisation organisations (e.g. 3GPP, ETSI) as a sustainable activity through continued partner participation. White Papers published by the 5G PPP: leading editors and co-authors and 5G PPP Annual Journals. Peer-reviewed papers and presentations at technical/scientific conferences. Demos presented at external events (exhibitions and trade fairs). Executive Summaries from WP5 International Workshops. An engaged community and extensive visibility.
5G PPP Joint Programme	White paper by the Security WG (June 2017); EuCNC Workshop on Phase 1 outcomes; Face-to-face meeting of the Security WG (October 2017). Participation in the 5G PPP WGs: Pre-Standardisation; Architecture and SMEs.

Each asset has branding aligned with 5G PPP branding, for example:

Figure 32: Example of Asset Branding

2.3 Measurable Impacts

WP5 uses both quantitative and qualitative metrics to gauge the relevance and impact of its activities in WP5. We use two straightforward processes for defining and measuring an initial core set of key performance indicators (KPIs) for four complementary activities: communications and community building, including stakeholder engagement; standardisation related activities; joint 5G PPP activities and the technical results dissemination.

2.3.1 Key Performance Indicators

The table below shows final progress on the core set of KPIs for WP5 up to October 2017.

Table 25: KPIs for core WP5 activities

KPI	Target EoP	Delta	Total to date	May - October 2017 (D5.5 Ext.)
Twitter followers	500	+176	**676**	69
LinkedIn Connections	650	+388	**1038**	228
Community DB (total contacts)	900	+340	**1240**	120
PR/media content	4	+2	**6**	1
Media coverage & visibility	15	+39	**54**	11
LinkedIn Updates	36	+44	**80**	25
Events, Meetings, Calls - standardisation (excl. project workshops)	6	+12	**18**	6
Events - 5G-PPP Joint activities (incl. Project workshops)	8	+5	**13**	3
Publications and presentations disseminating technical results	12	+7	**19**	4
Technical conferences	8	+21	**34**	13
Publications: joint 5G-PPP	2	+4	**6**	2
2nd Open Consultation on 5G security (starts 04.05.2017)	60	-23	**37**	17

5G-ENSURE has incrementally adjusted its KPIs to achieve high impact: in terms of

- **Community development**: highly relevant community covering the full 5G ecosystem with a wide geographical coverage expanding over time. Linkedin has an average 64 new connections/month (from July 2016) and 28 new Twitter followers/month, including associations and partner organisations acting as multipliers.

- **Stakeholder engagement**: from close interactions with the 5G PPP phase 1 and 2; technical constituencies; standardisation organisations; vertical industries and policy makers.
  LinkedIn has proved to be a very interactive forum, essential for the regular sharing information and increasing consensus around the work of 5G-ENSURE and related 5G topics. 5G-ENSURE is regularly engaged in discussions and achieves high visibility of its activities and achievements through quality and relevant content.
- **Publications**: 5G PPP annual journals and white papers; dissemination of research findings and technical results.
- **Media coverage**: technical media (cyber security; IT); business media and mainstream press.

The only KPI not reached relates to the number of respondents for the Open Consultation. However, the main findings are aligned with prevailing views at 5G events and on professional networks, discussed in more detail in Section 4.

2.3.2 Qualitative Metrics

WP5 has also implemented a set of qualitative aspects to measure the relevance of media activities, technical publications, workshop organisation and external events, and the standardisation roadmap.

QM1*: Readership of media channels where 5G-ENSURE is visible, analysing professions, geographies.* 5G-ENSURE has successfully conveyed issues related to 5G security and privacy to a broad range of stakeholders covering the full spectrum of dissemination and media channels. Good relations with media organisations (e.g. onsite interviews; online engagement) has meant that research findings and new solutions presented at peer-reviewed technical conferences have been made more accessible to IT journalists and the average "wo(man) in the street", for example, with articles published by WIRED and Sky News. 5G-ENSURE partners have also ensured that SME innovations have received excellent media visibility as the basis for post-project dissemination.

QM2*: Readership of journals where technical articles are published, such as reputation, readership and geographies.* 5G-ENSURE has achieved a high number of presentations at technical conferences (1+/month average) and acceptance of peer-reviewed papers by organisations such as IEEE and ACM, demonstrating that its 5G research advances are relevant not only in the EU but also globally (e.g. the U.S. and Australia).

QM3*: Workshops – Matching actual participants with the stakeholder targets.* The 2nd Workshop, From Research to Standardisation took place during the ETSI Security Week, as a premier forum attracting renowned experts and many participants actively involved in standardisation. It complements the recruitment of standards specialists, including high-profile specialists (e.g. chairs, co-chairs), as part of the 5G-ENSURE community development and engagement strategy.

QM4*: Workshops – gauging consensus of participants and the level of interest, e.g. passive and active supporters; passive and active opponents; fence-sitters.* Insights on most technical and standards events have been broadcast on LinkedIn to gauge interest in the community, achieving between 350-850 views per event over the past 12 months. Communications on standards have been extremely well received with over 1400 views/post, while helping to recruit new stakeholders (15-30/announcement). 5G PPP and specialist groups have also been used to share updates. Results point to clear consensus on the goals pursued. Moreover, 5G-ENSURE has continued to engage with ITU-T and NIST as good benchmarks for evaluating the value of R&I and standardisation within 5G-ENSURE.

QM5*: External events, assessing the audiences actually reached at commercial and technical events, influential participants, new contacts and main takeaways.* 5G-ENSURE has played an active role within the

5G PPP and several of its work groups. Promotional activities have ensured good visibility at EuCNC and at the 5GIA level, through a workshop, demo stand and F2F meetings. The community has several large and influential members (as reported below) and has received support on social media from several partners, notably Ericsson and Nokia.

***QM6**: Standardisation roadmap and engagement with standardisation organisations – quality of contributions, types of endorsements, as well as circulation and visibility.* 5G-ENSURE work on standardisation has been very well received by the community, helping to bring in a good number of senior specialists. There have been interactive discussions on the importance of security, privacy and trust on LinkedIn showing that it is a very effective forum for stakeholder engagement, sharing insights from organisations like ETSI and the 5G PPP, reports and slidedecks. Posts on core messaging around 5G have been among the most popular topics. Also, 5G-ENSURE has received positive comments from NIST and its Advisory Board on the direction undertaken for contributions to the 3GPP.

3. Dissemination of Research Findings: Papers and Technical Conferences

3.1 5G-ENSURE papers

Four papers have been published in the period May-October 2017, listed in the table below. The complete list of papers over the 24-month period is provided in Annex 1. Overall, the publications on the website have been viewed a total of **1056 times**, http://5gensure.eu/publications, and over 4000 on LinkedIn.

Title	*Mobile subscriber WiFi privacy*
Author(s)	Piers O'Hanlon; Ravishankar Borgaonkar; Lucca Hirschi
Main findings	The paper details a range of attacks, on a set of widely deployed authentication protocols, that enable a malicious user to obtain and track a user's International Mobile Subscriber Identity (IMSI) over WiFi. These attacks are possibly due to a lack of sufficient privacy protection measures, which are exacerbated by preconfigured device profiles. The paper provides a formal analysis of the protocols involved, examine their associated configuration profiles, and document experiences with reporting the issues to the relevant stakeholders. Lastly, the paper details a range of potential countermeasures to tackle these issues to ensure that privacy is better protected in the future.
Publication/Event proceedings	IEEE Symposium on Security and Privacy's Mobile Security Technologies Workshop (MoST), San Jose, USA, 25 May 2017.

Title	*White-Stingray: Evaluating IMSI Catchers Detection Applications*
Author(s)	Ravishankar Borgaonkar; Shinjo Park; Altaf Shaik; Andrew Martin Jean-Pierre Seifert
Main findings	Evaluating Android apps and test how resistant they are against various attacking techniques. Such an evaluation is important for not only measuring the available defense against IMSI catchers attacks but also identifying gaps to build effective

	solutions.
Publication/Event proceedings	11th USENIX Workshop on Offensive Technologies (WOOT 17)

Title	*Security and Resilience in 5G: Current Challenges and Future Directions*
Author(s)	Ghada Arfaoui, Jos´e Manuel Sanchez Vilchez, Jean-Philippe Wary (Orange Labs)
Main findings	A 5G vision based on softwarisation, providing a non-exhaustive list of current security, trust and resilience issues that are critical to be explored in 5G with reference to 5G outputs.
Publication/Event proceedings	16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-17), 1-4 August 2017.

Title	*Runtime Verification of Temporal Properties over Out-of-order Data Streams*
Author(s)	David Basin, Felix Klaedtke, and Eugen Zalinescu
Main findings	5G tends to be a multi-layered, multi-actor, and multi-access mobile network in order to fulfil the stringent availability, security, privacy and resilience requirements that are usually contradictory. In this paper, we propose a 5G vision based on softwarisation. We provide a non-exhaustive list of current security, trust and resilience issues that are critical to be explored in 5G. Finally, we give some directions to overcome these issues.
Publication/Event proceedings	Proceedings of the 29th International Conference on Computer Aided Verification (CAV). Lecture Notes in Computer Science, volume 10426, pages 356-376. Springer, 2017

3.2 5G-ENSURE at international technical conferences

The tables below show the main impacts of 5G-ENSURE at international technical conferences. A complete list of events is provided in Annex 1.

Event	BCS Action Research Forum: Safety Critical Systems Club
Date and Venue	31 October 2017, BCS (The Chartered Institute for IT), London
Focus	This invitation only meeting focuses on the question whether the Cloud and IoT make a difference to our understanding of SafeSec software. The presentation will.
Stakeholder category/ies	IT researchers and practitioners involved in developing and operating safety-critical and security-critical applications.

5G-ENSURE role	Mike Surridge gives a presentation highlighting the need to consider security risks in the end-to-end system, the network as an active component, and to have a clear understanding of security responsibilities and trust assumptions between developers and manufacturers, network operators, and users.
Web link	https://scsc.org.uk/e532

Event	**ACM SIGCOMM 2017**
Date and Venue	21 -25 August, UCLA campus in Los Angeles, CA, U.S.
Focus	Annual conference of the ACM Special Interest Group on Data Communication (SIGCOMM) on the applications, technologies, architectures, and protocols for computer communication. The event focus on aspect related to Network Functions Virtualization and Network monitoring of main interest for 5G-ENSURE. The event also dedicates sessions for demonstrations showing works-in-progress in the field of communications networks, including technical design and engineering.
Stakeholder category/ies	Industry, professionals and researchers for deeply technical hands-on sessions and discussions.
5G-ENSURE role and outcomes	RISE SICS presented a demo on Bootstrapping Trust - Safeguarding VNF Credentials
Web links	http://conferences.sigcomm.org/sigcomm/2017/program.html | http://www.5gensure.eu/events/5g-ensure-demo-sigcomm-2017

Event	**11th USENIX Workshop on Offensive Technologies (WOOT'17)**
Date and Venue	14-18 August 2017, Vancouver
Focus	Security is the main focus of the event with particular attention to tools and techniques for attack, offensive security technology, exposing poorly understood mechanisms.
Stakeholder category/ies	Bring together researchers and practitioners in all areas of computer security. Offensive security is today a large-scale operation managed by organized, capitalised actors. In the field's infancy, offensive security research was conducted separately by industry, independent hackers, or in academia. Collaboration between these groups could be difficult. Since 2007, the USENIX Workshop on Offensive Technologies (WOOT) has aimed to bring those communities together.
5G-ENSURE role and outcomes	Ravishankar Borgaonkar and Andrew Martin (University of Oxford) presented paper on *White-Stingray: Evaluating IMSI Catchers Detection Applications.* The paper complements on-going work by the University of Oxford on release 2 of the enabler "Security Indicator" for 5G networks. This is one a set of enablers developed within 5G-ENSURE.

Web links	https://www.usenix.org/conference/woot17 | http://www.5gensure.eu/events/new-research-paper-privacy-mobile-networks-woot-17

Event	**TrustCom conference**
Date and Venue	1-4 August 2017, Sydney, Australia
Focus	A forum to present and discuss emerging ideas and trends in highly challenging research field with particular focus on Trust, Security and Privacy in Computing and Communications.
Stakeholder category/ies	Bring together researchers and practitioners in the world working on security, privacy, reliability, dependability, survivability, availability, and fault tolerance aspects of computer systems and networks.
5G-ENSURE role and outcomes	Presentation of a research paper "5G: Current Challenges and Future Directions"
Web links	http://www.5gensure.eu/events/5g-ensure-demo-sigcomm-2017

Event	2017 ACE-CSR Conference
Date and Venue	28-29 June May 2017, Nottingham
Focus	Understanding the potential future developments of software, services and big data applications.
Stakeholder category/ies	Cyber security researchers and practitioners from UK/Allied government agencies, academia and industry.
5G-ENSURE role	Mike Surridge from IT Innovation participated in the discussions, running demos of Trust Builder and using them to promote consideration of trust as well as security in end-to-end networks. Interaction between government officials and researchers. Mike Surridge had a useful meeting with NCSC staff leading to a potential exploitation opportunity involving an evaluation of Trust Builder.
Web link	N/A: meeting is classified UK OFFICIAL.

Event	**Blackhat Las Vegas Conference**
Date and Venue	22-27 July 2017, Mandalay Bay
Focus	Black Hat is the world's leading information security event, providing attendees with the very latest in research, development and trends. It is an event dedicated to security and latest vulnerabilities, with talks covering everything from reverse engineering and cryptography to network defense and human factors of security.

Stakeholder category/ies	More than 15.000 attendees. Researchers, industry security experts, vendors.
5G-ENSURE role and outcomes	Ravishankar Borgaonkar and Andrew Martin (Cyber Security at Oxford University) presented the research on *New adventures in spying 3G and 4G users: Locate, Track & Monitor"*
Web links	https://www.blackhat.com/us-17/ | http://5gensure.eu/events/oxford-university-presents-new-adventures-spying-3g-and-4g-users-blackhat-las-vegas

Event	**Shakacon IX 2-Day IT security conference**
Date and Venue	12-13 July 2017, Hawaii Prince Hotel Waikiki
Focus	The conference focuses on security topics and is an opportunity for industry, government, academia, and independent experts to exchange together
Stakeholder category/ies	Shakacon attracts top security professionals and executives
5G-ENSURE role and outcomes	Piers O'Hanlon, University of Oxford, presented the paper, "*Mobile subscriber WiFi privacy".*
Web links	https://www.shakacon.org/conference/ | http://5gensure.eu/events/shakacon-ix-2-day-it-security-conference-july-12-13-2017-hawaii-prince-hotel-waikiki

Event	**Cyber Security Oxford Industry Day**
Date and Venue	9 June 2017, Oxford, UK
Focus	Bringing together experts from around the world to address the cyber security challenges Interaction between members from the cyber security industry, and students and academics at Oxford. Ravi and Piers had a meeting with a Vodafone security engineer
Stakeholder category/ies	Researchers and industry security experts
5G-ENSURE role and outcomes	University of Oxford (Piers & Ravi).

Event	VIVACE Expert Advisory Board Meeting
Date and Venue	07 June 2017, London

Focus	Focus on law enforcement.
Stakeholder category/ies	VIVACE is a consortium established to support UK law enforcement agencies by providing innovative solutions to problems in the communications data space.
5G-ENSURE role	Mike Surridge from IT Innovation contributed to the debate, highlighting the likely impact of 5G technology on the use of communication data for law enforcement. By attending this event, we were able to ensure that results from 5G-ENSURE will be taken into account by public authorities who set policies and provide for law enforcement agencies to access communication data.
Web link	See www.vivace.tech.

Event	**Security BSides London 2017**
Date and Venue	7 June 2017, London, UK
Focus	Security BSides is a community-driven event built for and by information security community members. The goal is to expand the spectrum of conversation beyond the traditional confines of space and time. It creates opportunities for individuals to both present their research and encourages collaboration.
Stakeholder category/ies	Researchers and security experts. A large audience (about 200) interested in the presentation. Piers was interviewed by a journalist from Sky news.
5G-ENSURE role and outcomes	Presentation of paper on *Mobile Subscriber WiFi Privacy*
Web links	http://5gensure.eu/events/university-oxford-present-bsides-security-conference-7-june-2017-london
Impact	http://news.sky.com/story/too-easy-to-track-mobile-phones-because-of-security-weakness-expert-warns-10908517 http://www.ohirensblog.com/2017/06/experts-warn-of-ways-hackers-track-our.html http://5gensure.eu/events/university-oxford-present-bsides-security-conference-7-june-2017-london http://5gensure.eu/news/5g-ensure-reseach-findings-time-address-privacy-issues-wireless-networks-5g.

Event	**Öresund Security Day**
Date and Venue	30 May 2017, Copenhagen, Denmark
Focus	The objective of the Oresund Security Day was to increase the scientic interaction in security in the Oresund region. It provided a platform for exchange of ideas, discussion and co-operation among the research groups tha focus on security in the Oresund area. It provided the opportunity to meet one another, create an

	environment for joint work, and strengthen the visibility of security research in Scandinavia.
Stakeholder category/ies	Security researchers
5G-ENSURE role and outcomes	Presentation of the Bootstrapping Trust enabler
Web links	http://www.demtech.dk/publications/osd17-program/
Impact	The workshop was an occasion to demonstrate in live one of the security enabler developed in 5G-ENSURE project. https://vimeo.com/217788815

Event	**Most 2017 IEEE Symposium on Security and Privacy's Mobile Security Technologies Workshop**
Date and Venue	25 May 2017, San Jose, CA (US)
Focus	Present the research findings on mobile privacy and security. Best Paper Award: https://www.ieee-security.org/TC/SP2017/awards.html.
Stakeholder category/ies	Brings together researchers, practitioners, policy makers, and hardware and software developers of mobile systems to explore the latest understanding and advances in the security and privacy for mobile devices, applications, and systems
5G-ENSURE role and outcomes	Presentation of paper on *Mobile Subscriber WiFi Privacy*
Web links	http://www.ieee-security.org/TC/SPW2017/MoST/ | http://5gensure.eu/events/5g-ensure-paper-ieee-mobile-security-technologies-most-2017 with post-event report: http://5gensure.eu/events/5g-ensure-paper-ieee-mobile-security-technologies-most-2017

Event	**RISE SICS Open House**
Date and Venue	17 May 2017, Kista, Sweden
Focus	Annual event showcasing R&I and facilitating new colaborations with industry.
Stakeholder category/ies	Brings together researchers, practitioners, policy makers, and hardware and software developers of mobile systems to explore the latest understanding and advances in the security and privacy for mobile devices, applications, and systems
5G-ENSURE role and outcomes	Demo of the IoT Enabler
Web links	https://www.sics.se/events/sics-open-house-2017 | http://5gensure.eu/events/sics-open-house-2017-17-may-2017

	https://twitter.com/rasty1611

3.2.1 Visibility and Coverage of Research Results

The research findings on privacy issues (University of Oxford) has been one of the most popular topics on social media (Twitter) and professional networks (LinkedIn).

The research findings have also received considerable media coverage (interviews and articles). The following images provide a sample of the impacts achieved.

Figure 33: Twitter Impacts on Wireless Flaws

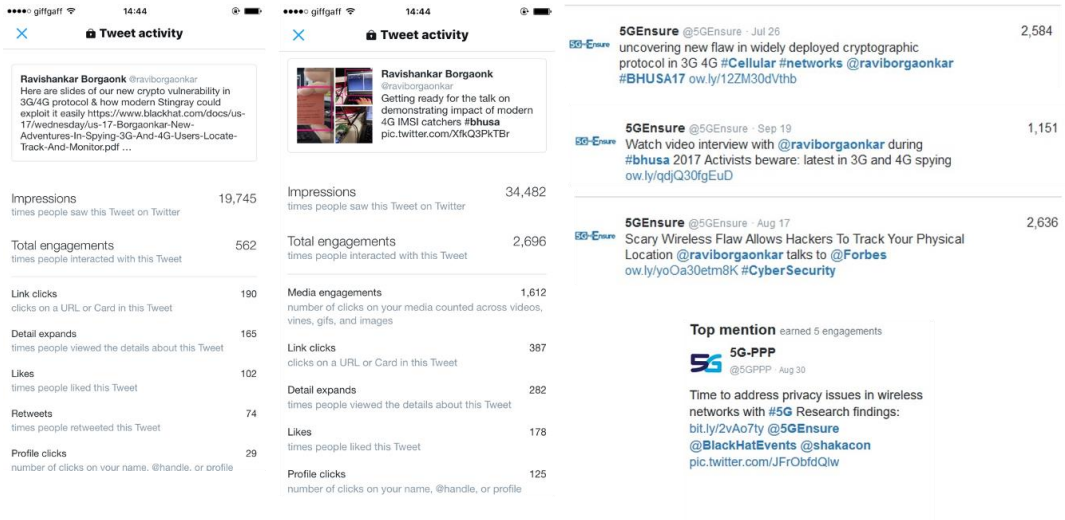
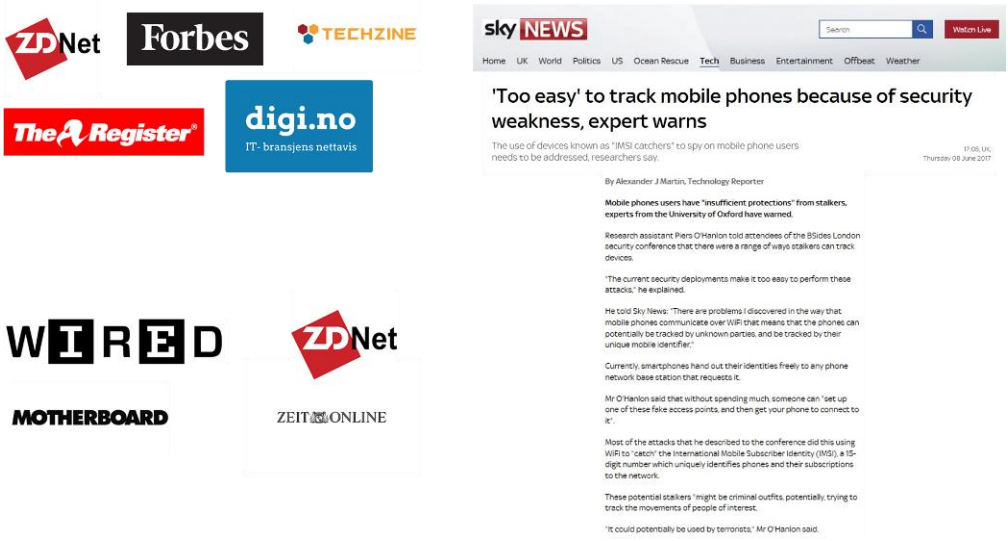


Figure 34: Shakacon: LinkedIn Engagement

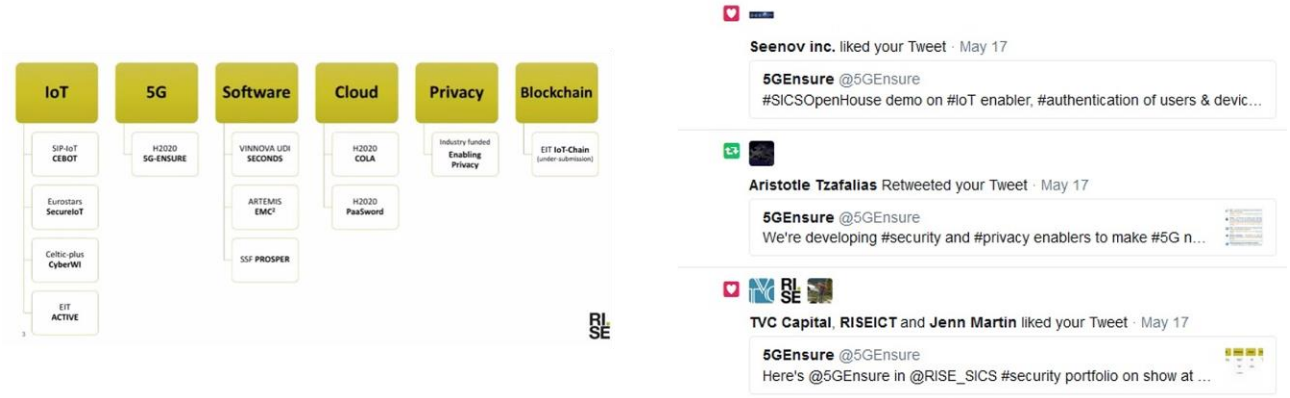
Events like B-Sides London, and Black Hat U.S. have attracted journalists from technology media and mainstream press, who have engaged with representatives from the University of Oxford for interviews. Coverage is reported on the project website, http://5gensure.eu/news/oxford-university-uncovers-wireless-flaw-blackhat-usa-2017 and http://5gensure.eu/news/imsi-catcher-detection-apps-key-research-findings-presented-usenix-workshop-offensive.

Figure 35: Press Coverage of Research Findings



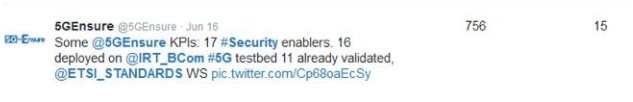
Other examples of visibility through social media include the **RISE SICS Open House**. More examples are presented in subsequent sections.

Figure 36: RISE SICS Open House



During the period, 5G-ENSURE has continued to support the visibility of B<>COM at external events and in relation to the test-bed as a solid basis for post-project promotion of the sustainable test-bed services.

Figure 37: B-COM Visibility



3.3 5G-ENSURE at EU Exhibitions

3.3.1 EuCNC Demo Stand

EuCNC 2017 was an opportunity to host a booth in the exhibition area and showcase the main achievements to date, particularly to show in action some of the security and privacy enablers developed within 5G-ENSURE.

5G-ENSURE partners VTT, Thales, NIXU and SICS were hosts and played a key role in providing and showing the demos and videos on display.

The demo presented by VTT was in two parts. The first part showed how the enablers can detect anomalies from a substantial network attack, thereby blocking suspicious users. The second part featured an end-to-end connection between VTT and b<>com testbed. The demonstration showed how to gain the access to a website running in the microsegment at b<>com premises using IMSI.

SICS provided a demonstration of the “Internet of Things Enabler”. The enabler provides a new definition of protocols for credential management and authentication of users and devices, such as sensors and IoT devices in general. The demo showed the capacity of the group-based AKA protocol to make simultaneous authentication of groups of devices.

Thales showed the “VNF Certification Enabler”. The enabler certifies trustworthy implementation of the VNF and exposes their characteristics through a Digital Trustworthiness Certificate. The demo showed the different steps to create the certification.

Figure 38: Visitors at the EuCNC 2017 Booth

Figure 39: Features at the EuCNC 2017 Booth

The booth was widely promoted before and after the event to ensure engagement with interested EuCNC participants and complementarities with the goals of the 5G PPP security WG workshop.

Overall, the demo booth attracted 5,307 Twitter impressions over the 3.5 days of the exhibition, with an average of 1,326/day, illustrating that the event was an important venue for showcasing 5G-ENSURE, and particularly its security and privacy enablers. A sample of the impacts is showed in the image below.

Figure 40: Impact of EuCNC Demo Booth on Twitter

Finally, hosting the EuCNC stand was an opportunity to contribute to the 5G PPP video suite recorded at the event based on a set of pre-defined questions to the coordinators. The 5G-ENSURE video also features demos at the stand and an overview of how the project has contributed to the joint programme. The video is available on YouTube and the 5G PPP Video Channel: https://5g-ppp.eu/video/.

3.3.2 EU Cyber Security Month Events

5G-ENSURE has leveraged October 2017 as the EU Cyber Security Month to support the dissemination of its outputs, particularly the 5G-ENSURE Trust Model.

Two events were choosen as suitable venues:

- **DSS ITSEC 2017, 19 October 2017, Riga**: DSS ITSEC is an annual conference series that gathers participants from local, regional, and international businesses, governments and government agencies, tech communities, national and public sectors. The event counts the **European Cyber Security Organisation** (ECSO) among its supporters.
  Website: https://www.dssitsec.eu/
  The presentation on the Trust Model will be included in the event proceedings. In addition, 5G-ENSURE hosted a small stand aimed at increasing the visibility of the Trust Model and at promoting:
  - The 5G PPP Security WG White Paper: Phase 1 Security Landscape.
  - The 5G-ENSURE main outputs: security and privacy enablers, test-bed and security architecture.
- **European Cyber Threat Summit, 24 October 2017 in Dublin:** https://cyberthreatsummit.com/: it attracts cyber security experts from all over Europe to discuss all aspects of cyber security including issues such as GDPR, the NIS Directive and of course BREXIT. There were three distinct streams running concurrently; "Strategic", "Operational" and "Technical" https://cyberthreatsummit.com/agenda.php. The presentation on Trust Model was part of the Technical stream devoted to present solutions in action also to demonstrate technical solutions in operation. 5G-ENSURE also hosted a small stand from which to distribute the white paper and branded gadgets.

Figure 41: Dissemination of the 5G Trust Model

3.4 Joint Programme Collaboration

3.4.1 5G PPP Work Groups

5G-ENSURE has continued to play an active role in the 5G PPP joint programme, particularly in the Security WG, ensuring its sustainability beyond the life cycle of the project funding. The main activites and outputs are summarised in the table below, with detailed accounts in subsequent sections for Security, Pre-standardisation, an architecture. A complete overview over the project life cycle is provided in Annex 2.

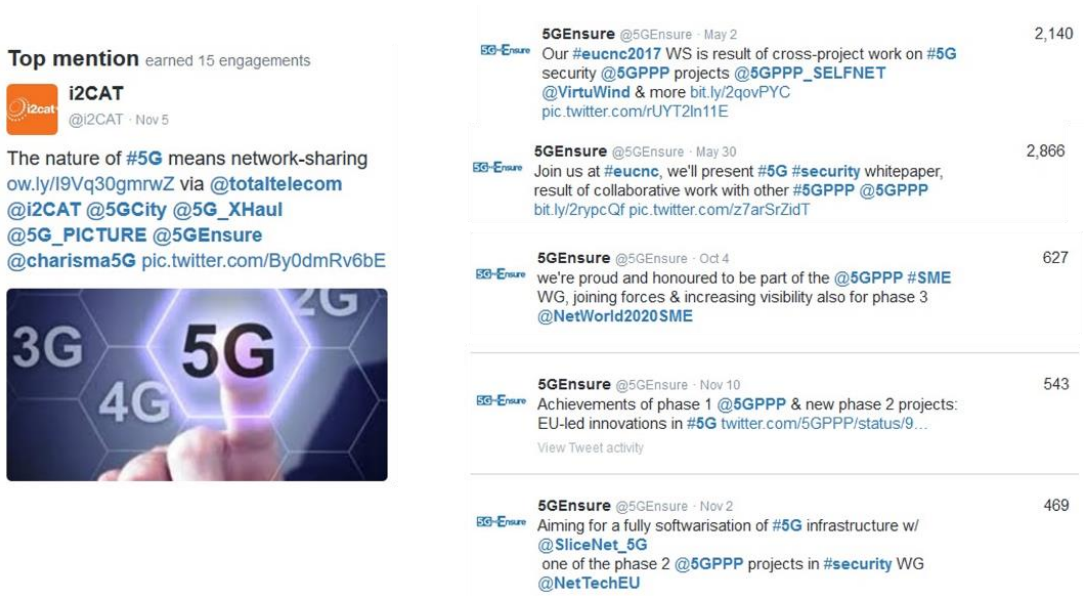
Table 26 Summary of contributions to 5G PPP

5G PPP Work Group	Participating Partner(s)	Main inputs/outputs
Security – sustainable through continued activities in phase 2 and as a newly appointed 5G IA Group	Thales (co-chair), Orange (co-chair), Telecom Italia	Sharing of 5G-ENSURE results to encourage re-use and sharing of newly acquired expertise within the 5G PPP. Production and distribution of 5G-PPP Security Landscape Whitepaper. Organisation of "5G Security: Phase 1 landscape and foreseen evolutions" workshop at EuCNC17 Bring on board Phase 2 projects Ensure forward on security aspects and re-use also extension of security achievements coming from Phase I projects.
Architecture	SICS	Facilitate consensus building on the 5G architecture. Contribution to the 5G PPP White Paper "View on 5G Architecture".
Pre-standardisation	TIM	Sharing of the contributions produced for the targeted standardisation organisations. Contribution to the whitepaper on the impact of the H2020 funded project on the 5G Specification during the phase 1.
SME – sustainable activity	Trust-IT	Recommendation: projects/organisations

in phase 2 through Global5G.org		involved in trials should feed back results into standardisation activities, share any security and spectrum requirements. Promotion of the SMEs, including phase 3 calls under WP 2018-2020 (Budapest, November 2017).
Vision & Societal Challenges	IT Innovation	Enforce the need for security to be maintained and demonstrated while seeking other improvements in agility, scalability and performance.
Network Management & Quality of Service	NEC	Contribution to the security session of the "Cognitive Network Management for 5G" whitepaper. Joint workshop with CHARISMA: 2nd IEEE International Workshop on NFV/SDN Security, 4 July 2017, Bologna (IT).
COMMS Group	Trust-IT	Highlighting importance of communication and dissemination activities within and beyond the 5G PPP to maximise impact. Social media campaign for EuCNC covering all workshops and stands led by 5G PPP projects. Guide on channels to use for press releases, and in general, facilitating technical members of the group in shaping their activities.

The image below shows different ways in which 5G-ENSURE and its peer projects have promoted collaboration at the programme level with regard to 5G security (all dates refer to 2017).

Figure 42: Communication of 5G PPP Collaboration



3.4.1 5G PPP WG Security Workshop at EuCNC 2017

EuCNC was chosen as the best venue to present the work of the Security WG after one year of activities based on a proposal to which Thales, Orange, Telecom Italia and Trust-IT contributed. The workshop "5G Security: Phase 1 landscape and foreseen evolutions" took place on 12 June.

Figure 43: Coverage of 5G security and privacy issues:

Coverage of 5G security and privacy issues:

Opening of the workshop by 5G-ENSURE Technical Coordinator Pascal Bisson (Thales) with an overview of the main activities of the 5G PPP SEC WG, the driving forces behind the group, which is to reach a view on priority security aspects for 5G networks that is coherent and consistent across the 5G PPP Phase 1 projects. Such an approach is illustrated in the Security Landscape white paper.

The first session of the workshop was devoted to sharing the main findings of the whitepaper with ad-hoc presentations targeting specific security aspects selected as priorities for 5G. Presentations covered major 5G security risks and requirements that have been identified by 5G PPP Phase 1 projects. These risks and requirements are by no means final as they relate mostly to Phase 1. The goal is therefore for them to be completed and taken forward first by 5G PPP Phase 2, and subsequently in Phase 3, where the aim should be to cover all important aspects, whether they are general security challenges or specific to vertical markets.

- The high-level Security Architecture for 5G network was illustrated. The logical characteristic of the 5G network, the support of multi domains and the management aspects are only a subset of the design principles reported as building blocks for the architecture design. They have resulted from an agreed vision between the projects involved. The architecture was presented in its first "iteration" and highlighted some of the work on-going regarding the second iteration due in October 2017.
- Privacy was another aspect covered during the workshop, with a focus on the perspectives of various 5G stakeholders (users, service providers and law enforcement). Although not exhaustive, the white paper provides a good illustration of the many facets of privacy in 5G, together with the

main challenges. Some suggestions on how to address privacy issues were also provided as part of the workshop. The important message is that a privacy-by-design framework should be established and applied over the 5G infrastructure (operator under regulation) but at the same time over services from vertical industries, with each potential actor contributing to the entire E2E delivery of 5G services.

- Trust aspects in 5G network was another discussion topic. 5G faces a complex trust issue because of the different roles played by the stakeholders. According to the view of the Security WG, trust assumptions should be an explicit part of the security architecture and trust concepts also have to evolve to liability concepts between actors of the 5G ecosystem.
- Security monitoring and management was another point raised as being important and should be included by design. Several questions were shared with the attendees, such as:
    - How to combine the needs for end to end security monitoring with the request for strong isolation between slices?
    - How to adapt in real time an end-to-end security monitoring system?

  These are some of the key challenges highlighted for future research to further advance 5G security.
- Security standardisation plays a key role in 5G PPP projects. As presented during the workshop some actions have been performed by each single project to help ensure security, privacy and liability issues are natively addressed in the standardisation processes according to the "Security by Design" approach. The next step for the 5G PPP Security WG is to encourage co-signed contributions to be elaborated by the H2020 projects and presented to those standardisation organisations/groups considered to be the most applicable.
- Pascal Bisson concluded the first session of the workshop with a look at the next objectives for the Security WG, which is ensuring further advances of the 5G Security Vision and also its realisation by taking advantage not only of the findings but also of assets coming from Phase 1 projects. The concrete action in this respect is bringing 5G PPP Phase 2 projects on-board, with a face-to-face meeting planned in the Autumn as the opportunity to update the work plan also with the engagement of Phase 2 projects.
- Further insights into the state of play and possible ways forward came from industry in the key note by Emmanuel Dotaro, head of ICT & Security labs at Thales Secure Communications & Information Systems on 5G and Security Transformation.
- The workshop panel discussion on "5G Security Perspectives" brought together key invited speakers as representatives from SMEs, manufacturers, researchers and verticals. Gabriele Rizzo explained the vision on 5G security as head of Strategic Innovation within Leonardo, where he is CTO, and also as professional futurist advisor to NATO ACT, and NATO expert for Cyberspace and Cyber Defence. Tommi Parnila, gave his perspective as Senior Security Consultant at Nixu cyber security company. Raimo Kantola provided his view as professor of Networking Technology at Aalto University, Communications and Networking, in Finland. Finally, Olav Queseth provided his perspective as both researcher at Ericsson and project leader of the METIS-I and II projects.
- The panel was an opportunity to discuss 5G specific security needs/requirements, especially related to vertical domains. Based on their knowledge of the "security" eco-system and on the insights gathered from the work done and presented during the Security WG workshop, the invited speakers provided suggestions on security aspects not covered or requiring further investigation in future work.

3.4.2 5G PPP WG Security Meeting

Meeting details: 11 October 2017, Turin. **Hosts**: Telecom Italia. **Nature of the meeting**: Closed

The main objective of the workshop was to bring together security representatives from **Phase 2 projects**, and start an exchange on 5G security work. Specifically:

- Understand possible synergies in terms of reuse of key results delivered during phase 1.
- Foster progressing on the key results.
- Complement phase 1 achievements wherever possible with the additional security features planned in phase 2.

The first part of the meeting was dedicated to the presentation of Phase I project results by representatives of **5G-ENSURE**, **VirtuWind and SelfNET**, which are mostly captured in the white paper. The second part of the meeting was an opportunity to listen to the activities within Phase II projects and understand what security aspects will be addressed. Presentations came from **SLICENET, ONE5G, 5G-Monarch 5G-MEDIA** and the **NRG5** project**.**

Although there is not a Phase II project dedicated to security aspects, it was useful to see how security is a cross-cutting concern to each project, thus ensuring progressing in phase 2 in some way. Most of Phase 1 achievements are available as resources for Phase 2, not only in terms of security use cases and requirements but also as tools/enablers on which phase 2 projects can leverage. It was agreed that it is important to start from these achievements, evaluate possible advancements and complementary solutions, as well as an opportunity to fill gaps in areas such as «security and resilience» identified as one of the areas not yet completely addressed.

The common view was the importance for Phase 2 projects to rely on the recommendations included in 5G-PPP Phase 1 Security Landscape white paper and also to progress on the many unresolved research challenges the Phase I projects have indicated as a way forward, such as “Key Research Challenges in Security Monitoring and Management” in the Landscape whitepaper). It was very useful to see some sort of security prioritisation emerging from Phase 2 projects on which we expect to see some answers emerging in coming months.

Another useful topic of discussion was related to the standardisation work done during Phase 1 where several recommendations were provided for the way forward by considering the experience gained in the first phase. One most important suggestions from Phase 1 projects was the need for timely actions, pro-active steps in view of the actions in view of the defined timelines and expected practices. There was also agreement on the importance within Phase 2 of extending security contributions to ETSI NFV and also ITU for regulatory aspects and to continue the work started within 3GPP as the main industry standard for 5G. Another important action in the plan is to try to also bring some verticals into the activities.

Pascal reported on the major achievements of the 5G PPP Security WG in Phase 1:

- The 5G PPP Phase 1 Security Landscape white paper.
- 5G-ENSURE Golden Nuggets: the security enablers, the test-bed and the security architecture.
- The 5G PPP Security WG Workshop at EuCNC 2017.
- The 5G-ENSURE 2nd International Workshop during ETSI Security Week (June 2017).
- Liaison with other 5G PPP WGs, such as Architecture and Vision.
- Relevant parallel work on cyber security, such as the ECSO WG6 SRIA (Strategic Research and Innovation Agenda).
- The two Open Consultations on 5G Security.

Some points for consideration:

- Decision to move the 5G Security WG to the 5G-IA level as (1) there is no project in Phase 2 whose main focus is on security and (2) there is interest to have members of the 5G-IA on board. A key benefit in this is ensuring the involvement of industry in the WG with direct support and contributions to priority activities.
- One concern raised regards possible implications for Phase 1 projects that are now coming to an end and the contributions made their respective projects.

Next Steps for the Security WG:

The meeting ended with an agreement on next actions.

- The first and most urgent action point for all the projects is the revision of WG Terms of References necessary in view of the transition from Phase 1 to Phase 2 projects and to cope with the fact that the 5G PPP WG has now moved to the 5G IA.
- Need for liason with other public private partnerships like ECSO and to formalise their involvement.
- Need to progress on the next steps and deliverables. A preliminary plan is to provide an update of the *5G PPP Phase 1 Security Landscape* White Paper based on the information collected from Phase 2 projects and the new security needs and proposed approaches. There is also the plan to release a whitepaper dedicated to Vertical security/safety covering potential new liability schemes, and trust relationship models between actors.
- Fundamental for the progress of the Security WG (5G-IA) progress is driving common work in terms of a cartography on existing security standards to cover, security risks to be addressed and the evolution of 5G architecture.

Summary of presentations

- Pascal Bisson, Technical Coordinator: main results of 5G-ENSURE available to Phase 2 projects. There is an important opportunity to progress on the Golden Nuggets, e.g. progress on the security architecture by capturing the needs of vertical industries covered in Phase 2. The set of security and privacy enablers represent useful “tools” on which Phase 2 projects can leverage for AAA, Privacy, Security Monitoring, Virtualisation and trust aspects. Although the enablers are released as a closed source, they come with open specifications and are therefore available as a starting point for enhancements or adaptation. Access to the enablers is possible via the 5G test-bed, which has been set up by 5G-ENSURE not only for integrating and evaluating the enablers but also as a tool for Phase 2 projects.
- Konstantinos Fysarakis presented the main objectives of the **VirtuWind** project. It focuses on the adoption of virtualisation and softwarisation technologies for industry control network. In this context, the new security threats and risks have been careful investigated. The project has defined and analysed two security use cases as representative scenarios of industrial networks and conducted an initial risk assessment and analysis of security requirements. They have designed a virtual and programmable architecture with some components which will be developed in Phase 2 related to Proactive & Reactive Security Mechanisms, Security Manager module, AAA functionality and Secure Interfaces. The presentation hightlighted possible enablers complementing the ones developed by 5G-ENSURE project in the AAA area. Also the work in the context of security use cases and security requirements complements the results coming from 5G-ENSURE.
- Gregorio Martínez presented the Security Perspective of the **SELFNET** Project and what the project is doing regarding 5G Security in particular in the context of proactive detection and

mitigation of DDoS attacks conducted by a potential botnet.

- Zdravko Bozakov, **SLICENET** (phase 2) explained the objective to achieve a fully softwarisation 5G infrastructure by addressing the associated challenges in managing, controlling, and orchestrating the new services running in such infrastructures for vertical sector users. Security is also part of this challenges and will be addressed by developing security and privacy mechanisms for the establishment of end-to-end encrypted channels between the different architectural elements of the SliceNet architecture, including NFV functions, security for control and data planes, security and privacy for the management plane, etc. This approach to slice security aims to mitigate risks associated with lack authentication, encryption and security by design, protection against attacks, etc. The presentation showed the importance of starting and reusing the results of phase 1 projects. In particular, in the context of slice isolation the project will investigate the Group authentication schemes (to reduce signaling overhead). In this context, the presentation from Pascal was useful in providing a reference to the work done in 5G-ENSURE regarding the specification and development of the Group-based authentication enabler.
- Reaz KHAN presented **ONE5G**, which aims to focus on mMTC and URLLC based services, covering a wide array of verticals by capturing the key requirements for the use cases, so that the technical studies and components will be aligned with these requirements. Currently the security aspects have not yet been identified. The set of security use cases identified by 5G-ENSURE will be taken into consideration for this purpose.
- Beatriz Gallego presented **5G-Monarch**, which has identified two representative use cases one related to Vertical industry (smart sea port) and one related to Mobile operator deployment (tourist city). The project scope is to develop specific Network Functions for use case requiring security and resilience. They have identified this area as one not yet addressed neither by 5G-PPP Phase 1 nor by on-going SDO initiatives. For this a WP is dedicated to the “resilience and security” aspects. The project therefore expects to progress on security aspects of 5G network.
- Gino Carrozzo provided an overview on the **5G-MEDIA** project whose focus is the interworking of media-related applications with the underlying 5G network. From the point of view of security, media and entertainment systems need to ensure globally the protection of resources. Security encompasses several dimensions such as authentication, data confidentiality, data integrity, access control, non-repudiation, privacy, etc. Many recommendations just included in 5G-PPP Phase 1 Security Landscape are essential for 5G-MEDIA project to relyon/integrate Phase 1 results and solutions. It is also useful to dig into the many unresolved (yet) Research Challenges Phase 1 project have indicated as a way forward (“Key Research Challenges in Security Monitoring and Management” from the Landscape whitepaper).
- Filippo Rebecchi presented **NRG5**, which is aimed at enabling smart energy as a service via 5G Mobile Network Advances. Three main use-cases for extensive 5G deployment have been identified. These are Smart Grid application (mission-critical), Advanced metering (massive deployment) and EV charging. High level of security, resilience and availability are the areas the project will adddress as intrisical requirements for Smart energy vertical.

3.4.3 5G PPP Pre-standardisation WG

The main focus of this WG is to ensure alignment between all the 5G PPP WGs on standardisation activities and related time plans through regular calls to share information on contributions to standardisation. The

main activity in the period May-October 2017 was the production of a document «Summary for Phase 1» aimed at describing standardisation results achieved during 5G PPP Phase 1 (2015-2017).

The document covers:

- The standardisation landscape and the main standardisation organisations and groups targeted (e.g. 3GPP, ETSI, IEEE, etc.).
- Achievements in terms of direct contributions to standardisation by each funded project in the WG.
- A detailed list of the contributions made by the projects. The document lists the main standardisation organisations/groups that have seen the most inputs from the phase 1 projects, their positioning in terms of 5G, explaining which ideas and concepts have been transferred into the standardisation process but without detailing all the interactions involved.
- More then 260 contributions by 10 Phase 1 projects have been traced at the time of writing this document, showing a very active commitment.

3.4.4 5G PPP 5G-PPP Architecture WG

The main outcome of the WG activities has been the 5G PPP Architecture WG Whitepaper. 5G-ENSURE has actively contributed by providing inputs coming from the 5G Security Architecture designed in D2.7 (October 2017) and earlier iterations.

The revised version of the white paper highlights the key design recommendations identified by the Phase 1 projects toward the 5G architecture design and provides a baseline architecture to be facilitated by the new Phase 2 projects to assist further development. 5G PPP Architecture WG Whitepaper (V2.0) was put under public consultation to receive comments and suggestions. All contributions have been considered and where appropriate, included in the final version, which will be produced in Q4 2017.

3.5 Joint Publications

The production and publication of the 5G PPP Security WG white paper: *5G PPP Phase 1 Security Landscape* in June 2017 with contributions from 9 projects and 45 authors is a major output of this reporting period. Thales and Orange served as the main editors of the white paper, with contributions from Ericsson, TIM, NEC, IT Inovation, and VTT. Trust-IT acted as style editor and designed the publication.

The white paper features insights from phase 1 member projects on:

- Major 5G security requirements and risks.
- 5G security architecture.
- Access control to 5G.
- Privacy
- Trust Model
- Security Monitoring and Management
- Slicing/virtualisation and strong Isolation
- Security Standardisation

Figure 44: 5G PPP Security White Paper

The white paper has been widely distributed and promoted, not only by 5G-ENSURE but also by project co-authors in a truly collaborative fashion. One example is SELFNET promotion with the option to download the publication: https://selfnet-5g.eu/2017/06/16/security-group-5g-ppp-white-paper-phase-1-security-landscape/.

Distribution of the white paper:

- EuCNC 2017: conference and exhibition, June 2017 (Oulu)
- 2nd International Workshop, June 2017 (Sophia Antipolis)
- IEEE 5G Summit (Global5G.org session on 5G health), June 2017 (Helsinki)
- 5G PPP Security WG Meeting, October 2017 (Turin)
- DSS ITSEC, October 2017 (Riga)
- European Cyber Threat Summit 2017 (Dublin)

Figure 45: External Endorsement of SEC WG WP

Figure 46: Visibility of white paper on Twitter

Plans are already under way for a second edition of the white paper with phase 2 projects in the Security WG (see section 3.4.2).

5G-ENSURE has also contributed to the **5G PPP Annual Journal**, which was published in September 2017. Contributions comprise an updated overview on the project progress and advances, particularly the golden nuggets. The introduction to the journal also covers 10 key results from the past 12 months, with reference to the various 5G PPP white papers published, including the one by the Security WG.

The image below captrues the main contributions from both perspectives.

Figure 47: 5G PPP Annual Journal

4. 5G Security Standardisation

4.1 Overall achievements and takeaways

- 5G-ENSURE has continued to contribute to standardisation, including participation at technical meetings.
- Standardisation work within 5G-ENSURE will be sustained and carried forward mainly by TIM.
- Discussions with NIST have been very positive in relation to standardisation work by 5G-ENSURE, including efforts on privacy aspects within the 3GPP.
- The 2nd International Workshop (June 2017) during ETSI Security Week was an excellent opportunity to share 5G-ENSURE findings and outputs at a premier forum for standardisation.
- Besides the technical meetings, 5G-ENSURE has continued to recruit standards specialists, including high-profile representatives and corporate/institutional delegates.

Results of the standardisation work has also been shared with the 5G IA (Secretariat General). It is also interesting to note, through LinkedIn network discussions, that there is valuable preparatory work on going at the 5G IA level to help smooth out the complex 5G standardisation process within 3GPP & other bodies.

TIM, strongly involved in the 5G definition at different levels (e.g. GSMA, NGMN, 3GPP, etc.), will continue its activities related to the standardisation and the dissemination of the main project results (e.g. enablers), which means that the **standardisation work** is **sustainable**.

In fact the "full" standardisation of the results achieved within the 5G-ENSURE workshop have not yet finished and it will be needed to continue the standardisation activities also after the termination of the project:

3GPP SA3 TS 33.501 "Security architecture and procedures for 5G System", that represents the first 3GPP specification in the 5G security field (Release 15), it is expected to be finalised and published by the end of March 2018, whereas the ETSI works on the PII protection, and the usage of ABE as a suitable protection mechanism, will continue till the end of 2018. For example, also the new SA3 proposal "New Study on security aspect of 5G Network Slicing Provisioning" that will complete the security landscape scenario from 3GPP point of view, will be elaborated mainly during 2018.

Since 3GPP is now in the middle of Release 15 definition (the 5G Phase 1 specification for 3GPP) and in particular defining the stage 3 of the specification (the actual solutions) it is important to continue to be present at the table in order to be effective and maximize the transfer of reseach results from the projects to the SDO. Phase 2 funded projects should start immediately to contribute to the specification of 5G Security, in particular leveraging the 5G PPP Security WG and the 5G PPP Pre-Standard WG support. TIM plans to continue to be linked to both WGs, in particular to be able to collaborate on finalising security aspects of the Release 15 and then of the (final) Release 16.

The following lists all the contributions prepared by the project members and submitted at standardisation meetings.

Table 27: Summary of contributions to 5G security standardisation

Standardisation Organisation	Title of Contribution	Meeting detail	Short link to document
3GPP SA3	Study on Architecture and Security for Next Generation System	SA3#821-5 February 2016	http://ow.ly/N4bk30agl2z
3GPP RAN	pCR on Section "Security and Privacy" of TR38.913 - Requirements on user identity	RAN#71 March 7-10, 2016	http://ow.ly/ju9l30agl5m
3GPP RAN	pCR on Section "Security and Privacy" of TR38.913 - Requirements on security visibility	RAN#71 March 7 - 10, 2016	http://ow.ly/lheD30agl8i
3GPP RAN	pCR on Section "Security and Privacy related requirement	RAN#71 March 7 - 10, 2016	http://ow.ly/mZJn30aglbY

	relevant for Radio Access" of TR38.913 – Requirements on radio signaling messages		
3GPP SA3	pCR - New security area for subscriber privacy	SA3#83 9-13/05/2016	http://ow.ly/MeUs30aglUB
3GPP-SA3	pCR - New key issue for subscriber identifier protection	SA3#83 9-13/05/2016	http://ow.ly/QqLA30agmuh
3GPP-SA3	pCR to draft-TR 33.899 on New security area for AAA	SA3#83 9-13/05/2016	http://ow.ly/PxTu30agnaS
3GPP-SA3	pCR to draft-TR 33.899 on Core Network Control Plane Security	SA3#83 9-13/05/2016	http://ow.ly/1Vh930ago3T
3GPP-SA3	pCR to draft-TR 33.899 on New security area for network virtualisation security	SA3#83 9-13/05/2016	http://ow.ly/4IkR30agokp
3GPP-SA3	pCR to draft-TR 33.899 on Radio Access Network security	SA3#83 9-13/05/2016	http://ow.ly/7xsg30agotn
ETSI-TC-CYBER	Access control mechanisms and policy rules for PII protection on smart devices, cloud and mobile services	CYBER#7 15-17 June	http://ow.ly/hnWQ30agoDP
ETSI-TC-CYBER	PII Protection in mobile and cloud services	CYBER#7 15-17 June	http://ow.ly/ZzpC30agoMI
3GPP-SA3	Enhancing the concealment of permanent or long-	SA3#84 25.-29.07.2016	http://ow.ly/glH130agoRu

	term subscriber identifier		
3GPP-SA3	Deletion of key issue #7.1 on subscriber identifier privacy	SA3#84 25.-29.07.2016	http://ow.ly/VZmH30agoVB
3GPP-SA3	New privacy key issue on transmitting permanent subscriber identifiers only when needed	SA3#84 25.-29.07.2016	http://ow.ly/fkPU30agoYD

5.2 Contributions May to October 2017

During the period from May to October 2017, the 5G-ENSURE project has concentrated its standardisation effort on the preparation of the contributions for the following two groups:

- **3GPP SA3**, the security comptetence center for mobile security in the 3GPP context
- **ETSI TC CYBER**, the ETSI Technical Commette dedicated to the cyber security.

By the second half of 2017 the focus of 3GPP work shifted to Release 15, to deliver the first drop of 5G standards. The functional freeze date, including stable protocols, is set for 14 September 2018 (SA#81 meeting).

The following meetings of the 3GPP SA3 have taken place during the period May-October 2017:

- **SA3#87 in May 2017.** Ljubljana. Presentation of **7 project contributions**, which were accepted for inclusion in TR33.899. All the contributions were related to privacy aspects and consolidating the related clause in the document.
- **SA3#88 in August 2017** Dali (China). The main decisionagreed by SA3 group is to stop the TR 33.899 (part of Release 14, initial 5G study) and to concentrate all the effort only to the TS 33.501 (Release 15, the actual specifications for 5G). In practice, this means switching on the “new” TS 33.501 with completion planned for the end of March 2018. The TS develops the Stage 2 normative specification of Phase 1 of the 5G security architecture, based on the prioritisations and interim agreements that have been captured in TR33.899 and on requirements from other working groups, e.g. SA2, RAN2 and RAN3. During the meeting, 5G-ENSURE project presented **13 contributions** focused again mainly on the privacy section of the TS 33.501, most of them agreed and incorporated into the specification. In particular the IMSI protection mechanism based on one of the enablers elaborated in by the project (the “Home Network centric IMSI protection” enabler based on the usage of a standard PKI, where the IMSI is encrypted by using the the public key of the MNO. More information available in D3.6) is part of the TS. For the meeting 5G-ENSURE also submitted a contribution on the 5G Security Architecture, designed by the project and described in D2.4 and D2.7, as a way to move forward on security concepts and principles elaborated within the

projects. The contribution has been noted by the SA3 delegates as work to be further investigated and analysed in detail.

- **SA3#88bis, Singapore October 2017**: it was an ad hoc meeting dedicated to 5G aspects and focused on the progression of the TS 33.501. Due to the large amount of contributions received, about 300, not all of the topics were discussed, for example, the discussion on the Privacy contributions discussion were postponed to the next meeting.

An agenda item of the October ad-hoc meeting was the new 5G network slicing provisioning study (SP-170636 "New Study on security aspect of 5G Network Slicing Provisioning"). Any normative work in SA3 or recommendations to other SA groups, should be done in the Release 15 time frame.

In summary, during the May-October 2017, project partners have elaborated more then **20 direct contributions** to SA3 dedicated to the Privacy and Security Architecture topics.

ETSI TC CYBER#10 F2F meeting (June, Sophia Antipolis) and TC-CYBER#11 (September).

During the TC-CYBER#10 meeting, PII protection was discussed and the following decisions taken:

- Approval of the Work Item DTS/CYBER-0020 "Application of Attribute-Based Encryption (ABE) for data protection on smart devices, cloud and mobile services". This document (used as the basis for the Technical Specification TS 103 458) will be used to collect the results of the SFT-529, the Specialist Task Force, which was created also with the support of Telecom Italia at ETSI Board level, is focused on defining a concrete framework based on the ABE (Attribute Base Encruption public Key mechanism) for the protection of the PII in mobile, cloud and IoT scenarios.
- The latest version of the DTS/CYBER-0025 (Attribute Based Encryption for Attribute Based Access Control), which is a Technical Specification, has also been approved. This version contains the full description of the mobile use case that describes the "IMSI catcher" issue in the 3G/4G scenario introducing the need to have a mechanism for the IMSI privacy protection in 5G. The text, proposed by Telecom Italia, describes the use case already defined in the D2.1 called "Use Case 2.2: Subscriber Identity Privacy". The actual mechanism proposed to overcome the issues is the usage of ABE PK encryption, the enabler described in the D3.6: "Encryption of Long Term Identifiers".

During the e-meeting dedicated to the ABE (CYBER-WI-020-ABE, 8 September), the mobile use case was discussed and revised. As per TC CYBER's request, the STF 529 was required to revise the topic based on CYBER delegate feedback, including clarifications on the use case. The results of the call have been included in the new verison of the drafts of both: DTS-020 on use cases and the DTS-025 on architecture and protocols. Both revisions (DTS-020 and DTS-025) were presented during the CYBER#11 meeting.

Other "direct" standardisasion activities performed during the May-October period are related to the 5G PPP PRE-Standardisation WG, as reported in Section 3.3.

4.2 5G-ENSURE 2nd International Workshop

"From Research to Standardisation" was the focus of the 2nd International Workshop organised by 5G-ENSURE in June 2017 during ETSI Security Week as an important forum for security and related standardisation work aimed at tackling major issues.

Co-location with this event was an important success factor in bringing a very large audience on board, including members of the 5G-ENSURE Advisory Board and NIST as part of the on-going collaborative work.

In particular this year the following topics were addressed:

- The standards needed to support legislation such as the Directive on the security of Network and Information Systems (NIS Directive or NISD), General Data Protection Regulation (GDPR), and the proposal for a Regulation on Privacy and Electronic Communications Code.
- The new types of threats introduced by the virtualisation of network functions and the means to mitigate them.
- The future challenges of securing 5G networks.

ETSI Security Week was therefore a very suitable opportunity for 5G-ENSURE to share its work with over more than 70 attendees, spanning standards representatives, device and infrastructure manufacturers, network operators and SMEs, particularly its security vision, showcase the achievements and the possible solutions to some of the 5G security issues. The agenda of the workshopis is showed below.

Figure 48: 2nd Int'l Workshop Agenda

4.2.1 Main Takeaways from presentations

Future priorities and collaborative work were among the discussion topics, taking stock of 5G-ENSURE results and ensuring the **transfer of relevant research results into the standardisation process**. The presentation by Anand Prasad, chairman of 3GPP SA3, was very insightful in this respect. In reporting the updated timeline for 5G security standardisation work, Dr Prasad also gave the view of 3GPP SA3 work and its approach to security areas in next-generation networks.

There is a match between the security areas covered by 5G-ENSURE and 3GPP SA3 work on 5G security. This means great opportunities for 5G-ENSURE to contribute. Architectural aspects of Next Generation Security, Authentication, RAN Security, Network Slicing security and Subscription Privacy are the areas where 5G-ENSURE can contribute within 3GPP SA3, Anand Prasad, chairman of 3GPP SA3.

The picture below, presented during the workshop, illustrates the match between the SA3 activities and the 5G-ENSURE project scope.

Figure 49: 3GPP SA3 topics

In this context, it was useful to see an alignment with the 5G-ENSURE Standardisation Plan showed by Paolo De Lutiis (TIM) and the approach taken by SA3 in the area of 5G security standardisation. The active role of 5G-ENSURE in contributing to issues and solutions related to privacy where over 30 direct contributions have been submitted and in large part also accepted. The work done received a valuable recognition from the SA3 chairmain with the advice to extend the involvement also to other security areas. The plan was in fact to build on this with contributions to the security architecture.

4.2.3 Main Takeaways from International Panel

The International Panel discussed the way forward for 5G security and related standardisation.

Charles Brookson, Chair ETSI TC CYBER; Roberto Cascella, Senior Policy Officer at the European Cyber Security Organisation (ECSO), Jovan Golic, Lead NGMN Security Competence Team, Telecom Italia and Anand Prasad, Chairman 3GPP SA3 took part at the panel. Pascal Bisson, technical coordinator of 5G-ENSURE project, was the moderator of the panel where the focus of the discussion was the actions needed towards security research on 5G network.

- More work needs to be done in **standardisation on slicing**, **IoT security** aspects and **virtualisation**. This was one of the main outputs of the discussion.
- The **security of the data lifecycle** needs a lot of attention in the context of 5G. Security relys on digital infrastructure, network and computers and also data. Big data is driving the economy of new

applications but they are the most critical. In the lifecycle of data, 4 stages are relevant: data collection, data transmission, data storage and sharing, and data processing. Data collection very much relates to the user's control on privacy in terms of user consent. The research is there but improvements are needed. Data storage and sharing can use encryption but there is the problem of key management. Sophisticated encryption mechanisms like searchable encryption and Attribute Base Encryption for data sharing are available. Data processing (basically the computing processing) runs the data so it should be trusted. To protect data, enhanced techniques like homorphic encryption and fully homorphic encryption are needed. This is where more work is required in terms of techniques to process or elaborate encrypted data, to not having to trust the server with regard to the confidentiality of data.

- Most of the relevant 5G security topics, like trust, risks, liability and data, were covered during the workshop. Applications are another important thing to consider for the 5G enablers. Investigations are needed into what will be provided by the **application layer**, understanding also the impacts in terms of data with regard to privacy, authentication and protection against potential Denial of Service (DoS) because the application does not function as it should. This calls for a cross layer investigation in terms of what is provided at the application layer that affect security at the lower layer.
- Several projects in **Phase 2 of the 5G PPP** are expected to address currently missing solutions for physical security. There are big issues around data and the need for data protection techniques. Work is necessary to speed up standards for data protection techniques and to ensure secure data access. However, encrypting everything in the network will not work very well. How do we give quality of services if everything is encrypted?

5.2.4 Insights from the Advirory Board

The workshop was the occasion to also bring together many members of the 5G-ENSURE Advisory Board. Discussions focused on action items for the next steps of the project. Each of the AB members came up with concrete actions to support dissemination of the work of 5G-ENSURE and more largely the 5G PPP Security WG. In particular:

- **Charles Brookson, Chair ETSI TC CYBER** encouraged the creation of an ETSI Special Interest Group on Cybersecurity where all topics and more could get discussed. He also invited to present 5G-ENSURE and 5G-PPP SEC WG results at a GSMA/Security & Fraud Forum (close session : dedicated to MNO) and after at GSMA board
- **Roberto Casella (ECSO)** encouraged the promotion of 5G-ENSURE and 5G PPP Security WG Whitepaper in the context of ECSO SRIA since it is highly relevant there
- **Anand Prasad, Chairman 3GPP SA3** welcomed contribution from 5G-ENSURE to privacy as previously done or to security architecture as now planned.

All the Advisory Board members committed to support 5G-ENSURE in the suggested actions. Also they welcomed the willingness of 5G-ENSURE to make the 5G PPP Security WG open to a wider community. As such they welcome the idea to get it moved to the level of the 5G Industry Association.

4.2.5 Insights from NIST

NIST has been one of the main actors interested in the work of the project and periodical exchanges have been organised from the very start. NIST was rappresented by Nelson Hastings from the Computer Security Division. Some actions were agreeded in order to continue the co-operation. In particular NIST takes the action to provide some feedback/viewpoints on 5G-ENSURE achievements presented at the 5G-ENSURE Workshop. NIST accepted to investigate potential new standards of interest for the enablers realeased by the project and in particular for the second set, under development at the time of the workshop. NIST takes also the action to present the vision stemming from potential 5G security results after the FCC NOI on 5G cybersecurity (FCC [PS Docket No. 16–353; DA16–1282] Fifth Generation Wireless Network and Device Security AGENCY: Federal Communications Commission[2]. Finally NIST will investigate under which conditions 5G-ENSURE could share/discuss on evolution of existing framework of cyber security management.

One of the follow-up actions has been a dedicated call organised in October the 4th where 5G-ENSURE presented details of some the enablers of the second release to which NIST expressed particular interest during the workshop in ETSI. Specifically during the call the following enablers were described:

- SIM-based anonymisation.
- Privacy Policy Analysis.
- Federative Auth+ID.

An update for the following enablers, already presented since part of R2, was also provided to show the features which were added.

- Fine-grained Authorisation Enabler.
- Privacy Enhanced Identity Protection.
- Device identifier(s) privacy.
- IoT/Group-based authentication.

4.3 The second open consultation on *"Security in 5G"*

5G-ENSURE project has worked to drive the 5G Security Vision to get it shared and agreed upon within the 5G PPP and beyond. The first Open Consultation on 5G Security was a step towards this direction, by consulting stakeholders, including other 5G-PPP Projects, on the areas of security and privacy challenges and priorities. The outcomes have been shared and used as part of this type of cooperation among the 5G-PPP projects, in particular within the 5G-PPP Security WG created on behalf 5G-ENSURE in March 2016.

After more than one year of work on security aspects of 5G networks, the project is seeking the views on the work that has been done by 5G-PPP project and beyond, in particular to:

- Identify the security aspects which have not yet been addressed or which have been only partially covered to understanding the main barriers on progressing on them and how they can impact on the 5G adoption, if not solved in time.
- Report on 5G security perspective (mainly industry driven) and get it complemented from the perspectives of others stockholders (e.g. regulator and policy makers, SME, business verticals, etc..)

[2] http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db1216/DA-16-1282A1.pdf.

- Evaluate the usefulness of the results coming from 5G-PPP funded projects and beyond, including their ability to influence the 5G security specification work.
- Understand and establish the way forward for future 5G Security work by identifying what else needs to be done on 5G security.

The OC has been opened on 04-05-2017 until the end of October.

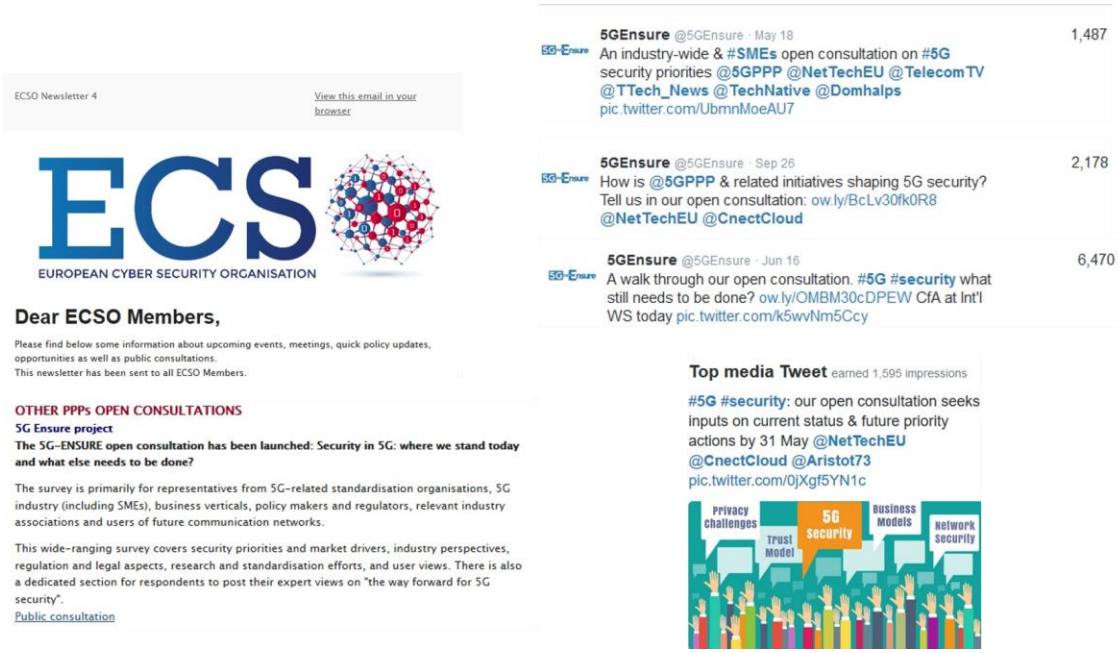
"Security in 5G: where we stand today and what else needs to be done?" has been the focus of the second open consultation. The survey targets were primarily representatives from 5G industry (including SMEs), business verticals and 5G-related organisations. It has structured in several sections:

- The general section **"Security in 5G: where we are and what else needs to be done"** covered a set of questions aiming to understand what is the general perspective regarding the work and progress done on 5G security.
- The **Industry** section devoted to capture the perspective of industry on 5G Security. The scope was to understand which security the industries expect from the 5G network or which security functions do the industries not trust to "outsource" to the network.
- The **Regulatory** section investigated the priorities regarding the distribution and allocation of responsibilities and obligations and in particular for potential delegation of regulation obligation to non-regulated third parties.
- The **Standardisation** section aiming to understand the role the research projects have played in driving standardisation work as well as potential issues.

Finally the survey was used to capture the work and actions to be put in place over the next few years towards the integration and uptake of 5G security solutions ,as we move towards the launch of the first commercial 5G networks.

Details of the openc onsultation are available at .

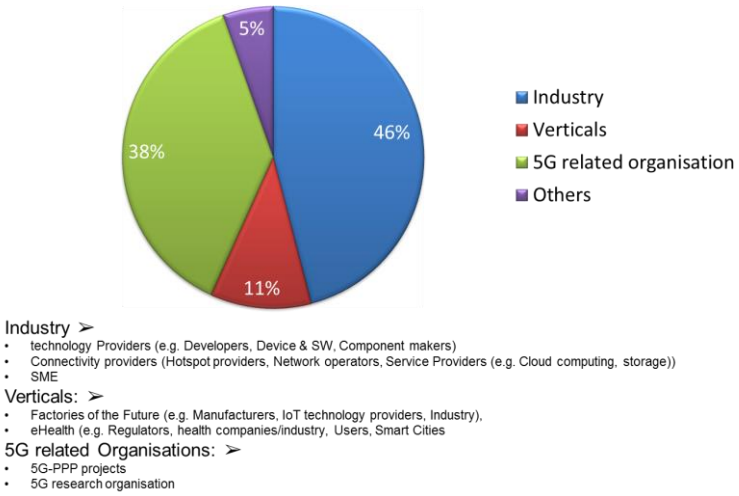
Figure 50: OC Campaign Impacts



Sample of respondents

A total of 37 answers were collected. The main answers come from Industry sector followed by 5G related organisation and 5G verticals as showed in the figure below.

Figure 51: Breakdown of OC Respondents



All responses collected were handled anonymously. A detailed analysis is provided in Annex 4. Here we report on the main findings.

Main findings:

- 5G security issues have only been partially addressed.
- Security requirements for vertical industries are not yet fully understood [industry view]. The main difficulties in defining the security of 5G network are mainly related to the different usage scenarios which imply different security requirements and consequently more flexibility in terms of security functionalities supported.
- The most challenging security issues are considered to come from IoT and network slicing. This finding is aligned with the conclusions of the ETSI 5G Summit (April 2017), where security was not only a recurrent theme but also considered the most important takeaway from the summit[3]. CapacityEurope (October 2017) also highlighted the considerable security challenges around IoT[4].

These findings are not surprising given the early focus of 5G on enhanced mobile broadband (5G phase 1 and 2 as defined by the industry, e.g. GSMA), with a shift in focus towards mission critical services supporting applications requiring high reliability, low latency connectivity and robust security and privacy expected in phase 2[5].

Some conclusions can be drawn, however, from the consultation on network support requirements. For example, the need to perform authentication, ensuring privacy protection and confidentiality and integrity of service traffic, for vertical industries if verticals cannot build it themselves. There is a general agreement on the need for end-to-end security.

[3] http://www.5gensure.eu/news/takeaways-etsi-summit-5g.
[4] On this point, see D5.6, section 2.5.
[5] On the two phases and related standardisation timelines, see D5.6, section 2.1.

- There is consensus among industry and vertical representatives about several design principles emerging from the work in 5G PPP Security WG. Further debate and assessment would be a valuable contribution towards increasing consensus and/or possible other approaches.
- Inputs related to 5G PPP contributions are clearly only relevant to respondents familiar with the programme. However, those respondents involved in the programme believe that anticipating security issues and research results has helped to influence 5G standardisation to some extent. There is an overall consensus that standardisation and compliance with standards is key to widespread adoption.
- Risks associated with new technologies point to possible delays in adoption. 5G is no exception, with similar view points emerging from industry, verticals and 5G-related organisations. Increased exposure to cyber threats is also highly relevant.[6] A key point emerging from the verticals is the lack of coherent regulations and policies for industry applications.
- Trust is another aspect of 5G that requires further investigation. Trust and liability model between the different stakeholders is considered to be the first step towards the widespread adoption of 5G, especially for vertical services. An emerging priority for regulatory bodies emerging from the survey is the inrtroduction of new responsibility schemes in terms of distribution and allocation of responsibilities and obligations in particular to address breach of Trust/ security between parties.
- Another area for regulatory action is greater clarity on responsibilities and liabilities, as well as "access regulation". In the context of 5G, regulators should seek to create and apply a consistent standard across the entire ecosystem so that the same criteria could be applied when evaluating the benefits and costs of open access mandates, regardless of sector or technology.

4.3 5G Security standardisation: the way forward

5G-ENSURE effort on security standardisation will not terminate with the end of the project. There is in fact the engagement of the partners to proceed in delivering the main results and outputs of the project as part of the 3GPP Phase 1 (Rel 15) and also Phase2 (Rel 16) standardisation. We expect that most of the security aspects investigated by the project will have more relevance during the next mounths.

SA3 will be still the main group for 5G security standardisation given its specific Study Items on 5G. This is also backed up by the survey, where most respondents see the 3GPP as the main standardisation organisation. Besides the large amount of contributions related to the current TS 33.501, the following new proposals have been presented during the last meeing in Singapore or during the preparatory conference calls:

- Study on Supporting 256-bit Algorithms for 5G: Quantum computing poses a threat to information security with the current protection measures in 3GPP networks. There are commercial applications (e.g., critical infrastructure, financial, medical, and pharmaceutical) and government organisations that require enhanced (i.e., 256-bit key) protection for confidential information.

[6] ETSI 5G Summit, op cit. and CapacityEurope, op cit.; see also D5.6, section 2.5 on the socio-economic impacts, including regulatory impacts, of a cyber-attack.

- New WID on Security for 5G Core Network with Service Based Architecture: The objective of this WID are to identify security requirements and solutions to support of 5G core network with service based architecture;
- TR 33.811 Study on security aspects of 5G network slicing management: a study on the threats, potential security requirements and solutions for the features of 5G network slicing management.

ETSI ISG NFV: during the latest plenary meeing in the U.S. (September 2017) the following new Work Items were started and are expected to have a direct impact on 5G infrastructure:

- **VNF Package Security specification:** This work item will define VNF package security requirements and procedures.This work item will address the following security issues related to VNF packages, but not limited to: Integrity of VNF Packages, Authenticity for VNF Packages, Methods to ensure Confidentiality for VNF Packages, Credential storage and provisioning of VNF packages during Onboarding. The WI will also include security use cases for VNF package during on-boarding, instantiation, termination, run-time verification etc.
- **System Architecture Specification for NFV Security Enhancements:** This Work item will identify architectural gaps in existing NFV security capabilities and specify new normative security enhancements. The work item will address both sensitive and lower sensitivity VNFI / VNFCIs, as well as NFVI and MANO aspects.
- **Identity Management and Security:** This Work item will specify normative requirements for secure VNF identity management and trust relationships in NFV. The work item will specify how identities are securely managed, trusted and attested. The work item will address both horizontal and vertical relationships.
- **Report on NFV Remote Attestation Architecture:** Trustworthy and up-to-date platform integrity information is an enabler for reliable and secure management of NFV deployments. Remote Attestation is the process through which this information is collected, verified and distributed to stakeholders. This report will identify and study Remote Attestation architectures applicable to NFV systems, including the definition of attestation scope, stakeholders, capabilities, interfaces and protocols required to support them.

TC CYBER, although generally committed to high-level policy and regulatory aspects (e.g. NIS Platform, Lawful Interception, Privacy Mandates), will continue to be interesting also from the more technical point of view on specific topics, such as Privacy preserving mechanisms (PII). It is expected that the mentionated Work Items DTS/CYBER-0020 (use cases and requirements) and DTS/CYBER-0025 (actual ABE mechanism definition) will be the main deliverables directly related to the 5G security topics throughout 2018 as the expected minimum time frame.

5. Community Development and Stakeholder Engagement

5.1 LinkedIn Professional Network

5G-ENSURE now has a LinkedIn community of 1038 connections analysed in this section (up from 810 LinkedIn connections since April 2017), with an **average of 65 new members a month** since July 2016 when the network became operational. Members of the LinkedIn network have been recruited through a

continuous flow of insightful information on this professional network encouraging organic growth. The community continues to grow with 1060 in mid-November 2017.

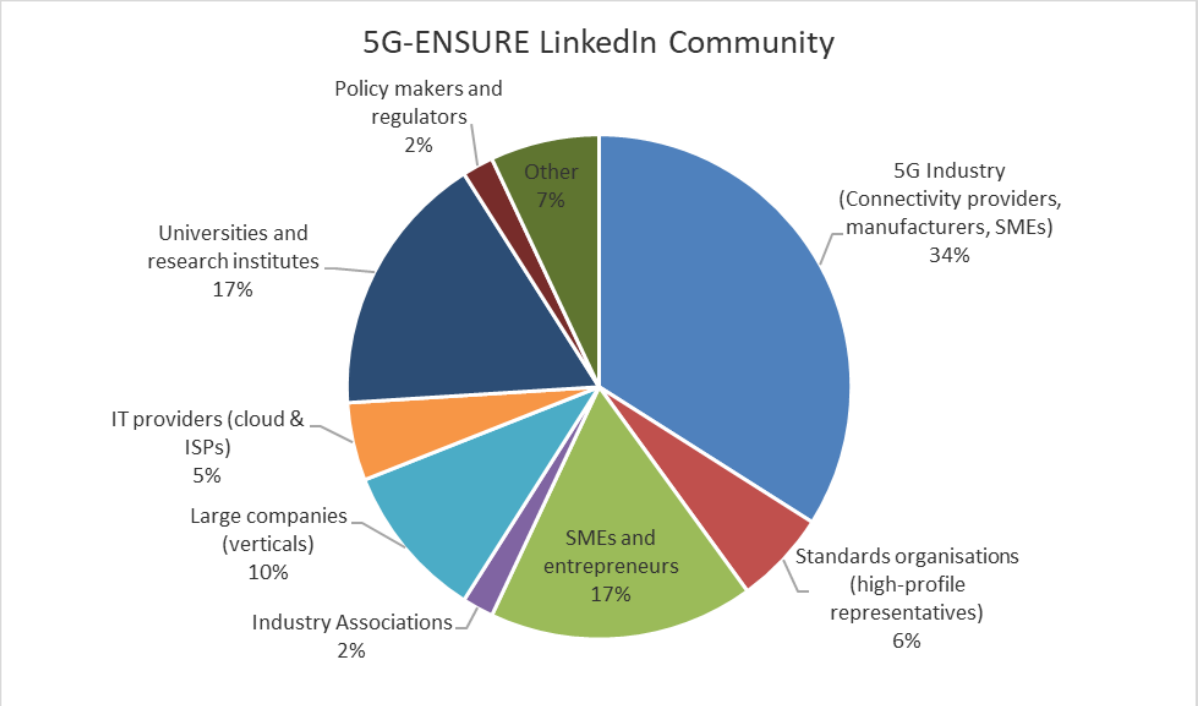
It is interesting to note that the network shows how the actors within the 5G ecosystem are assuming multiple roles, e.g Swisscom emerging as a large IT company and Deutsche Telekom's portfolio spanning artificial intelligence and verticals like connected cars/automotive and health, blurring the boundaries between traditional stakeholder categories. The network also includes new entries into the ecosystem, including representatives from the 5G PPP SME WG, e.g. Montimage, Incelligent, Real Wireless.

- 5G Industry (connectivity providers, manufacturers, SMEs):
    - Operators (e.g. connectivity providers, MNOs): 138 (up from 118 representatives).
    - Suppliers (HW and SW): 213 (up from 153 representatives.
    - Professional roles in the above include heads of standardisation/technology standards, OSS mobile network standards specialists, RAN operational teams, wireless standardisation specialists, standards strategists.
- SMEs and start-ups: 175 (up from 136), including 2 new verticals.
- Large companies (vertical industries): 104 (up from 84), including 12 new verticals.
- Standardisation organisations 57 high-profile representatives, i.e., chairs, co-chairs of 5G-related standards groups, (up from 28 representative) and corporate/institutional delegates from ITU (3), ETSI (2), IEEE (1), CEN-CENELEC (1).
    - Professional roles in the above include heads of standardisation/technology standards, OSS mobile network standards specialists, RAN operational teams, wireless standardisation specialists, standards strategists.
- Industry Groups (including ICT clusters): 29 (up from 20).
- Universities and research institutes: 178 (up from 137).

Geographical coverage has extended to cover the following countries outside the EU: Argentina, Bangladesh, Brazil, Canada, Congo, Egypt, India, Iran, Japan, Libya, Mexico, Saudi Arabia, Singapore, South Africa, South Korea, Trinidad, U.S. Most of the new connections in May-October 2017 have come from Argentina, Bangladesh, India, Iran and Saudi Arabia.

The figure below shows the percentage break down of the 5G-ENSURE LinkedIn Community at project end, where industry (suppliers; large companies, IT providers and SMEs, including verticals) represents the largest portion.

Figure 52: 5G Ecosystem in 5G-ENSURE LinkedIn Community



The table below provides a sample of community members from both the primary and secondary stakeholder categories.

Table 5: LinkedIn Stakeholder

PRIMARY STAKEHOLDERS (including representatives from 5G PPP phase 1 projects	
5G telecommunications industry	AT: A1 Telekom Austria AG; BE: KPN BASE, Proximus/Belgacom, Orange Belgium; DE: Vodafone Germany; Deutsche Telecom, T-Systems International GmbH; ES: Telefonica, Parlem; FR: France Telecom/Orange, Bouygues Telecom, Com4Innov; Orange Labs; SFR GR: OTE/COSMOTE, Intracom Telecom; IT: TIM/Telecom Italia; LU: Tango S.A (Proximus); NL: Vodafone Ziggo Netherlands, T-Mobile Nederland; SE: Ålands Telefonandelslag; SL: Telekon Slovenia; UK: BT; 02/Telefonica, Vodafone UK. CH: Swisscom; Monaco Telecom; NO: Telenoir. Outside EU - Argentina: Frixtel; Bangladesh: Robi Axiata ltd; Brazil: Oi S.A; China: China Telecom; Egypt: Vodafone; India: Jio; Iran: MTN Irancell; Japan: NTT DOCOMO; KDDI Corporation; Saudi Arabia: Mobily; South Korea: SK Telecom; Vietnam: Viettel Network Technologies Center - Viettel Group; US: Verizon & Verizon Wireless, Liberty Global, T-Systems. Suppliers/manufacturers: Cisco Systems, Ericsson, Huawei Technologies European Research Center, Intel, Nokia, Qualcomm, Samsung Electronics.
Industry 4.0, IIoT, & SMEs and Vertical Industries	**Companies** – SMEs and large companies include supply chain providers, hi-tech companies and vertical industries. **SMEs**: 3IF - Internet of Things and Industrial Internet Future (Industry 4.0), 5G UP, EICT GmbH, EnvOps, Green Communications, Incelligent, InnoRoute, InterDigital Communications, IS-Wireless, Lime Micosystems, OTREMA, Montimage, Nextworks, naudit High Performance Computing and Networking, PRISMA Telecom Testing, RESEIWE A/S, RED Technologies, RedZinc, Rohde & Schwarz, SETECS, SpinalCom (fog middleware), TerUsus. **Verticals - SMEs**: Alterest Ltd., GHIG GmbH, hardwear.io, Policy Impact Partner, SmartEnds, Square Strategic FinTech, Sudwestrundfunk, Tatung Czech, Ubiwhere.

	Vertical industries – large companies: aerospace, automotive, energy, financial services, hi-tech manufacturing/factories of the future, media and entertainment, with some covering industry digitisation across verticals and some IT/solution providers also covering multiple industries. Examples include: ABB, Accenture, Agfa Healthcare, AIRBUS, Banca d'Italia, Bosch & Robert Bosch GmbH, BNP Paribas Fortis, Comesvil, Credit Agricole Bank Poland S.A., Daimler, DEXMA Tech, DFRC, Dyson, FIAT Research Centre, Gemalto, Hyundai kia, Italtel, Lloyds Banking Group, Maersk Line, Pagero, Philips, Primark Stores, Renault Software Lab, Siemens, Sony EU & Sony China, tec ICT, Thales, Toyota, Volkswagen, Volvo.
Standards Bodies - sample	ETSI: 13+ leading representatives and decision makers, e.g. TC CYBER Vice Chair; ETSI NFV ISG Chair; ETSI NFV ISG Vice-Chair; ETSI SCP; TC RRS (Reconfigurable Radio Systems) WG 1 Chair; Director of Technical Strategy, ETSI Standardisation Projects; ETSI CTO; ETSI Board Member and IPR committee chair. 3GPP: 12+ leading representatives in, e.g.: 3GPP TSG SA Chairman; 3GPP TSG SA Vice Chairman; 3GPP RAN Standards Strategist; 3GPP SA2 Vice Chairman; Chairman 3GPP SA3; 3GPP RAN Chairman; 3GPP TSG RAN Vice-Chair; 3GPP Ran1 delegate; 3GPP RAN working group 1 Chairman; Chairman of 3GPP SA6. 3GPP SA3. AIOTI WG03: Chair (ETSI); high level architecture leader (NOKIA). IEEE: 7 leading representatives, e.g. Chair of IEEE Tactile Internet Sub-Committee; IEEE Sensors Council; IEEE 1914 WG Chief Editor; IEEE IoT Initiative Chair scenario track; IEEE 5G Initiative Co-chair; IEEE Privacy; IEEE ComSoc – VP Elect for Industry and Standards. IETF: Chair; CCAMP Working Group Co-Chair; ACE Group Chair. Leading representatives and members in the ITU SG17 (Security) and SG20 (IoT); Kantara Initiative; Open Mobile Alliance - Vice-Chairman of Communications Group (COM WG); Open Networking Foundation. **New connections**: 17 delegates (10 from 3GPP, others from IEEE, ETSI and ITU).
Industry Groups	**New connections:** EIT Ditigal (Dir. EU-US Industrial Relations; Head Industrial Doctoral School EIT Digital); APRE – NCP IT (agency for the promotion of EU research); GSMA (3 representatives); Digital Catapult; Sunderland Software City). **EU-based**: EIT Digital (Directors/Co-location Managers - France, Italy & Netherlands), EUROCITIES, Digital Catapult (Personal Data and Trust), EuroCloud Germany, Irish Internet Association, Connected Smart Cities Network (EU founded), EERA - The European Energy Research Alliance, DIMECC Oy, European Privacy Association, Cap Digital, DIGITAL EUROPE - Technology Regulation & Policy Group company representative, Finnet Association, European Cyber Security Organisation (ECSO). **International**: GSMA Latin America; GSMA - Head of Networks; 5G Americas - Head of Latin America; NGMN; Wireless World Research Forum; World Economic Forum; The Khronos Group (U.S.); Taiwan-Japan Industrial Collaboration Promotion Office (TJPO), Ministry of Economic Affairs; OSGi Alliance.
5G PPP projects & National Projects	**New connections**: 5G CORAL, 5G PHOS, 5G TANSFORMER, Global5G, 5G MEDIA, 5G TANGO; representatives from SLICENET. 5GinFIRE (BR). UK 5G programme (Bristol Open); University of Surrey. Coordinators and representatives from: EURO5G, 5GEX, CHARISMA,

	mmMAGIC, SELFNET, SPEED 5G, 5G-Crosshaul, Sonata and international 5G project: 5G!PAGODA. (EU-JP) and PICASSO (EU-U.S.).
SECONDARY STAKEHOLDERS	
Policy - EC: Chief Science Officer, Dep. For International Trade (HM Government); Head of Spectrum Allocation and Licensing Division (Libya); Spanish Ministry of f Economics and Competitiveness – NCP**;** Satellite Centre (IT). Thibaut KLEINER, Head of Cabinet of @GOettingerEU; European Commission, Programme & Policy Officer - Smart Mobility, Connected and Automated Driving, Electromobility; European Commission - DG CONNECT - Innovation and Starts-Up Unit, Head of Sector ICT Standardisation. **EU Regulars and governments**: Ofcom and IP Networks & Digital Media, HM Cabinet Office (UK – 2 connections); Ministere de l'Economie et des Finances, European and international spectrum harmonisation adviser at DGE (FR); SFR Spectrum Policy Manager; Flemish Government (Vlaamse Overheid) (BE); OFCOM - Swiss Telecom Regulator (CH). **CERTS/CSIRTS/national cyber security centres**: Andalucia CERT, national cyber centre (DK).	
Universities & research institutes : Aarhus University (IoT), Aalto University, BISDN at Berlin Institute for Software Defined Networks, CTTC, HHI Fraunhofer, Iowa State University, King's College London, KTH, Peking University, Technical University of Madrid, TELECOM SudParis, Trinity College Dublin, Universidad de Murcia, University of Oxford, University of Southampton, University of Surrey 5G Innovation Centre, Federal University of Ceará, Brazil, 5G Lab (DE).	
EU and International initiatives: European Cyber Security Organisation (ECSO); GDPR Awareness Coalition.	

5.2 5G-ENSURE Twitter Followers

5G-ENSURE has extended its followers to 673 from 504 reported in D5.5 (April 2017)., with an average of 28 new followers a month since Twitter was set up in November 2015.

Figure 53: Geographical Coverage on Twitter

The geographical spread of 5G-ENSURE Twitter followers has increased to 55 countries (49 in April 2017). Top ten countries: UK (stable at almost 20%), U.S. (13%, from 10%), Belgium (7%, down from 8%), Germany

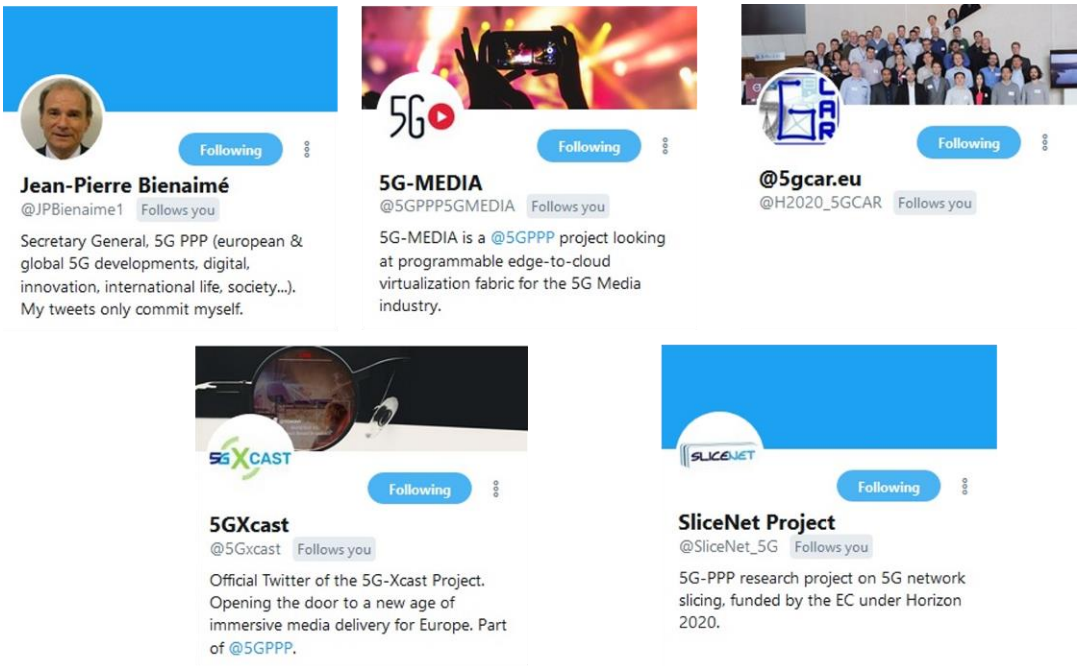
(6%, from 3.6%), France (6%, down from 7%), Italy (5.02%, from 4.8%), Spain (5%, as before), Finland (4.7%, down from 6.4%), India (4.4%, from 3.6%) and Brazil (3%, as before). Top cities also remain similar, with capital cities/IT hubs being the top followers: London leading at 8.7%, followed by Barcelona on 3%, Sweden on 1.3%, New York, San Francisco, San Paulo and New Delhi.

The figure below shows a snapshot of top social media influencers that 5G-ENSURE has recruited through its regular engagement on Twitter, adding to a rich pool of influencers including two authors of digital transformations.

Figure 54: Recent Top Followers

5G-ENSURE has continued to engage at the 5G PPP joint programme level. A sample of new engagements is showed in the figure below.

Figure 55: Recent Engagements with 5G PPP



5.3 5G-ENSURE Impact on Social Media

The use of twitter in 5G-ENSURE is an important part of the communications strategy, designed to raise awareness of 5G-ENSURE activities and outputs, engage with primary and secondary stakeholders, and share results across the 5G PPP. Six twitter metrics are used to gauge impact of twitter campaigns, e.g. tweets, followers (identifying top followers each month), following, impressions (number of times users are served a tweet in a given timeline, search results or from twitter profile), profile visits (number of times profile page visited), mentions (number of times @5GEnsure is mentioned in tweets). Some of these

metrics are also used to benchmark performance against peer projects, e.g. tweets, followers, likes and lists.

The table below shows monthly twitter performance based on the metrics used and overall achievements.

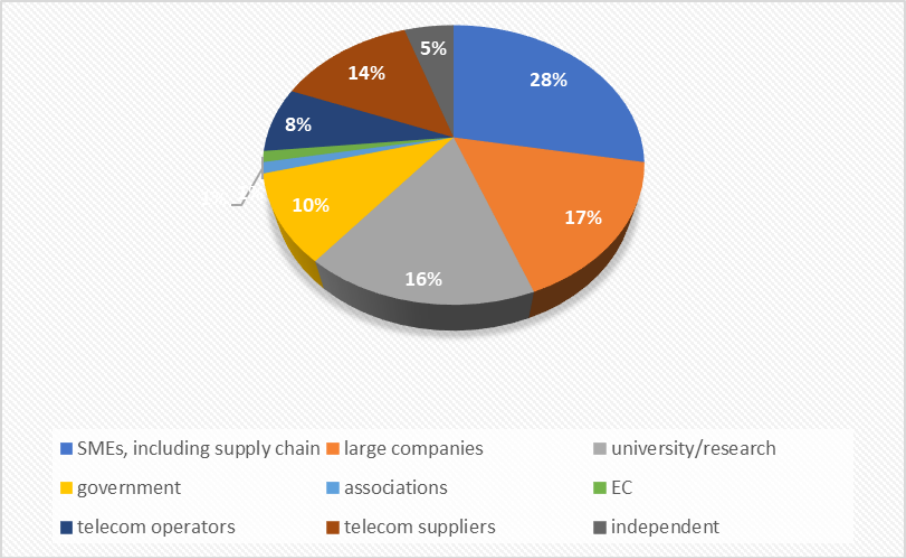
Tweets	*1350 (av./month: 56)*
Followers	*678 (av./month: 28)*
Following	*320*
Total impressions	*804,278 (av./month: 33,500)*
Total profile visits	*13,767 (av./month: 573.6)*
Total link clicks: 1417 | Total Reteets: 2030 | Total likes: 1235	
November 2017 top follower: Brian Evans, 392,000 – top 7 influencer, blockchain, Forbes (last updated 13.11.2017)	
Total in period May – October 2017: *Number of Tweets: 302* *Number of profile visits: 4210* *Tweet impressions: 182,500* *New followers: 156* *Mentions: 114*	*Link clicks: 433* *Retweets: 432* *Likes: 357*
October 2017	
Number of Tweets	*25*
Number of profile visits	*251*
Tweet Impressions	*16,200*
New followers	*31*
Top follower	*Joel Comm, @joelcomm, 915,000*
Mentions	*29*
September 2017	
Number of Tweets	*16*
Number of profile visits	*307*
Tweet Impressions	*15,700*
New followers	*20*
Top follower	*Katrin Boeke-Purkis, @BoerkeKatris, 85,300*
Mentions	*11*
August 2017	
Number of Tweets	*45*

Number of profile visits	*413*
Tweet Impressions	*27,000*
New followers	*7*
Mentions	*16*
July 2017	
Number of Tweets	*69*
Number of profile visits	*860*
Tweet Impressions	*32,800*
New followers	*30*
Mentions	*14*
June 2017	
Number of Tweets	*85*
Number of profile visits	*1028*
Tweet Impressions	*53,300*
New followers	*29*
Top follower	*Bill McCabe, @IoTRecruiter: 90,300 followers; IoT, cybersecurity, artificial intelligence and blockchain*
Mentions	*36*
May 2017	
Number of Tweets	*62*
Number of profile visits	*1351*
Tweet Impressions	*37,500*
New followers	*39*
Top follower	*n/a*
Mentions	*8*

5.3.1 Standardisation Network

The 2nd International Workshop at ETSI was an important opportunity to engage with representatives from standardisation organisations coming from the public and private sectors, helping extend our community. The figure below shows the breakdown of participants per organisation type, with 67% of the 79 particpants (excluding 5G-ENSURE partners) coming from the private sector: SMEs, large companies and suppliers/operators while 16% come from research and industry. 33/79 (almost 50%) are involved in standardisation organisations at different levels with most of them coming from ETSI and the 3GPP.

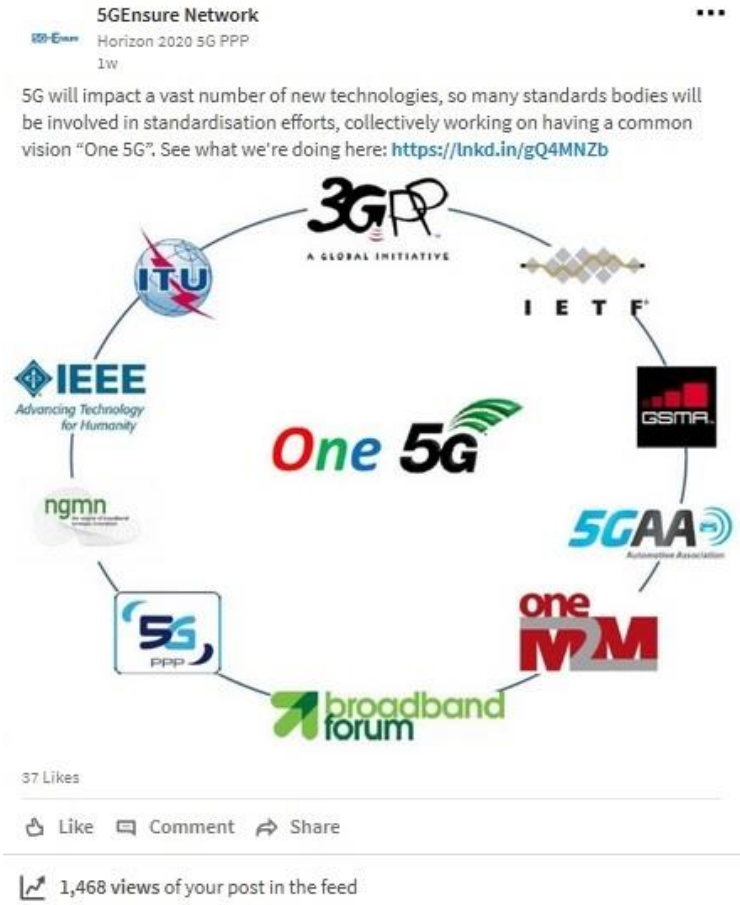
Figure 56: Breakdown of 2nd Int'l Workshop Participants



Activity/Network	Number of representatives
2ND International WS: ETSI	11
2ND International WS: ETSI &3GPP	22
LinkedIn high-profile specialists and delegates	57 chairs/co-chairs and many specialists representing their respective organisations.

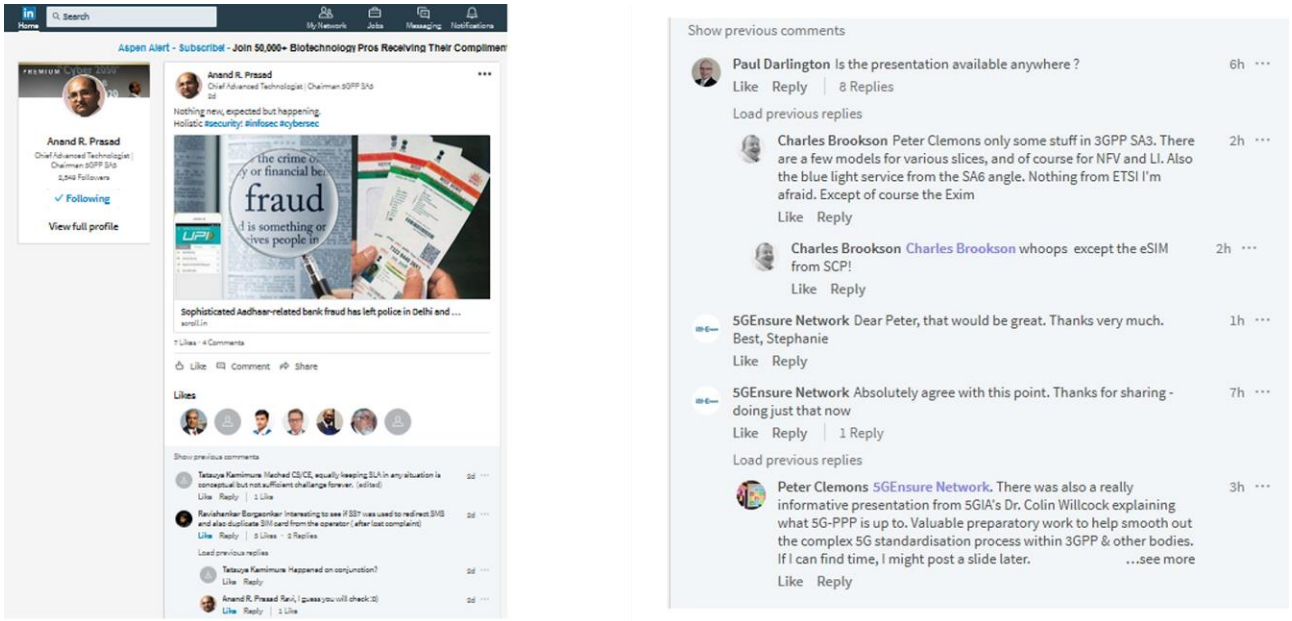
Core messages on 5G standardisation and specific examples of 5G-ENSURE contributions have been very well received on LinkedIn, as the image below shows. The post was viewed by over 1400 people with 6 reshares and 37 likes. Top countries outside Europe include U.S. (Washington, Dallas, San Francisco) and India, including 100+ representatives from the supply side and representatives outside the core network. At the time of writing, the post was also Top Tweet.

Figure 57: LinkedIn Engagement on 5G Standardisation



The next image shows interactive discussions on standards with LinkedIn professionals and also a member of the Advisory Board (ETSI chair), sharing ETSI insights and work being done within the 5G PPP, and other discussions.

Figure 58: Sample of Interactive Discussions on LinkedIn



6. Post-project Plans

Main takeaways from this extended report to D5.5 are:

- Standardisation work within 5G-ENSURE will be sustained and carried forward mainly by TIM and Ericsson.
- Discussions with NIST have been very positive in relation to standardisation work by 5G-ENSURE, including efforts on privacy within the 3GPP.
- The 2nd International Workshop (June 2017) during ETSI Security Week was an excellent opportunity to share 5G-ENSURE findings and outputs at a premier forum on security standardisation.
- Beyond this, 5G-ENSURE has conveyed key messages on security standardisation withint the 5G PPP and to the entire 5G ecosystem recruited through its LinkedIn professional network.
- Building a strong, international community is keystone work for security-by-design approaches like 5G-ENSURE, ensuring that the core message is relayed in the future.
- Importance of communicating research findings/results through multiple channels tailored to different audiences. The work done with the University of Oxford is a good example of ensuring coverage across technical constituencies, reputable IT magazines and the mainstream press.
- Professional networks like LinkedIn prove to be an essential forum for interactive discussions with a truly global and multi-stakeholder community and keeping the community abreast of developments on 5G security and standardisation.

With most of the 5G-ENSURE results coming at the end of the project life cycle, it is important to ensure full coverage of all results. The 5G-ENSURE **communication marketing plan** for the following months aims to support the MRLs indicated in D5.6 for each enabler and more generally the full suite of results achieved at project end, including the security architecture, the test-bed, and the trust model. This approach is aligned with the Horizon 2020 objective for the continued dissemination of results, and with the joint and individual exploitation plans defined in D5.6, as an opportunity to highlight sustainable activities, spanning the test-bed, the continued 5G PPP Security WG, continued standardisation, participation in the 5G PPP SME WG.

The plan includes but is not limited to:

- Completion of an on-going extensive website update covering all major outputs and assets accrued over the project lifecycle with newly designed branded images and statistical tools.
    - New page designs for the Golden Nuggets: 5G enablers, test-bed and security architecture.
    - Video suite on major outcomes.
- Updated LinkedIn profile to reflect website updates.
- Continued engagement on Twitter and LinkedIn with posts designed to inform and engage audiences.
- Reinforced core messages on the importance of security, privacy and trust in future 5G networks, as recently highlighted by ETSI CTO, Adrian Scrase, at URLLC 2017: “5G will only succeed if we all focus on security, privacy and trust”.

7 Annexes

Annex 1 Complete list of papers and conferences

The table below provides the complete lists of publications on 5G-ENSURE research results, during the two years.

Title	*Authors*	*Partner*	*Publication*
On the Fingerprinting of Software-defined Networks	Heng Cui, Ghassan O. Karame, Felix Klaedtke, and Roberto Bifulco.	NEC	IEEE Transactions of Information Forensics and Security 11(10):2160-2173, 2016. DOI & Open Access
Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems	Altaf Shaik, Ravishankar Borgaonkar, Jean-Pierre Seifert, N. Asokan, Valtteri Niemi	University of Oxford	The Network and Distributed System Security Symposium 2016.
Towards Micro-Segmentation in 5G Network Security	Olli Mämmelä, Jouni Hiltunen, Jani Suomalainen, Kimmo Ahola, Petteri Mannersalo, Janne Vehkaperä	VTT	In Proc. of the EuCNC 2016 Network Management, QoS and Security workshop.
Threats to 5G Group-Based Authentication	Rosario Giustolisi and Christian Gehrmann	SICS	In Proc. of the 13th International Conference on Security and Cryptography (SECRYPT 2016).
Cases for Including a Reference Monitor to SDN. (Demo)	Dimitrios Gkounis, Felix Klaedtke, Roberto Bifulco, and Ghassan O. Karame	NEC	In the Proc. of the 2016 ACM SIGCOMM Conference.
TruSDN: Bootstrapping Trust in Cloud Network Infrastructure	Nicolae Paladi and Christian Gehrmann	SICS	In Proc. of the 12th EAI International Conference on Security and Privacy in Communication Networks (SECURECOMM 2016).
White Rabbit in Mobile: Effect of Unsecured Clock Source in Smartphones	Shinjo Park, Altaf Shaik, Ravishankar Borgaonkar, and Jean-Pierre Seifert	University of Oxford	6th Annual ACM CCS 2016 Workshop on Security and Privacy in Smartphones and Mobile Devices

			(SPSM).
Analysis of Trusted Execution Environment usage in Samsung KNOX	Ahmad Atamli-Reineh, Ravishankar Borgaonkar, Ranjbar A. Balisane, Giuseppe Petracca, Andrew Martin	University of Oxford	In Proc. of the Workshop on System Software for Trusted Execution (SysTEX 2016)
A Secure Group-Based AKA Protocol for Machine-Type Communications	Rosario Giustolisi Christian Gehrmann, Markus Ahlström, Simon Holmberg	SICS	International Conference on Information Security and Cryptology ICISC 2016: Information Security and Cryptology – ICISC 2016 pp 3-27
Mobile subscriber WiFi privacy	Piers O'Hanlon; Ravishankar Borgaonkar; Lucca Hirschi	University of Oxford	In IEEE Symposium on Security and Privacy's Mobile Security Technologies Workshop (MoST), San Jose, USA, 25 May 2017.
Stingray: Evaluating IMSI Catchers Detection Applications	Ravishankar Borgaonkar; Shinjo Park; Altaf Shaik; Andrew Martin Jean-Pierre Seifert	University of Oxford	In the 11th USENIX Workshop on Offensive Technologies (WOOT 17)
Security and Resilience in 5G: Current Challenges *and Future Directions*	Ghada Arfaoui, Jos´e Manuel Sanchez Vilchez, Jean-Philippe Wary (Orange Labs)	Orange Labs	In 6th International Workshop on Security & Optimization for Wireless Networks (SOWN 2017)' inside TrustCom2017
Runtime Verification of Temporal Properties over Out-of-order Data Streams	David Basin, Felix Klaedtke, and Eugen Zalinescu	NEC	Proceedings of the 29th International Conference on Computer Aided Verification (CAV). Lecture Notes in Computer Science, volume 10426, pages 356-376. Springer, 2017

The table below presents the complete list of 5G-ENSURE research results presented at technical conferences.

Conference	***Partner***	***Presentation title***
International Workshop on RVM	B-COM	Presentation of 5G-ENSURE " How

and Security for multi-RAT and reconfigurable systems 10 March 2016, Rennes (FR)	Orange	5G-ENSURE may address and manage software define Radio"
Networld2020 Annual Event and GA 2016 19 April 2016, Bedford Hotel & Congress Center, Brussels (BE)	VTT	Presentation of 5G-ENSURE: Security enablers for 5G
ETSI Summit: 5G: From Myth to Reality 21-04-2016, ETSI, Sophia Antipolis (FR)	VTT	Participation in a poster session on invited topics (mainly 5G-PPP projects) to trigger an exchange of views on aspects of 5G that are not covered in the summit sessions. The 5G-ENSURE poster introduced the project and its main achievements, i.e., the use cases and early vision of security enablers.
Net Futures 2016, 20-21 April 2016, The Egg, Brussels (BE)	ORANGE, TIM	Attendance in the session on the 5G vision and roadmap to key standards. Direct interaction with Orange Labs and Telecom Italia, vice chair of the 3GPP RAN. Distribution of the bookmark promoting the Open Consultation and the 1st International Workshop on Standardisation
First 5G-ENSURE Workshop, 16 June, Sophia Antipolis, FR	Thales, Orange, VTT, Trust-IT, SICS	Presentation of 5G-ENSURE activities and results
NDSS 2106 Security Conference, 21-24 February 2016, San Diego, U.S.,	University of Oxford	"Practical attacks against privacy and availability in 4G /LTE mobile communication systems"
Troopers Security conference, 16-17 March 2016, Heidelberg, Germany,	University of Oxford	"Don't connect to my 4G base station: investigation into leaks in 4G baseband"
SICS Security Day, May 2016, Stockholm, Sweden,	University of Oxford	"Security in cellular-radio access networks"
Qualcomm Mobile Security Summit, May 2016, San Diego, U.S.,	University of Oxford	"Analysing LTE/4G air interface protocols"
GSMA Device Security Group 28-29 August 2016 at San Ramon, CA, U.S.	University of Oxford	Device Security Issues and 5G Considerations

Black Hat Europe 2016, 3-4 November 2016 in London.	University of Oxford	"Wifi-based IMSI Catcher"
1st International Workshop on Security in NFV-SDN (SNS2016), 7 November 2016, Palo Alto, U.S.	Nokia	Presentation of 5G-ENSURE project and its outputs
National Security and Resilience Conference 2016, 09 November 2016, London, UK	IT Innovation	Talk on trust and security modelling, including the Trust Builder from 5G-ENSURE.
19th Annual International Conference on Information Security and Cryptology, 30 November – 2 December 2016, KIISC (Korean Institute of Information Security and Cryptology)and NSR (National Security Research Institute), Korea	SICS	Paper entitled: A Secure Group-Based AKA Protocol for Machine-Type Communications
Cross-Project Workshop organised by METIS-II. 6-7 February 2017, Athens	Thales	5G-ENSURE technical coordinator, Pascal Bisson (Thales) chaired the session on security and also presented the main findings and outputs of the project.
Most 2017 IEEE Symposium on Security and Privacy's Mobile Security Technologies Workshop, 25 May 2017, San Jose, CA (US)	Oxford	Presentation of paper on *Mobile Subscriber WiFi Privacy*
VIVACE Expert Advisory Board Meeting, 07 June 2017, London	IT INNOV	Partecipation at talk on impact of technology on the use of communication data for law enforcement
Security BSides London 2017, 7 June 2017, London, UK	Oxford	Presentation of paper on *Mobile Subscriber WiFi Privacy*
Cyber Security Oxford Industry Day, 9 June 2017, Oxford, UK	Oxford	Interaction between members from the cyber security industry, and students and academics at Oxford
EUCNC 2017, June 12-15 2017, Oulu, Finland,	Thales	Presentation of 5G-PPP Security Landscape whitepaper 5g-PPP Security WG workshop
ETSI Security Week, 2th 5G-ENSURE Workshop, 16 June 2017, Sophia Antipolis, FR	Thales, TIM, Orange, Trust-it,IT-INNOV, NEC, SICS	Presentation of the 5G-ENSURE project results
2017 ACE-CSR Conference,	IT INNOV	Partecipation in talks

28-29 June May 2017, Nottingham		
Shakacon IX 2-Day IT security conference, 12-13 July 2017, Hawaii Prince Hotel Waikiki	Oxford	,Presentation of the paper, "*Mobile subscriber WiFi privacy".*
Blackhat Las Vegas Conference, 22-27 July 2017, Mandalay Bay	Oxford	Presentation of research work on *New adventures in spying 3G and 4G users: Locate, Track & Monitor"*
11th USENIX Workshop on Offensive Technologies (WOOT'17) 14-18 August 2017, Vancouver	Oxford	Presentation on the paper *White-Stingray: Evaluating IMSI Catchers Detection Applications.*
BCS Action Research Forum: Safety Critical Systems Club, 31 October 2017, BCS (The Chartered Institute for IT), London	IT INNOV	Presentation highlighting the need to consider security risks in the end-to-end system, the network as an active component, and to have a clear understanding of security responsibilities and trust assumptions between developers and manufacturers, network operators, and users.

The table below presents the exhibition events of some of 5G-ENSURE tangible results.

Exhibitions	***Partner***	***5G-ENSURE demo results***
Global 5G, 9-10 November 2016, Rome	TIM	Exhibition 5G-ENSURE demos
International Cyber security Forum 2017, 24-25 January 2017, Lille	BCOM	Stand promoting 5G-ENSURE, the test bed and enablers.
RISE SICS Open House, 17 May 2017, Kista, Sweden	SICS	Demo of the IoT Enabler
EUCNC 2017, June 12-15 2017, Oulu, Finland,	VTT, Thales, NIXU and SICS	Demo showing end-to-end connection between VTT and b<>com testbed, the "Internet of Things Enabler", "VNF Certification Enabler".
ETSI Security Week, second 5G-ENSURE Workshop,	Thales,TIM,NEC,Orange,SICS, Nokia, Ericsson	Demo on Privacy Enhanced Identifier enabler,

16 June 2017, Sophia Antipolis, FR		
2017 ACE-CSR Conference, 28-29 June May 2017, Nottingham	IT INNOV	demos of Trust Builder
ACM SIGCOMM 2017, 21 -25 August, UCLA campus in Los Angeles, CA, U.S.	SICS	demo on Bootstrapping Trust - Safeguarding VNF Credentials

Annex 2 – Overview of contributions to the joint 5G PPP Programme

The table below reports the main joint activities at 5G-PPP level where 5G-ENSURE actively contributed..

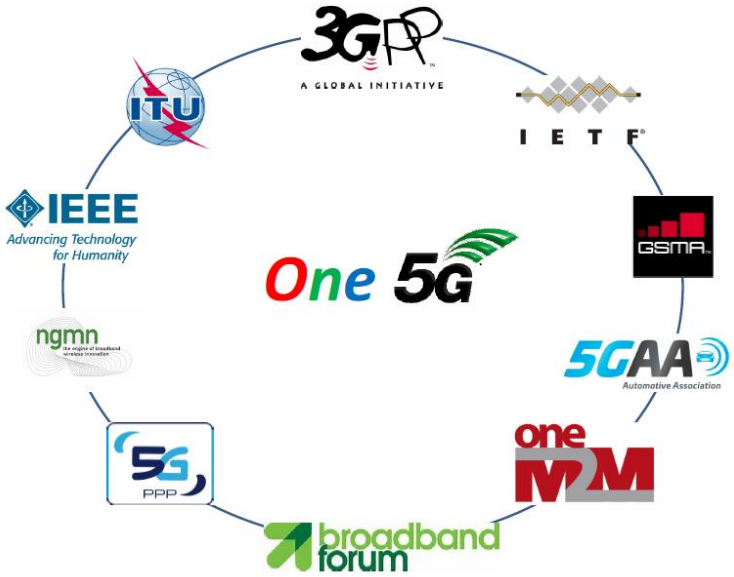
5G-PPP	*Partner*	*5G-ENSURE contribution*
5G-PPP Security Work Group	**Thales, Orange, TIM**	• WG created by 5G-ENSURE • Bring together the projects within the 5G-PPP phase 1 having a common interest in the development and progression of topics related to security. • Ensure, to as great an extent as possible, co-operation between the projects. • Get a common vision on security and privacy aspects. • Contributions to 5G-ENSURE public consultation on 5G security; • Sharing of 5G-ENSURE results to encourage re-use and sharing of newly acquired expertise within the 5G PPP. • Production of 5G-PPP Security Landscape Whitepaper • Organisation of "5G Security: Phase 1 landscape and foreseen evolutions" workshop at EuCNC17 • Bring on board Phase 2 projects Ensure forward on security aspects and re-use also extension of security achievements coming from Phase I projects • Physical meeting in Turin, 19 October 2017
5G-PPP Pre-Standard WG	**TIM**	• Sharing of standardisation study and activities related to security and privacy aspects. • Sharing of the contributions produced for the targeted standardisation organisations. • Contributions for standardisation message at MWC2016 on security and privacy aspects.

		• Contribution to the whitepaper on the impact of the H2020 funded project on the 5G Specification during the phase 1.
5G-PPP VISION & SOCIETAL CHALLENGES WG	**IT INNOVATION**	• Enforce the need for a well-defined but also flexible trust model, a flexible approach to use network slicing within and between domains, and even slicing of slices to support agile and complex business relationships within vertical sectors • Enforce the need for security to be maintained and demonstrated while seeking other improvements in agility, scalability and performance. • Contribution to the white paper for MWC 2017 • Contribution to the survey and analysis of verticals opportunities • Contribution to the white paper explaining the significance of Phase 1 achievements
5G-PPP ARCHITECTURE WG	**SICS**	• Facilitate consensus building on the 5G architecture. • Contribution to the 5G PPP White Paper "View on 5G Architecture"
5GPPP Network Management & Quality of Service Working Group	**NEC**	• Contribution to the security session of the “Cognitive Network Management for 5G” whitepaper.
COMMS Group	**Trust It**	• Active participation in supporting joint promotional activities. • Contribution on action on social media with concrete examples, offering tips on how to engage online. • Guidance on press releases and in driving the setting-up of the LinkedIn Group
European 5G Annual Journal e	**5G-ENSURE**	• Contribution
Second edition of the European 5G Annual journal	**5G-ENSURE**	• Contribution
5G-PPP TB Whitepaper	**5G-ENSURE**	• Contribution to the GoldenNuggetsBoxes for 5G-PPP TB Whitepaper
5G PPP Cross-project workshop	**Thales**	• Pascal Bisson (Thales) chaired the session on security and also presented the main findings and outputs of the project

Annex 3 – Standardisation Landscape

Snapshot of relevant Standards Organisations and Industry Associations

As 5G will impact a vast number of new technologies, many standards bodies will be involved in standardisation efforts, all together working on having a common vision "One 5G".



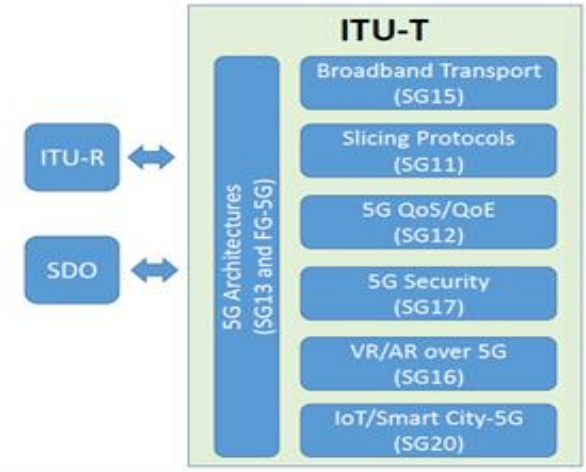
Today's 3G and 4G mobile broadband systems are based on the ITU's IMT standards. ITU established the detailed specifications for IMT-2000 and the first 3G deployments commenced around the year 2000. In January 2012, ITU defined the next big leap forward with 4G wireless cellular technology –IMT-Advanced– and this is now being progressively deployed worldwide.

The scope of IMT-2020 is much broader than previous generations of mobile broadband communication systems. Use cases foreseen include enhancement of the traditional mobile broadband scenarios as well as ultra-reliable and low latency communications and massive machine-type communications. The ITU is working in developing the specifications for IMT-2020 by:

- synchronizing with ITU-R, the ITU's Radio Communication Sector (ITU-R) has completed the "Vision" for "5G" mobile broadband connected society in September 2015. The horizon for the future of mobile technology is considered instrumental in setting the agenda for the the World RadioCommunication Conference 2019.
- developing architectures and non-radio technology in ITU-T, SG13, SG11 and FG-5G. The Focus Group (FG) on network aspects of ITM-2020 (International Mobile Telecommunication system) was established in May 2015 to analyse how emerging 5G technologies will interact in future networks

as a preliminary study into the networking innovations required to support the development of 5G systems,

- strengthening use of Broadband transport capabilities (G.fast and Optics) in ITU-T SG15,
- identifying QoS/QoE requirements in ITU-T SG12,
- identifying Security capability in ITU-T SG17,
- focusing on VR/AR over 5G in ITU-T SG16 and on the use of IoT and Smart City in ITU-T SG20.



However IMT-2020 is also a collaborative effort between ITU and other SDOs such as 3GPP for Mobile aspects. The following figure provides the view of this type of collaboration based on the agreed timeline on 5G .

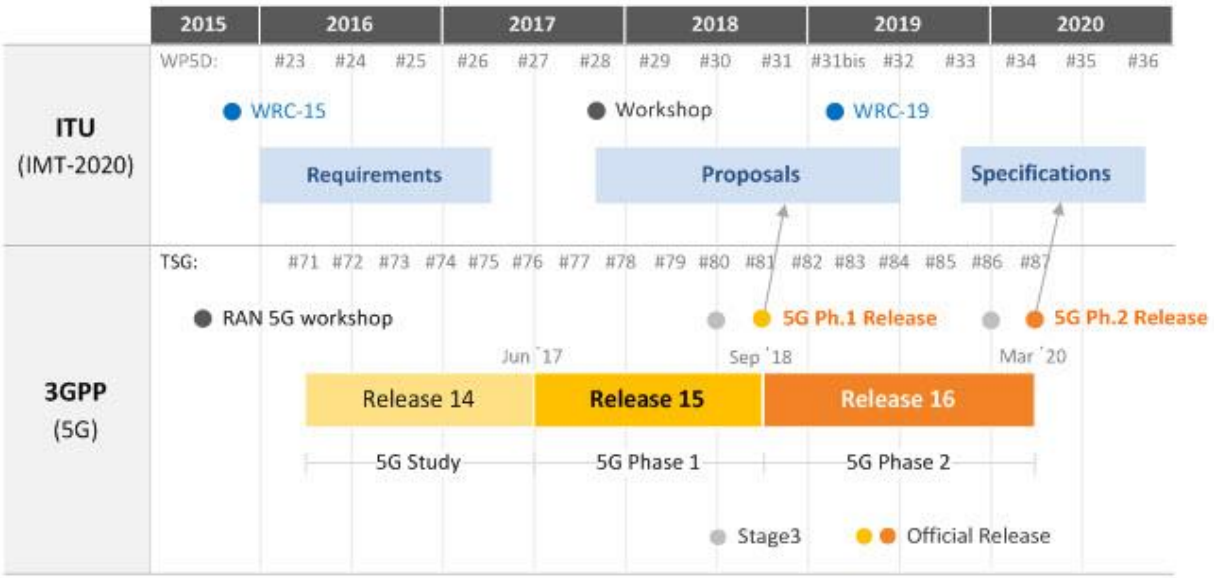


Figure 59: Timeline of 5G in ITU-R and 3GPP

3GPP- 3rd Generation partnership project

3GPP is the main organisation for creating standards in mobile communications. Its current 5G standardisation time plan currently spans 2016-2019 and it covers three stages of specification:

- Stage 1: Requirements

- Stage 2: Architecture
- Stage 3: Protocols

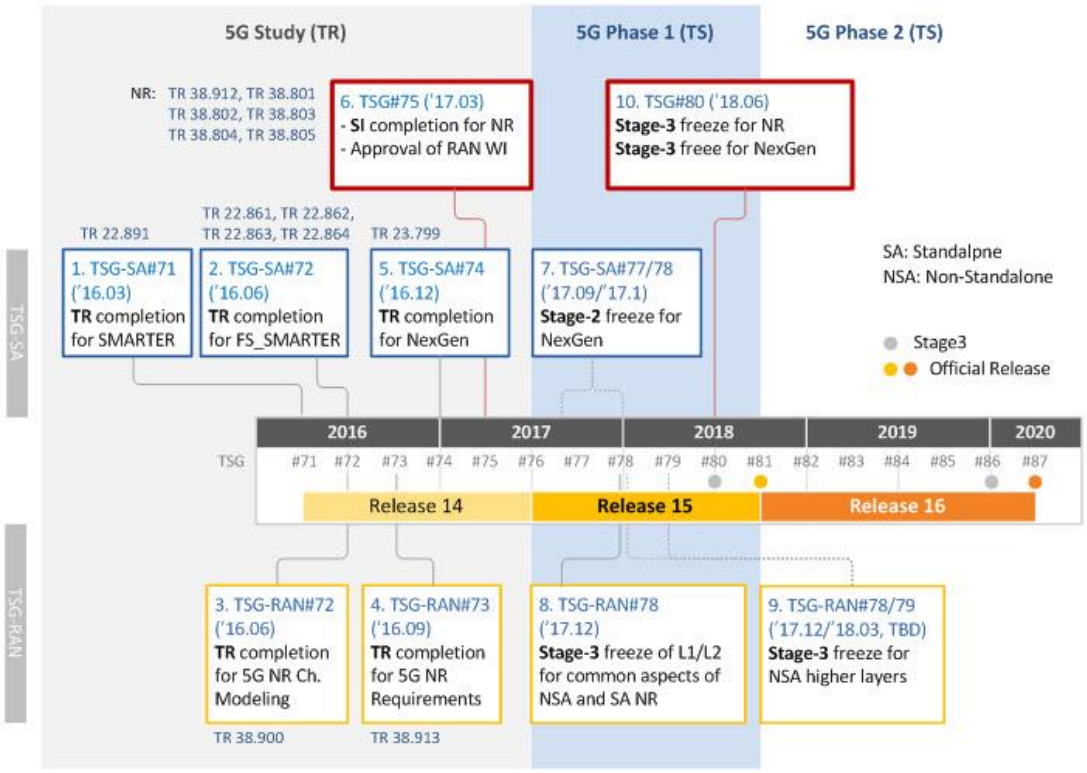


Figure 60: 3GPP Detailed Timeline of 5G

The study phase concerning 5G Requirements, Architecture, Security and the new Radio has been concluded sd showed in the following figure.

Report No.	Title	Completion
TSG-RAN		
TR 38.900	Study on channel model for frequency spectrum above 6 GHz	2016.06
TR 38.912	Study on New Radio (NR) Access Technology	2017.03
TR 38.801	Study on New Radio Access Technology; Radio Access Architecture and Interfaces	
TR 38.802	Study on New Radio Access Technology; Physical Layer Aspects	
TR 38.803	Study on New Radio Access Technology; RF and co-existence aspects	
TR 38.804	Study on New Radio Access Technology; Radio Interface Protocol Aspects	
TR 38.805	Study on New Radio Access Technology; 60 GHz Unlicensed Spectrum	
TR 38.913	Study on Scenarios and Requirements for Next Generation Access Technologies	2016.09
TSG-SA		
TR 22.891	Study on New Services and Markets Technology Enablers	2016.03
TR 22.861	FS_SMARTER - Massive Internet of Things	2016.06
TR 22.862	FS_SMARTER - Critical Communications	2016.06
TR 22.863	FS_SMARTER - Enhanced Mobile Broadband	2016.06
TR 22.864	FS_SMARTER - Network Operation	2016.06
TR 23.799	Study on Architecture for Next Generation System	2016.12
TR 33.899	Study on the security aspects of the next generation system	2017.03

Figure 61: 3GPP Release 14: 5G Technical Reports (TR)

The 5G normative work is instead currently ongoing and it is aimed at gradually realising the full 5G capabilities in two phase:

- Phase 1 (Rel-15) to be completed by June 2018: it addresses the more urgent subset for commercial deployments
- Phase 2 (Rel-16) to be completed by March 2020 (IMT 2020 submission): it addresses all identified use cases and requirements

Following the main reference for the ongoing normative work:

- **High-Level 5G Requirements** – TS 22.261 http://www.3gpp.org/DynaReport/22261.htm
- **Architecture** – TS 23.501 http://www.3gpp.org/DynaReport/23501.htm
- **System Flows** – TS 23.502 http://www.3gpp.org/DynaReport/23502.htm
- **Security** – TS 33.501 http://www.3gpp.org/DynaReport/33501.htm

ETSI – European Telecommunications Standards Institute

ETSI produces globally applicable standards for Information & Communications Technologies including fixed, mobile, radio, broadcast, internet, aeronautical and other areas. ETSI has a number of component technologies which will be integrated into future 5G systems: Network Functions Virtualization (NFV), Multi-access Edge Computing (MEC), Millimetre Wave Transmission (mWT) and Next Generation Protocols (NGP).

The ETSI Industry Specification Group for Network Functions Virtualization (ETSI ISG NFV) plays the main role to standardise the infrastructure aspects of 5G networks, that is more and more virtualised and softwarised. Moreover, ETSI TC CYBER, the Technical Commeetee dedicated to the cybersecurity, is coordinating all the security aspects carried-on within each TC operating under the ETSI umbrella. In particular the TC CYBER is working on Privacy and LI aspects and other strategic topics related to the security of the ICT. Also TC CYBER has been identified as one of the most relevant group by the 5G-ENSURE project, in particular because of its horizzontal view (not related to a specific technology) on cyber security.

Internet Engineering Task Force (IETF)

The IETF is the standards body that specifies the basic communication protocols to be used in the Internet.

The mission of the IETF is to produce high quality, relevant technical and engineering documents that influence the way people design, use, and manage the Internet in such a way as to make the Internet work better (RFC 3935).

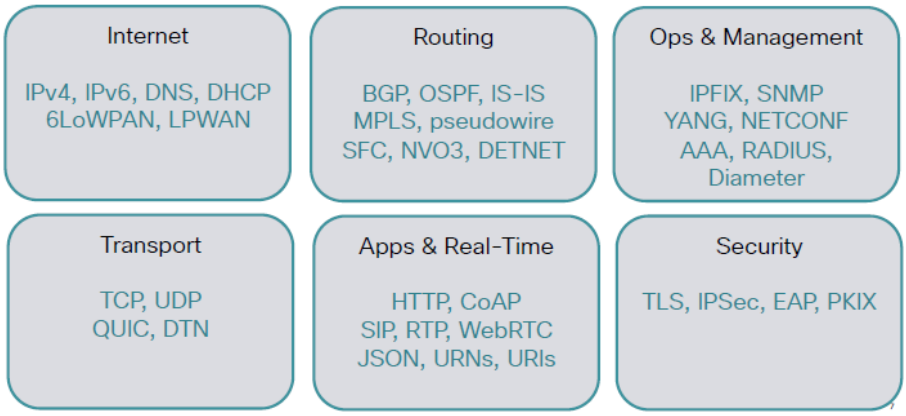


Figure 62: IETF technical areas

The IETF and 3GPP have a long history of cooperation work, including SIP/IMS, EAP-AKA, and Diameter. Last June 2017, during the 3GPP TSG Plenary meeting, the IETF Chair shares her views on how 3GPP and IETF can cooperate on 5G standardization.

Some areas of existing IETF work that may be of relevance in the 5G context have been highlighted, including the work on data models, service chaining, deterministic networking, and QUIC a new working group recently formed. The aim of QUIC WG is to create a UDP based protocol that would minimize connection establishment, reduce overall latency, support stream multiplexing and multipath communication. For security, the goal is to use TLS 1.3 to protect the QUIC communication.

In addition the new uses of the following existing technology have indicated as of interest for 5G: (http://www.3gpp.org/ftp/Information/presentations/Presentations_2017/3GPP%20-%20IETF%20and%205G%20v2.pdf)

- Extensible Authentication Protocol (EAP): it is a framework for network access authentication (RFC 3748). It includes SIM and AKA-based authentication methods. Draft 5G security specification from 3GPP SA3 includes the use of this framework. There is also work ongoing on an EAP method for bootstrapping security for devices with restricted user interfaces and no pre-configured authentication credentials.

- HTTP/2: it is a revision to HTTP standard, published as RFC 7540 in 2015. It is potentially of interest for 5G and IoT applications generally due to focus on reducing latency and conserving network/server resources.
- Internet of Things (IoT): it is one of the areas where IETF has been dedicating a considerable amount of effort. Whilst HTTP can be used for IoT devices, a new lighter weight version of the protocol has been defined for Constrained Devices. That protocol is called "The Constrained Application Protocol (CoAP)", which is specified in RFC 7252. CoAP is based on the same Representational State Transfer (REST) architecture and provides a generic request/response interaction model similar to the Hyper-Text Transfer Protocol (HTTP). However, unlike HTTP, messages in CoAP are exchanged asynchronously over the unreliable datagram-oriented transport such as UDP with optional reliability. Access control mechanisms are a necessary and crucial design element to any application's security. Therefore, IETF is also investigating how web-based access control and authorisation solutions can be applied to resource-constrained devices that are part of the IoT. It is currently defining an authorisation and access control framework for resource-constrained nodes based on the OAuth 2.0 framework, which is currently the de-facto standard for authorisation on the web.

GSM Association

GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 250 companies in the broader mobile ecosystem. As the association represents mobile industry, GSMA is playing a significant role in shaping the strategic, commercial, and regulatory development of the 5G ecosystem. This includes areas such as *defining roaming and interconnection for 5G, and identifying and aligning suitable spectrum bands*.

Figure below shows the role of GSMA to the road of 5G that is devoted to bring together all stakeholders in the mobile industry to ensure that the visions of the 5G era are well defined, understood and delivered. On behalf of its members, the GSMA is focusing on how to influence the development of 5G technologies and standards, on how to support the rollout of 5G networks and development of new business models for the 5G era, on guiding the development of government agenda and policies, and on moderating the messaging around 5G.

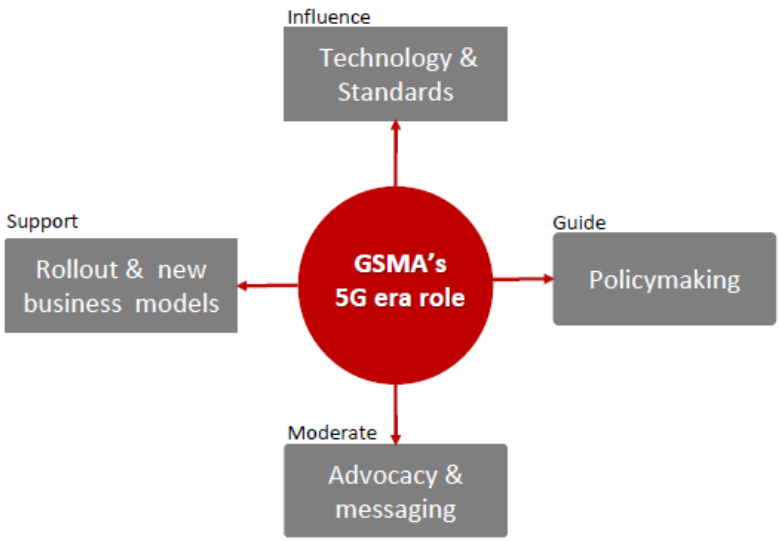


Figure 63: GSMA role on the road to 5G

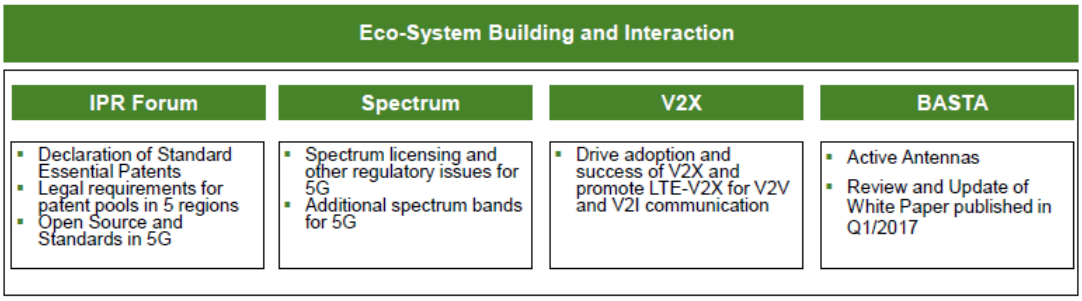
.

NGMN Alliance

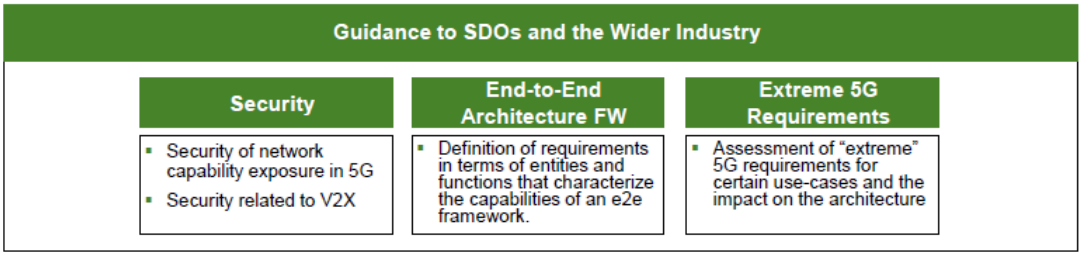
The NGMN Alliance comprises a leadership network of more than 90 partners. The focus of the Work Programme is on 5G. NGMN will develop end to end operator requirements to satisfy the needs of customers and markets in 2020+

In 2016, the NGMN Board announced three key NGMN focus areas for the coming years:

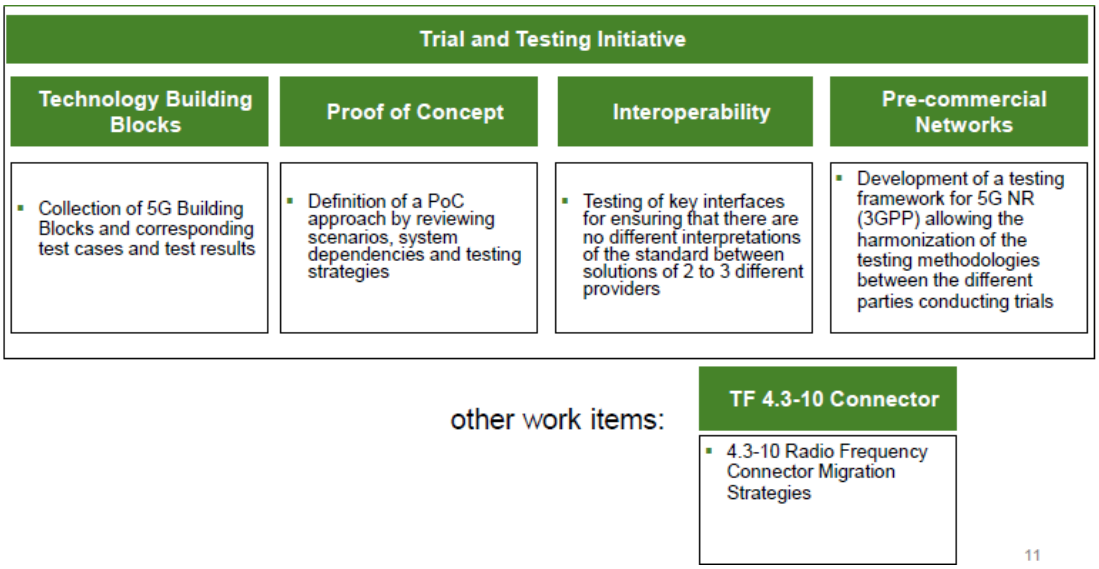
- Eco-system building and interaction: the objective is to establish platforms for collaboration with representatives from vertical industries, IPR experts and other business communities. The current activities are devoted to develop implementation plans for the 5G IPR recommendations outlined in the NGMN 5G White Paper such as to address the emerging need for software licensing in the mobile industry and, in particular, as regards Open Source. In addition NGMN provides continuous contributions to international fora and groups regarding NGMN spectrum requirements, in order to ensure the allocation of sufficient spectrum for future 5G services.



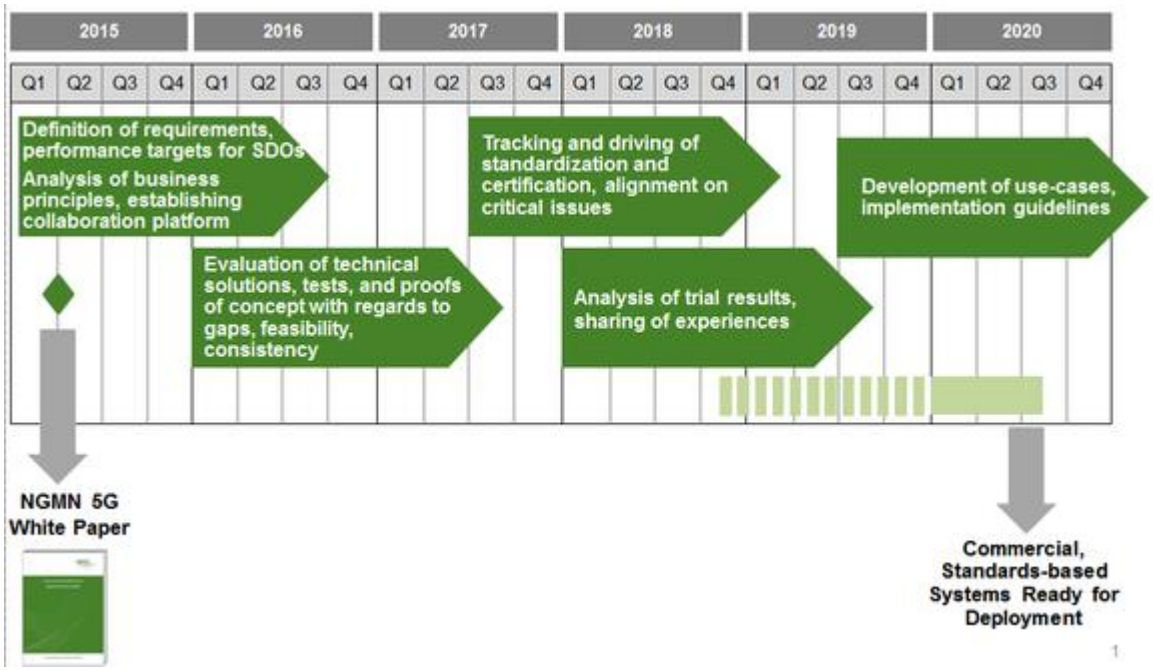
- Guidance to SDOs and the wider industry: the goal is to provide recommendation of technical requirements and performance targets as well as recommendation of enabling conditions. Currently NGMN is working on the development of a high level architectural framework with building blocks in order to guide a possible new 5G architecture. Major items considered are mobile access, fixed access, edge core, core NW, control plane, user plane, SGiLAN, slices, etc. Recently a 5G Security Competence Team has been created. It focuses on 5G security related topics raised by other NGMN gropus. The Team is currently working on security of network capability exposure in 5G and security aspetcs of V2X.



- Evaluation of test and proof of concept results: the focuses is to analyse initial, internationally proposed 5G technical solutions with regards to gaps, feasibility, consistency.



Over the last year several NGMN 5G White Papers have been released as essential information for industry stakeholders on the business, technology, and architecture aspects of 5G. Following it is reported the NGMN timeline.



5G-PPP

The 5G Infrastructure Public Private Partnership (5G PPP) is a joint initiative between the European Commission and European ICT industry (ICT manufacturers, telecommunications operators, service providers, SMEs and researcher Institutions). The 5G PPP is planned in three phases, encompassing research, optimisation (2016-2017) and large scale trials (2019-2020). It aims to deploy 5G as from 2020, which will require before 2020 to develop a series of ground-breaking technologies and global standards. On the 1st of July 2015, the projects from the 1st phase of the 5G PPP started. The 5G-PPP is now in its second phase where 21 new projects were launched in Brussels in June 2017.

Broadband Forum

Broadband Forum, a non-profit industry organization, is focused on engineering smarter and faster broadband networks. The Forum's new Broadband 20/20 vision is about unlocking the potential for new markets and profitable revenue growth by leveraging new technologies in the home, intelligent small business and multi-user infrastructure of the broadband network. The innovative use of NFV, SDN, Ultra-Fast access and IoT (Internet of Things) and, when formally defined, 5G, enables the delivery of exciting ultra-fast broadband services, with distributed computers and storage to anywhere and any device in the home and business locations.

One machine to machine (oneM2M)

oneM2M is the global standards initiative for Machine to Machine Communications and the Internet of Things. The purpose and goal is to develop technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with M2M application servers worldwide.

5G Automotive Association (5GAA)

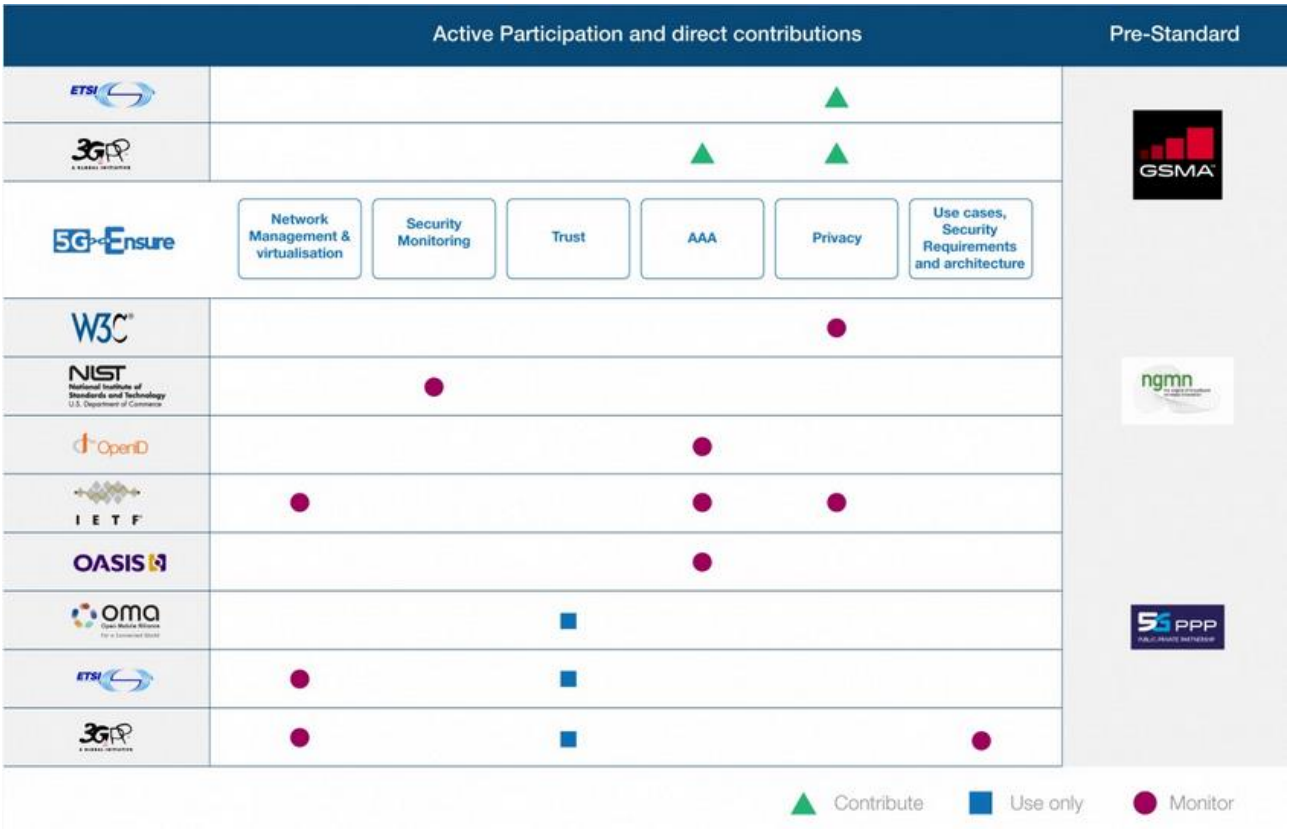
5G Automotive Association is a global cross-industry association that was formed in September 2016 to foster the development of connected and self-driving cars as well as intelligent transport systems. The association will develop, test and promote communications solutions, support standardization and accelerate commercial availability and global market penetration. 5GAA's activities are organised into five working groups:

- Use cases and technical requirements
- System architecture and solution development
- Business models and go-to-market strategies
- Evaluation testbeds and pilots
- Standards, policy, certification and regulation

The impact of 5G-ENSURE within the 5G standardization landscape

5G-ENSURE draws on the representation of consortium partners and its Advisory Board in relevant standards bodies.

Figure below indicated the standardization plan defined by 5G-ENSURE. It define the strategy adopted in terms of *primary SDOs to target*, based on the main results achieved by the project and *the timeline*, that is the opportunity to present and propone a contribution at the right SDO.



In the following table is reported the main impact achieved within the target SDO

SDO	Type of engagement	Impact
SA3-Security WG	Active contributions through submission of 47 contributions: • 47 related to 3GPP SA3 Study item on the Security Aspects of the Next Generation System (TR 33.899) and TS 33.501	• Supported the creation of a dedicates study item on the Security Aspects of the Next Generation System (TR 33.899) • The majority of the proposed requirements in the context of privacy aspects have been accepted and are now also part of the normative phase (TS 33.501 Rel 15) • 2 Privacy enablers have been included as possible solutions in the TR 33.899 and one of them has been selected for the normative phase (Rel 15) • 5G-ENSURE Security architecture has been presented

RAN	Active contributions through submission of 3 contributions related to security requirements proposal	• 3 proposed contributions. The proposals had been trsnferred to SA3 via liaison directly by RAN for comments and support
ETSI TC CYBER	Active collaboration through submission of 3 contributions.	• TR 103 304 “Personally Identifiable Information (PII). Protection in mobile and cloud services” has been extended to cover also the mobile scenario (i.e. “5G”) with the description of the use case related to the protection of the IMSI taken from 5G-ENSURE D2.3. • TS 103 458 “Application of Attribute-Based Encryption (ABE) for data protection on smart devices, cloud and mobile services” has been proposed and approved as a new WI with the goal to feed 5G-ENSURE project results into the mobile part by describing the use of ABE encryption and decryption mechanisms, the key distribution protocols and any related architectural aspect. • Promoted the liason with 3GPP SA3 (TCCYBER#8) to inform SA3 about the new activities and asking for support. • Sponsored the creation of a Specialist Task Force, the STF-529 “Attribute Based Encryption - Common protocol for data access control for Cloud, Mobile and IoT” that is a Specialist Task Force. It is used by ETSI to accelerate the standardization process in areas of strategic importance and in response to urgent market needs.
	Active partecipation	• Information sharing and collaboration about the various

5G-PPP Pre-Standard WG		dissemination activities of the group (e.g. whitepapers).
5G PPP The 5G Infrastructure Public Private Partnership **5G-PPP Security WG**	Active partecipation	• Contribution to the 5G-PPP Security landscape whitepaper about the standardisation landscape
GSMA	Partecipation to FSAG (Froud and Security) WG	• Privacy Enhanced Identity Protection Enabler, developed in 5G-ENSURE, has been presented during the GSMA FSAG#43 meeting on 6-7 December in Bonn. The solution has collected lot of interest and valuable feedbacks have been received. • The work on "WiFi-based IMSI Catcher" in part related to the activities conducted within the 5G-ENSURE project in the context of privacy issue in 5G network has been presented (26 September 16). Two issues have been reported resulting in the exposure of the IMSI on WiFi networks. • The Trust Model works has been presented to FSAG as part of the discussion the group started on the trust model for 5G aimed to provide an input doc for the SA3. This has opened future interactions with GSMA FSAG and 5G-ENSURE on the trust model aspects.
ITU	Exhange with ITU-T SG-17	• Analysis of the 5G standardization landscape submitted to ITU-T SG 17

Annex 4 – Analysis of the Second Open Consultation

In the following are reported the main findings based on the more relevant questions in the survey.

- **Where are we today with 5G security? What is the progress of 5G security work, 12 months on?**

In general all the sectors, industry, standardisation and 5G related organisations, reported the same perspective regarding the work done on 5G security indicating that a progress on different aspects of 5G Security has been achieved, even if the work cannot be considered complete. Part of the industry sector however consider that vertical requirements have not yet been covered and this maybe suggest that there are some vertical use cases which need more evaluation.

Most of 5G related organisations consider the proposition of security solutions as well as the work on the security architecture completed. This perspective can derive from the proposition of several innovative solutions as well as security architectures for 5G network coming from the research sector.

- **What areas still require lot of effort, since they raise serious security questions not yet solved?**

*There is a common agreement that lot of effort shall be put on **IoT security** and **Network slicing security**.*

IoT security is the area where most effort is required. Respondents reported that:

- Resource constraints in IoT environments are a major roadblock, but agreed concepts or frameworks have yet to emerge.
- Many IoT-based systems remain vulnerable: lack of necessary resources and legacy systems need to be addressed.
- Myriads of things, gateways, services can cooperate in creating new services. Distributed ownership and management.

Regarding *Network slicing security* the respondents reported that:

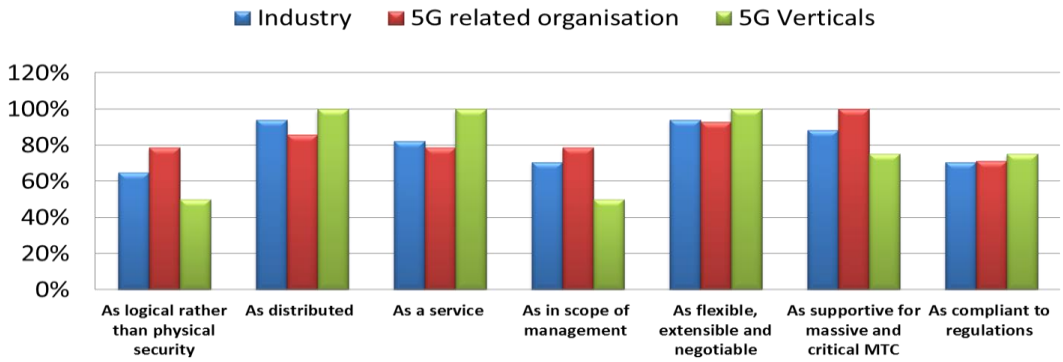
- Still unclear what network slice means and which security mechanisms should be applied.
- Not clear how security will be designed and implemented for slices crossing administrative domains.
- Lack of experience in actual deployments.
- This is key in encouraging enterprises to host applications in MNO core/edge data centres in dedicated slices.

Trust and Liability is another aspect that has been commonly indicated as one an aspect that has to be further investigated.

In addition, respondents indicated other areas for future work:

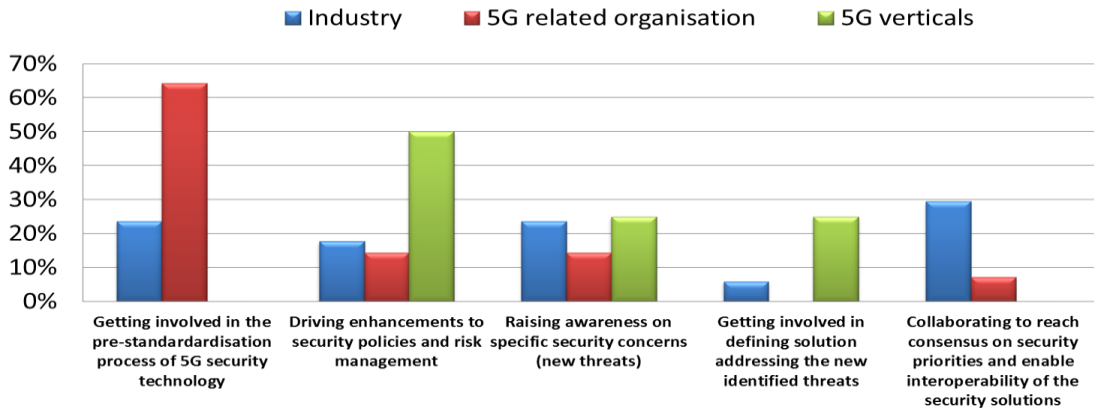
- Long term maintenance of security solutions is unsolved. Current equipment and devices have a rather short expected life time compared to the equipment and machines in the vertical sectors. Today software vendors do not care to maintain secure software in their devices 5-10 years after its initial deployment.
- Cyber-physical resiliency of telecommunication systems viewed as a critical infrastructure.
- Physical security of multi-access edge data centres (before MNOs carried data and now they're storing and enabling the analysis of it).

➢ **Do you agree on 5G-PPP security vision of 5G security architecture?**



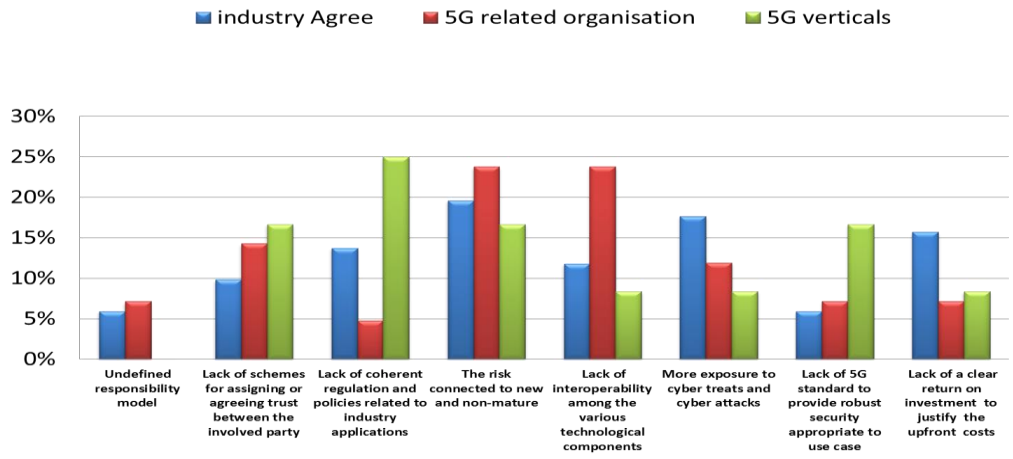
The figure below captures the perspective of Industry and verticals on the principles on which the design of 5G security architecture should be based on. These principals come from the work done by 5G PPP Security WG [https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf]. To build a viable security architecture for 5G, several design principles for such an architecture have been identified and discussed. The answers show that there is a general acceptance of these principles also by Industry and verticals.

➢ **How is 5G PPP (and others 5G related organisations) influencing 5G system security design?**



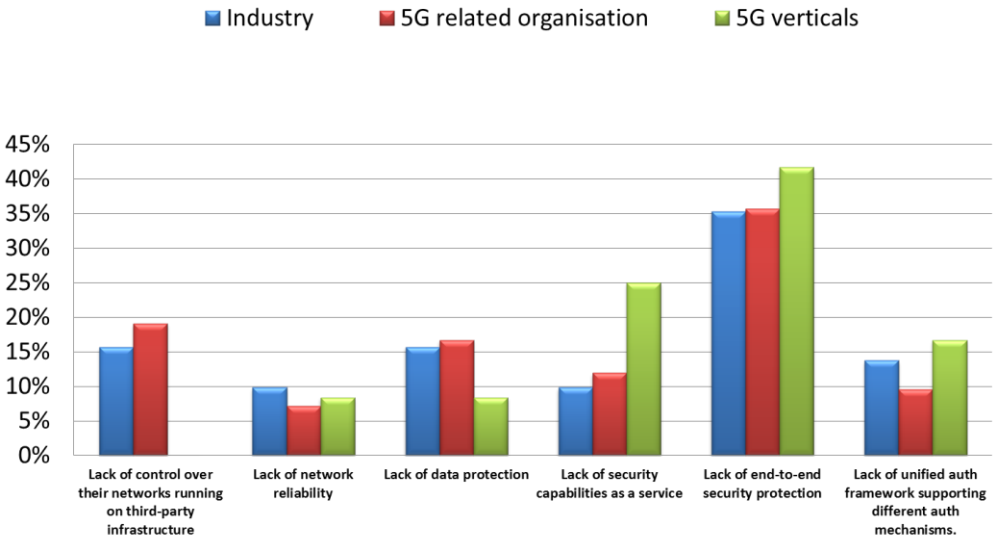
A well-defined common vision between the different sectors on the role of the 5G PPP (and other 5G related organisations) has influenced 5G system security design does not emerge. According to the Vertical perspective, the 5G PPP has mainly contributed to driving enhancements to security policies and risk management providing solutions to address the threats identified. From the Industry point of view, while there is not a strong position, the main contribution recognised to the 5G PPP is related to its attempt to reach consensus on key security aspects. 5G related organisations attributed to the 5GPPP the role of influencing 5G standardisation work by anticipating security issues and providing advice and research results.

- **From a vertical industry perspective what do you think are at "5G system level" the greatest security barriers for 5G adoption?**



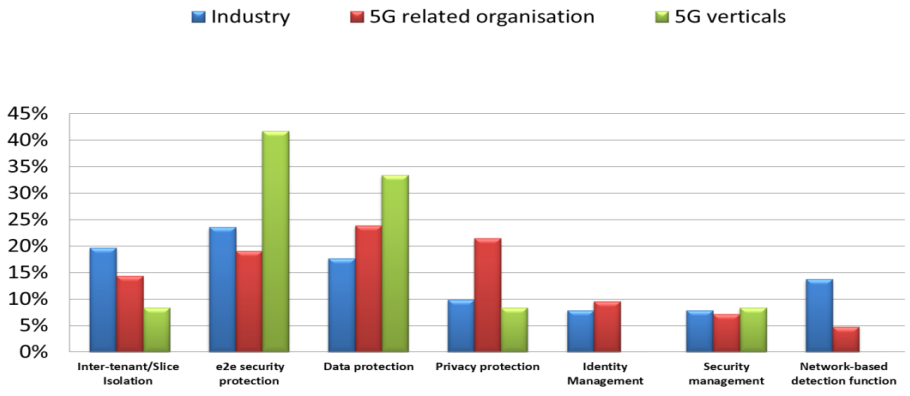
The risks associated with the adoption of new technologies influence or in some way rappresents a delay for 5G adoption. This is what results from the Industry respondents and it is also agreed by the verticals and 5G related organisations. Connected to it, there is also the increased exposure to cyber threats. Based on Verticals view the main barrier is the lack of coherent regulations and policies for industry applications. With software defined networking as part of 5G and network slicing concept, different needs in terms of services and quality of service can be provided simultaneously serving specific industry verticals. As a consequence, for a successful deployment of 5G, verticals suggest the need for mutual understanding of regulations, in terms of purpose and content. This includes potential impact on data protection and privacy, and liabilities aspects crossing traditional boundaries require attention from regulator.

- **From a vertical industry perspective what do you think are at "5G network level" the greatest security barriers for 5G adoption?**

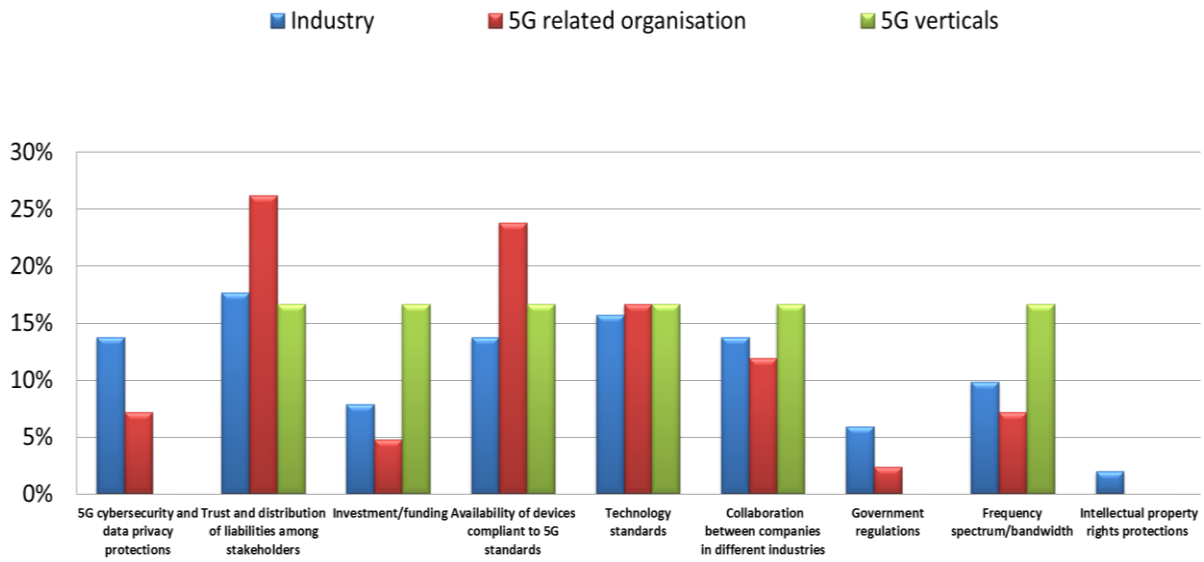


On the network side, there is a common agreement between all the sectors on the need to have an end-to end security. This is correlated on the availability of security capabilities at the network level to be opened up and provided as a "Service". This view results in particular from the vertical respondents and is supported also by the others answers, verticals have provided, showing that performing authentication, ensuring privacy protection and confidentiality and integrity of service traffic, for vertical industries are functionalities where support by the network is required, in the case they can't built it on their own. This is confirmed by the next figure where it was asked to indicate the security functions 5G industry and verticals can benefit to have supported by the network.

- **From an industry perspective, which of these security functions would be beneficial to place in the "5G network**

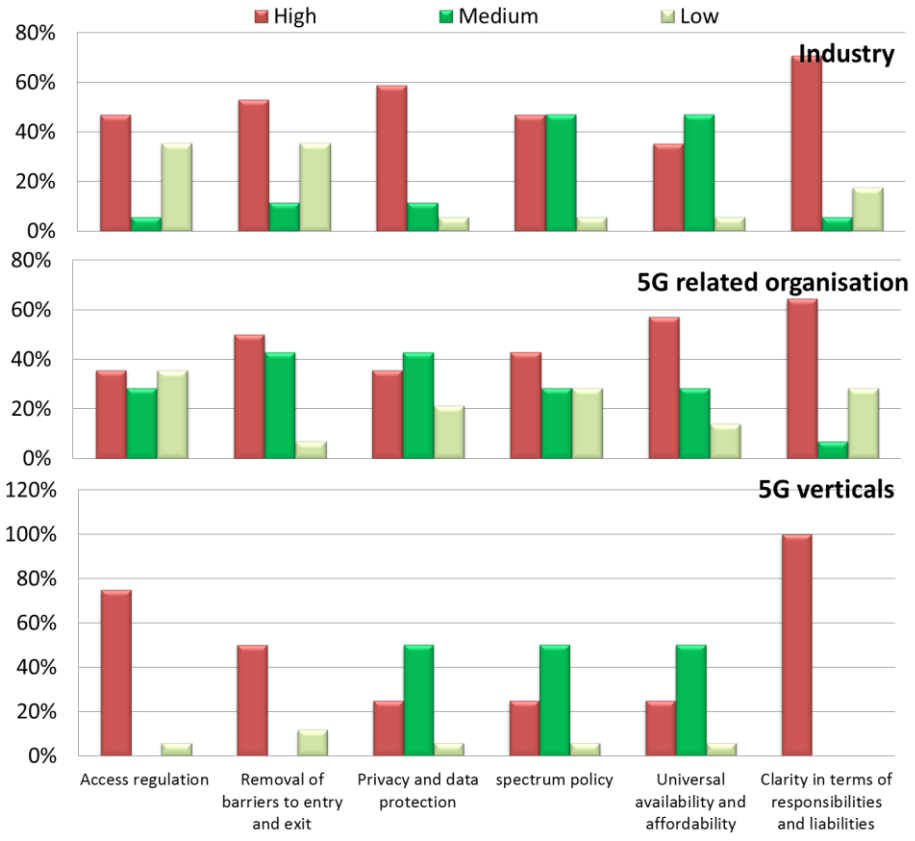


- **Where more progress is needed to ensure widespread adoption of 5G? Please select at maximum 3 choices**



Trust and liability model between the different stakeholders is the first stone towards the widespread adoption of 5G and particularly regarding the delivery of vertical services. This is confermed also in figure, where one of the main priority for regulatory body resulted by the survey is the proposition of new responsibility schemes in terms of distribution and allocation of responsibilities and obligations in particular to address breach of Trust/ security between parties. Others factors which influence 5G roll out are the availability of technology standards and conseguently products compliant with these specifications.

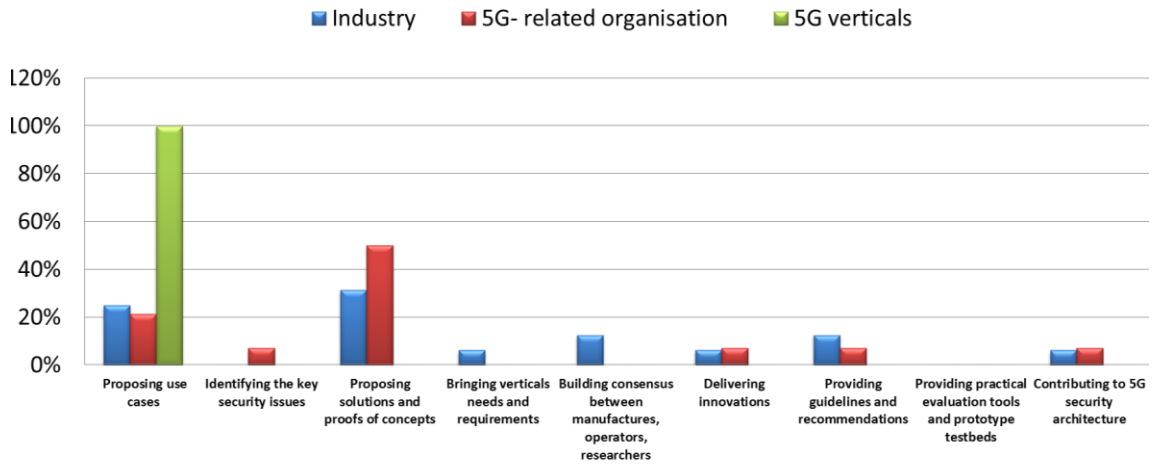
- **In which areas should regulation and regulatory policy focus with the highest priority?**



A common agreement on the most priority for regulator is on the need to have *more clarity in terms of responsibilities and liabilities* followed by the *"access regulation"*. Mandated access regulation exists in one

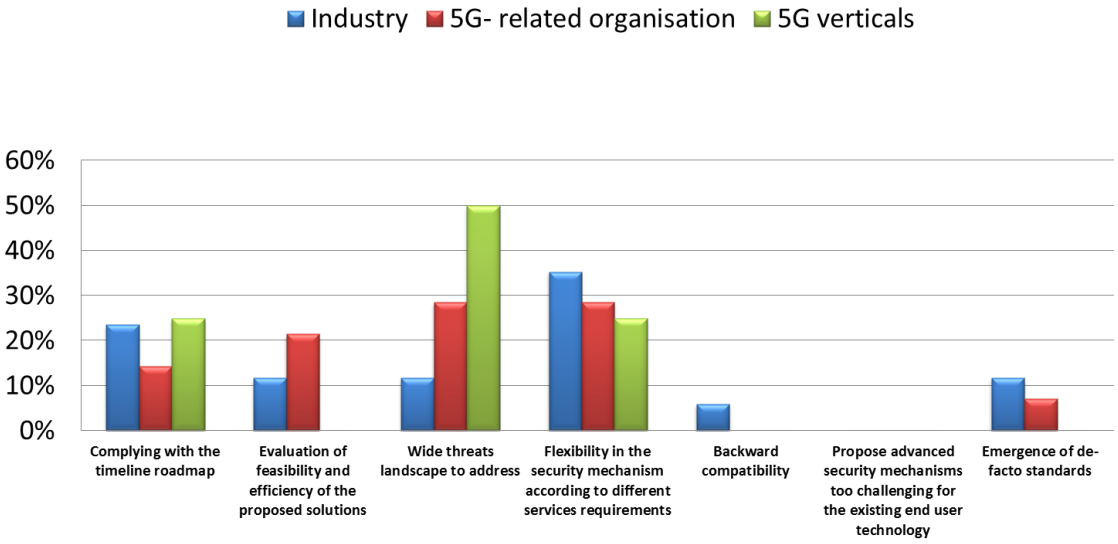
form or another throughout the digital ecosystem. The broadest and most extensive requirements apply to carriers, which are required to interconnect with other carriers in most countries. In many cases the infrastructure is leased to competitors, generally under regulatory price control regimes. These kinds of mandates are also present in other digital ecosystem markets. In the context of 5G regulators should seek to create and apply a consistent standard across the entire ecosystem so that the same criteria could be applied when evaluating the benefits and costs of open access mandates, regardless of sector or technology.

- **How have funded projects contributed to 5G pre-standardisation work?**



Most respondents from vertical sector have indicated that the main contribution to 5G pre-standardisation work is related to the proposition of use cases related to vertical needs. From the industry point of view, as well as the 5G related organisation funded projects have also contributed in defining innovative solutions supported by proofs of concepts.

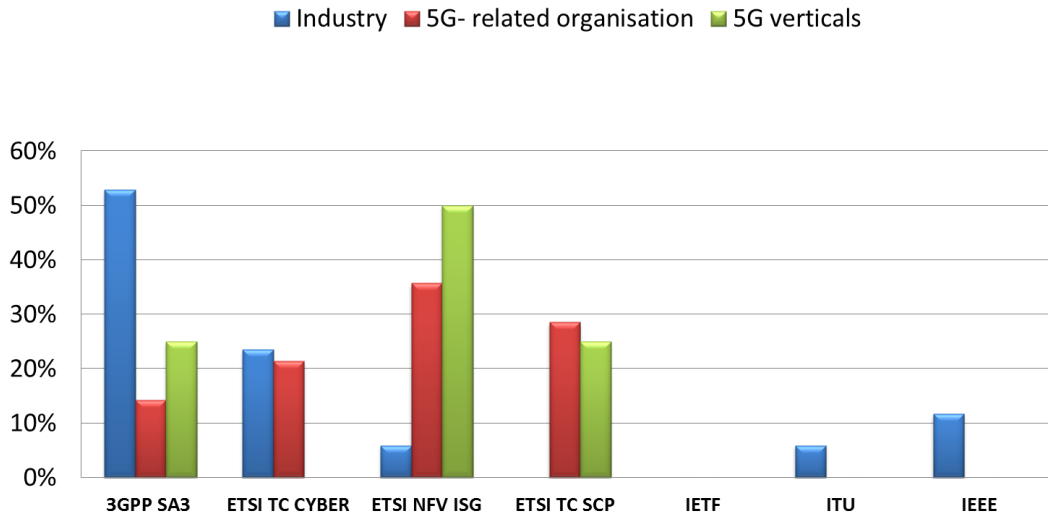
- **What are the main difficulties security standardisation work is encountering, if any?**



5G Security standardisation was reported as one of a critical factor for 5G adoption to ensure products aligned and conformant to the specifications and to a common security baseline. The main difficulties on defining the security of 5G network are mainly related to the different usage scenarios which imply different security requirements and conseguently more flexibility in terms of security functionalities supported.

- **Please select the key Standardisation Development Organizations for 5G security**

  3GPP SA3 is confirmed to be the main standardisation body for 5G security followed by ETSI for what concern virtualisation aspects (NFV securtity) and cyber security (TC Cyber).



- **Please highlight here the way forward for security in 5G network.**

The most useful findings are related to suggestions on the way forward for security in 5G network. Here are reported based on the respective sector.

INDUSTRY
• Elaboration of Proof-of-Concept platforms • Consider distributed multi-owned system at both physical and logical level • More collaborative research and innovation projects with real-world use cases • Focus on establishment of a chain of trust from the device endpoint to the SP cloud through the radio, multi-access edge and core using a combination of hop-by-hop security and end-to-end security. The security MUST not be one-size fits all but adapted to the value of the data being exchanged and the automated decisions being based upon that data. • Do not fall in the usual design error of making security come after the rest of the technology, once everything is decided • Complete the standardisation work • High priority of security and push towards standardisation. For many of the questions above, e.g. Q7 it would be interesting to assign a value to each one and seek consensus on which ones are priorities. Regulations that work for, not against, EU industry (supply and demand sides) is important. • Implement POCs of security mechanisms, use case field trials • Learn from past experiences, not re-invent the wheel but also avoid disagreement on key security issues

5G Verticals
• Network slicing security • Drive forward innovations with high socio-economic impacts as in the eHealth sector • Encourage government backing of large-scale pilots in key verticals to test security, privacy, trust, usability. • Addressing IoT security. Important also to see impact of new regulations on security practices and possibly adapt better to cyber threats and privacy issues in the context of 5G

5G Related organisations
• Putting more efforts to identify clearly the use cases and scenarios in short and long term, providing a higher investment on R&D programmes to make pre-evaluation feasible and allowing end users to get into the loop of 5G technologies. • Better capture requirements by the vertical industries • Slice specific security • The way forward for security in 5G networks must address the following 3 essential aspects • Reliable authentication and authorisation • Flexible isolation policy - to prevent or control the damage from the (inevitable) compromises of end devices • Control over data streams - data generated by end-users (personal or otherwise) represents a valuable resource, the importance of which is stating be to realized. It is therefore important that 5G networks also incorporate this point of view. • Addressing the above three aspects is necessary (but not sufficient!) to enable *trust* in 5G networks, which in turn is essential for their adoption. • The threats for 5G need to be clearly defined and end-to-end isolation should be implemented. • Taking an evolutionary path forward from the existing standards to encompass IoT and dense and diverse deployments. The security failures of the existing systems need to be fixed or discarded if not suitable for 5G requirements. It's important to utilise building blocks based upon for existing standards for security protocols and algorithms, although there will also be some need to develop a limited number of new building blocks - which should be carefully justified. Trust of the system will be built through robust design, modelling, development and testing of the systems. • Promote rigorous specification of trust assumptions for specific networks especially serving industry verticals. • High priority of security and push towards standardisation. For many of the questions above, e.g. Q7 it would be interesting to assign a value to each one and seek consensus on which ones are priorities. Regulations that work for, not against, EU industry (supply and demand sides) is important. • Promote rigorous specification of trust assumptions for specific networks especially serving industry verticals.

Annex 5 – Social Media Statistics and Press Clippings

April 2017

Number of tweets	*29 – accounting for EU holiday break*
Number of profile visits	*405*
Tweet Impressions	*18,900*
New followers	*14*
Top follower	*DBmaestro (DevOps), 9,754 followers*
Mentions	*7*
March 2017	
Number of tweets	*42*
Number of profile visits	*584*
Tweet Impressions	*31,600*
New followers	*38*
Top follower	*Roger James Hamilton, Founder of Entrepreneurs Institute, 1.09M followers*
Mentions	*16*
Febraury 2017	
Number of tweets	*56*
Number of profile visits	*584*
Tweet Impressions	*38,100*
New followers	*31*
Top follower	*Jim Harris, author of Disruptive Innovation, 221,000 followers*
Mentions	*15*
January 2017	
Number of tweets	*50*
Number of profile visits	*801*
Tweet Impressions	*31,500*
New followers	*34*
Top follower	*Simon Porter, leaing influencer for cloud, big data and IoT, 133K followers*
Mentions	*11*
December 2016	
Number of tweets	*25 – accounting for EU holiday break*
Number of profile visits	*552*

Tweet Impressions	*17,800*
New followers	*32*
Mentions	*10*
November 2016	
Number of tweets	*63*
Number of profile visits	*773*
Tweet Impressions	*31,600*
New followers	*28*
Mentions	*30*
November 2015	
Number of tweets	35
Number of profile visits	659
Tweet Impressions	11,400
New followers	25
Top follower	TechTank: 16,200
Mentions	25
December 2015	
Number of tweets	38
Number of profile visits	402
Tweet Impressions	11,300
New followers	27
Top follower	Dave Waterson: 17.8K
Mentions	15
January 2016	
Number of tweets	46
Number of profile visits	343
Tweet Impressions	15,500
New followers	13
Top follower	N/A
Mentions	15
February 2016	

Number of tweets	77 (specific focus on Mobile World Congress)
Number of profile visits	427
Tweet Impressions	22,900
New followers	25
Top follower	Commissioner Oettinger: 36,800
Mentions	11
March 2016	
Number of tweets	58
Number of profile visits	471
Tweet Impressions	28,500
New followers	22
Top follower	Philip Solis, ABI (5G and wireless connectivity): 2727
Mentions	7
April 2016 (26-04-2016)	
Number of tweets	70
Number of profile visits	467
Tweet Impressions	26,200
New followers	18
Top follower	GeoThings, @GeoThings, 12,100 followers
Mentions	11

Press clippings:

Major research findings on the research conducted by the University of Oxford were presented and demonstrated by Piers O'Hanlon and Ravishankar Borgaonk at the Black Hat Europe security conference in early November 2016: WiFi-based IMSI Catcher, leading to considerable press coverage. Visibility will help to flag privacy issues at the highest levels and ensure they are swiftly addressed.

The Register: Build your own IMSI slurping, phone stalking stingray-lite box, using bog-standard Wi-Fi, http://www.theregister.co.uk/2016/11/03/wifi_imsi_catcher/.

Network World: The great smartphone security scare: Your mobile can be hijacked and tracked without you knowing!, http://www.networkworld.com/article/3138468/security/mobile-subscriber-identity-numbers-can-be-exposed-over-wi-fi.html.

PC World: Mobile subscriber identity numbers can be exposed over Wi-Fi, http://www.pcworld.com/article/3138472/security/mobile-subscriber-identity-numbers-can-be-exposed-over-wi-fi.html.

SC Magazine: Black Hat EU: researchers remind that IMSI catchers still a threat, http://www.scmagazineuk.com/blackhat-eu-researchers-remind-that-imsi-catchers-still-a-threat/article/570453/.

International Business Times: The great smartphone security scare: Your mobile can be hijacked and tracked without you knowing!, http://www.ibtimes.co.uk/great-smartphone-security-scare-your-mobile-can-be-hijacked-tracked-without-you-knowing-1589716.

Best Security Search: Cell phones can be traced via Wi-Fi, http://bestsecuritysearch.com/cell-phones-can-easily-traced-via-wifi/.

The Intercept: Hackers and law enforcement could hijack Wi-Fi connections to track cellphones, ttps://theintercept.com/2016/11/07/hackers-and-law-enforcement-could-hijack-wifi-connections-to-track-cellphones/.

The Hacker News: Wi-Fi can be turned into IMSI Catcher to track cell phone users everywhere, http://thehackernews.com/2016/11/imsi-track-cellphone.html

Bitshacker: Wi-Fi can be turned into IMSI Catcher to track cell phone users, http://bitshacker.com/2016/11/04/wi-fi-can-turn-imsi-catcher-track-cell-phone-users/

Naked Security: Who needs a stingray when Wi-Fi can do the job?, https://nakedsecurity.sophos.com/2016/11/08/who-needs-a-stingray-when-wi-fi-can-do-the-job/

01 Net.com (French): Comment le Wi-Fi des opérateurs mobiles permet de pister les abonnés, http://www.01net.com/actualites/comment-le-wi-fi-des-operateurs-mobiles-permet-de-pister-les-abonnes-1055430.html.

Computer World (Hungarian): Ellophatók a mobil előfizetők azonosítói wifin keresztül, http://computerworld.hu/computerworld/ellophatok-a-mobil-elofizetok-azonositoi-wifin-keresztul.html.

Version (Danish): Mobilbrugeres ID-nummer kan opfanges fra almindeligt wifiudstyr, https://www.version2.dk/artikel/forskere-forvandler-almindeligt-wifi-prisvenlig-imsi-catcher-1020909.

Intelligence Online: Fake Wi-Fi hotspot replaces IMSI catcher, https://www.intelligenceonline.com/corporate-intelligence_terabytes/2016/11/09/fake-wi-fi-hotspot-replaces-imsi-catcher,108188976-ART.

TechWorm: Cell Phone Users can be tracked easily using just WiFi and here's how, http://www.techworm.net/2016/11/cell-phone-users-can-tracked-easily-using-just-wifi-heres.html.

XaKep: WiFi IMSI-Catcher, https://xakep.ru/2016/11/04/wi-fi-imsi-catcher/.

SecNews: Πώς μπορείτε να εντοπίσετε εύκολα χρήστες κινητών μέσω WiFi (Greek), https://secnews.gr/150196/%CF%80%CF%8E%CF%82-%CE%BC%CF%80%CE%BF%CF%81%CE%B5%CE%AF%CF%84%CE%B5-%CE%B5%CE%BD%CF%84%CE%BF%CF%80%CE%AF%CF%83%CE%B5%CF%84%CE%B5-wifi/.

The Tech News: Learn Tracking Cell Phones Using WiFi Connection, http://thetechnews.com/2016/11/12/learn-tracking-cell-phones-using-wi-fi-connection/.

Univers Free Box: Deux chercheurs dénoncent le Wi-Fi opérateur qui piste les abonnés (French), http://www.universfreebox.com/article/37017/Deux-chercheurs-denoncent-le-Wi-Fi-operateur-qui-piste-les-abonnes.

Autobild: Si usas WIFI publico, ten cuidado con esto, http://www.autobild.es/noticias/si-usas-wifi-publico-ten-cuidado-con-esto-304613.