Deliverable D5.3
Second 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	31-10-2016	
Dissemination Level:	Public	
Lead beneficiary	Trust-IT	Stephanie Parker, s.parker@trust-itservices.com
Authors	Trust-IT: Stephanie Parker, Roberto Cascella and Silvana Muscella TIIT: Luciana Costa and Paolo de Lutiis SICS: Rosario Giustolisi OXFORD: Piers O'Hanlon LMF: Kazi Ullah, Mohit Sethi, and Bengt Sahlin EAB: Göran Selander	

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 second report covers the results achieved for communication, marketing and standardisation as core activities within WP5 in the period May to October 2016 and provides a plan for the next six months. The report measures impact based on a core set of KPIs for communication and marketing and dissemination of results, with qualitative metrics for activities related to 5G security standardisation.

In terms of standardisation, the deliverable reports on the main findings of the open consultation on 5G security and the outcomes of the 1st International Workshop on 5G Security Standardisation, including results from stakeholder engagement and promotional activities. It also provides an analysis of the dissemination of project results through publications, technical conferences and across professional networks.

An update is provided on the joint activities within the 5G PPP, where 5G-ENSURE is now also supporting stakeholder engagement across different channels and at events to share advances and increase impact. A detailed analysis is given of the impact achieved through 5G-ENSURE community building, communications and engagement with primary and secondary stakeholders.

The last section of the deliverable covers current plans for the period November 2016 to April 2017, based on current opportunities. The overall aim is to increase stakeholder engagement and ensure the outputs of 5G-ENSURE for the benefit of 5G stakeholders in Europe and beyond, by building on the promising results to date.

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 challenges are very complex and global. Security, privacy, and resilience of data require a multi-stakeholder dialogue, with the right kind of collaboration.

Industry Panel, CeBIT 2016

Integrating security and privacy (trust) early on in the innovation process – this is key in an increasingly digital environment, by design rather than a mere afterthought.

20th Global Standards Collaboration meeting

5G will enable mobile networks to dramatically evolve from 3/4G with new concepts and technologies such as Massive Machine Type Communication (mMTC), infrastructure virtualisation (SDN, NFV), and network resource sharing, among others. 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. Standardisation is a key requirement for these new technologies, also in the face of growing cyber threats and the increasing need to defend national and European critical infrastructure through cyber security. 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 under the umbrella of the 5G Infrastructure Public Private Partnership (5G PPP) in the Horizon 2020 Programme. The project covers research and innovation - from technical solutions (5G security architecture and test bed with 5G security enablers) to market validation and stakeholders' engagement - spanning various application domains. To this end, 5G-ENSURE works collaboratively with the other projects funded in phase one of the 5G PPP.

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 CeBIT2016 [1].
- 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 D5.3 is to report on the results and impacts of actions performed during the period May to October 2016 and plans for the period November 2016 to April 2017. The report provides a revised stakeholder definition, updated engagement plans and 5G standardisation landscape, as well as joint activities at the programme level. D5.3 also reports on Key Performance Indicators (KPI) and qualitative metrics achieved within the reporting period. Several new KPIs targets have been set where the numbers have already been achieved. The results achieved form the basis for the activities in the next six months of the project, that is, November 2016 to April 2017.

Structure of this report

Section 2 - Communication Strategy - goals for communications and marketing, goals for standardisation, stakeholders and KPIs, reporting on results achieved in the first 12 months.

Section 3 - Updated analysis of the current standardisation landscape, relevant standards for 5G-ENSURE and how the project is contributing.

Section 4 - Impact of Actions Taken for 5G Security Standardisation and Dissemination of Results, including the open consultation, the 1st International Workshop on 5G Security Standardisation, and dissemination of results through publications, technical conferences and stakeholder engagement.

Section 5 - Impact of actions within the 5G PPP Joint Programme, including current contributions and outcomes of priority Work Groups for the project, and joint publications.

Section 6 - Impact for Community Building, Communications,and Stakeholder Engagement, showing how the community is growing and stakeholder engagement through social media.

Section 7 - Plans and Targets for next six months, building on current achievements.

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 [2]. 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 the communication and marketing plan are:

- Capture and promote the benefits of 5G-ENSURE and related technology and market insights.
- Advertise 5G-ENSURE focus on security requirements, mobilising 5G PPP peers in coming forward with their requirements.
- Promote opportunities for shared contributions to standardisation.
- Showcase best practices in security implementation within the 5G PPP (https://5g-ppp.eu/, @5GPPP) and internationally.
- Share 5G PPP achievements, events/webinars etc., and publications.
- Ensure visibility of the 5G-ENSURE community at relevant stakeholder events, including joint 5G PPP activities such as shared stands, workshops, roundtables and webinars.
- Promote the support of the European Commission to this strategic project.

2.2 Goals for Standardisation

Standardisation efforts in 5G-ENSURE aim to transfer knowledge to relevant standards groups and 5G PPP stakeholders with a particular focus on security and privacy. Activities also include engagement with the Advisory Board members, where knowledge exchange also feeds into the international conferences, the two 5G-ENSURE Workshops and liaison at global level.

Specific goals of the standardisation plan are to:

- Contribute to standardisation by providing the high-level security requirements to drive 5G specifications. This draws on work in WP2 in terms of security requirements and architecture that need to influence the future work of standardisation, with particular focus on:
    - Privacy and security issues identified through the use cases (D2.1, February 2016), 5G PPP initiatives and external sources.
    - Risk assessment, mitigation and requirements (D2.2 and D2.3, June 2016).
- Provide contributions on the 5G system definition, by proposing the integration of the innovative security solutions that will result from the project. This draws on the work in WP3 in terms of concrete solutions for 5G Security enablers, as well as WP4 in terms of the vision for the 5G Security test bed and operational plan.
- Interface with the 5G PPP for the submission of joint standards contributions.
- Leverage relevant ongoing work by the EIT Digital Action Line on Privacy, Security and Trust, and expertise on 5G spectrum within the global community.
- Engage in international exchanges on standardisation, for example with NIST in the US, 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.

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 and future iterations therefore (D5.3 and D5.5), indicating any interconnections across the four categories.

2.3 Primary and Secondary Stakeholder Targets

It is expected that 5G networks will be commercialised in 2020, replacing legacy network and services step by step. According to estimates by ETRI Industrial strategy research lab [3], the market size of the global 5G services will post a high grown rate with a CAGR of 92.7%, from €32bn ($36bnin 2020 to €1658bn ($1861bn in 2026).

The essence of the 5G vision and its major economic interest is not defined in terms of mere data volumes or geographical coverage. Eventually, anyone/anything, including e-businesses and enterprises will be connected over global 5G system(s) and entire industries will be able to replace proprietary communication solutions by much more low-cost COTS solutions. Similarly, society-critical sectors such as utilities, public transport, health, etc., will be able to re-use the 5G system for critical services.

The fastest uptake compared to previous mobile technologies is justified by the wider range of services offered and the opportunities in new industries and verticals [1]. Ensuring security remains a priority for the industrial sector exploiting new business opportunities on 5G network. Enterprises and operators are looking to dramatically reduce the number of physical security devices and both require assurance that virtual networks are as secure as physical ones.

2.3.1 Primary stakeholders for 5G-ENSURE

5G-ENSURE is evolving its primary stakeholders as the project progresses with the aim of encouraging uptake of outputs as part of the forthcoming engagement plans and to build consensus around standardisation efforts. Engagement plans for primary stakeholders have also evolved to take on board upcoming vertical industry involvement and use case requirements around security and privacy.

- **5G industry** within and beyond the 5G PPP, such as vendors/manufacturers, telecom operators and supply chain companies.
- **Standards bodies** and related international associations, regulators and policy makers targeted to ensure that 5G-ENSURE makes timely 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.

Table 1: 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, **twitter** 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.

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 1st 5G-ENSURE International Workshop on 5G Security Standardisation and the face-to-face session organised by the Security Work Group during EuCNC 2016.

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 [7], 5G-NORMA [8], COHERENT [9], FANTASTIC-5G [10], Flex5Gware [11], METIS-II [12], mmMAGIC [13], CHARISMA [14], SPEED-5G [15]

Network technology projects: 5G-Crosshaul [16], 5GEx [17], CogNet [18], SESAME [19], SELFNET [20], SONATA [21], Superfluidity [22], VirtuWind [23]

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, e.g. EuCNC or common exhibition spaces, e.g. Global 5G.

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 in D5.2):

- 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, Networld2020 ETP, related projects from EUREKA, and related national initiatives.

Joint publications, e.g. 5G PPP WG white papers.

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

2.3.2 Secondary stakeholders for 5G-ENSURE

5G-ENSURE secondary stakeholders are mostly channels that are used to reach primary stakeholders, that is, telecom, IT and business media channels. Engagement goals include:

- 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.

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.

2.4 Key Performance Indicators and Qualitative Metrics

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 QR2 (August – October 2016).

Table 2: KPIs for WP5 Core Activities

Communication & community	Standardisation	5G PPP Joint Activities		Dissemination of outputs		
5G-ENSURE - Community KPIs						
KPI	**Target End of Project (EoP)**	**Total to date**	**EoP Delta**	**QR3: May-July 2016**	**QR4: Aug-Oct 2016**	**Achieved QR1-2 (Reported in D5.2)**
Twitter followers	300*	318	**18**	169	148	*164*
Community DB for LinkedIn	800	565	235	142	213	*210*
PR/media content	4	3	1	1	0	*2*
Media coverage & visibility	15	13	2	2	2	*9*
Open Consultations on 5G security/Roadmap	110 (50 +60)	45	65	45	not applicable	*0*
Meetings/Events - standardisation/5G security (excl. project workshops)	6	4	2	1	1	*2*
Events - 5G-PPP Joint activities (incl. Project workshops)	8	4	4	2	0	*2*
Publications to disseminate technical results	12	8	4	3	1	*2*
Technical conferences	8	5	3	2	2	*1*
Publications: joint 5G-PPP	2	4	**2**	0	2	*2*
LinkedIn Connections	350	464	**114**	120	342	*2*
LinkedIn Updates	36	14	22	4	8	*2*
LinkedIn Updates counted on monthly basis, min. 2/month						

5G-ENSURE is on track to achieve the defined KPIs, and in some cases has surpassed the target set. 5G-ENSURE has therefore increased the following KPIs for the second year of the project:

- New KPI for Twitter followers: 500
- New KPI for LinkedIn connections: 600
- New KPI for future public consultations on 5G security and future roadmap: 60 respondents or more, given the growth of the community, including new 5G security/standardisation experts recruited.

KPIs for social media (twitter) and professional channels (LinkedIn) are checked on a monthly basis so plans can be made for web and social media activities, using detailed statistics on community interests and

trends coming from a free online tool, as well as an updated database with detailed profiling of primary and secondary stakeholder groupings.

WP5 will also measure outcomes related to the web platform, which is currently under a SEO review to optimise content tagging, as well as the production and circulation promotional material (e.g. posters, videos, bookmarks, fliers etc.), project newsletters and presentations.

WP5 will also implement 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.* To date, 5G-ENSURE has received visibility from telecom media and has established close links with several journalists. Channels like TelecomTV, the Mobile Network and Inside5G are considered valid also to promote the contributions on 5G security standardisation. From a community perspective, 5G-ENSURE has mostly targeted 5G stakeholders from industry and academia (including the 5G PPP and international initiatives). The current LinkedIn community is analysed in section 6.1 and twitter impact in section 6.2, with a good coverage of the targeted stakeholders and geographical spread, upon which to build in year 2 of the project. A similar analysis is being made for the community, including twitter followers & LinkedIn connections.

QM2*: Readership of journals where technical articles are published, such as reputation, readership and geographies.* Preliminary results have been already published in perr-reviewed journals, conferences and workshops. The focus was on attacks and threat scenarios. During the first year 8 publications have been already submitted and accepted, which is a good base for the second period of the project, where the security enablers can be further promoted.

QM3*: Workshops – Matching actual participants with the stakeholder targets.* The 1st International Workshop on 5G Security Standardisation and the 1st open consultation targeted people familiar with the security and privacy challenges in 5G. The 2nd Workshop and the 2nd public consultation will target a wider group of stakeholders, also to get consensus on the 2 iterations of the Standardisation Roadmap.

QM4*: Workshops – gauging consensus of participants and the level of interest, e.g. passive and active supporters; passive and active opponents; fence-sitters.* A good level of consensus on the value of the work being done within 5G-ENSURE was achieved during the 1st International Workshop, as demonstrated also in the testimonials published as videos on the project website. The 5G PPP Security WG chaired by the project has received valuable contributions for the enablers and the security architecture. Valuable feedback was also received for the open consultation questionnaire.

QM5*: External events, assessing the audiences actually reached at commercial and technical events, influential participants, new contacts and main takeaways.* 5G-ENSURE has been visible not only at external events but also within the 5G PPP with positive feedback on its work, testified also by the publications and technical conferences. 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.* This QM will be implemented from January 2017, as defined in the Future Plan.

3 Current Standardisation Landscape

3.1 5G-ENSURE Focus

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.

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.

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.

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 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 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.

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 3 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 3: 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	Study on Security Aspects of the Next Generation System (TR 33.899)

		NOKIA	
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

In the long term it will be evaluated the opportunity to contribute also in other SDOs based on the representation of consortium partners.

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.

3.2 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.

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.

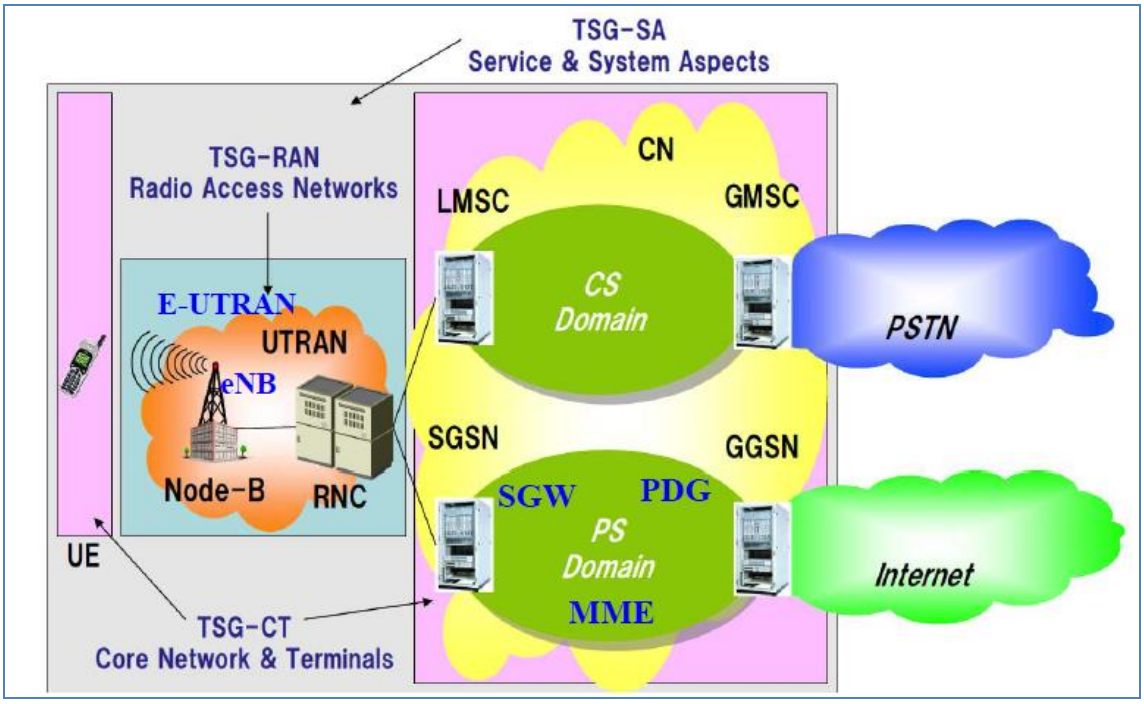


Figure 1: Scope of the TSG

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.

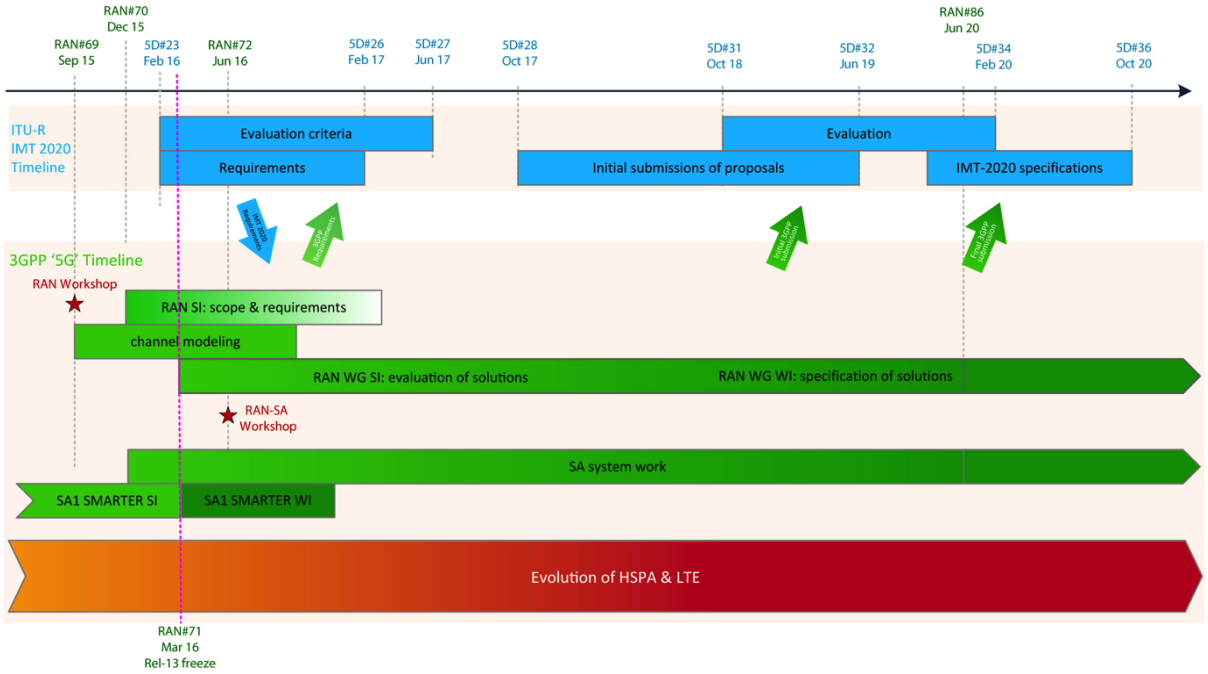


Figure 2: Initial 3GPP 5G Timeline

3.2.1 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 will be based on:

1. Channel modelling for bands above 6 GHz. A new study item (SI) on “channel modelling for spectrum above 6 GHz” has been approved in September 2015 and its results should be available by the RAN#72 meeting (June 2016). According to this SI:
    - In the first part of the SI, RAN will identify status and expectations on high frequencies (e.g. spectrum allocation, scenarios of interest, measurements, etc).
    - Then RAN1 WG will develop a channel model(s) for frequencies up to 100 GHz (from Q1 2016).
2. Scenarios and requirements for next generation radio technology. RAN has approved the SI in December 2015 (TR 38.913). According to this SI:
    - 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.

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.

3.2.2 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. 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. 3GPP SA1 is now starting to consolidate 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. A draft version of this specification is expected to be available in December 2016; an approved version is planned for March 2017. Of course each Phase of SMARTER needs to be compatible and consistent with the previous Phase.

Other Working Groups can use these four SMARTER Technical Reports 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].

3.2.3 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. Many progress have been achieved, and the release date for the document is now December 2016

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, the deadline of the document has been postponed to December 2016.

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. A joint workshop between RAN and SA (or the relevant WGs) is foreseen in H2 2016.

3.2.4 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.

A single TR is proposed to capture the output of this study. The complete or partial conclusions of this study will form the basis for the normative work and/or for any further study. It is expected that the normative part will start in early 2017. For sush 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.

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.

The rapporteur of this SI is Vesa Torvinen from Ericsson.

3.2.5 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 recent 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, 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. To be noted that the deadline of the TR 23.799 has been postponed in order to "wait" the results of the TR33.899. Such an aspect confirm that SA2 and SA3 will work aligned and the project effort can be focused on the SA3 works. It is expected (but not yet decided at the time of writing) that the specification works will start in 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
- Finally SA3, the 3GPP security group, with its SI on the Security Aspects of the Next Generation System (TR 33.899) is actually the main target for 5G-ENSURE. All the main results of the project foreseen for 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 elaboration of the TR33.899 (finalization expected during SA3#86 in 2017, the meeting will be held in Sophia Antipolis), and the future specification works expected during 2017 (although at the present time there is not a specific plan, it is expected that a new Work Item will be started during SA3#86).

The following GANTT chart illustrates the main 3GPP action plan for 5G and the relevant results of 5G-ENSURE foreseen for this year and the beginning of the 2017 .

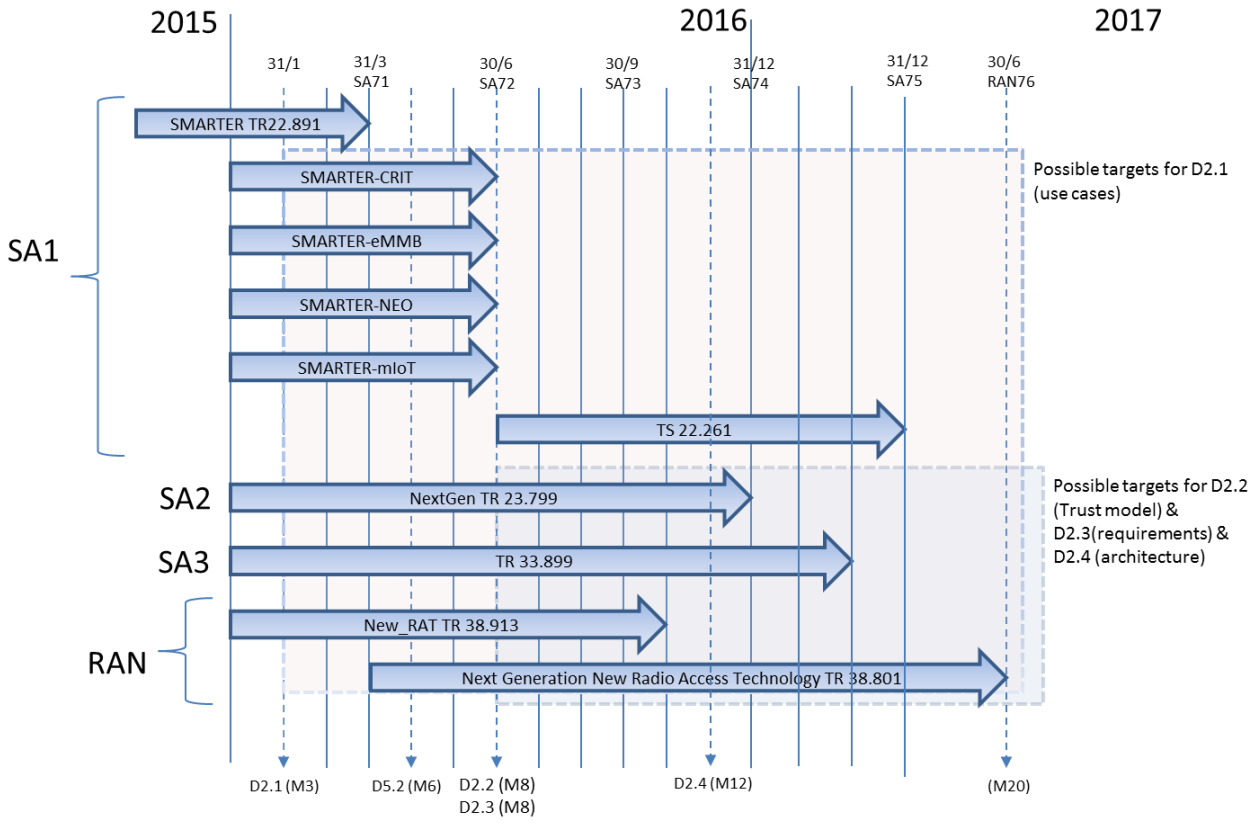


Figure 3: 3GPP GANTT 1 - Updated

3.3 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.

3.3.1 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 ToR modifications will occur at CYBER#9 in February 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 new schedule is to have a TB approval for September 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 postponed to 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 postponed to 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.

3.3.2 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 Figure 4.

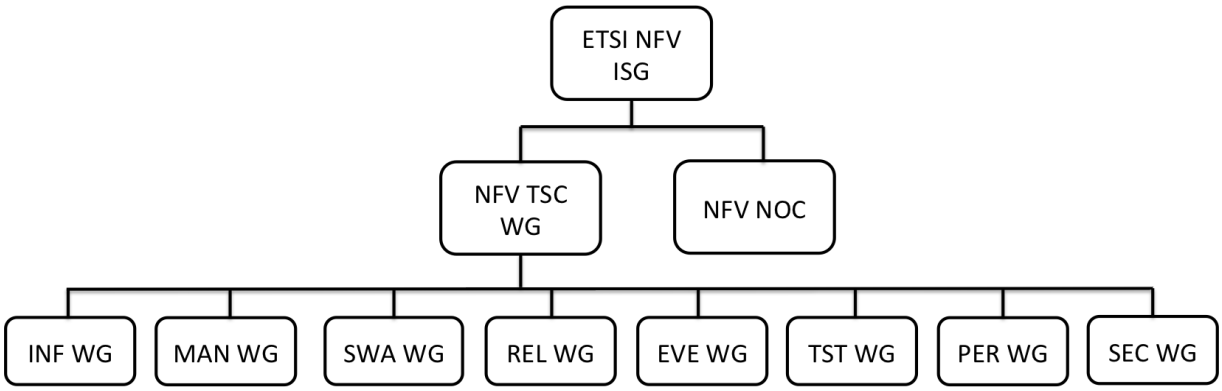


Figure 4: ETSI ISG NFV operational structure

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

3.3.3 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.

3.3.4 Threat Landscape

Figure 5 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.

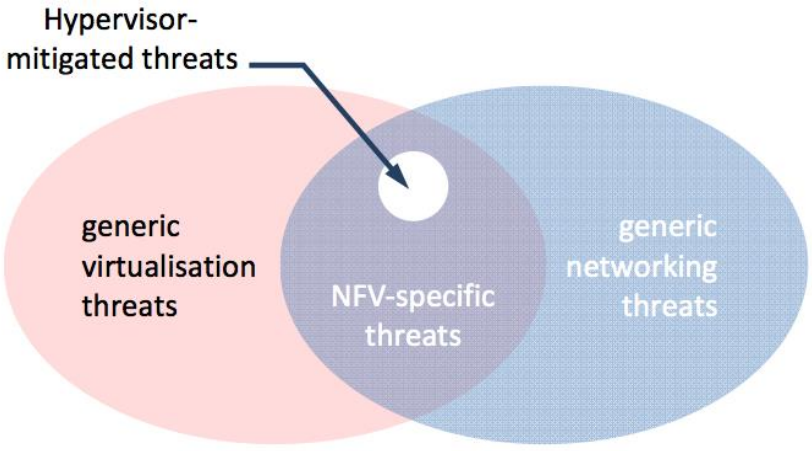


Figure 5: Visualisation of the NFV threat surface [source: ETSI GS NFV-SEC 001]

3.3.5 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.

3.3.6 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 009: Report on use cases and technical approaches for multi-layer host administration.

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 006: Security & Regulation report.
- ETSI GS NFV-SEC 007: NFV Attestation report.
- ETSI GS NFV-SEC 010: Retained Data Report.
- ETSI GS NFV-SEC 011: Lawful Interception Architecture Report.
- ETSI GS NFV-SEC 012: Architecture for sensitive components – Specification.
- ETSI GS NFV-SEC 013: Security management & monitoring specification.
- ETSI GS NFV-SEC 014: MANO Security Specification.

3.3.7 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 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 report, 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, and finally by sponsoring the approval of the new Technical Specification TS103.458 during CYBER#7 (June 2016). 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 deliverable (to be noted that the dealine of the Work Item is 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).

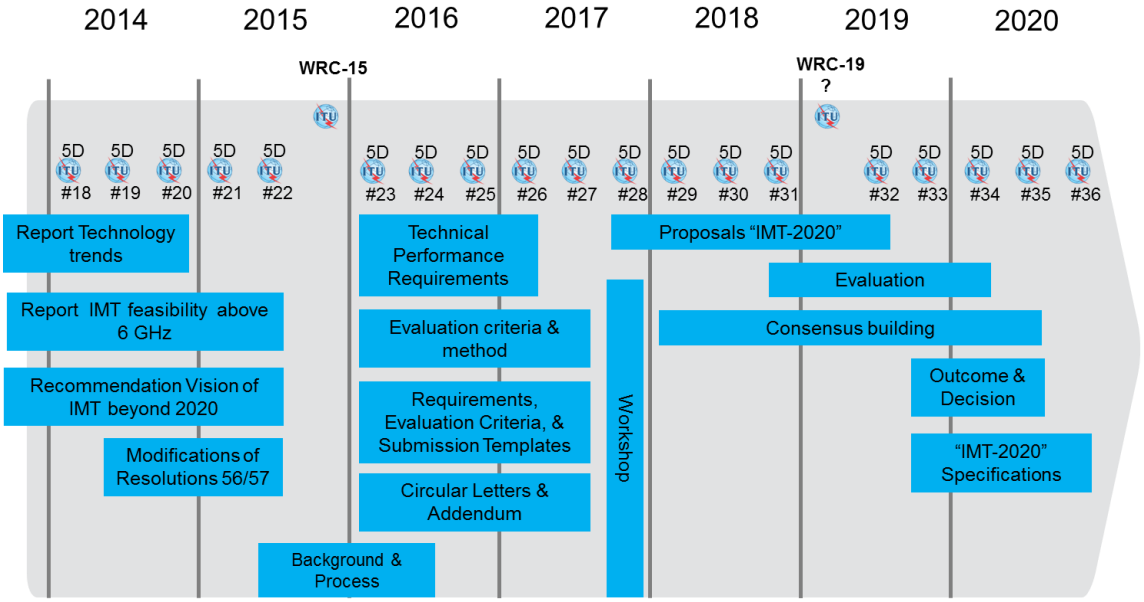


Figure 6: 5G Time Line for ITU [Source: 3GPP RP-150483]

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. New Terms of Reference call 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 include:

- 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 is not particularly interested in security aspects, and that has also been confirmed during the lates 5G-ENSURE Workshop in Sophia Antipolis. 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

The next, and final deliverable, it is expected to be published at the end of 2016.

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), it is not considered one of the main target for the 5G-ENSURE project.

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. During the next months the collaboration will continue by specific discussion and information sharing about a possible gap-analysis of such a map. For example it is expected that additional NIST standard will be identified by the NIST people as relevant for the project enablers and vice-versa.

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.

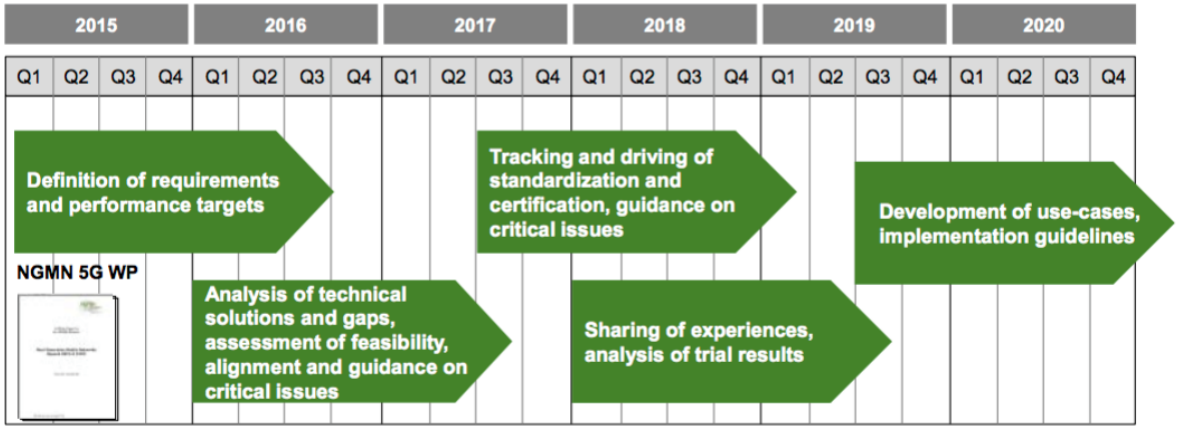


Figure 7: NGMN Role in 5G Development

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 8: 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..

3.10.1 5G-ENSURE opportunities in NGMN

The NGMN P1 WS1 5G Security group has now concluded its work. Its deliverables have been sent to 3GPP SA3 and SA2, in which most of the 5G-ENSURE project partners participate. Thus, the insights from the deliverables could be leveraged by 5G-ENSURE in developing 5G security enablers.

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. This WG rappresents an opportunity for 5G-ENSURE as the project that has identified Privacy as a key enabler for 5G network. The plan is to present in the next face to face meeting the solution that has been defined within the project for the protection of the user long term identifier (IMSI) during its transmission over the air interface when a pseudonym is not yet available.

4 Impact of Actions Taken for 5G Security Standardisation and Dissemination of Results

4.1 Public Consultation on 5G

In order to drive consensus on security, privacy and trust in future 5G networks, 5G-ENSURE has produced and promoted an open consultation as a detailed online questionnaire. Feedback and inputs were provided by the 5G-ENSURE consortium and from the members of **5G PPP Work Group on Security**. The open consultation ran from 20 March to 27 May 2016, targeting primary stakeholders and also cloud security experts. Specific actions carried out include:

- Online questionnaire created and published on the 5G-ENSURE website with option for respondents to leave contact details (Drupal module).
- Downloadable spreadsheet providing all the responses for analysis (Drupal module).
- Dedicated twitter and web banners were also graphically designed to increase visibility of the open consultation.
- A bookmark promoting the open consultation and 1st International Workshop on 5G Security Standardisation was produced for distribution at events.
- Promotion of the public consultation took place through the 5G PPP COMMS mailing list, a twitter campaign, direct messaging and events, such as:
    - Networld 2020 (presentation, bookmark distribution), 19 April 2016 in Brussels.
    - The ETSI 5G Summit (poster presentation, bookmark distribution), 21 April 2016 in Sophia Antipolis.
    - Net Futures 2016 (face-to-face interactions, bookmark distribution), 20-21 April 2016 in Brussels.
    - ETSI From Research to Standardisation (face-to-face interactions, bookmark distribution), 10-11 May 2016 in Sophia Antipolis.
- Results of the open consultation were presented at the 5G-ENSURE 1st International Workshop on 5G Security Standardisation, published on line and shared with primary stakeholders: http://www.5gensure.eu/sites/default/files/Costa_5G-ENSURE-Results_Open_Consultation_5G_Security.pdf
- Specific outcomes of the promotional campaign are reported below. All respondents with a LinkedIn account are members of the 5G-ENSURE community.

Web link: http://www.5gensure.eu/open-consultation-survey

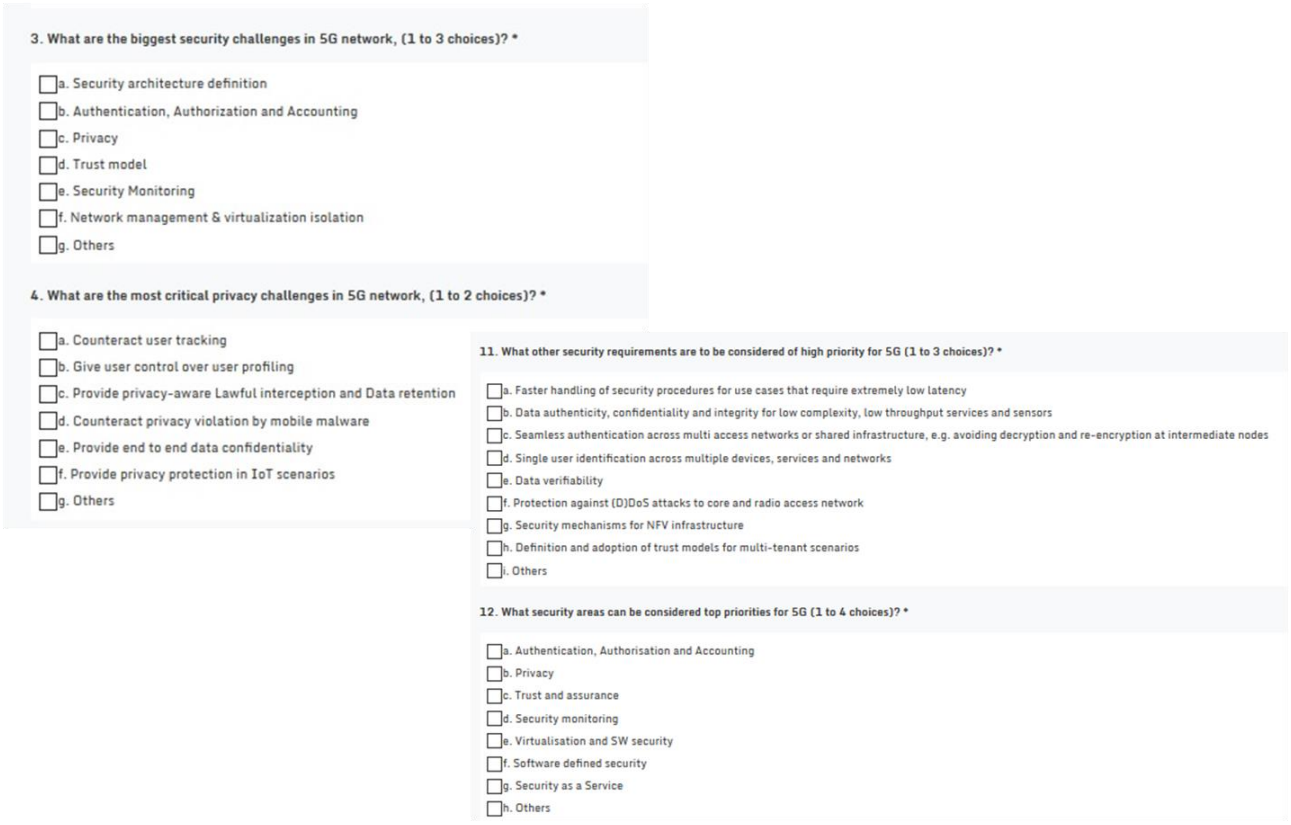


Figure 9: Sample of Open Consultation Questionnaire

4.1.1 Approach

The open consultation was designed as part of the project's efforts to collect and analyse the expert views of primary stakeholders within the 5G PPP and more broadly from specialists and potential 5G stakeholders with regard to 5G security topics. Specifically, the consultation sought inputs on:

- Security and privacy challenges.
- Security and privacy priorities.
- Security impacts emerging from the adoption of technological advances in 5G.
- Opportunities and risks foreseen in the security domain.
- Key actions towards security standardisation.

The findings of the open consultation provide a valuable source of information to ascertain whether security aspects in 5G are being addressed in line with 5G stakeholder expectations and whether further research improvements are required.

4.1.2 Respondents

45 responses were received compared with the target 50, with several members of 5G PPP Security WG providing inputs before publication online. The KPI can be considered a reasonable target for a first consultation though higher targets have been set for future consultations as 5G-ENSURE can now count on a larger community base, which is growing organically.

The figure below shows the breakdown of the respondents to the open consultation, where the 5G PPP and 5G industry represent the largest portion of respondents as primary stakeholders of 5G-ENSURE.

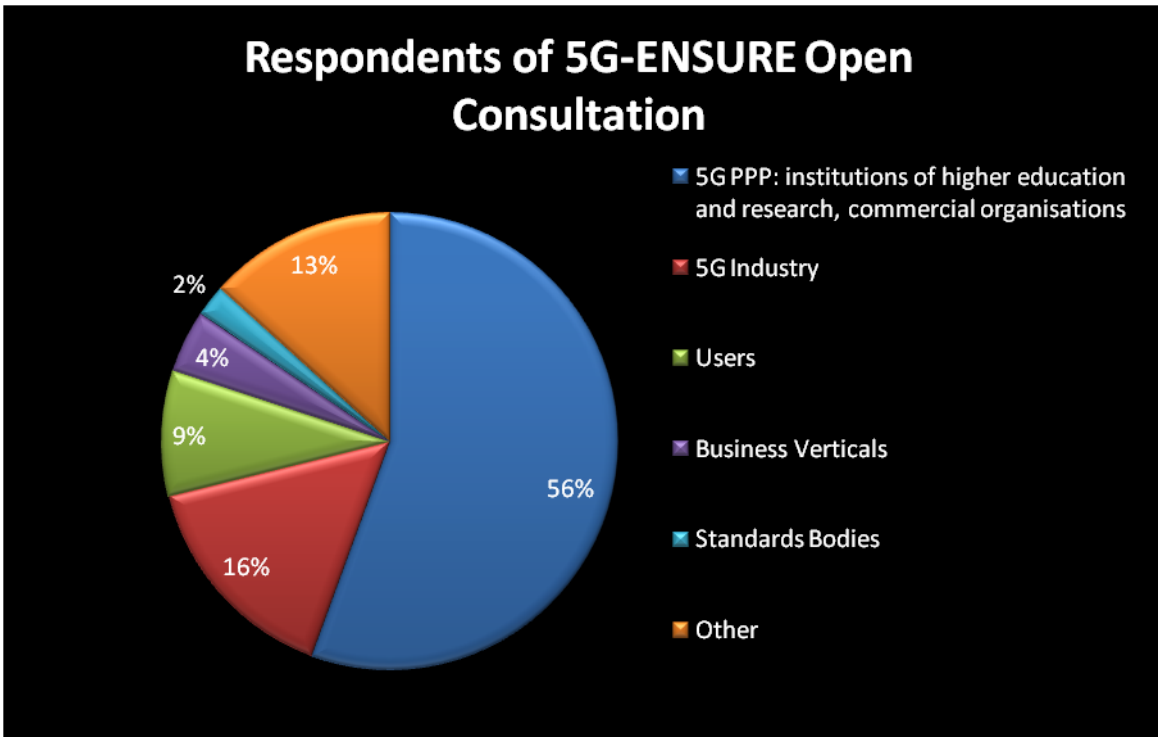


Figure 10: Respondent Breakdown of the 5G-ENSURE Open Consultation

4.1.3 Main Findings

The results of the open consultation were combined into a single set of findings in order to draw global conclusions on 5G security topics, thus providing a valuable understanding of the views on opportunities and challenges related to 5G security and possible ways to address them. The open consultation findings are also the basis for revising the 5G-ENSURE standardisation plan.

5G Security

What are the biggest security challenges in 5G networks?

Respondents agreed on **6 major security challenges** (with no significant differences in responses). In order of importance, the biggest security challenges are: **network management and virtualisation isolation** (20.88%); defining the **security architecture** (20%); **privacy** (19.13%); **trust model** (15.65%); **AAA** (14.78%) with **security monitoring** being of less importance (9.56%).

Should 5G security be built on previous networks and, if yes, what can be reused?

66.6% of respondents agree that 5G security should build on previous networks, such as 4G, re-using the following (in order of importance):

- Authentication and key agreement AKA mechanism (16.07%).
- Crypto algorithms (13.78%).
- Device confidentiality and user identity (temporary identities) (13.01%).
- Network security architecture, e.g. RAN access (9.18%).
- Confidentiality and integrity protection for signalling (6.98%).

What are the new security aspects with a high priority for 5G?

- Security mechanisms for NFV infrastructure (18.89%).
- Data authenticity, confidentiality and integrity for low complexity, low throughput services and servers (16.53%).
- Seamless authentication across multi-access networks or shared infrastructure (16.53%).
- Faster handling of security procedures for use cases that require extremely low latency (13.38%).

Others include the protection against (D)DOS attacks to core and radio access networks, definition and adoption of trust models for multi-tenant scenarios and data verifiability.

5G Privacy

What are the biggest privacy challenges?

- End-to-end data confidentiality (24.73%).
- User control over user profiling (22.58%).
- Privacy protection in IoT scenarios (20.43%).

Other privacy challenges include counteracting privacy violation by mobile malware, counteracting user tracking and privacy-aware lawful inception and data retention.

What are the most important privacy requirements from a user perspective?

- Supporting user awareness about how and where user data is handled (28.91%).
- Visibility of security/privacy features enabled, e.g. use of strong/weak algorithms; protection of user identity (24.09%).
- Ability to decide whether to use a 5G service or not depending on the security/privacy features available on the network (20.48%).

Should privacy and anonymity techniques also provide built-in data recovery capabilities for government agencies in charge of law enforcement and/or national security?

The majority of respondents (62%) agree that such techniques should be used. Privacy should be independent from law enforcement agencies to avoid backdoors. Several respondents indicated that lawful interception/back doors make for less secure deployments, as anyone can take advantage of them and there is no way to guarantee who uses a back door once it is installed.

LI as a network service: lawful interception needs to be explicity specified, with rights management and provided as a network service. However, this is a delicate issue that needs to carefully consider which functions interoperate with LI.

5G Trust

What makes trust complex in future networks?

- Support of new business models with new actors and relationships (30.17%).
- Adoption of virtualisation technology, e.g. 3rd-party NVFs running inside a 5G network (25.86%).
- Support of new devices, e.g. sensor nodes (18.97%).

Other aspects include massive adoption, and the lack of a definition and adoption of a common trust model.

What are the key actions required to build trust in 5G networks?

- Using trusted execution technologies to support the adoption of virtualisation technology e.g. third party VFNs running inside a 5G network (30.10%).
- Making trust is more objective (measurable and evidence-based) (26.21%).
- Ensuring trusted and authorised interconnection (23.30%).

In this respect, some respondents highlighted the need for a new trust model.

5G virtualisation and multi-tenant environments

What key issues emerge from the adoption of virtualisation?

- Lack of logical and physical isolation between distinct virtual network functions (21.37%).
- Integrity of a virtualisation platform (20.58%).
- Issues related to interoperability with legacy systems (3G, 4G) (18.80%).
- Lack of authentication between virtual functions (17.09%).

Another relevant issue is the potential impact of vulnerabilities that can affect the segregation of virtual instances.

What are the most relevant security risks associated with a multi-tenant environment?

- Respondents consider the most important risk to be data confidentiality and integrity due to the lack of isolation (38.89%).

Of equal importance (19.44%):

- Performance and availability risks based on the activities of other tenants on the same infrastructure and platform.
- Side channel attacks due to the lack of authorisation mechanisms for sharing physical resources.
- Uncoordinated change controls and misconfigurations, i.e. one tenant gaining access to the data and resources of another tenant.

The current trust model poses an important security risk because it requires complete trust in the cloud provider.

What key actions are needed to ensure security in 5G virtualisation and multi-tenant scenarios?

- Relying on properly implemented isolation at the virtualisation layer (25.45%).
- Implementing monitoring mechanisms to control the allocation of virtual network functions to physical computing resources (21.81%).
- Providing a capability to verfy the integrity and confidentiality of images of virtual network function implementations, at start-up as well as run-time (20%).
- Implementing access control mechanisms to limit the reachability/visibility of the NFV components (17.27%).
- Implementing mechanisms to ensure traffic-type segregation, e.g. between data, control and management planes (13.63%).

5G Certification

Should security in 5G networks undergo a certification process?

74% of the respondents believe that security certification is needed, with 36% saying it should be used to verify the support and correct implementation of security functions.

How can security assurance be provided in a 5G network?

- Using trusted computing techniques, i.e. root-of-trust, attestation, secure storage (42.22%).
- Creating security assurance standards to be applied, recognised and accepted (31.11%).
- Requiring security certification (13.33%).

Which security aspects should 5G standardisation focus on?

- Virtualisation security (21.09%).
- Privacy and security architecture (21.31%).
- Trust model (14.84%).
- User privacy (13.28%).

4.1.4 Sample of promotional campaign outcomes

The open consultation was widely shared across social media and through Euro 5G as the 5G PPP umbrella project. Direct personalised messages were also sent to over 80 5G stakeholders from industry and academia as part of the campaign.

The consultation was published on the 5G PPP website.

Figure 11: Promotion of the open consultation on 5G PPP website

The figure below shows examples of engagement on twitter in terms of impressions, engagement and engagement rates between 17 and 25 May 2016.

Figure 12: Engagement on Public Consultation via Twitter

5GEnsure @5GEnsure · May 20 You have exactly 1 week to complete our public consultation on #5G security ow.ly/4njqa1 Thanks! twitter.com/Ox_CyberSec/st… View Tweet activity	565	2	0.4%
5GEnsure @5GEnsure · May 17 Our public consultation on #5G security is open until 27.05, ow.ly/4njqa1 @enisa_eu @usnistgov View Tweet activity	807	12	1.5%
5GEnsure @5GEnsure · May 25 Just 2 days left to contribute to our public consultation on #5G security ow.ly/4njqa1 @ETSI_STANDARDS pic.twitter.com/OXVdKa4ilu View Tweet activity	1,456	11	0.8%

The figure below shows a sample of who helped promote the public consultation on twitter, spanning EC units and representatives, standards bodies, partners, the 5G PPP and the telecom media.

Figure 13: Social Media Support of the Open Consultation

4.2 Outcomes of the 1st International Workshop on 5G Security Standardisation

The EG-ENSURE 1st International Workshop on 5G Security Standardisation took place on 16 June 2016 at Orange Labs in Sophia Antipolis during ETSI Security Week. The overriding objective of the workshop was to stimulate efforts on 5G security as a key driver towards the future 5G-connected digital society, pushing for a "Security by Design" approach and ensuring security becomes an integral component of the 5G architecture design.

Specific goals of the workshop were:

- Present the current outputs of 5G-ENSURE and key findings of its open consultation on 5G security.
- Share technical insights and perspectives on 5G security, privacy and trust.
- Deliberate 5G security standardisation efforts and the contributions of 5G-ENSURE.
- Encourage coordinated work on 5G security within the 5G PPP and through international synergies.

WEB LINKS

Main workshop page: http://www.5gensure.eu/1st-international-workshop-5g-security-standardisation

Agenda with presentations: http://www.5gensure.eu/agenda-1st-international-workshop-5g-security-standardisation

Speakers and Chairs: http://www.5gensure.eu/speakers-and-panellists-1st-5g-ensure-international-workshop-5g-security-standardisation

Executive Summary (Post-event report): http://www.5gensure.eu/sites/default/files/5G-ENSURE_1st_Workshop_on_Security-post_event_report-16062016.pdf

4.2.1 Workshop Participants

Around 30 international stakeholders attended the workshop, representing a total of six European countries. The largest group came from France (30%), followed by Italy (20%), Germany (13%), UK (10%), Belgium and Finland (7%) and Greece (3%).

Participants attending the workshop were mostly primary stakeholders for 5G-ENSURE, that is, 5G industry, including representatives from the 5G PPP, followed by EU and national organisations on the same level as institutions of higher education and research. Other important groups include SMEs and standardisation organisations. The figure below shows participant breakdown in terms of organisation type.

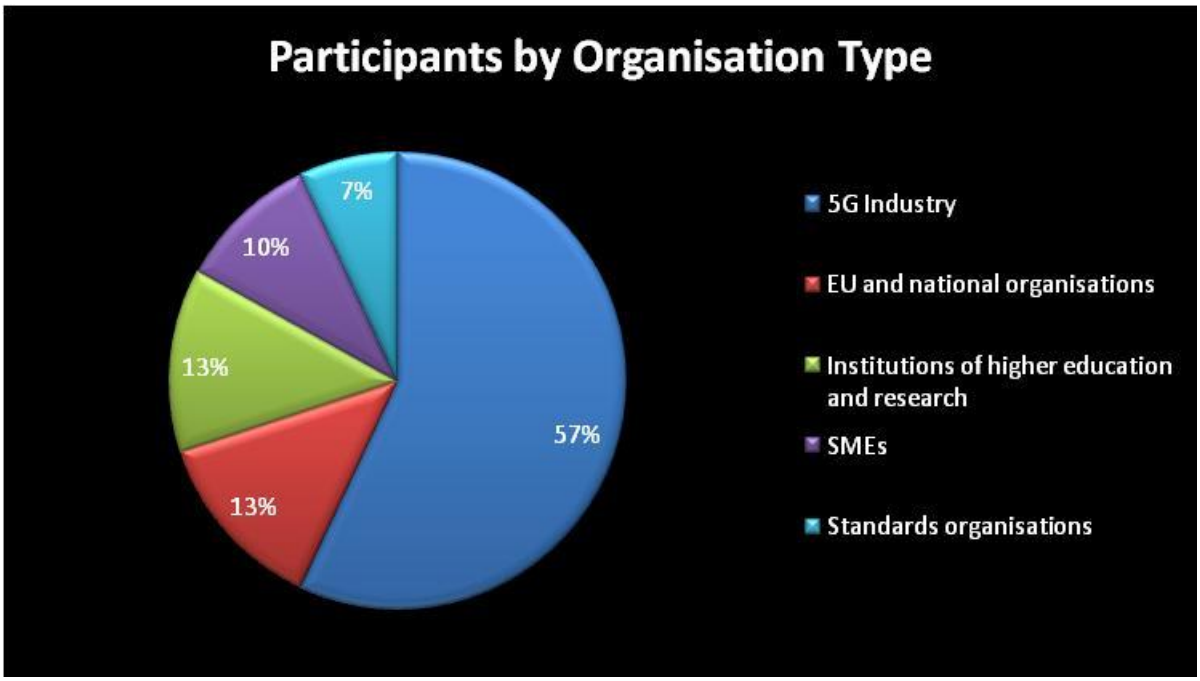


Figure 14: Participant breakdown by organisation type

4.2.2 Executive Summary on Workshop Take-aways

The workshop proved to be an effective forum for discussing and sharing technical insights into 5G security emerging from preliminary 5G-ENSURE findings. The workshop also offered an opportunity to exchange European perspectives on security work and related standardisation actions within the project. The discussions have helped in charting a course for coordinated work on 5G security with the involvement of 5G PPP projects, standards groups, international initiatives and the 5G PPP Work Group on Security.

The main outcomes of the workshop are captured in the **5G-ENSURE Executive Summary**, which has been widely promoted through social media channels, through the 5G PPP COMMS and on the website of the 5G PPP. The Executive Summary has also been shared with the Members of the 5G-ENSURE Advisory Board and the Co-Chair of the IEEE 5G Initiative, among others.

OPENING KEYNOTE

5G Standardisation and Security: Supporting the DSM Objectives, Pavlos Fournogerakis, Programme Officer, EU Policies, Network Technologies, DG CONNECT, EC.

- Common standards will ensure interoperability, guarantee that technologies work smoothly and reliably, provide economies of scale, foster research and innovation, and keep markets open.
- Europe must play a leading role in the drive towards 5G standardisation, helping to avoid a fragmented 5G by smoothly co-operating with all regions of the world through joint collaboration agreements.
- The EC Communication for Digital Single Market on ICT priorities for standardisation (April 2016) demonstrates importance of active participation of all national players, standards groups, and key stakeholders in defining 5G standardisation from the very outset.

- Business verticals drive the 5G vision by introducing new and complex requirements, for example, in terms of softwarisation of the core network, as well as security, which is transversal to many verticals.
- 5G-ENSURE is the first 5G PPP project that deals with the horizontal area of security. It will thus provide inputs to other 5G projects in defining the 5G security architecture and in contributing to the standardisation process.

SESSION 1: 5G ENABLERS FOR NETWORK AND SYSTEM SECURITY AND RESILIENCE

5G-ENSURE project presentations

- In early 2017, 5G-ENSURE will have the results from its test bed, contributing to its global position and pushing for standardisation.
    - Mapping security enablers at network or protocol level for an enhanced version of the 3GPP-ETSI security architecture.
- Greater co-operation on security aspects is fundamental for building consensus within the global ecosystem. To deal with the complexity of 5G, we need to design a research road map and build a security landscape at the EU level. Key concerns around network softwarisation include trust and liability.
- Contribution to ETSI TC CYBER on access control enforcement mechanisms and policy rules for PII protection on smart devices, cloud and mobile services. **An extension on specific 5G privacy needs has been proposed**.
- Open consultation: privacy in 5G should provide end-to-end data confidentiality and enable user control. Security certification is required for security assurance in 5G networks. Security in multi-tenant virtualisation scenarios requires isolation and monitoring mechanisms to avoid abuse.

SESSION 2: 5G THREATS AND CHALLENGES

ENISA Thematic Threat Landscape SDN & 5G, Adrian Belmonte, ENISA.

- 5G is an opportunity to introduce a security/privacy-by-design approach. Preparedness against current and new cyber threats is fundamental.
- 5G is an important driver for IoT, smart cities and in enabling seamless communication between different layers.
- SDN/NFV have a key role to play in improving 5G security. ENISA is to set up a new expert with a focus on security aspects of virtualisation. ENISA work on IoT could also be relevant for 5G.

EIT Digital – Towards More Security and Privacy in Digital World, presented by Luciana Costa (TIM IT) on behalf of Jovan Golic, TIM IT & EIT Digital

- Action line on Security, Privacy and Trust pushes for security- and privacy-by-design.
- It is important to make privacy and security a business opportunities despite all the challenges.
- Homomorphic encryption could be a viable opportunity to protect data while not revealing keys to untrusted parties.

SESSION 3: STANDARDS PANEL

The session provided a focus on some of the hot security topics, on the on-going study items and work required with a focus on the standardisation effort in 5G, with insights and views coming from Zarrar Yousaf (NEC Laboratories Europe) actively involved in ETSI NFV standardisation activities, Alf Zugenmaier vice-chairmain of 3GPP SA3, Luca Pesando vice-Chair of the IMT2020 FG of ITU-T SG 13 and chair of the WG on Mandate 493 in ETSI NTECH, and Hugo Tullberg chair of the 5G PPP Work Group Pre-standardisation[1].

- 5G-ENSURE is a timely project for 5G security but it is important to move swiftly and push security aspects in standardisation. We need a minimal security baseline based on consistent technology and procedures, guaranteeing security from both an end-user standpoint and the provider's side.
- Security is not just a technical issue but also a business opportunity and an opportunity to educate on social risk management.
- ETSI ISG NFV is investigating new NFV management and orchestration (MANO) framework expected to impact on other working groups such as Interfaces and Architecture (IFA), Security and Reliability. It is key to analyse threats to security in virtualised environments and derive services and security requirements.
- DevOps can help telecom operators reduce time-to-market but might also be a source of more threats. Key areas include defining appropriate measures for operational efficiency and features supporting regulatory requirements such as lawful interception, privacy and data protection. A close monitoring of de-facto standards for virtualisation (e.g. OpenStack, Dockers) is important because of reduced time to market.
- On-going work within the 3GPP SA3 illustrates the importance of taking action now on standardisation. The 5G standardisation process is now underway so the potential impact on new security requirements is still an open book. 5G-ENSURE can also make a contribution to authentication and subscriber privacy. Co-operation is key to delivering co-sourced contributions also around LI mechanisms.
- The 5G PPP Work Group on Pre-Standardisation also sees co-operation as the way forward in reaching common agreements and in providing co-signed contributions to relevant standards groups.
- Regulation plays a very important role.

4.2.3 Video Testimonials

Three video interviews were recorded during the 1st International Workshop and made available on the project website and on YouTube:

- Pavlos Fournogerakis, Programme Officer, EU Policies, Network Technologies at DG Connect, EC, http://www.5gensure.eu/interview-pavlos-fournogerakis.
- Hugo Tullberg, chair of the 5G PPP Pre-standardisation work group[1], http://www.5gensure.eu/interview-hugo-tullberg.

[1] Olav Queseth has been appointed as new chair of the 5G PPP Work Group Pre-standardisation to substitute Hugo Tullberg on October 2016.

- Adrian Belmonte, Network Security Officer at ENISA, http://www.5gensure.eu/interview-adrian-belmonte.

Ericsson Research has also promoted the video interview with Hugo Tullberg, which was Top Mention in September 2016.

Figure 15: Partner Promotion of Video Testimonials

4.2.4 ETSI Article

The outcomes of the workshop in terms of 5G-ENSURE standardisation efforts are also reported in the article published in the September issue of the ETSI newsletter. The article explains the 5G-ENSURE focus on security standardisation and its participation in the 3GPP SA3, ETSI TC CYBER and ETSI ISG NFV groups as the most relevant to the project's standardisation goals. The article also covers the main takeaways from the workshop and future plans for 5G-ENSURE work.


5G-ENSURE: Takeaways from 1st International Workshop on 5G Security Standardization

5G-Ensure

LightReading 5G

THE CUTTING EDGE OF WIRELESS

5G

ETSI is pleased to recommend LightReading's focus on 5G, a roundup of today's top stories in mobile communications!

www.lightreading.com/etsi

THE STANDARD | 5

Figure 16: 5G-ENSURE article in ETSI Newsletter

4.3 Dissemination of 5G-ENSURE results

4.3.1 Scientiic publications and talks

The dissemination of 5G-ENSURE results to the scientific community is one of the main objectives of the project to engage the research scientists and receive relevant feedback about the importance of the achievements attained. The target of the dissemination acitivities is primarily technical papers for submission to peer-reviewed journals, conferences, and workshops in the area of security, 5G and mobile networks, and networking relevant for the project. To ensure timely dissemination of the results, 5G-ENSURE partners have also considered submission of talks and demos at technical events.

During the first year of the project, the scope of the scientific dissemination has convered primarily security studies on Software-Defined Networking (SDN) with three different contributions as part of the work carried out in the Network Management & Virtualisation Isolation 5G-ENSURE Security Enablers. Research papers present potential attacks on SDN networks and their implications, a proof-of-concept implementation of the reference monitor for SDN controller ONOS and its effectiveness in protecting the network, and an analysis of key aspects of micro-segmentation and how this concept can be used to isolate applications in 5G mobile networks. Relevant for SDN is a novel framework for bootstrapping trust in SDN infrastructure. This latter research result is within the scope of the Trust 5G-ENSURE Security Enablers.

Research results recently published have focused on 5G group-based authentication mechanisms, including an analysis of the threat model to pave the way for the design of more secure protocols. This contribution is within the scope of the AAA 5G-ENSURE Security Enablers.

The table below summarises the publications on 5G-ENSURE research results, cited on the project website: http://5gensure.eu/publications.

Table 4: Current 5G-ENSURE Publications

Title	Authors	5G-ENSURE contributing partner	Publication information
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	Nicolae Paladi and	SICS	In Proc. of the 12th EAI International Conference

Infrastructure	Christian Gehrmann		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)

The talks have focused primarily on demonstrating attacks and analysis of security in cellular systems. The table below presents the complete list of 5G-ENSURE research results presented at technical conferences.

Table 5: Current 5G-ENSURE talks

Conference	Partner	Presentation title
GSMA Device Security Group at San Ramon, CA, U.S., 28-29 August 2016.	University of Oxford	Device Security Issues and 5G Considerations
NDSS 2106 Security Conference, San Diego, U.S., 21-24 February 2016	University of Oxford	Practical attacks against privacy and availability in 4G /LTE mobile communication systems
Troopers Security conference, Heidelberg, Germany, 16-17 March 2016	University of Oxford	Don't connect to my 4G base station: investigation into leaks in 4G baseband
SICS Security Day, Stockholm, Sweden, May 2016	University of Oxford	Security in cellular-radio access networks
Qualcomm Mobile Security Summit, San Diego, U.S., May 2016	University of Oxford	Analysing LTE/4G air interface protocols

4.3.2 Dissemination of outputs to the 5G PPP

All major outcomes and outputs from 5G-ENSURE have been shared with the 5G PPP projects through Euro 5G, as illustrated in the figures below.

Figure 17: Outcomes of the 5G-ENSURE 1st International Workshop

Figure 18: Security Enablers and Specifications

Figure 19: 5G-ENSURE Risk Management (1st iteration)

Figure 20: 5G-ENSURE Trust Model (1st iteration)

4.3.3 Dissemination of outputs through social media

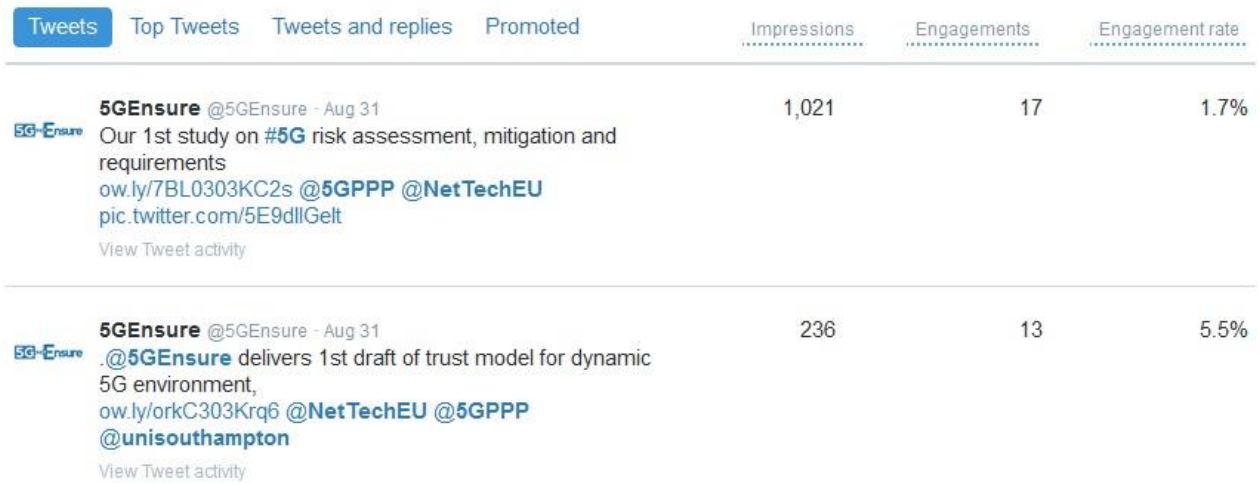
5G-ENSURE has dedicated effort to disseminating project findings and outputs through social media. The figures below show some examples of the impact achieved.

The publication of the first set of deliverables on the website in early June was endorsed by a member of Advisory Board and a cyber security expert.

Figure 21: Dissemination of 5G-ENSURE Deliverables

Figure 22: Dissemination of Test Bed Architecture

Figure 23: Dissemination of D2.2 and D2.3



The announcement of the publication of the open specifications for the security enablers and launch of the test bed were top mentions in June and August 2016 respectively.

Figure 24: Dissemination of Test Bed

Examples for LinkedIn updates include:

- The LinkedIn announcement on 17 October 2016 of the 5G-ENSURE visit to the test bed during the 4th Plenary Meeting in Rennes has so far received **175 views** (av. 53 views/day).
- The LinkedIn post on a presentation by Ericsson partner has 159 views (Mats Näslund, Principal researcher at EricssonLabs talks about 5G and the project 5G-ENSURE at the HITS research profile annual WS. Thanks to Computer Science for sharing).

4.3.4 Newsletters

5G-ENSURE has produced and distributed two newsletters. The first newwlstter, shown in **Error! Reference source not found.** promotes the first 5G-ENSURE outputs and fearures highlightes from the first F2F 5G PPP Security Work Group.

The second newsletter, shown in **Error! Reference source not found.**, describes the presence of 5G-ENSURE at events, also giving highlightes about the contributions to events.

Figure 25: 1st 5G-ENSURE newsletter

5G Enablers for Network and System Security and Resilience

5G-ENSURE is the flagship project for security and privacy in the 5G PPP of the European Union under Horizon 2020 (public private partnership on 5G infrastructure).

As part of the drive to realise the full potential of 5G and boost innovation across European industrial verticals, Europe is working towards a common understanding of 5G solutions and scenarios, including security and privacy with a new 5G trust model.

How is 5G-ENSURE contributing to European excellence?

5G-ENSURE core activities range from analysing and prioritising 5G security and privacy requirements, defining a security architecture for 5G, to developing and testing an initial set of security and privacy enablers for 5G.

5G-Ensure has a strong focus on early security standardisation for 5G.

5G-ENSURE outputs

5G Use Cases

5G-ENSURE has identified a set of use cases illustrating security and privacy aspects of 5G networks. Based on similarities in technical, service and/or business-model related aspects, the use cases are grouped into clusters covering a wide variety of deployments including, for example, the Internet of Things, Software Defined Networks and virtualisation, ultra-reliable and standalone operations. The use cases address security and privacy enhancements of current networks as well as security and privacy functionality needed by new 5G features.

Read more

Early Vision for the 5G PPP security enablers technical roadmap and open specifications

5G-ENSURE has produced its early vision for the 5G security and privacy enablers it plans to release in two major releases. The open specifications of the 5G security enablers are now also available in preparation for the first software release (v1.0) planned in Autumn 2016. The final release is planned for August 2017.

Read more

Collaboration with the 5G PPP

5G PPP Security Work Group: takeaways from 1st F2F Meeting

The 5G PPP Security Work Group has been created by the 5G-ENSURE project as a forum for discussion among the projects within the first phase of the 5G PPP interested in 5G Security aspects.
The first F2F meeting at EuCNC 2016 in Athens has led to a set of concrete actions towards a 5G PPP Security Whitepaper in late 2016. Next steps will be to elaborate good practices and recommendations for 5G PPP projects.

Read more

Connect with 5G-ENSURE to share insights on 5G.

5G ENSURE receives funding from the EU Framework Programme for Research and Innovation H2020 under grant agreement No 671562 | Duration November 2015 / October 2017
You are receiving this newsletter because you have expressed interest in 5G security.
If you do not wish to receive future newsletters unsubscribe from this list .

Figure 26: 2nd 5G-ENSURE newsletter

5G-Ensure
5G Enablers for Network and System Security and Resilience

5G-ENSURE is the flagship project for security and privacy in the 5G PPP of the European Union under Horizon 2020 (public private partnership on 5G infrastructure).
In this newsletter you'll out where you can meet the 5G-ENSURE team in November and learn about our outputs to address security and privacy challenges in 5G networks.

5G-ENSURE visits its fully operational 5G test bed

5G-ENSURE partner, b<>com, hosted the project's 4th Plenary Meeting on 11-13 October. Over the 3 days, partners took stock of its achievements as it approaches the end of its first year in a 24-month project. The first cycle of project coincides with the initial definition of a 5G security architecture, in agreement with other 5G PPP projects contributing to the Security Work Group (chaired by 5G-ENSURE), and the first set of implemented enablers. A visit to the test bed was one of the highlights of the meeting to get a first-hand look of this key project asset, launched in August 2016.

Read more

5G-ENSURE showcase at the Second Global 5G event

The 2nd Global 5G Event takes place 9-10 November in Rome under the theme "Enabling the 5G EcoSphere". 5G-ENSURE will be showcasing its outputs so far at an Exhibition Stand. The conference agenda features high-level policy and industry keynotes with plenty of opportunities to debate key topics spanning standards and deployment of 5G.
Come and visit the 5G-ENSURE stand to learn more about latest developments in 5G security.

Read more

Oxford University presents WIFI-BASED IMSI CATCHER at Black Hat Europe

5G-ENSURE partner, Oxford University, is presenting the research results on Wifi-based IMSI Catcher at Black Hat Europe, 3-4 November 2016 in London. The presentation will introduce two new approaches which exploit authentication protocols that operate over WiFi and demonstrate how users may be tracked on a range of smartphones and tablets.

Read more

IT Innovation presents trust and security modelling at National Security and Resilience

5G-ENSURE partner, University of Southampton IT Innovation Center, will give a talk at the UK's National Security and Resilience conference on 9 November 2016 in London. The talk focuses on trust and security modelling, including the Trust Builder defined in the framework of the 5G-ENSURE project. IT Innovation is leading the development of a new trust model for 5G future networks as key to building consumer confidence.

Read more

Connect with 5G-ENSURE to share insights on 5G.

5G-ENSURE has received funding from the EU Framework Programme for Research and Innovation H2020 under grant agreement No 671562 | Duration November 2015 / October 2017
You are receiving this newsletter because you have expressed interest in 5G security.
If you do not wish to receive future newsletters unsubscribe from this list .

4.3.5 Downloads of outputs

The 5G-ENSURE deliverables have been downloaded 862 times since the first documents were published in February 2016, that is an average of 96 times/month.

5 Impact of actions within the 5G PPP Joint Programme

5.1 Contributions to 5G PPP Work Groups

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

- Security WG as chair.
- Pre-standardisation WG.
- Architecture WG.
- Vision and social challenges.

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.

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: 5G PPP Security White Paper. Good practices and recommendations for the 5G PPP.
5G PPP PRE-STANDARDISATION WORK GROUP	
Chair: Hugo Tullberg, 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. **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).
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. **Future steps**: Preparing a white paper for MWC 2017, which will be compiled from project contributions in the period October 2016 to January 2017.

5.2 Joint Publications

In the context of common actions with the 5G PPP projects, Euro-5G will publish the first printed edition of its European 5G Annual Journal early November 2016. A first electronic version was published in July 2016 and the update will be presented at 2nd Global 5G event. 5G-ENSURE has contributed late September with an update of the project description and objctives, highlighting the latest results of the project.

In light of the forthcoming participation to the 2nd Global 5G event, 5G-ENSURE has worked on a position paper shared with 5G PPP board as preparation of the joint 5G PPP project presentation. The paper is shown in Figure 27 and is complemented by a project progress report for a 5G PPP panel discussion at Global5G.

Figure 27: 5G-ENSURE paper for the 5G PPP panle at 2nd Global 5G

5G-Ensure http://5gensure.eu/ contact@5gensure.eu @5gensure

5G#ENSURE)–)5G)Enablers)for)Network,)System)Security,)Privacy)and) Resilience)to)make)5G)networks)and)systems)trustworthy)

The 5G-ENSURE project (http:// www.5gensure.eu/) brings to the 5G PPP a consortium of telecom and network operators, IT providers and cyber security experts addressing priorities for security and resilience. The overall goal of the 5G-ENSURE project is to deliver strategic impact across technology, business enablement and standardisation by realising a vision for a secure, resilient and viable 5G network. To achieve this overall ambition a number of specific objectives are targeted:

- Illustrate 5G security and privacy requirements through representative use cases.
- Define a 5G security architecture as a reference for future networked ecosystems to enable entirely new business opportunities.
- Develop enablers to make 5G networks trustworthy.
- Create a 5G test-bed to validate the security enablers.
- Contribute to security standards with a focus on 3GPP and ETSI.

Starting from the definition of representative use cases, the project was organised around two cycles. Each one encompasses the definition of the technical roadmap, the open specification, the development and release of the enablers together with documentation. In parallel, the project has progressed on 5G security architecture and on the set up of a test-bed that fulfils the enablers' requirements.

The end of the first cycle has coincided with the initial definition of the security architecture, in agreement with other 5G PPP peer projects through their contribution to the 5G PPP Security WG chaired by 5G-ENSURE. Working collaboratively with these projects, 5G-ENSURE has provided the security architecture needed to expand the networked ecosystem into an entirely new networked society, attracting new types of users and giving operators a platform for new business opportunities. The architecture well supports the mapping of the features of the 5G-ENSURE enablers developed. Equally important, it can be extended to accommodate new features coming from other 5G PPP projects.

The security enablers represent the major security building blocks for the 5G system. The initial technical roadmap identifies the following classes of enablers: AAA (Support for IoT and satellite systems; Trust and liability levels), Privacy (Increased assurance and confidence), Security Monitoring (Security by operation), Trust (Trustworthy dynamic 5G multi-stakeholder system with new trust models) and Network Management & Virtualisation Isolation (Mitigating security threats in SDN). The first set of implemented enablers will be validated in the test-bed by the end 2016.

The second cycle considers the feedback from the validation for further improvement of the security enablers to be continued and also to come up with new ones. These results will be widely disseminated to the 5G PPP project committee and beyond in order for them to be adopted.

5G ENSURE has received funding from the EU Framework Programme for Research and Innovation H2020 under grant agreement No 671562 Duration: November 2015 / October 2017 The 5G Infrastructure Public Private Partnership

5G-Ensure http://5gensure.eu/ contact@5gensure.eu @5gensure

A key asset of the project is the 5G test-bed designed and set-up to satisfy the needs/requirements of the security enablers against the threats emerging from the use cases. The test-bed remains open to additional requirements from the second cycle.

The 5G-ENSURE distributed test-bed was launched in 2016 and currently promotes a DevOps approach for 5G. On-going work focuses on the integration of VNFs based on OpenAirInterface, making it a core asset of the project.

Finally, standardisation is a common theme running through 5G-ENSURE, with partners contributing to relevant standards to generate trust and confidence between actors in future networks. Main targets for standardisation activities where the project has already made a number of contributions are the 3GPP study item on Next generation/5G security and ETSI TC CYBER.

5G-ENSURE is the first 5G PPP project that deals with the cross-cutting area of security. 5G-ENSURE is therefore building consensus across 5G PPP projects and other international initiatives in the domain of security and trust. Core activities have included an open public consultation on 5G security. The results of which have been reported during the 1st 5G-ENSURE workshop on standardisation, bringing together standard bodies, industry and academia to provide recommendation for 5G security.

About 5G ENSURE!

http://www.5gensure.eu | @5gensure

5G-ENSURE officially kicked off on 1st November 2015 and the first face-to-face meeting was held in Helsinki on 2nd and 3rd November. The 5G-ENSURE consortium is coordinated by VTT Technical Research Centre of Finland (FI) and technically managed by Thales (FR). The other partners are NOKIA Bell Labs (FR), b<>com (FR), Ericsson (SE & FI), University of Southampton IT Innovation Centre (UK); NEC Europe (DE), Nixu (FI), Orange (FR), SICS Swedish ICT (SE), Thales Alenia Space España (ES), Telecom Italia Information Technology (IT), Trust-IT Services (UK) and University of Oxford (UK).

5G ENSURE has received funding from the EU Framework Programme for Research and Innovation H2020 under grant agreement No 671562 Duration: November 2015 / October 2017 The 5G Infrastructure Public Private Partnership

6 Impact for Community Building, Communications,and Stakeholder Engagement

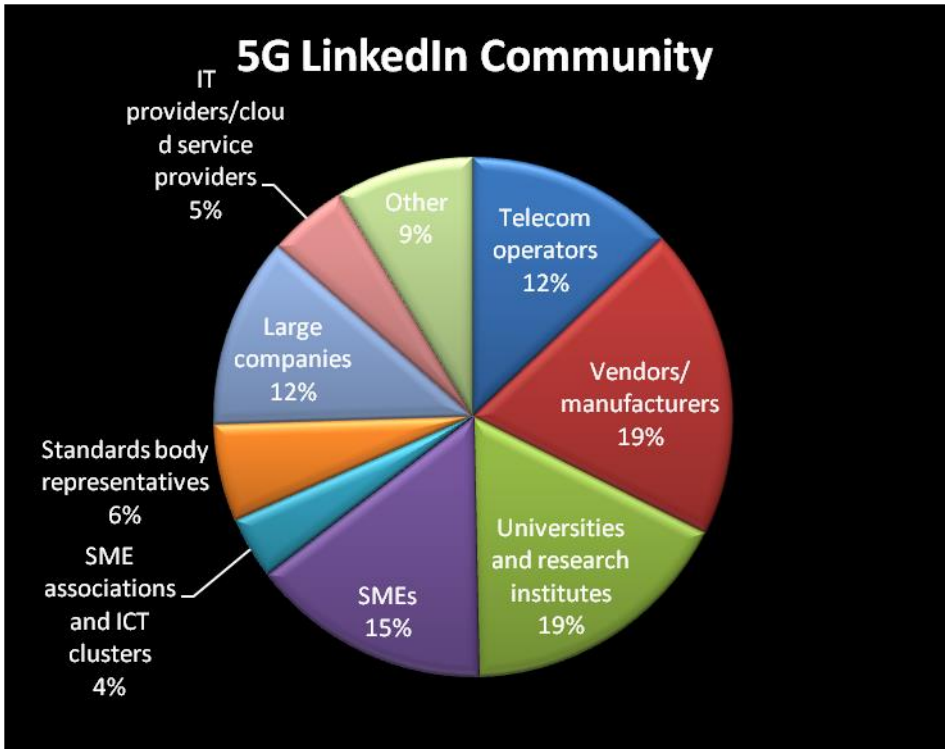
6.1 5G-ENSURE Community

5G-ENSURE currently has a LinkedIn community of **464 connections**. Members have been recruited from the project database of 5G PPP phase 1 projects, open consultation respondents, workshop participants. Much of the community has grown organically through selected partner contacts.

- Telecom operators: 60 representatives. This group includes representatives involved in standardisation.
- Vendors/manufacturers: 90 representatives This group includes representatives involved in standardisation.
- Universities and research institutes (telecommunications): 80 representatives, including experts contributing to standardisation.
- Standards body representatives: 28
- SMEs: 62 representatives; SME and sector-specific associations (e.g. ICT clusters): 18
- Large companies: min. 55 representatives
- IT providers/cloud service providers: 23 representatives
- Other: 40 (e.g. telecom journalists, publishers, social media influencers, educational courses, legal/privacy experts, policy such as the EC and ENISA).

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

Figure 28: LinkedIn Community



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

PRIMARY STAKEHOLDERS (including representatives from 5G PPP phase 1 projects	
5G industry	Telecom operators: Ålands Telefonandelslag, Belgacom, China Mobile, Deutsche Telekom, Mobistar (Orange / France Telecom Group), Oi S.A, Orange, OTE/COSMOTE, Proximus, Swisscom, Tango S.A (Group Proximus), Telecom Italia, Telekon Slovenia, Telefonica, Telenor, TeleSonria, Verizon, Viettel Group, Vodafone, VOO. Vendors/Manufacturers: Cisco Systems, Ericsson, Huawei Technologies European Research Center, Nexia DA, Nokia, Qualcomm, Samsung Electronics (EU, U.S.), Telenet.
Universities & research institutes	Aarhus University (IoT), Aalto University, BISDN at Berlin Institute for Software Defined Networks, CTTC, Iowa State University, King's College London, KTH, Technical University of Madrid, Trinity College Dublin, Universidad de Murcia, University of Oxford, University of Southampton, University of Surrey. Federal University of Ceará, Brazil.
Standards Bodies	3GPP - Security Engineer/3GPP SA3 Delegate, Vice Chairman of Security Group of 3GPP SA3, 3GPP TSG RAN Vice-Chair. ETSI Chair ISG NFV, ETSI Co-chair TC CYBER, ETSI Chair OSM, ETSI CTO, Rapporteur for FOG Computing White Paper ETSI, AIOTI WG3 Chair at ETSI. IEEE Privacy, IEEE 5G Initiative, IEEE IoT. IETF. Vice-Chairman of OMA Communications Group (COM WG).
5G PPP and International initiatives	Coordinators and representatives from: EURO5G, 5GEX, CHARISMA, SELFNET, SPEED 5G, 5G-Crosshaul. National and International initiatives on 5G: 5G Innovation Centre, 5G Lab (DE), 5G!PAGODA (EU-JP), PICASSO (EU-U.S.).
SECONDARY STAKEHOLDERS	
Companies – SMEs and large companies can be divided into supply chain providers, hi-tech companies and verticals. Some examples include: **SMEs**: 3IF - Internet of Things and Industrial Internet Future (Industry 4.0), 5G UP, EnvOps, Incelligent, InnoRoute, IS-Wireless, OTREMA, Montimage, Nextworks, SETECS, SpinalCom (fog middleware), TerUsus. **Verticals**: ABB (utility), Accenture (IIoT, smart cities), AIRBUS (aerospace), Banca d'Italia, BNP Paribas Fortis (financial services), DEXMA Tech (utilities), Comesvil (transport), DFRC (smart cities), Dyson (high-tech engineering), Gemalto (5G transport), Lloyds Banking Group (financial services), Pagero (SME - Fintech), Philips (healthcare), Siemens, Sony EU, Sony China, Square (SME - Fintech), Strategic FinTech (SME), Tatung Czech (utilities – energy efficiency), Sony, tec ICT (SME, utilities), Toyota, Technicolor (gaming/media), Ubiwhere (SME – smart cities), Volvo.	

6.1.1 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 6 metrics used.

Table 6: Impact on Twitter

Overall Performance (31-10-2016)	
Tweets	*733*
Followers	*318*
Following	*142*
Total impressions	*462,278*
Total profile visits	*5858*
October 2016	
Number of tweets	60
Number of profile visits	499
Tweet Impressions	26,600
New followers	21
Top follower	Marina Ashurkina (23,300)
Mentions	19
September 2016	
Number of tweets	67
Number of profile visits	533
Tweet Impressions	35,200 (1.2K/day)
New followers	30
Top follower	Santiago BoNet (29,300)
Mentions	17
August 2016	
Number of tweets	53
Number of profile visits	479
Tweet Impressions	25,900 (av. 835/day)

New followers	16
Top follower	N/A
Mentions	11
July 2016	
Number of tweets	46
Number of profile visits	293
Tweet Impressions	21,200 (683/day)
New followers	25
Top follower	Evan Kirstel (86,600)
Mentions	7
June 2016	
Number of tweets	92
Number of profile visits	748
Tweet Impressions	55,500 (1.9K/day)
New followers	44
Top follower	Tight To Spectrum (7,907)
Mentions	13
May 2016	
Number of tweets	53
Number of profile visits	501
Tweet Impressions	36,000 (1.2K/day)
New followers	42
Top follower	5G World Series (12,000)
Mentions	13

6.1.2 5G-ENSURE website activities

5G-ENSURE has published 48 web content items in the period from May to October 2016 (av. 8/month), covering all four thematic news items (policy pulse, standards, tech insights and market insights) and relevant events for 5G-ENSURE. The table below reports on the content creation for the website to ensure it remains dynamic and up-to-speed with key developments within 5G-ENSURE, the 5G PPP and the wider 5G landscape.

Table 7: Web content creation on 5G-ENSURE

Topic Focus	Links
Events (October 2016)	http://5gensure.eu/events/ouluhealth-ecosystem-day-demodate-oulu
Market Insights (October 2016)	http://5gensure.eu/news/new-mission-critical-communications-alliance-aims-improve-public-safety
Tech insights (October 2016)	Project output: http://5gensure.eu/news/5g-ensure-visits-its-5g-test-bed-bcom
Market insights (October 2016)	http://5gensure.eu/news/nokia-latin-america-iot
Market insights (October 2016)	http://5gensure.eu/news/insights-socio-economic-impact-5g
Tech insights (September 2016)	http://5gensure.eu/news/industry-updates-arvr-and-wifi-network-optimisation
Events (September 2016)	http://5gensure.eu/events/picasso-webinar-eu-us-policy-recommendations-data-protection-privacy
Events – Global 5G (September 2016)	http://5gensure.eu/events/second-global-5g-event-9-10-november-2016-rome
Events – 5G-ENSURE partner presentation at Black Hat 2016 (September 2016)	http://5gensure.eu/events/oxford-university-presents-wifi-based-imsi-catcher-black-hat-europe
Tech insights - – 5G-ENSURE output (August 2016)	http://5gensure.eu/news/5g-ensure-takes-first-steps-towards-trust-model-5g-networks
Tech insights – 5G-ENSURE output (August 2016)	http://5gensure.eu/news/5g-ensure-publishes-initial-study-5g-risk-assessment-mitigation-and-requirements
Market insights (August 2016)	http://www.5gensure.eu/news/nokia-and-bt-agree-collaborate-development-5g
About – new section on 5G PPP WGs and current outcomes (August 2016)	http://5gensure.eu/5g-ppp-wgs
Policy pulse (August 2016)	http://5gensure.eu/news/us-perspectives-security-and-privacy-5g
Standards – 5G-ENSURE AB member (August 2016)	http://www.5gensure.eu/news/etsi-elects-5g-ensure-expert-its-nfv-chairman
Standards – testimonial from chair of 5G PPP Pre-Standardisation WG	Accessible from the home page
Events – CfP (August 2016)	http://www.5gensure.eu/events/secsac17-call-papers-security-track
Standards (August 2016)	http://www.5gensure.eu/news/will-5g-standards-deliver-time

Events (August 2016)	http://www.5gensure.eu/events/securecomm-2016-10-12-october-guangzhou-china
Update on AB member Diego Lopez (elected chair of ETSI ISG NVF) (August 2016)	http://5gensure.eu/advisory-board
Tech insights – 5G-ENSURE test best (August 2016)	http://www.5gensure.eu/5g-ensure-testbed
Standards – outcomes of 5G-ENSURE public consultation	http://www.5gensure.eu/news/5g-ensure-public-consultation-5g-security-and-standardisation
Tech insights – 5G PPP joint programme level activity (July 2016)	http://5gensure.eu/news/5g-ppp-security-work-group-takeaways-1st-f2f-meeting
Standards – 5G-ENSURE 1st International Workdshop (July 2016)	http://www.5gensure.eu/news/outcomes-1st-eg-ensure-international-workshop-5g-security-standardisation
Policy pulse (July 2016)	http://5gensure.eu/news/europes-5g-ppp-becomes-model-us-investments
Market insights (July 2016)	http://www.5gensure.eu/news/ericsson-new-business-opportunities-5g
Policy pulse (July 2016) – reference to 5G-ENSURE partners	http://www.5gensure.eu/news/five-5g-ensure-partners-sign-manifesto-timely-deployment-5g-europe
Tech insights – 5G-ENSURE output (July 2016)	http://www.5gensure.eu/news/5g-security-test-bed-architecture
Policy pulse (July 2016)	http://www.5gensure.eu/news/tech-and-telecom-industries-call-review-e-privacy-directive
Market insights (July 2016)	http://www.5gensure.eu/news/3-takeaways-5g-world
Events (July 2016)	http://www.5gensure.eu/news/call-papers-1st-intl-workshop-security-nfv-sdn
Tech insights – 5G PPP joint programme level activity (July 2016)	http://5gensure.eu/news/5g-ppp-white-paper-5g-architecture
Standards (June 2016)	http://www.5gensure.eu/news/3gpp-agrees-plan-first-release-5g-specifications
Policy Pulse (June 2016)	http://www.5gensure.eu/news/commission-oettingers-key-message-5g-eu-industry-gsma-m360-europe
Policy Pulse (June 2016)	http://www.5gensure.eu/news/calls-action-gsma-m360-europe

Tech insights (June 2016)	http://www.5gensure.eu/news/ieee-software-defined-networks-and-eit-digital-launch-international-open-test-bed-community
Market insights (June 2016)	http://www.5gensure.eu/news/talking-5g-business-models-professor-mischa-dohler
Standards (June 2016)	http://www.5gensure.eu/news/global-collaborative-work-5g-standardisation
Market Insights (June 2016)	http://www.5gensure.eu/news/can-privacy-beat-content-and-low-cost-connectivity-future-telco-business-model
Policy Pulse (June 2016)	http://www.5gensure.eu/news/wrap-beijing-5g-event
Tech insights - 5G-ENSURE output (June 2016)	http://www.5gensure.eu/news/5g-ensure-publishes-its-5gppp-security-enabler-open-specifications-v1
Standards (June 2016)	http://5gensure.eu/news/operators-push-stronger-role-5g-development-through-new-ngmn-initiatives
Tech insights (May 2016)	http://5gensure.eu/news/5g-ppp-architecture-work-group-releases-their-views-5g-architecture
Standards (May 2016)	http://www.5gensure.eu/news/takeaways-etsi-summit-5g
Standards (May 2016)	http://www.5gensure.eu/news/takeaways-20th-global-standards-collaboration-meeting
Standards (May 2016)	http://www.5gensure.eu/news/guy-daniels-telecomtv-interview-luis-jorge-romero-director-general-etsi-may-2016
Standards (May 2016)	http://www.5gensure.eu/news/guy-daniels-telecomtv-interview-marcus-brunner-swisscom-may-2016
Tech insights (May 2016)	http://www.5gensure.eu/news/5g-ensure-partner-bcom-becomes-5g-test-operator

6.1.3 Stakeholders Engagement at Events and Synergies

Standardisation Organisations

The main liaisons with standards groups are described below. The list contains all the main contributions, since the beginning of the project.

- Internal discussion about new 3GPP SA3 Study Item on Study on Architecture and Security for Next Generation System (i.e. **TD S3-160278**). The SI, agreed by the SA3 group, has been supported by many companies, and among them are also some 5G-ENSURE partners. The SI draft has been discussed internally in the project in order to stimulate cooperation and agreement among the partners. The SA3 SI has been identified as the main opportunity for the standardisation of the results of the project.
- 5G-ENSURE Project presentation during the ETSI TC CYBER#6 meeting, 8-10 February, Sophia Antipolis. The presentation stimulated a discussion about possible new Work Items related to the security of 5G. In fact, at the present time TC CYBER does not have a specific WI dedicated to it but

a set of WIs that can be considered relevant for the topic. A new Work Item proposal dedicated to the privacy aspects of 5G, which emerged during the activities of the project, could be of interest for the group.

- 5G-ENSURE Project presentation during 5G PPP Pre-Standardisation WG conference call on the 12th of February. The presentation stimulated some general questions about the structure of the project, its main objectives and preliminary results (the deliverable D2.1 about the use cases) and the list of possible SDO/groups that the project has selected for its standardisation activities (i.e. 3GPP).
- Contributions to the 3GPP TSG-RAN#71 in Gothenburg, Sweden, March 7 - 10, 2016. During the meeting TIIT presented a set of contributions related to possible security and privacy requirements elaborated by TIIT for the project and relevant for RAN. Such contributions have been circulated and discussed among the 5G-ENSURE partners before the meeting during WP5 and Task5.1 conference calls and, although the final version weren't co-signed by other partners, they contained some of the comments received. The contributions have not been approved during the meeting, but anyway considered relevant for RAN and sent, via Liaison, to SA3 for additional analysis.
- Contributions presented to the 3GPP SA3#84 meeting in Chennai, July 25-27, 2016. Different contributions have been proposed for agreement and incorporation into the current draft of the TR 33.899 (Security of 5G). Many of them co-signed by Telecom Italia, Nokia and Ericsson. The topics proposed were mainly related to Privacy aspects.
- Contribution to the ETSI TC CYBER#7 in Sophia Antipolis, June 15-17, 2016. As anticipated during CYBER#6, a specific work item about Privacy aspects has been proposed. The new WI working title is "Application of ABE for data protection on smart devices, cloud and mobile services". The scope is to define specific technical measures for the protection of the privacy in the mobile scenario (for the project scope).
- Contribution to the ETSI TC CYBER#9 in Sorrento, September 21-23, 2016. A Liaison to the 3GPP SA3 has been proposed and approved by the group. The liaison is aimed to inform SA3 about the new WI dedicated to the Privacy protection and to ask possible support. In this manner the two main target standardisation gropups of the project have been aligned about the ongoing specification works on Privacy.
- Presentation to the GSM Association's Freud and Security Group (FASG), September 26, 2016. Oxford presented work on "WiFi-based IMSI Catcher" - via teleconference/Webex

Event	GSMA Device Security Group
Date and Venue	28-29 August 2016, San Ramon, CA, U.S.
Focus	Meeting of the GSM Association's Fraud and Security Group (FASG) steering industry management of freud and security issues related to GSM technology, networks and services. Oxford University gave a presentation on research conducted in relation to device security issues and 5G considerations.
Stakeholder engagement	The FASG has the objective to maintain or increase the protection of mobile operator technology and infrastructure and customer identity, security and privacy such that the industry's reputation stays strong and mobile operators

	remain trusted partners in the ecosystem. FASG provides an open, receptive and trusted environment within which fraud and security intelligence and incident details can be shared in a timely and responsible way.
5G-ENSURE role and outcomes	Presentation from Oxford University
Web links	http://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group

Date and Venue	EuCNC 2016 - 27-30 June 2016, Athens
Focus	Technical aspects of 5G and future research directions
Stakeholder engagement	Visibility at the Euro5G stand with the circulation of project promotional material. Interaction with peer projects in the 5G PPP and other 5G stakeholders.
5G-ENSURE role and outcomes	5G-ENSURE organised a F2F meetng with the Security WG, which was also attended by the Project PO. The WG discussed current issues around security and defined future actions, e.g. white paper on 5G security.
Web links:	http://www.eucnc.eu/

Date and Venue	UK 5G Info Day – October 2016, London
Focus	Information about the 5G PPP work programme, organised by the Georgios Papadakis of Innovate UK and Richard Foggie of the UK KTN and with a presentation from Ari Sorsaniemi, Future Connected Systems Unit, DG CONNECT.
Stakeholder engagement	Research and industry representatives with an interest in 5G and funding opportunities (20 participants).
5G-ENSURE role and outcomes	IT Innovation gave a presentation on 5G-ENSURE.
Web links	N/A

Date and Venue	Security Day - Ericsson, 5 October 2016, Kista
Focus	Educate company employees working on security about emerging threat landscape and 5G
Stakeholder engagement	Corporate event – 200 employees
5G-ENSURE role and outcomes	5G-ENSURE poster presentation.

Web links	N/A

Date and Venue	Karlstads Universitet – 20 October 2016
Focus	HITS research profile annual Workshop discussing emerging technologies
Stakeholder engagement	Research community
5G-ENSURE role and outcomes	Ericsson gave a presentation on 5G and 5G-ENSURE
Web links	N/A

7 Plans and Targets for next six months

7.1 Standardisation Organisations

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 particular the SA3 meetings in Santa Cruz (November 2016) and Sophia Antipolis (February 2017) will be decisive for the definition of the plan on 5G Security. Moreover, SA3 will also 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. In particular, the current version of the TR 33.899 will be finalised and a new (or two) new Study Item and/or Work Item will be opened. Regarding ETSI, it is expected that the actual work on the definition of the technical measures to protect privacy in mobile environments will start during the next meeting in Sophia Antipolis (February 2017).

Table 8: Meeting Schedule of main Standards Bodies for 5G Security

TITLE	DATES	LOCATION
3GPPSA2#117	17 - 21 Oct 2016	Kaohsiung city
3GPPSA3#63-LI	25 - 28 Oct 2016	San Antonio
3GPPSA1#76	7 - 11 Nov 2016	Tenerife - Santa Cruz
3GPPSA3#85	7 - 11 Nov 2016	Tenerife - Santa Cruz
3GPPSA2#118	14 - 18 Nov 2016	Reno, Nevada
3GPPSA#74	7 - 9 Dec 2016	Vienna
3GPPSA2#118-Bis	16 - 20 Jan 2017	US
3GPPSA1#76-Bis	16 - 20 Jan 2017	US (TBC)
3GPPSA3#64-LI	24 - 27 Jan 2017	Sophia Antipolis
3GPPSA3#86	6 - 10 Feb 2017	Sophia Antipolis
ETSI TC CYBER	13 – 15 Feb 2017	Sophia Antipolis
3GPPSA2#119	13 - 17 Feb 2017	Dubrovnik
3GPPSA1#77	13 - 17 Feb 2017	Jeju Island
3GPPSA#75	8 - 10 Mar 2017	Dubrovnik
3GPPSA2#120	27 - 31 Mar 2017	South Korea
3GPPSA3#65-LI	25 - 28 Apr 2017	US

7.2 Stakeholder Engagement on LinkedIn

5G-ENSURE has recently joined a number of LinkedIn groups to share results and insights on a range of 5G-related topics. The groups have also been selected for potential content to shared more widely across the social media. Planned engagement for the period November 2016 to April 2017 is showed in the table below.

Table 9: Contributions to LinkedIn Groups

LinkedIn Group	Current Members	Planned Engagement
3GPP LTE/LTE-A Standards	52,457	Focus on technical issues related to 3GPP standardisation of the Radio Access Network. Engagement: discuss security and privacy related requirements in RAN, , provide information on 5G-ENSURE activities on 5G security standardisation, the open consultation and roadmap.
Wireless Communications & Mobile Networks	13,542	Focus on future wireless communication networks, including 5G. Engagement: provide technical insights about 5G security and trust issues addressed by 5G-ENSURE to ensure optimal planning and implementation of mobile networks.
IEEE Communications Society Members	12,505	Focus on advancing all communications and networking technologies. Engagement: share insights on threats to SDN, techniques for network virtualisation and isolation, including the open specifications of the 5G-ENSURE Network Management & Virtualisation Isolation Security Enablers.
Global mobile Suppliers Association (GSA)	12,132	Represent mobile suppliers worldwide and advise governments and policy-makers on optimum conditions for market development. Engagement: share the practical results of the validation of the 5G-ENSURE security enablers for potential uptake and insights about the need to integrate security and privacy by design in 5G services.
OpenStack Forum	8,684	Focus on OpenStack deployment. Engagement: discuss and receive support for the practical development and usage of OpenStack for the test phase of the security enablers.

Radio Microwave, Satellite & Optical Communications	8,406	Focus on satellite communications, including comprehensive analysis of the applications. Engagement: discuss security and privacy risks inherent to satellite communications.
SDN - Software Defined Networking	6,877	Focus on SDN and OpenFlow. Engagement: discuss about security issues related to SDN and OpenFlow, including plans for the future.
5G and IoT in India	4,479	Focus on India development of 5G and IoT. Engagement: India is signing an agreement with Europe on 5G. The plan is to present the latest results of the 5G-ENSURE project and potentially facilitate the penetration of the 5G technology in India via their members.
Europe's Digital Agenda Initiatives	4,260	Focus on initiatives related to the Digital Agenda for Europe. 5G is one of the key technologies. Engagement: share success stories about new 5G security enablers and discuss the standardisation roadmap to support the EU Digital Single Market strategy.
5G	2,806	Focus on 5G technology. Engagement: share technical insights and discuss about 5G security and privacy issues, including the open specifications of the 5G-ENSURE security enablers and the 5G security architecture.
Industry 4.0	1,149	Focus on Industry 4.0 with a special interest on 3D printing. Engagement: at the moment we do not plan to engage with the members of this group, but we are interested to monitor the potential growth and interest in verticals pertinent to 5G networks.
Connected Car, Autonomous Driving, Telematics, Self-Driving, In-vehicle WiFi, LTE in Cars	650	Focus on the automotive sector. Engagement: share technical insights about 5G security solutions that could be integrated in next generation connected cars. The automotive sector is one of the relevant verticals for 5G.

5G CHAMPION (H2020)	332	Focus on the EU-KR collaborative project 5G CHAMPION Engagement: discuss potential interest of the 5G CHAMPION in some of the 5G-ENSURE security enablers.
Market Research Reports and Analysis - LTE, 4G, 5G, IoT, M2M, Wi-Fi, Small Cells, HetNets	325	Focus on market analysis. Engagement: discuss market trends and potential impact of 5G technologies across verticals.
5G PPP - 5G experts, analysts, large companies, SMEs, and 5G PPP	81	Launched on 20-10-2016, this group is the place for facilitating engagement across phase 1 5G PPP projects, sharing updates, outputs, insights and events. Engagement 5G-ENSURE has strongly endorsed this group through COMMS activities and will provide updates and insights from the project.
PICASSO – EU/US ICT research, innovation and policy collaboration	40	Focus on EU-EU PICASSO project. Engagement: a synergy with the PICASSO project has been already established. The group can facilitate the promotion of common initiatives.
5G NetWorld2020 SME Working Group	9	Focus on NetWorld 2020 SME Working Group to foster cooperation in Europe. Engagement: the group is rather small and focus specifically on SMEs more to facilitate forming consortiums for proposal. This could represent a forum of discussion to promote further the results of the 5G-ENSURE project and facilitate their reuse by new funded initiatives.

7.3 Stakeholder Engagement at Events

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	Oxford University will present research on Wifi-based IMSI Catcher at Black Hat Europe

Web links	http://5gensure.eu/events/oxford-university-presents-wifi-based-imsi-catcher-black-hat-europe

Event	1st International Workshop on Security in NFV-SDN (SNS2016)
Date and Venue	7 November, Palo Alto, U.S.
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	Nokia will highlight the focus of 5G-ENSURE and its outputs, such as the security and privacy enablers, the security architecture and standardisation efforts.
Web links	http://5gensure.eu/events/1st-international-workshop-security-nfv-sdn-sns2016

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 will give a talk on trust and security modelling, including the Trust Builder from 5G-ENSURE. The updated flier will also be distributed.
Web link	http://www.nsr-conference.co.uk/

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.
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 has an exhibition stand featuring demos and project promotional material, including a brochure on project standardisation efforts. 5G-ENSURE will interact with 5G PPP peer projects, collect feedback from the members of the security WG and interview AB member, Diego Lopez.
Web link	http://5gensure.eu/events/5g-ensure-showcase-second-global-5g-event

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

Event	*International Cyber security Forum 2017*
Date and Venue	24-25 January 2017, Lille
Focus	Cyber security
Stakeholder category/ies	5000 IT professionals
5G-ENSURE role	BCOM will have a stand at the event and promote 5G-ENSURE, especially the test bed and enablers.
Web link	https://www.forum-fic.com/

Event	RSA 2017
Date and Venue	13-17 February 2017, San Francisco, U.S.
Focus	New approaches to information security and latest technologies with a mix of hands-on sessions, key notes and informal gatherings.
Stakeholder category/ies	Security leaders, demand and supply side for information security products and services
5G-ENSURE role	Ericsson will give a presentation on 5G and 5G-ENSURE (tbc)
Web link	https://www.rsaconference.com/events/us17

7.4 Website Revamp and Newsletters

The plan for the website will be simiar to activities undertaken, which have proven effective. Major actions are described below.

In November 2016, 5G-ENSURE will update all the pages related to the project, taking on board the deliverables due. A campaign for disseminating the results will be implemented and target primary stakeholders.

The website revamp will take place between September 2016 to January 2017, and will mostly focus on making it more interactive, making it an additional channel for community building. Three specific actions will be taken to achieve this goal:

- Promote the newsletter subscription on the home page across social media and through the 5G PPP COMMS (implemented in September).
- December 2016: Create a slider on the security and privacy enablers to promote opportunities for uptake. The link will lead to a short online form to make an expression of interest and to the revamped section on the enablers. Opportunities will be widely promoted.
- January 2017: Develop an online forum on the major 5G-ENSURE outputs and findings with a regular campaign to encourage an online, multi-stakeholder dialogue. The forum will be designed to facilitate navigation across different 5G-ENSURE topics, e.g. enablers, test bed and standardisation.

Future Newsletters

KPI: 6 newsletter, circulated on a monthly basis. The newsletters will focus on:

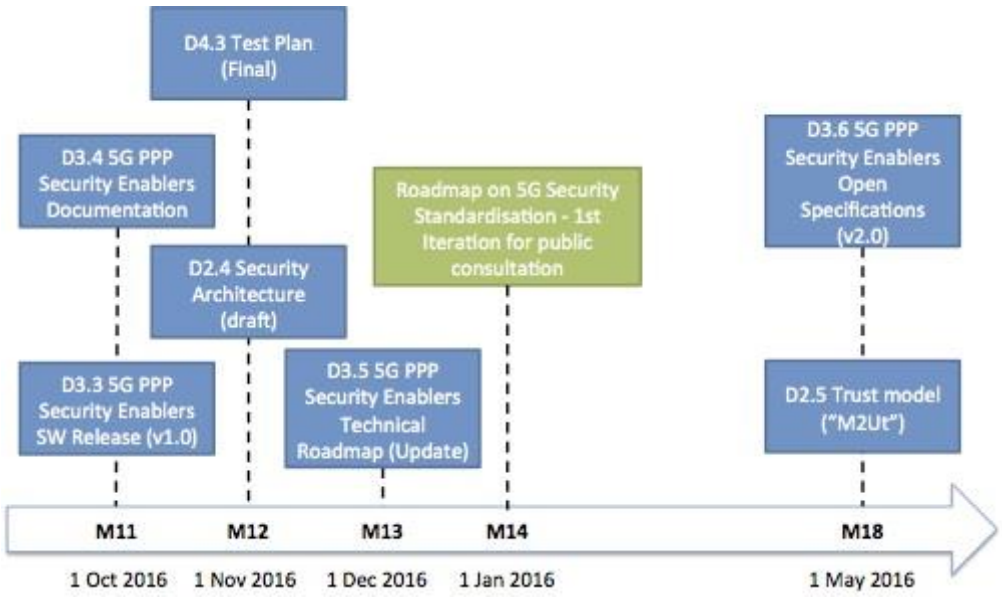
- Project outputs and opportunities for uptake.
- Project events as part of the 5G-ENSURE "On the Road" series.
- Outcomes of the 5G PPP Security Work Group, and contributions to other WGs.
- The first iteration of the Roadmap on 5G Security Standardisation, inviting subscribers to participate in the open consultation.
- International synergies, e.g. the PICASSO project.

Each newsletter will invite subscribers to join 5G-ENSURE on twitter and LinkedIn based on the weekly actions defined for the communications strategy.

7.5 Plan for Dissemination of Results

The figure below shows the plan for disseminating project results, outputs and standardisation efforts. The communication strategy will focus on current actions taken but to a wider pool of stakeholders.

Figure 29: Plan for Dissemination of 5G-ENSURE Results



7.6 Publications planned

During the second year of the project, the consortium plans to prepare and submit publications to present the scientific achievements. A list of initial targets has been already defined with venues focusing on security aspects of 5G networks, trust and privacy issues at large, and SDN. For instance, within the scope of the 5G-ENSURE are the annual conferences IFIP SEC International Conference on ICT Systems Security and Privacy Protection, 5G Global Conference, 5G World Summit, IEEE International Conference on Trust, Security and Privacy in Computing and Communications, and the ACM Conference on Security and Privacy in Wireless and Mobile Networks.

Publications will target the 5G-ENSURE security enablers, including threat analysis and potentially the validation of the enablers on the test bed, the 5G security architecture, the trust model and risk management model.

Open access publication will be encouraged and accepted papers will be advertised on the project website, including a link to the document and the Document Information Object (DOI) number.

7.7 2nd 5G-ENSURE International Workshop on 5G Security Standardisation and Open Consultation on Roadmap

5G-ENSURE has recently produced a new brochure on 5G security standardisation, drawing on the updated analysis in this report. This brochure will be one of the means of drawing attention to 5G-ENSURE standardisation efforts within the global landscape, notably amongst the 5G PPP projects to identify the potential for further co-operation.

Figure 30: New 5G-ENSURE Standardisation Brochure

The brochure also provides the basis for the first iteration of the 5G-ENSURE Roadmap on 5G Security, the first iteration of which is planned for January-February 2017. The plan for producing the Roadmap includes:

- Sharing a first draft with members of the consortium and the AB for feedback and inputs. This includes interviews with the chairs of ETSI TC CYBER and ETSI ISG NFV, and also Chair of SA3.
- Sending personalised messages to the representatives of standards bodies on LinkedIn, inviting them to give feedback on the revised draft.
- Creating the open consultation questionnaire and requesting feedback, particularly from the Security WG, and the PRE-Standardardization WG.
- Promoting the open consultation to the 5G PPP, selected Twitter followers and LinkedIn connections, with contacts also selected from the project database.
- Consortium agreement on content of the 1st iteration.
- Promotional campaign, including distribution of the roadmap with integrated relevant findings from the public consultation at external events and at the 2nd International Workshop on 5G Security Standardisation.
- Raising awareness amongst EC, national and international policy makers involved in 5G programmes.

While the 2nd International Workshop on 5G Security Standardisation will take place in late spring 2017, its planning and organisation will start in early 2017. Key actions include:

- Concept paper to select the date and venue based on an analysis of pros and cons, and avoiding collision with main Standardisation events (e.g. 3GPP meetings).
- Set up of the web page and registration form.

- Agenda development and speaker/panellist/chair management.
- Promotional plan and engagement through social media channels, the 5G PPP COMMS and the telecom media, including post-event activities.
- Production of promotional material for distribution at events.

5G-ENSURE will leverage its growing community to encourage participation at the event.

8 References

[1] 5G-ENSURE. Industry panel at CeBIT 2016 calls for collaboration on 5G Security and Privacy URL: http://5gensure.eu/node/630 (Last access on October 31, 2016).

[2] 5G-ENSURE Grant Agreement, p. 175.

[3] 5G Service Roadmap 2022, 5G White Paper, 5G Forum, March 2016. http://kani.or.kr/5g/whitepaper/5G%20Service%20Roadmap%202022.pdf

[4] http://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/Pages/default.aspx (Last access on October 31, 2016).

[5] http://www.cept.org/ecc/groups/ecc/ecc-pt1/client/introduction/ (Last access on October 31, 2016).

[6] https://www.enisa.europa.eu/ (Last access on October 31, 2016).

[7] http://www.5g-xhaul-project.eu/ (Last access on October 31, 2016).

[8] https://5gnorma.5G PPP.eu/, @5G_NORMA. (Last access on October 31, 2016).

[9] http://www.ict-coherent.eu/ (Last access on October 31, 2016).

[10]http://fantastic5g.eu/, @FANTASTIC5G (Last access on October 31, 2016).

[11]http://www.flex5gware.eu/ (Last access on October 31, 2016).

[12]https://5G PPP.eu/metis-ii/, @metis2020 (Last access on October 31, 2016).

[13]https://5g-mmmagic.eu/ (Last access on October 31, 2016).

[14]http://www.charisma5g.eu/, @charisma5G (Last access on October 31, 2016).

[15]https://speed-5g.eu/, @SPEED_5G (Last access on October 31, 2016).

[16]http://5g-crosshaul.eu/ (Last access on October 31, 2016).

[17]http://www.5gex.eu/ (Last access on October 31, 2016).

[18]http://www.cognet.5G PPP.eu/, @5GPPPCogNet (Last access on October 31, 2016).

[19]http://www.sesame-h2020-5G PPP.eu/, @Sesame_H2020 (Last access on October 31, 2016).

[20]https://selfnet-5g.eu/ (Last access on October 31, 2016).

[21]http://www.sonata-nfv.eu/, @sonataNFV (Last access on October 31, 2016).

[22]http://superfluidity.eu/, @Superfluidity5g (Last access on October 31, 2016).

[23]http://www.virtuwind.eu/ (Last access on October 31, 2016).

[24]http://www.3gpp.org/ (Last access on October 31, 2016).

[25]http://www.etsi.org/ (Last access on October 31, 2016).

[26]http://www.itu.int (Last access on October 31, 2016).

[27]http://www.gsma.com/ (Last access on October 31, 2016).

[28]https://www.ngmn.org/home.html (Last access on October 31, 2016).

[29]http://www.3gpp.org/specifications-groups/ran-plenary (Last access on October 31, 2016).

[30]http://www.3gpp.org/specifications-groups/25-sa (Last access on October 31, 2016).

[31]http://www.3gpp.org/specifications-groups/28-rubrique34 (Last access on October 31, 2016).

[32]http://www.3gpp.org/DynaReport/33899.htm (Last access on October 31, 2016).

[33]New Services and Markets Technology Enablers" (SMARTER), http://www.3gpp.org/DynaReport/22891.htm (Last access on October 31, 2016).

[34]http://www.4gamericas.org/en/resources/technology-education/5g/ (Last access on October 31, 2016).

[35]http://www.imt-2020.cn/en/introduction (Last access on October 31, 2016).

[36]http://www.5gforum.org/#!eng/cvb1 (Last access on October 31, 2016).

[37] ITU-T Report on Standards Gap Analysis. http://www.itu.int/en/ITU-T/focusgroups/imt-2020/Documents/T13-SG13-151130-TD-PLEN-0208!!MSW-E.docx

[38]http://www.itu.int/en/ITU-T/studygroups/2013-2016/13/Pages/default.aspx (Last access on October 31, 2016).

[39]https://www.ietf.org/ (Last access on October 31, 2016).

[40]https://tools.ietf.org/html/rfc7540 (Last access on October 31, 2016).

[41]https://datatracker.ietf.org/doc/draft-ietf-httpbis-http2-encryption/?include_text=1 (Last access on October 31, 2016).

[42]https://datatracker.ietf.org/doc/draft-ietf-tls-tls13/ (Last access on October 31, 2016).

[43]https://datatracker.ietf.org/wg/quic/charter/ (Last access on October 31, 2016).

[44]https://tools.ietf.org/html/draft-raza-6lo-ipsec-04. Other relevant references for the IETF in chronological order include: https://tools.ietf.org/html/draft-selander-ace-object-security 29 June 2015; https://tools.ietf.org/html/draft-hartke-core-e2e-security-reqs-00, 19 March 2016; https://tools.ietf.org/html/draft-aks-lwig-crypto-sensors-00, October 7, 2015; https://tools.ietf.org/html/draft-selander-ace-cose-ecdhe-01, April 12, 2016.

[45]https://datatracker.ietf.org/doc/draft-aura-eap-noob/ (Last access on October 31, 2016).

[46]https://www.ieee.org/index.html (Last access on October 31, 2016).

[47]https://standards.ieee.org/develop/project/802E.html (Last access on October 31, 2016).

[48]http://www.ngmn.org/5g-white-paper.html (Last access on October 31, 2016).