Deliverable D5.2
First report on communication, marketing and standardisation

Project name	5G Enablers for Network and System Security and Resilience	
Short name	5G-ENSURE	
Grant agreement	671562	
Call	H2020-ICT-2014-2	
Delivery date	30 April 2016	
Dissemination Level:	Public	
Lead beneficiary	Trust-IT	Stephanie Parker, s.parker@trust-itservices.com
Authors	Trust-IT: Stephanie Parker, Roberto G. Cascella, and Silvana Muscella TIIT: Luciana Costa and Paolo de Lutiis Ericsson: Bengt Sahlin, Kazi Wali Ullah, and Vesa Lehtovirta ALBLF[1]: Hong-Yon Lach	

[1] Nokia Bell Labs since Jan 14, 2016

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.

The purpose of this deliverable is to provide the first report on communication, marketing and standardisation as core activities within WP5. It provides a detailed analysis of the standardisation landscape, including on-going and planned work of particular relevance to 5G-ENSURE. It sets out an initial set of KPIs (for communications and marketing) and qualitative metrics against which to measure the impact and relevance of 5G-ENSURE. It also reports on the outcomes of the first six-monthly plan across four key activities: communication and community building, standardisation, joint activities with the 5G-PPP and the dissemination of results.

We identify and prioritise stakeholder engagement in the first year of the project, providing tangible evidence of relations established with peer projects, the media and policy decision makers, as well as targeted actions at events. We detail the strategy for the 1st International Workshop on Standardisation in June 2016, which will lead to the first iteration of a standards roadmap, as well as the imminent public consultation with the diverse stakeholders to collect and analyse their perspectives and priorities in relation to 5G security. Finally, we set out plans for the next six months.

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.

The first WP5 report focused on the Web platform as an interface with the umbrella 5G-PPP platform (D5.1). D5.2 – First Report on communication, marketing and standardisation – marks an important first step in documenting the impact of related activities to date (November 2015 to April 2016) and in ensuring partner "sign-off" on the plans and targets for the next six months (May to October 2016).

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

"*5G will be the most critical building block of digital society*", Günther Oettinger, Commissioner – Digital Economy and Society, a twitter follower of 5G-ENSURE.

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 D5.2 is to report on the results and impacts of actions performed during the first months of the project, specifically related to the period from November 2015 to April 2016, including joint activities at the programme level, and the planning of new actions on a 6-month basis. This report also defines the Key Performance Indicators (KPI) and qualitative metrics for WP5 which have been identified to monitor the efficacy of the dissemination activity. Finally the plans and targets for the next period from May to October 2016 is indicated.

Structure of this report

Section 2 focuses on the strategy for Communication, Marketing, and Standardisation, defining the overall goals, the plan for the first six months of WP5 activity. This section also provides the KPIs and metrics against which current and future actions will be measured.

Section 3 deals with stakeholder mapping and engagement planning with regard to the primary and secondary stakeholders of 5G-ENSURE based on a joint mapping exercise at the 5G-PPP programme level.

Section 4 provides a detailed analysis of the current standardisation landscape, the bodies involved, on-going and future activities planned, indicating the most relevant ones within the life-cycle of 5G-ENSURE.

Section 5 is dedicated to the actions taken in the first six months of the project and the impact achieved, including media visibility and initial community building and awareness-raising.

Section 6 outlines engagement with the different stakeholders that has taken place at events, indicating the focus and impact.

Section 7 provides the plan and targets for the period May to October 2016, including the project's First International Workshop on Standardisation.

Section 8 concludes the report.

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 activities of the 5G-PPP, 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 (p. 175). 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. Also modern social media techniques like twitter.
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:

1. Ensure a continuous stream of activities around the project and
2. 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 [2] and internationally.
- Share 5G-PPP achievements, events/webinars etc., and publications.
- Ensure visibility at relevant stakeholder events, including joint 5G-PPP activities such as shared stands, workshops, roundtables and webinars.

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, where knowledge exchange also feeds into the international conferences, the two 5G-ENSURE Workshops and liaison at the 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 [3], 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.

WP5 will host two international workshops on standardisation. The goals of the workshops are to disseminate the standardisation activities, interact with companies, large and small, and offer a springboard for feedback and future steps. The workshops and activities around them are a key element for building consensus on standards from the very start of the project and beyond its funding cycle.

Workshop 1: 16 June 2016, Sophia Antipolis (FR) in conjunction with ETSI Security Week

Objectives: exchange perspectives on the 5G-ENSURE Open Consultation and the Security Work Group (WG) within the 5G-PPP, with the involvement of relevant standards organisations. Its focus is on taking

stock of progress on early standardisation efforts, identifying gaps, defining potential contributions to the evolved edition of the cyber security framework introduce strategies around implementation and further developments to the framework.

Objectives: report on progress of the Open Consultation, Security WG and the levels and types of consensus reached through the involvement of all relevant stakeholders.

Output → Road map for international co-operation on 5G standardisation (1st iteration)

Workshop 2: in April 2017 (M18) with location to be confirmed based on 2017 calendar of relevant events, possibly in collaboration with the EC on EU workshops related to 5G or within a 5G-PPP focused event to report on progress of the Open Consultation, Security Work Group and the levels and types of consensus reached. Its aim is to contribute to road mapping activities both at the 5G-PPP programme level and internationally.

Output → Road map for international co-operation on 5G standardisation, covering security and privacy, as well as best practices around trust models. Consensus on Calls for Actions related to future 5G-PPP projects for the 2020 goal line (2nd iteration). First Plan for Communication, Marketing and Standardisation

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.

Below we provide the plans covering the period November 2015 to January 2016 and February to April 2016.

Table 1: 5G-ENSURE Plan for November 2015 to January 2016

Communication & community	Standardisation	Joint 5G-PPP activities	Dissemination of outputs

5G-ENSURE - Monthly checklist	November to January 2016		
Action	**M1 November 2015**	**M2 December 2015**	**M3 January 2016**
Static web page	Launch of static website		
Website design & rollout		**Technical specifications & development**	Achieved - D5.1
Website content	Core project information & press release		22 items
Twitter posts	35 posts	38 posts	46 posts
PR/Media Content	Creation of Media Channel database	5G-ENSURE Launch PR	
PR/Media Content			Monitoring of media visibility
Communication Material (print & web)	1st 5G-ENSURE flier		
LinkedIn Profile & Updates	DB of twitter handles & key initial targets	DB of twitter handles & key initial targets	DB of twitter handles & key initial targets
Notes on related activities	**WP5 Flash Report (Trust-IT)**	**Media coverage report & WP5 Flash Report.**	**D5.1 Submission. Media coverage report. QR 1 - WP5 (D1.2) and WP5 Flashreport**

Table 2: 5G-ENSURE Plan for February to April 2016

Communication & community	Standardisation	Joint 5G-PPP activities	Dissemination of outputs

5G-ENSURE - Monthly checklist	November to April 2016		
Action	**M4 February 2016**	**M5 March 2016**	**M6 April 2016**
Website content	11 items	8 items	8 items
Dissemination of Outputs & Results		Publication & promotion of D2.1 & D3.1	Publication & promotion of D4.1 (5G security testbed architecture)* possible delay to next quarter
Stakeholder Identification & Mapping	Stakeholder Mapping for 5G-PPP		
Twitter posts	77 posts	58 posts	min. 30
PR/Media Content			Article for European 5G Annual Journal
PR/Media Content	Monitoring of media visibility	Monitoring of media visibility	Inside 5G article
Communication Material (print & web)			Poster for ETSI Summit
Communication Material (print & web)			Web, twitter & LinkedIn banners on the 1st Int. WS
Communication Material (print & web)			Bookmark on the workshop & open consultation
Event	Mobile World Congress - 5G-PPP White Paper & Press Conference	B-COM/ETSI Workshop	NetWorld2020
Event	Mobile World Congress - industry trends & national initiatives	CeBIT 2016 - Oettinger keynote & industry panel on 5G	Net Futures 2016 - Concertation Meeting
Event			SICS Open House - poster
Event			ETSI Summit on 5G
LinkedIn Profile & Updates	DB of twitter handles & key initial targets	Creation of texts for the 5G-ENSURE profile	Launch of LinkedIn with updated profile & achievements to date
Linkedin blog posts			Min. 2 Blog posts on project
In-house newsletter tool dev.		**Achieved**	
Newsletter			Core messages to Stakeholders (industry & standardisation groups)
Liaison on Standardisation		3GPPRAN#71 - security requirements	Open Consultation
Liaison on Standardisation		3GPPSA#71 - Approval of the SID on "Architecture and Security for next Generation System"	
Notes on related activities	**WP5 Flash Report (Trust-IT)**	**WP5 Flash Report (Trust-IT)**	**D5.2 Submission. D1.3 Quarterly Management Report (WP5 - TIIT). D1.4 Progress report to Steering Committee (WP5 - TIIT). WP5 Flash Report (Trust-IT)**

2.3 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), allowing for target adjustments and new KPIs to be added over time depending on a more thorough assessment of outcomes.

Table 3: KPIs for Communication and Marketing

Communication & community	Standardisation	Joint 5G-PPP activities	Dissemination of outputs

5G-ENSURE - Community KPIs					
KPI	**Target EoP**	**Delta**	**Total to date**	**QR1: Nov 2015 - Jan 2016**	**QR2: Feb - April 2016**
Twitter followers	300	131	169	84	80
Community DB for LinkedIn	800	580	210	113	97
PR/media content	4	2	2	**1**	1
Media coverage & visibility	15	6	9	**6**	3
Open consultation respondents	50	pending			
Events - standardisation/5G security (excl. project workshops)	6	4	2	0	2
Events - 5G-PPP Joint activities (incl. Project workshops)	8	6		0	2
Technical conferences and papers	8	6	2	1	1
Publications: joint 5G-PPP	2	1	1	0	1
LinkedIn Connections	350	348	2	0	2
LinkedIn Updates	36	34	2	0	2
LinkedIn Updates counted on monthly basis, min. 2/month					

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. A similar analysis being made for the community, including Twitter followers and LinkedIn connections.

QM2: Readership of journals where technical articles are published, such as reputation, readership and geographies.

QM3: Workshops – Matching actual participants with the stakeholder targets.

QM4: Workshops – gauging consensus of participants and the level of interest, e.g. passive and active supporters; passive and active opponents; fence-sitters.

QM5: External events, assessing the audiences actually reached at commercial and technical events, influential participants, new contacts and main takeaways.

QM6: Standardisation roadmap (2 iterations) – quality of contributions, types of endorsements, as well as circulation and visibility.

3 5G-ENSURE Stakeholder Mapping and Engagement Planning

5G-ENSURE target audiences include primary stakeholders with engagement commencing at the start of the project and secondary, long-term stakeholders. The primary stakeholders span the 5G-PPP phase 1 projects and Euro-5G [4] as the main coordination and support action, standards bodies, regulators, policy makers and telecommunications media channels. Secondary targets include the telecommunications industry and its supply chains, IT companies, including SMEs and start-ups that need to keep abreast of 5G developments, and a specific set of verticals and industry forums where 5G security and early contribution to standardisation are particularly relevant.

A common activity at the 5G-PPP programme level has been to share information on stakeholders targeted, including potential new stakeholders, as illustrated in the Figure 1 (Common target stakeholders as defined by the 5G PPP map, 02/2016).

This activitity will facilitate cross-fertilisation across the 5G-PPP projects and Euro-5G.

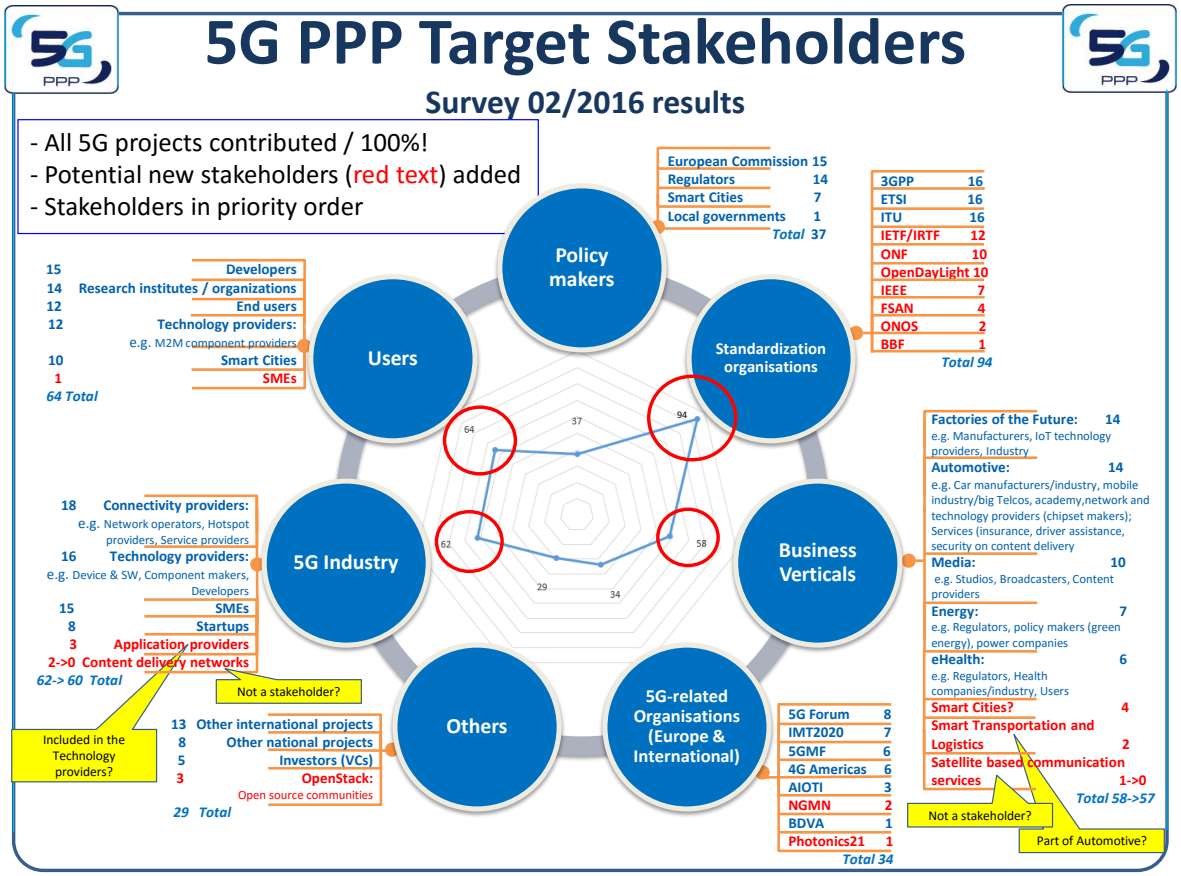


Figure 1: Positioning 5G-ENSURE Stakeholders across the 5G-PPP

3.1 Primary Stakeholder Engagement Plan

Main Motivations for Engagement with Peer 5G-PPP Projects in Phase 1

5G-ENSURE is the reference project for 5G security, privacy and trust for the 5G-PPP. It will contributing at the programme level with:

- A 5G security architecture to expand mobile ecosystem and enable entirely new business opportunities across the European economy and beyond.
- Non-intrusive security enablers for the core of the 5G Reference Architecture.
- A set of use cases to show integration with the security enablers and derive requirements.
- 5G security test bed to demonstrate the security enablers.
- Trust Model to help overcome a major challenge on moving to 5G, by working closely with partners involved in WP2 – Security requirements and architecture and WP3 – Security Enablers for 5G, and promoted under WP5.

Engagement with 5G-PPP Work Groups

WP5 places emphasis on prioritising timely contributions to standardisation and sharing knowledge across the 5G-PPP and relevant Work Groups [5].

Engagement will include participation at the 5G-ENSURE Workshops on International Standards in June 2016 and April 2017 respectively, as well as to the Public Consultations on 5G Security. The WGs will also be invited to provide feedback on the consultations prior to their circulation and links will be created between 5G-PPP outputs and relevant feedback from the 5G-ENSURE advisory board.

- 5G-ENSURE leadership of **Security Work Group** within the 5G-PPP. The purpose of this WG is bring together 5G-PPP projects with a common interest in developing and advancing aspects related to security, minimising duplication of effort, contributing to relevant standards and co-operating on the development of compatible components etc.
- Contributions to the **Pre-Standardisation Work Group** within the 5G-PPP. The purpose of this Work Group is to identify standardisation work and regulatory bodies to align with relevant standards bodies, and develop a road map for 5G within the 5G-PPP, which is aligned at international level. Its focus is also on influencing pre-standardisation on 5G and related research and innovation.
- Contributions to the **Vision and Societal Challlenges Work Group** within the 5G-PPP. The purpose of this WG is to build consensus in Europe on 5G systems, infrastructures and services. The WG is also identifying vertical application domain and related challenges and requirements, as well as the social, economic, environment, business and technological benefits of realising the main 5G concepts. It also prepares input documents for pre-standardisation and the spectrum work groups, taking on board international co-operation activities. Its ultimate goal is to develop Horizon 2020 call proposals for 5G-PPP in partnership with the EC.
- Contributions to the **Architecture Work Group** within the 5G-PPP. The purpose of this WG is to serve as a common platform for discussions on architectural concepts and components, also based on the KPIs described in the 5G-PPP contract. It also explores the potential to facilitate consensus building on 5G architecture. Important for 5G-ENSURE is the role of a security architecture to expand the mobile ecosystem and enable entirely new business opportunities.
- Contributions to **Network management, QoS and Security Work Group** within the 5G-PPP. The focus on network security is on the overall resilience of the network to fraud and instrusion or efforts to undermine the operations or integrity of the network. The focus on security is at the level of the control planes of the network.
- Contributions to **SDN / NDF Work Group** within the 5G-PPP. The purpose of this WG is to analyse and address unification and applicability of key research topics related to Software Networking including software defined concepts, infrastructures, systems and components for

Wire and- Wireless Networks, including Networked Clouds, IoT and Services, i.e. Software Defined Networks (SDN) and Network Function Virtualization (NFV) as developed and promoted by the 5G PPP projects.

- Contributions to **5G-PPP cross-project collaboration** (led by METIS-II) on use cases, requirements and performance evaluation.

The table below provides examples of stakeholder engagement with 5G-PPP projects.

Table 4: Engagement Plan for 5G-PPP

5G-PPP Projects	Stakeholder Engagement Plan
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. Support on WG liaison, promotion and outcomes. Publications and coordination of 5G-PPP project contributions. Press conferences. Newsletters.	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.
Radio technology projects: 5G-XHaul [6], 5G-NORMA [7], COHERENT [8], FANTASTIC-5G [9], Flex5Gware [10], METIS-II [11], mmMAGIC [12], CHARISMA [13], SPEED-5G [14] **Network technology projects:** 5G-Crosshaul [15], 5GEx [16], CogNet [17], SESAME [18], SELFNET [19], SONATA [20], Superfluidity [21], VirtuWind [22]	Timely contributions to standards bodies: focus on ETSI [23] and 3GPP [24] (Within the scope of the Pre-standardisation Work Group) Joint events/sessions: Workshop proposal for EuCNC (European Conference on Networks and Communications) [25] Joint publications, including White papers on 5G architecture for 5G Summit; White paper on network management; White paper on verticals and 5G Public consultation on security: feedback and inputs through the Security WG & participation to the 5G-ENSURE online consultation.

Main Motivations for Engagement with Regulators and Policy Makers

- Monitoring the latest regulations expected to impact on the definition of the security enablers.
- Aligning relevant use cases and scientific results of the project with the national, industrial, European regulations.
- Liaison with relevant 5G-PPP WGs will enable 5G-ENSURE to align its strategy with the priorities set by the funding agencies for future work programmes within H2020, including international perspectives (e.g. links with Brazil and the U.S.), including contributions to future programmes.

Regulators targeted: ITU, Working Party 5D – IMT systems (WP5D) [26], ECC, ECC Project Team 1 (ECC PT1) [27] 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 [28], national and European legislators.
Stakeholder Engagement Plan
Participating in policy and regulatory events. Demonstration of role as a reference project for 5G security. Contributing with cutting-edge solutions to the European leadership in 5G and in related market sectors through demos, event presentations, papers and policy briefings. Contributions to policy studies, e.g. ENISA, with expertise on aspects related to security, privacy and trust models. Awareness raising to the stakeholders affected by regulatory changes. Promotion of best practices and data protection laws coming from the definition of use cases and security enablers.

Main motivations for engagement with telecommunication Media Channels

- Maximise visibility of 5G-ENSURE across the telecommunications/network industry and supply chains.
- Support visibility of 5G-ENSURE through industry partners, including across social media channels.

Media channels targeted: TelecomTV, Inside5G, Mobile World, Telecoms.com, Total Telecom, Telecom News, Fierce Wireless Europe, Telecom Engine, Mind Commerce, RF Wireless World, Networking Plus, as well as major industry events, e.g. Mobile World Congress, CeBIT
Stakeholder Engagement Plan
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.

3.2 Secondary Stakeholder Engagement Plan

Existing mobile technologies will not be able to provide the capabilities to meet market demands beyond 2020. Already now communication networks are essential for all areas and sectors of our societies and economies. Today, the world's total mobile data volume is about 2 Exabyte/month and is estimated to

grow by a factor of ten until 2020. As such, fixed and mobile communication systems are continuously developing towards more capacity, higher throughput rates and improved Quality of Service (QoS) and Quality of Experience (QoE). These technology advances are however only part of what 5G is all about. 5G also brings in a convergence of various trends, e.g. , Cloud computing, IoT, etc., which are much more far reaching. Sustained research is needed to create a high performance 5G environment and unleash its full market potential.

The widespread introduction of mobile and wireless communication is providing access to global communication for a rapidly increasing number of users and devices, all of which helps emerging economies to grow and to improve the lives of their citizens. 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 [29].

It is expected that 5G network will be commercialised in 2020 and then replace the legacy network and services step by step. According to estimates by ETRI Industrial strategy research lab [30], 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.

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.

Main motivations for engagement with the business community, especially SMEs

Engagement with the business community and mainstream press is important to help communicate 5G in ways that are understandable by the audiences targeted. This outreach activity draws on experiences already gained in responding to questions about 5G, e.g. through twitter.

- Ensuring the business community is well prepared for 5G and the opportunities it brings in terms of business enablement.
- Raising awareness on security, privacy and trust as central to uptake.

Showcasing benefits for project business partners, including the key role of public-private collaborations.

Stakeholder Group	Stakeholder Engagement Plan
Businesses and telecom industry: end-users, SMEs, research institutes, developers, connectivity providers (Network operators, Hotspot providers), Service providers and Technology providers (Device & SW, Component makers, Developers).	Introduce a business oriented approach in 5G-ENSURE with direct impact on the telecom and business industry. Core activities: These groups will also be targeted through business associations and developer platforms. Demonstrate the relevance of 5G security enablers and provide specifications to implement trustworthy 5G services for the end-

	users.
Specific Business verticals targeted: Digital Health: Regulators, Health companies/industry, Users; Factories of the Future: Manufacturers, IoT technology providers, Industry; Automotive: Car manufacturers/industry, mobile industry/big telecoms, academy, network and technology providers (chipset makers); Services (insurance, driver assistance, security on content delivery); Smart cities; Satellite-based communications.	Define additional use cases and requirements for specific needs of the verticals. Gather feedback about the limitations of the current technology for these verticals, what are the security threats, and how the 5G=ENSURE enables enhanced services for their sectors. **Core activities:** Raise awareness about 5G-ENSURE outcomes through media channels and journalists. Promote the key value proposition of 5G-ENSURE and how the project will impact the business verticals. Demonstrate the need of 5G security via the use cases targeting specific business verticals.
SME Work Group, 5G-PPP: Help and support SMEs participation in the 5G PPP and more generally in EU R&D projects, including (but not limited to) reaching the target of at least 20% of the 5G PPP funding going to SMEs.	Contribute examples of 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.

Main motivations for engagement with IT and mainstream media channels

- 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.

Media channels targeted (multiple audiences): Computer Weekly, Tech Target, Business Insider, Inside Tech Europe, CloudPro, TechTankTalks, Business Europe, Disruptive Technology, Tech Week, Business Zone, national press, and IDC/IDG.
Stakeholder Engagement Plan
Production of articles for IT and mainstream channels, and increasingly in year 2,

4 Standardisation Landscape

4.1 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.

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.

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.

ETSI – European Telecommunications Standards Institute [29]**:** 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.

ITU-T - The ITU Telecommunication Standardization Sector [31]: 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.

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.

GSMA and NGMN Alliance: GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 250 companies in the broader mobile ecosystem [32]. 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 [33]. 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 5 are reported the actions which have been started within 3GPP where the project will focus in the short term.

Table 5: 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)

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 describe in detail the current plan of the main SDO/groups identified as the main target SDO/Groups for the first year of the 5G-ENSURE standardisation activities.

4.2 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 four Technical Specification Groups (TSG):

1. Radio Access Networks (RAN) [34] - a technology that connects individual devices to other parts of a network through radio connections.
2. Service & Systems Aspects (SA) [35] – architecture and capabilities of systems.

3. Core Network & Terminals (CT) [36].
4. GSM EDGE Radio Access networks (GERAN) [37] - GERAN is the radio part of GSM/EDGE together with the network that joins the base stations (the Ater and Abis interfaces) and the base station controllers, e.g.A interfaces, etc.

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

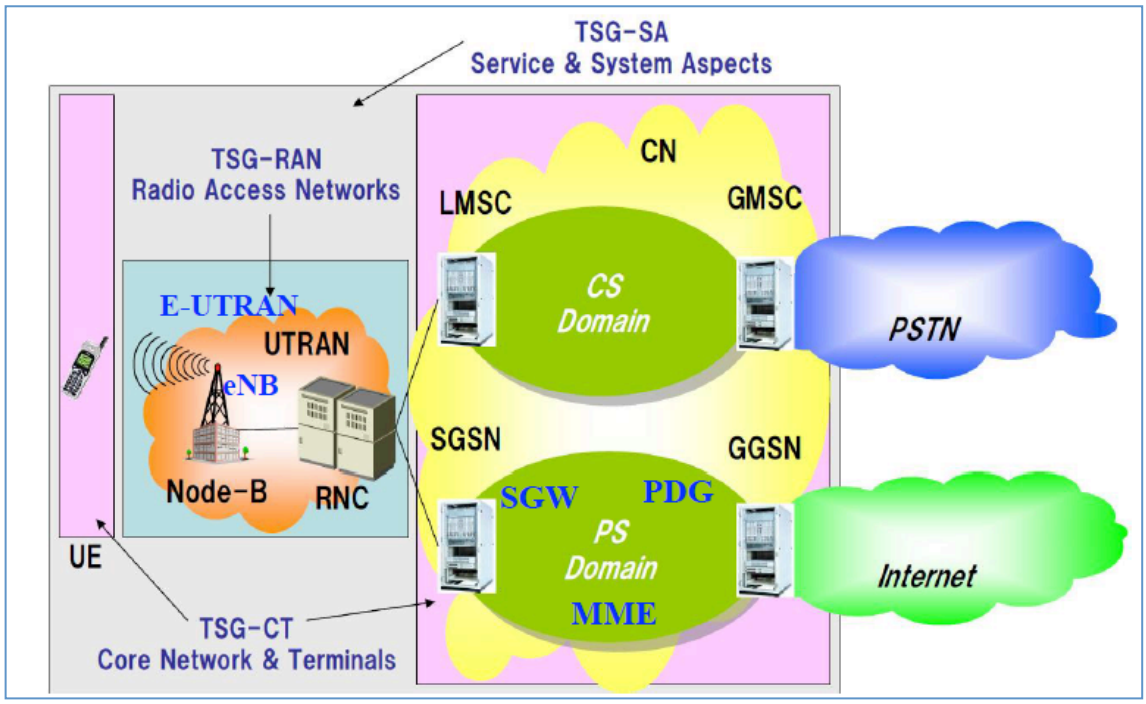


Figure 2: Scope of the TSG

Each TSG has Working Groups that are responsible for developing reports and specifications, which define the Cellular Phone System. These groups are showed below.

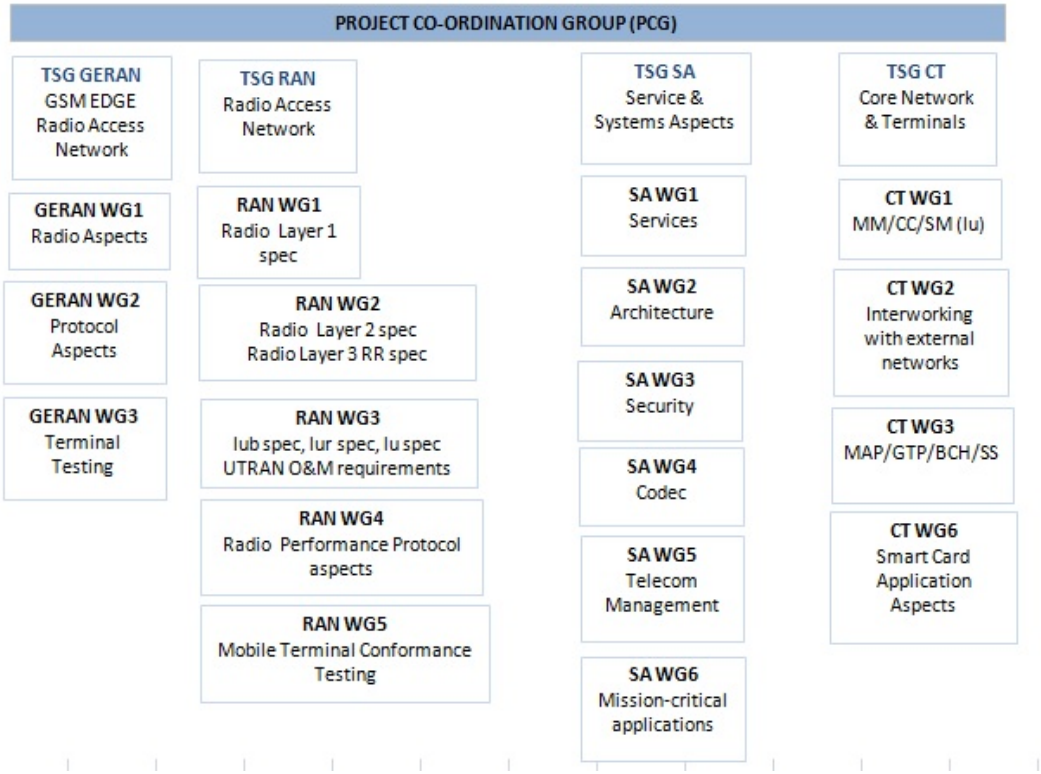


Figure 3: 3GPP Technical Specification Groups

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) [38], 3GPP discussed and endorsed the main 5G milestones. The following high level milestones were agreed to comply with the ITU-R IMT-2020 process constraints:

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

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

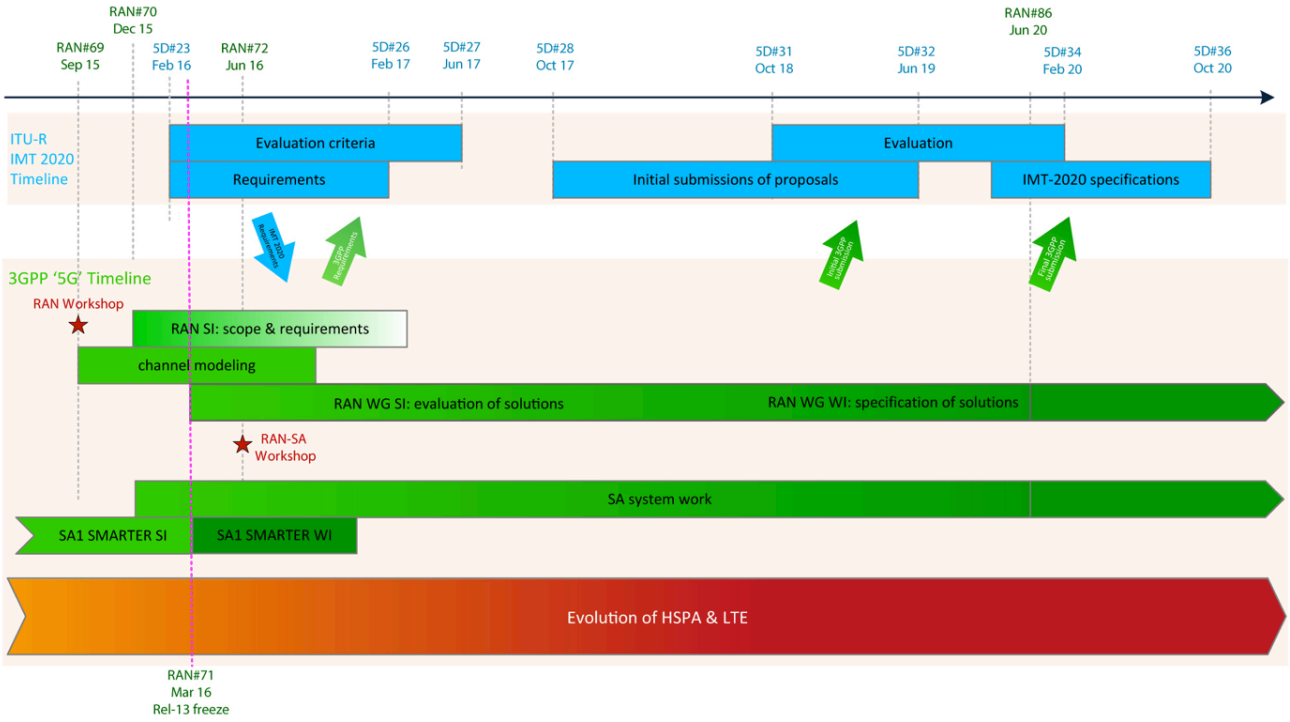


Figure 4: Initial 3GPP 5G Timeline (Source: [39])

4.2.1 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 project is "New Services and Markets Technology Enablers", a.k.a. SMARTER [40].

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 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 [41], Chinese IMT-2020 (5G) Promotion Association [42], ITU-R WP5Ds, 5G Forum [43], 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 [44]). 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 time of writing this report, 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.

A second phase of SMARTER will start with the selection of a few other use cases from TR 22.891 [44] to be further developed within SID to form new, detailed, TRs.

Each Phase of SMARTER needs to be compatible and consistent with the previous Phase.

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 Operator's proposal of maintaining the dedicated physical secured and tamper resistant entity (UICC) controlled and managed by mobile operator, and the Vendor's 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 [3].

4.2.2 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 [45]). 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 [46]) 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 draft of the TR 38.913 [45] already contains some high level security requirements proposals to take into consideration for the design of the radio access.

4.2.3 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" [47] with the objective of designing the system architecture for the next generation mobile network. The security aspects are not part of the objectives because they should be addressed by SA3.

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.

4.2.4 Security Aspects (SA3)

SA3 is the main target group for the standardisation actions within the 5G-ENSURE project, at least for the first year of activities, 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 [48]:

"*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#87 meeting in March 2016 the opening of a new SI dedicated to the security aspects of the 5G was agreed. Such a SI (TR 33.899 [49]), 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.

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.

4.2.5 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. This should be evaluated if the first set of selected use cases have a mapping with the use cases defined within the project.
- Within SA1, SMARTER TR 22.891 [40] (and the new SMARTER branches), add new use cases identified by 5G-ENSURE that are not already covered by the TR.
- Within SA2, it is important to take into consideration the evolution of the TR 23.799 [47], 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. Moreover 5G-ENSURE has to monitor also the results of the joint workshop between RAN and SA (or the relevant WGs) foreseen in H2 2016.

- RAN also has to be taken into consideration. The current draft of TR 38.913 [45] 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.
- Finally SA3, the 3GPP security group, with its new SI on Study on the Security Aspects of the Next Generation System (TR 33.899 [49]) can potentially be the main target for 5G-ENSURE. All the main results of the project foreseen for 2016 (D2.1 on use cases [3], 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.

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

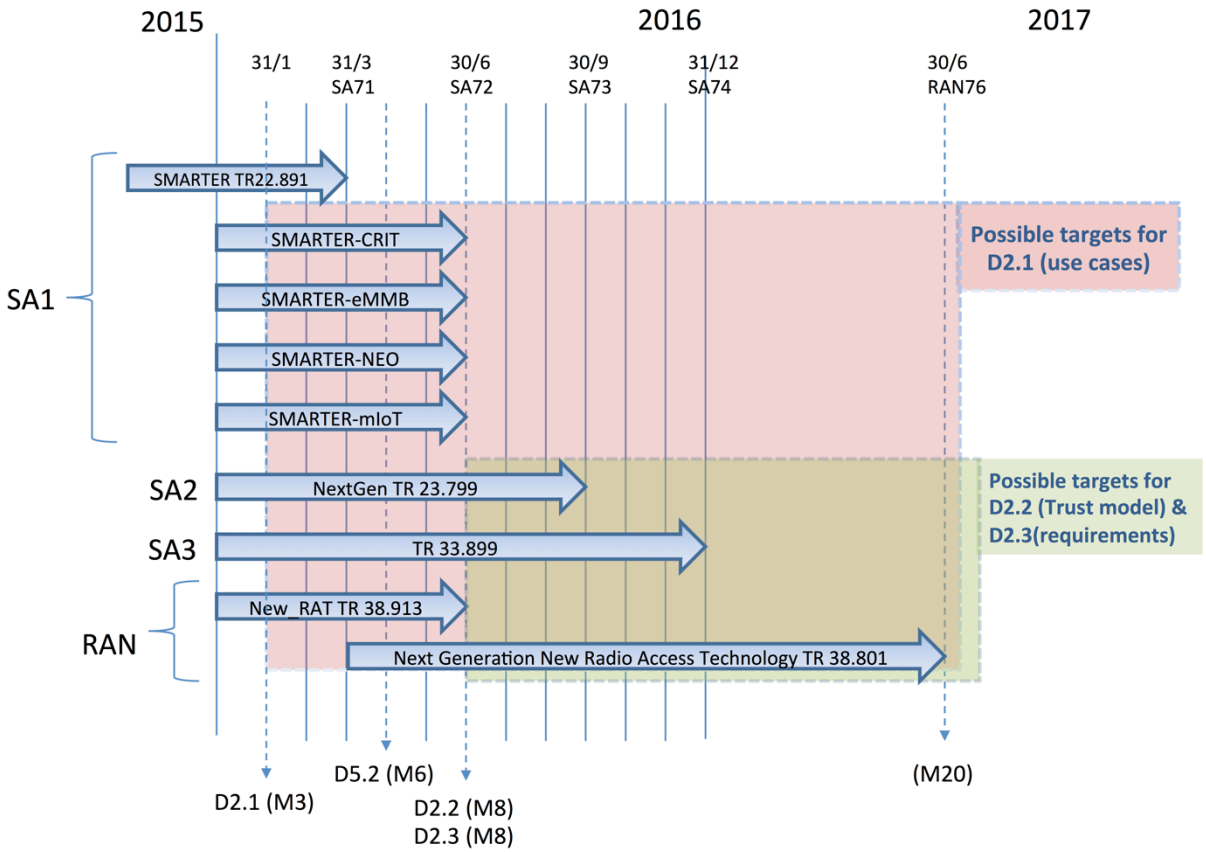


Figure 5: 3GPP GANTT 1

4.3 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.

4.3.1 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 can be the target group for at least some of the results of 5G-ENSURE. In particular, TC CYBER is active in the field of privacy aspects and security requirements for visualised environments. 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” [50]. 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).
- TR 103 370 “Practical introductory guide to privacy” [51]. 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.
- TS 103 485 “Mechanisms for privacy assurance and verification” [52]. 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.
- TS 103 486 “Identity management and naming schema protection mechanisms” [53]. 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.

- TS 103 487 “Baseline security requirements regarding sensitive functions for NFV and related platforms” [54]. The document defines security baseline requirements for sensitive functions including Lawful Interception (LI) and Data Retention (RD) in an NFV hardware/platform environment

4.3.2 ETSI ISG NFV

ETSI Industry Specification Group (ISG) for NFV is the home for developing requirements and specifications for NFV. 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 6.

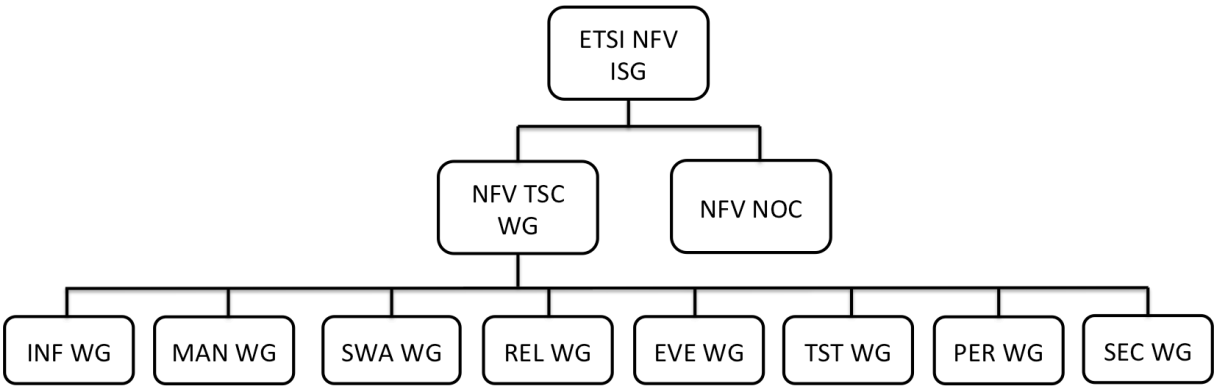


Figure 6: ETSI ISG NFV operational structure

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

4.3.3 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.

4.4 Threat Landscape

Figure 7 highlights the threat landscape for NFV deployments. The left hand side of the figure depicts the threats that are generated by using the virtualisation technology in general. Since NFV uses virtualisation at its core, the traditional virtualisation threats are also a concern for NFV deployments. At the same time, virtualisation mitigates some of the threats that are currently possible in physical device scenario. The right-hand side of the figure shows the generic networking threats. However, NFV SEC WG is mostly interested in threats that are specifically related to NFV when the virtualisation threats and traditional networking threats are combined. This is due to the fact that the generic virtualisation threats and the generic networking threats are already currently known and may be the solutions/best practices are readily available. However, the threats that are emerging by combining these two landscapes are quite new and require further study.

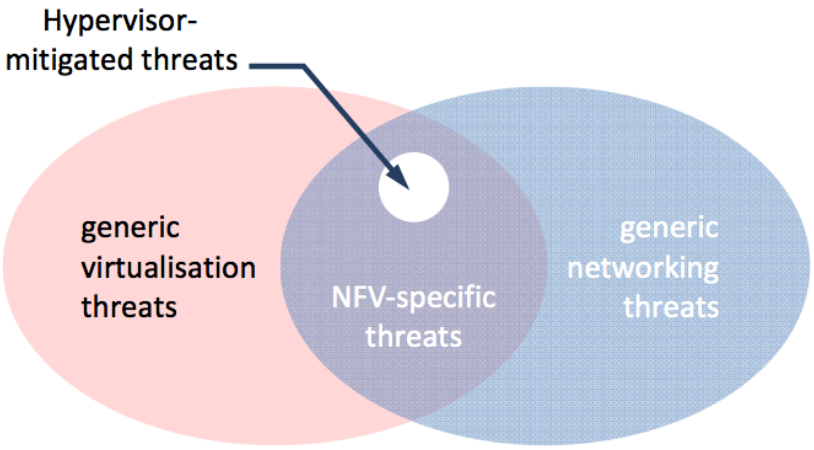


Figure 7: Visualisation of the NFV threat surface (Source: [55])

4.5 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.

4.6 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 [55].
- ETSI GS NFV-SEC 002: Cataloguing security features in management software [56].
- ETSI GS NFV-SEC 003: Security and Trust Guidance [57].
- ETSI GS NFV-SEC 004: Privacy and Regulation; Report on Lawful Interception implications [58].
- ETSI GS NFV-SEC 009: Report on use cases and technical approaches for multi-layer host administration [59].

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.

4.6.1 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. It will evaluate during the time of the project the opportunity to propose a specific Work Item about 5G privacy aspects. As part of the activities within the ETSI TC CYBER such proposal was already discussed during the last meeting (ETSI TC CYBER#6) in Sophia Antipolis (February 2016) . It is up to the project partners to evaluate and properly elaborate a specific proposal. Since at the present time most of the 5G-ENSURE effort will be dedicated to the 3GPP, it is expected that such a proposal could be elaborated not before the end of 2016.

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.

4.7 5G Time Line for ITU (IMT 2020)

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

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

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

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

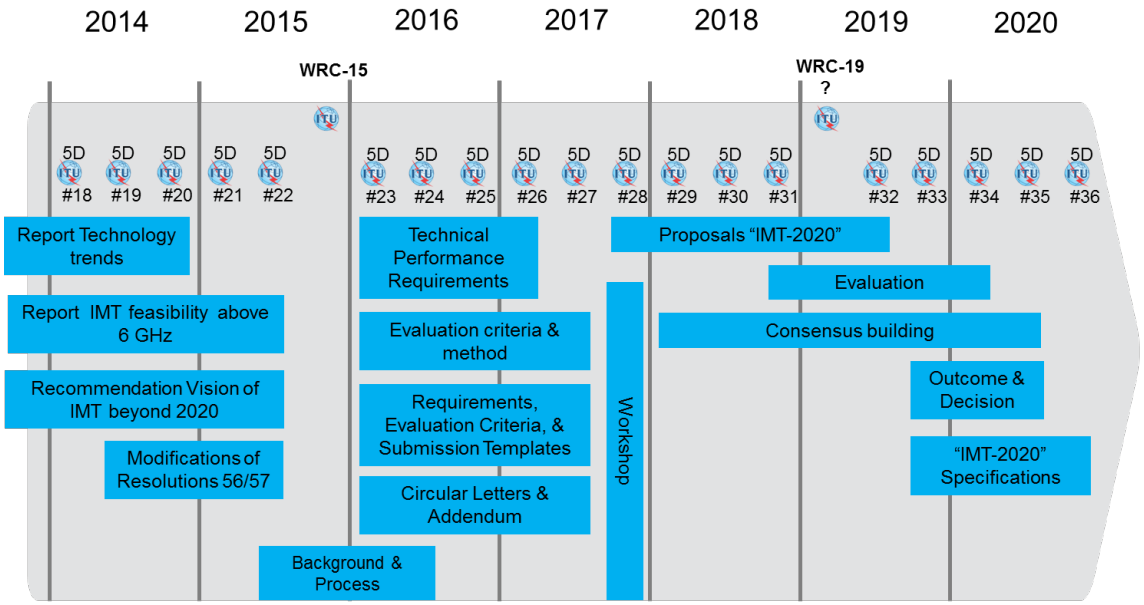


Figure 8: 5G Time Line for ITU (Source: [60])

4.7.1 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 [61] to its parent group, ITU-T Study Group 13 [62]. 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. 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.

4.8 IETF

The Internet Engineering Task Force (IETF) [63] 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) [64].

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 [65] (17 March 2016).

The IETF is also updating the TLS protocol (the latest draft is for TLS is v 1.3, 21 March 2016 [66]). 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.

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 [67]. 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 [68].

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.

4.8.1 5G-ENSURE opportunities in IETF

At the present time there are no specific opportunities for direct contributions for the 5G-ENSURE results, but a new assessment will be made in subsequent iterations of this deliverable.

4.9 IEEE

IEEE [69] 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” [70] 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.

4.9.1 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.

4.10 ONF

The Open Networking Foundation (ONF) [71] 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.

4.11 NIST

NIST [72] 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.

4.11.1 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.

Despite specific opportunities for international cooperation directly related to 5G-ENSURE have not been identified within NIST, discussions continue to update NIST about the progress of the project to align the activities on security topics and to evaluate possible collaboration.

4.12 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. It is a global partnership of 28 leading mobile operators as members, 34 leading technology vendors as sponsors, and 24 universities or research institutes as advisors. It drives global harmonisation and convergence of industrial standards and initiatives, by working on requirement levels and providing guidance to SDOs for standards development.

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

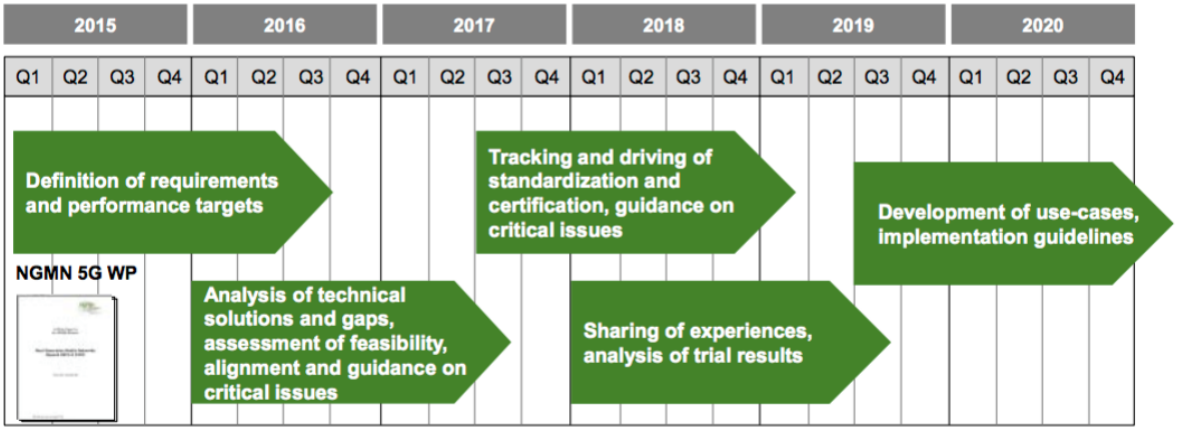


Figure 9: NGMN Role in 5G Development

Published in February 2015, the well-received NGMN 5G White Paper [73], 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.

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

- 5G requirements and design principles.
- Analysis of potential 5G solutions.

- Assessment of future use cases and business models.

Figure 10: NGMN 5G Work Programme

In particular, 5G security matters are addressed by the 5G Security group within P1 (Project 1) "Requirements & Architecture" WS1 (Work Stream 1) "Architecture". The NGMN P1 WS1 5G Security group is led by Orange and co-led by Vodafone. Its objective is to guide standardisation and implementation of 5G security features, based on but expanding as necessary, the security topics highlighted in the NGMN 5G White Paper covering, among others, radio architecture, virtualisation, privacy, availability and IoT.

The NGMN P1 WS1 5G Security group produces deliverables to identify 5G-specific security issues and provide recommendations to address them. For security issues that are relevant, but not specific to 5G, they will be captured in informal informative documents. The recommendations to address the identified security issues are intended to be high-level, avoiding too much detail and specifics, to allow appropriate solutions to be developed in the relevant SDOs.

The main challenge of the group in addressing the security issues is striking the balance across :

- Speculating on the overall 5G architecture, on which the security issues depend.
- Evolutionary versus revolutionary views of the 5G architecture and the associated backward-compatibility matters.
- Providing practical recommendations that do not confine solutions to known technologies to enable technological innovations in SDOs.

The first area addressed was virtualisation. Since all contributions are 5G-relevant but not 5G specific, in early March 2016 the group produced an informal informative document "Security Considerations for Virtualisation in 5G" (not publicly available at the time of writing this report).

Currently, the group intends to produce a deliverable in April 2016 to address security matters in the access network, including denial of service (DoS). It also aims to produce a deliverable towards end of April 2016 to address security issues in network slicing, with the hope of providing it as input for the ETSI NFV meeting in early May. Other areas will be prioritised and addressed afterwards.

4.12.1 5G-ENSURE opportunities in NGMN

The NGMN P1 WS1 5G Security group produces 5G security high-level requirements and recommendations. They could serve as insights for the 5G-ENSURE project in developing 5G security enablers.

5 Actions Taken & Impact Achieved

5.1 Joint Activities, Communications and Community Building

5.1.1 Joint 5G-PPP Communication Activities

Regular interaction with the 5G-PPP is ensured through a common mailing list for Communications (Comms@5g-ppp.eu) and Future Internet (all@future-internet.eu), a key tool used for sharing project updates, important announcements and upcoming events involving or of interest to the 5G community.

- Announcement on the launch of 5G-ENSURE and related press release.
- Creation of Telecommunication media channels database.
- Announcement on standardisation focus of 5G-ENSURE.
- Creation of 5G-PPP Community database.
- Promotion of the launch of the 5G-PPP white paper during the press conference at Mobile World Congress 2016 by Commissioner Günther Oettinger.
- Face-to-face interaction and knowledge sharing at events and workshops: detailed in Section 7.4.3.
- Creation of business network database.

5.1.2 Communication Actions

The communication measures for promoting the project and its findings are:

Press Release

- Production and circulation of press release on the launch of 5G-ENSURE in December 2015.
- Adaptation of the press release to cover also coordination of 5G initiatives in Finland.
- Translation of the project press release into Italian.
- Circulation of the press release by partners.
- Monitoring of press coverage.

5.1.3 Social media Channels

- Setting up of the 5G-ENSURE twitter account in September 2015 (Trust-IT).
    - Regular tweets posted since October 2015, gaining an average of 1 new follower/day (Trust-IT).
- Setting up of the 5G-ENSURE LinkedIn account.
    - Population and profile updates.

5.1.4 In-house Project Newsletter

The project has developed an in-house newsletter tool that is managed through the website. Monthly newsletters have the purpose to inform the target audiences on activities and results of the project. It will used also to attract any interested readers by a subscription to the 5G-ENSURE newsletter. The effectiveness of the newsletter in reaching its target audiences, like those for the website, will be closely

monitored by capturing the number of recipients and the level of response elicited by each edition. 5G-ENSURE will also contribute to the newsletters of other 5G-PPP projects wherever the opportunity arises.

5.1.5 Web content creation

The 5G-ENSURE website is online at the address http://www.5gensure.eu/ and it represent the first outcome of WP5, detained in D5.1 [74], which is used to communicate the project objectives and updates in the 5G and 5G-PPP context to the stakeholders targeted.

The table provides a sample of content creation published on the 5G-ENSURE website for our different stakeholders, grouped by the topic focus. The project website will be continuously updated to display the dissemination activity, either related to standardisation or to scientific publications.

Table 6: Sample of Web Content Creation

Topic Focus	**Links**
5G-ENSURE Outputs – Current suite of deliverables	Library (targeting 5G-PPP projects): http://www.5gensure.eu/deliverables *Tech Insights* - Non-technical news items on D2.1 and D3.1: http://www.5gensure.eu/news/5g-ensure-ouptut-early-vision-5g-ppp-security-enablers-technical-roadmap http://www.5gensure.eu/news/5g-ensure-ouput-use-cases
5G-ENSURE Outputs – Open Consultation	Online consultation with presentation of results at the 1st International Workshop in June 2016: http://5gensure.eu/open-consultation-survey
Standards – Progress on 3GPP IoT	Post on 3GPP outcomes by Anand R. Prasad, Advisory Board Member: http://www.5gensure.eu/news/progress-3gpp-iot
Events – partner hosted workshop for engagement with standards bodies	International Workshop RVM and Security for multi-RAT and reconfigurable systems (B-COM & ETSI): http://www.5gensure.eu/events/international-workshop-rvm-and-security-multi-rat-and-reconfigurable-systems
Events – engagement with standards bodies	ETSI Summit on 5G: http://www.5gensure.eu/events/5g-myth-reality
Policy Pulse – 5G-PPP outputs for policy makers	EC press conference at Mobile World Congress (Euro-5G): http://www.5gensure.eu/news/5g-ppp-media-analyst-event-mobile-world-congress-2016
Events – engagement with 5G-PPP and policy makers	Net Futures 2016: http://www.5gensure.eu/events/net-futures-2016-20-21-april-brussels
Events – engagement with 5G-	EuCNC 2016:

PPP technical constituencies	http://www.5gensure.eu/events/eucnc2016-27-30-june-athens
Market Insights - Industry event	Industry Keynote & Panel at CeBIT 2016 http://www.5gensure.eu/news/industry-panel-cebit-2016-calls-collaboration-5g-security-and-privacy
Tech Insights – partner 5G security activities	SICS survey on 5G security: http://www.5gensure.eu/news/sics-swedish-ict-releases-state-art-survey-5g-security-towards-secure-ubiquitous-mobile
Market Insights – partner corporate research	Research perspective on the Road to 5G: http://www.5gensure.eu/news/ericsson-research-blog-road-5g
Market Insights – about 5G, a popular topic on twitter	BBC video on 5G (filmed at Ericsson Research Lab): http://www.5gensure.eu/news/what-will-5g-devices-look

5.2 Standardisations and joint 5G-PPP engagement

5.2.1 Joint 5G-PPP Pre-Standard WG

Beyond the on-going activities in specific SDOs where 5G-ENSURE is represented by key partners, the project is also working in cooperation with the 5G PPP pre-standard workgroup. Together with the other projects under the 5G-PPP umbrella, 5G-ENSURE is contributing in the identification of standardisation bodies to align with the roadmap and work programme of such organisations.

The participation to 5G-PPP pre-standard WG permits to defines key stakeholder groups and initiatives with the aim of creating synergies, to increase knowledge exchange and to reinforce the standards message. The 5G-ENSURE project has been presented to the Pre-Standard WG illustrating the project's vision and activities. Contributions have been made for the message on standardisation at the MWC2016 by drawing attention to security and privacy aspects.

The 5G-ENSURE plan is to provide an Open Consultation service through the sharing to the Pre-Standard WG of the contributions which will be produced for the targeted SDOs in order to get support and facilitate joint activities on aspects which can have impact also for the other projects. The first action performed is the sharing of the study item started within the 3GPP SA3 group. The next action will be the sharing of contributions that will be prepared.

5.2.2 5G-PPP Security Work Group

The 5G-PPP Security Work Group was created by the 5G-ENSURE project in early April 2016. The objectives of WG, which are defined in the Terms of Reference (ToR), are to:

- 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.

Membership is open to any project with a primary focus on security that is in scope with the WG's ToR.

Current members of the Security WG are listed herein with more expected: 5G-ENSURE, 5G Norma, 5GEX, Charisma, CogNet, SelfNet, Superfluidity, Virtuwind, Sesame.

5.3 Impact: 5G-ENSURE Visibility

5.3.1 Press coverage and Mentions

The biggest coverage of 5G-ENSURE to date comes from Telecom TV, both through its website and daily newsletter, which is distributed to over 60,000 industry professionals in more than 200 countries worldwide.

Link: http://www.telecomtv.com/articles/5g/how-to-ensure-the-security-of-future-5g-systems-13151/

Figure 11: Coverage on Telecom TV Website

The 5G-ENSURE press release also featured in the Telecom TV newsletter of 16-12-2015 (circulated at 13:05 CET) and of 17-12-2015 (circulated at 8:00 CET), as showed in the figures below.

Figure 12: Coverage in Telecom TV Newsletter

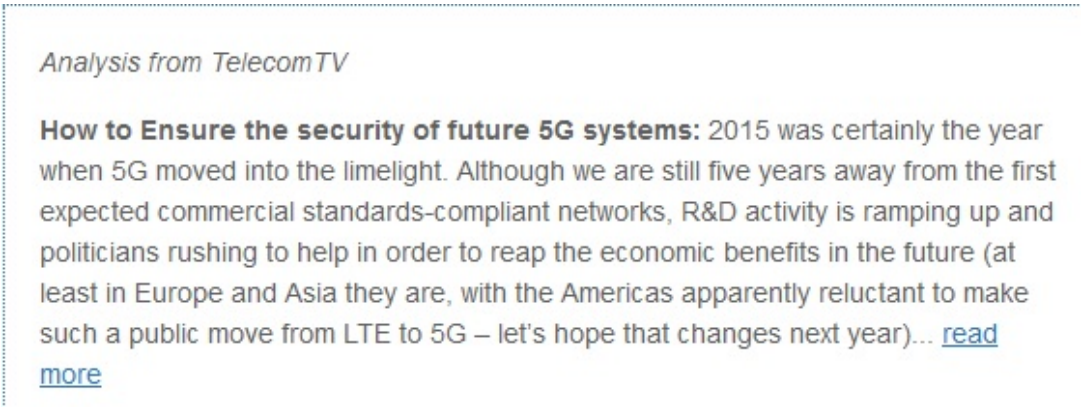
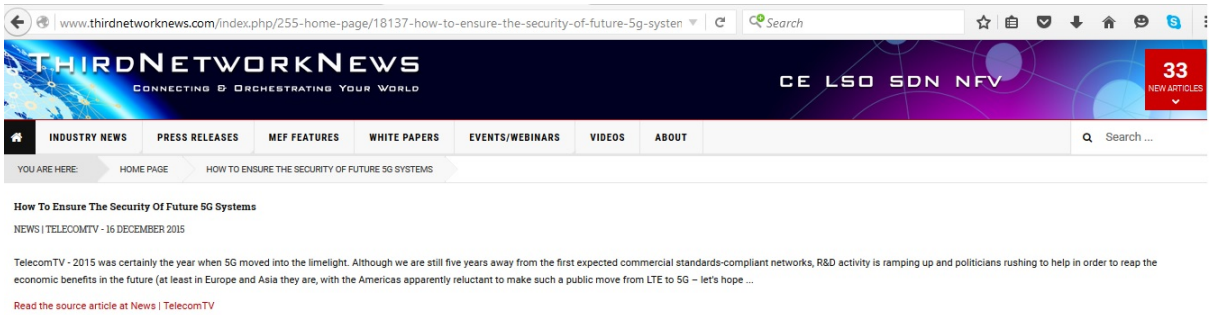


Figure 13: Coverage in Telecom TV - Analysis

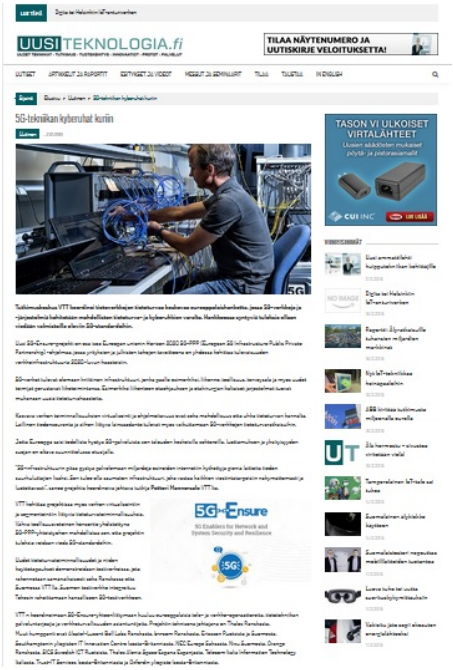
The press release was also published by Third Network News.



Link: http://www.thirdnetworknews.com/index.php/255-home-page/18137-how-to-ensure-the-security-of-future-5g-systems

Figure 14: Coverage by Third Network News

The related article on 5G-ENSURE was published in several Finnish media channels, as showed in the figures below.



Link: http://www.uusiteknologia.fi/2015/12/03/5g-tekniikan-kyberuhat-kuriin/

Figure 15: Coverage in UUSI Teknologia

Link: http://www.tivi.fi/Kaikki_uutiset/5g-verkkojen-tietoturvaa-rakennetaan-suomessa-6142539

Figure 16: Coverage by TIVI Finland

Visibility on partner websites

- **VTT**: http://www.vttresearch.com/media/news/5g-ensure-launches-to-make-5g-networks-and-systems-secure-and-trustworthy.
- **B-COM**: http://b-com.com/en/news/bcom-european-player-digital-technologies-strengthens-its-global-reach#.
- **University of Southampton**: http://www.it-innovation.soton.ac.uk/projects/5g-ensure.
- **Nixu Corporation**: https://www.nixu.com/en/insights/european-5g-ensure-project-improves-the-security-of-the-internet-of-things;

  https://www.nixu.com/fi/sijoittajat/tiedotteet/eurooppalainen-5g-ensure-hanke-kehittaa-esineiden-internetin-turvallisuutta.
- **Telecom Italia**: http://www.telecomitalia.com/tit/en/innovazione/rete/The-new-5G-PPP-European-Projects.html; http://www.telecomitalia.com/tit/it/innovazione/rete/Nuovi-progetti-Europei-del-5G-PPP.html
- **Oxford University**: https://www.europegateway.ox.ac.uk/news/list-selected-5g-ppp-projects

5.3.2 Social Media Engagement and Visibility

The table below shows the main outcomes of the activities related to social media engagement and results achieved.

Table 7: Impact on Twitter

Latest Update	*29-04-2015*
Tweets	*374*
Followers	*169*
Following	*72*
Total impressions	*126,689*
Total profile visits	*2769*
November 2015	
Number of tweets	35
Number of profile visits	659
Tweet Impressions	11,400
New followers	25
Top follower	TechTank: 16,200
Mentions	25
December 2015	
Number of tweets	38
Number of profile visits	402

Tweet Impressions	11,300
New followers	27
Top follower	Dave Waterson: 17.8K
Mentions	15
January 2016	
Number of tweets	46
Number of profile visits	343
Tweet Impressions	15,500
New followers	13
Top follower	N/A
Mentions	15
February 2016	
Number of tweets	77 (specific focus on Mobile World Congress)
Number of profile visits	427
Tweet Impressions	22,900
New followers	25
Top follower	Commissioner Oettinger: 36,800
Mentions	11
March 2016	
Number of tweets	58
Number of profile visits	471
Tweet Impressions	28,500
New followers	22
Top follower	Philip Solis, ABI (5G and wireless connectivity): 2727
Mentions	7
April 2016 (29-04-2016)	
Number of tweets	70
Number of profile visits	467
Tweet Impressions	26,200
New followers	18
Top follower	GeoThings, @GeoThings, 12,100 followers

Mentions	11

Twitter followers – top topic interests: Technology; Tech News; Business News; Mobile; Computer reviews.

Twitter followers – top countries: UK; Italy; Finland; France; India

The table below provides a sample of followers by stakeholder categories.

Table 8: Sample of Twitter followers

Stakeholder category	Followers
Policy Officials EU Commissioner for Digital Economy and Society.	Günther Oettinger, @GOettingerEU: 37,100
Policy/Funding Agency: Unit E1: EC Net Technologies, Network Technologies covering #5G, #InternetOfThings/#IoT, #spectrum & #DigitalSingleMarket/#DSMeu.	@NetTechEU: 2,497
Regulators Spectrum Policy Forum - Future spectrum management and regulatory policy	@UK_SPF: 290
5G-PPP Community – projects in phase 1 8 of the 18 other projects forming part of 5G-PPP phase 1: 5G Euro, SPEED 5G, NORMA, CHARISMA, SUPERFLUIDITY, METIS-II, H2020COHERENT, CogNet	@5GPPP (1243), @SPEED_5G (49), @5G_NORMA (1), @charisma5G (1), @Superfluidity5g (44), @metis2020 (462), @H2O2O_COHERENT (5), @5GPPPCogNet (146)
Member of 5G-ENSURE Advisory Board: United Nations Interregional Crime and Justice Research (UNICRI), Francesca Bosco	@francibosco, 3,581
Standards Body: ETSI. Globally applicable world class standards for Information and Communications Technologies (ICT) - fixed, mobile, radio, broadcast, internet.	@ETSI_STANDARDS, 3589
Media: TechTankTalks and Tech Tank News, collaboration community for business technology stakeholders. Technology in business. EnterpriseIT. InfoSec, Cloud, BigData, FinTech, DigitalHealth, Telecoms, MarTech, Developer, IoT.	@techtanktalks, 16,8000 and @techtanknews 12,400
Media: Inside5G, Blog on latest news, articles and analysis as 5G is defined.	@Inside5G 383
Media: Keith Dyer, Editor of The Mobile Network, @tmnmag, conversations and news from the mobile network tech sector. Also founded @inside5G, the industry's 5G blog.	@keithdyer 4,491
Media: Guy Daniels, Editor and co-founder of Telecom TV	@guydaniels 976
Media: Dominic Halpin Editor of IT, IoT and 5G, Tech Tank Talks	@Domhalps 6,271

Media: SDN Top News, news on Software-defined networking news	@SDNTopNews, 623
Media: Fierce Wireless, news and analysis from FierceWireless' European mobile editors, Anne Morris and Michael Carroll.	@FierceWirelessE, 417

The launch of 5G-ENSURE received good coverage also through social media channels, spanning the EC, partners, the 5G-PPP and media channels, as showed in the table and figures below. Since the launch, the project has continued to gain traction on awareness-raising around RG-ENSURE, and key messages on 5G security and standardisation. The table provides a summary of twitter engagement to date across different stakeholders targeted.

Table 9: Sample of Twitter Engagement

Engagement and Visibility on Twitter
@Orange_Brussels (Orange EU): *.@5GEnsure & security by design: preparing EU leadership for efficient & reliable infra fit for future #ThinkDigital http://bit.ly/1Qgwwub*; 14-12-2015
@5G-PPP: *.@5GEnsure #H2020 project launched to make #5G #networks & systems secure & trustworthy: http://bit.ly/1Qgwwub pic.twitter.com/uwfat3f9jJ*; 14-12-2015
@ETNOAssociation (the European Telecommunications Network Operators' Association): *.@5GEnsure & security by design: preparing EU leadership for efficient & reliable infra fit for future #ThinkDigital http://bit.ly/1Qgwwub*; 14-12-2016
@Ox_CyberSec: *Just a shout-out to welcome @5GEnsure, a promising-looking new project on 5G wireless networks: https://5g-ppp.eu/5g-ensure/ @CompSciOxford*
Ericsson Research retweeted 5GEnsure: *Coming together to build trustworthy #5Gsystems. We expect great things!*
Top mention February 2016: *Standardisation plays a key role in @5GEnsure 'security by design' approach ow.ly/Ynl4T @5GPPP @NetTechEU @netfuturesEU*
Top tweet March 2016: *Global collaboration, across #telecom and industry verticals is key for success of #5G, @HansV_Ericsson #CeBIT2016*
Ericsson liked your Tweet: *interesting industry panel at #netfutures16 with Ulf Ewaldsson from ericsson, @GOettingerEU, @tefdigital, via @mariocampolargo*; 30-03-2016
FCG, cspforum and EC Net Technologies Retweeted: Mar 14: *'#5G will be the most critical building block of #gigabit society. Here's our plan' @GOettingerEU, at #CeBIT, http://bit.ly/1P7JEez*; 14-03-2016
Factories of the Future - FoF_EU Retweeted you: *A visual explanation of #5G from the EC. @techdirt, @NetTechEU, @FoF_EU, @networkingplus, @DisruptiveTecho pic.twitter.com/3wk5G6iXQZ*; 09-03-2016
ETSI liked your Tweet: *Many thanks to participants @IRT_BCom Int'l WS on #5G #RVM on 10.03, @ETSI_STANDARDS, @5GPPP, @NetTechEU pic.twitter.com/3nkWygSaNm*; 11-03-2016 (Workshop hosted by B-COM and endorsed by ETSI
Net Futures and Net Technologies retweet + Karen Boers liked your Tweet: @5GEnsure will be at workshop on #5G vision & roadmap to key standards at #netfutures16, 20-21.04, http://ow.ly/ZBiLm, @@NetTechEU; 08-04-2016

The promotion of the first main outputs from 5G-ENSURE in March 2016 was well received on twitter, with the partner tweet showed below getting “Top Mention” of the month.

Figure 17: Visibility of 5G-ENSURE first Deliverables

The following figures are other examples of 5G-ENSURE visibility.

Figure 18: Coverage of launch by EC Net Technologies

Figure 19: Launch Announcement by CyberSec Oxford

Telecom TV published the Alcatel-Lucent tweet on the launch of 5G-ENSURE on 04-01-2016 and 11-01-2016. Telecom TV has published a total of 5 tweets by 5G-ENSURE in the period covered.

Figure 20: Telecom TV Coverage of Partner Tweet on 5G-ENSURE Launch

About 5G and related technologies

5G-ENSURE twitter discussions on cloud computing and 5G have received coverage by Telecom TV.

Figure 21: Twitter Coverage by Telecom TV

6 Stakeholder Engagement and Events

6.1 Liaison with Standards Groups

The main liaisons with standards groups are described below.

- 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.

6.2 Stakeholder Engagement and Joint 5G-PPP Activities

6.2.1 International Workshop on RVM and Security for multi-RAT and reconfigurable systems

Date and Venue	10-03-2016, B-COM, Rennes (FR)
Focus	Radio Virtual Machine concepts that can be considered an extension to the well-known Software Defined Radio (SDR) approach. So, specific improvements or entire several Physical layers can be embedded within a platform in a secure and controlled environment (virtual machine) combining software development with hardware accelerators for more powerful processing. Multiple Radio Access Technologies (RATs), Flexibility and scalability solutions for multi-RAT communications, Scalability radio virtual machine architecture, Security in multi-RAT environment, Security in data and control planes management

Stakeholder engagement	Partner workshop endorsed by ETSI. Standards groups and developers. Technical audience.
5G-ENSURE role and outcomes	Presentation of the 5G-ENSURE by Jean-Philippe Wary, Orange, presents: How 5G-ENSURE may address and manage software define Radio
Web links	5G-ENSURE: http://5gensure.eu/events/international-workshop-rvm-and-security-multi-rat-and-reconfigurable-systems B-COM: http://etsi-workshop.b-com.com/

6.2.2 Networld2020 Annual Event and GA 2016

Date and Venue	19 April 2016, Bedford Hotel & Congress Center, Brussels (BE) Annual event of NetWorld2020, the European Technology Platform for communications networks and services.
Focus	Main event: Updates on 5G-PPP actions, global standardisation, changes to the governance structure and the link between the 5G Infrastructure Association and NetWorld2020. Special session on 5G-PPP: 60-minute session on 5G-PPP projects current status and future steps.
Stakeholder engagement	5G-PPP projects. *Radio and efficient use of radio spectrum* -> Fantastic-5G; mmMagic, SPEED-5G; *Networking* (*wireless and optical networking; security enablers; intelligent management*) -> 5G-Crosshual, 5G-XHaul, COHERENT, 5G-ENSURE, CogNet; *Self-Organised Management* -> experimental experience of SDN/NFV integration in SELFNET; 5G-NORMA -> Architecture. Eurescom, coordinator of the 5G-PPP CSA.
5G-ENSURE role and outcomes	Presentation of 5G-ENSURE: Security enablers for 5G by Petteri Mannersalo, VTT Technical Research Centre of Finland. A short pitch talk in a session on 5G-PPP projects. The presentation introduced the project and its main achievements, i.e., use cases and an early vision of security enablers.
Web links:	5G-ENSURE: http://5gensure.eu/events/networld2020.eu NetWorld2020: http://networld2020.eu/networld2020-annual-event-and-ga-2016/

6.2.3 ETSI Summit: 5G: From Myth to Reality

Date and Venue	21-04-2016, ETSI, Sophia Antipolis (FR)
Focus	Three specific classes of 5G use cases emerging as candidates for early prioritisation: enhanced mobile broadband, massive machine type communications and ultra-reliable/low latency communications. Hence the

	workshop focuses on six key questions related to these use cases: Motivations and business models behind the use cases? Potential socio-economic consequences of 5G? Real requirements and expectations of the stakeholders and how can they influence the discussion? How the 5G roadmap departs from planned LTE roadmaps? Do we have a harmonized view, across different regions, or at least in Europe? Why is 2020 important? What can realistically be achieved by that date?
Stakeholder engagement	Decision-makers in technology strategy, standardisation management and product planning; Representatives of public authorities, local/regional and national governments, European institutions and the European Commission; Professionals and experts.
5G-ENSURE role and outcomes	5G-ENSURE poster presentation by Petteri Mannersalo, VTT. Participation in a poster session on invited topics (mainly 5G-PPP projects) to trigger an exchange of views on aspects of 5G that are not covered in the summit sessions. The 5G-ENSURE poster introduced the project and its main achievements, i.e., the use cases and early vision of security enablers. Promotion of the 1st International Workshop on Standardisation.
Web links	5G-ENSURE: http://5gensure.eu/events/5g-myth-reality ETSI: http://www.etsi.org/news-events/events/1025-2016-04-5g-from-myth-to-reality

6.2.4 Net Futures 2016

Date and Venue	20-21 April 2016, The Egg, Brussels (BE)
Focus	Unit E1 – Network Technologies Concertation Meeting (20-04-2016) **Conference**: The theme of the 2-day event is driving growth in the digital single market with keynotes by Commissioners Andrus Ansip and Günther Oettinger. Ericsson. Session on 5G vision and roadmap to key standards (21-04-2016): global research activities, including the launch of 20 EU projects coordinated by the 5G-PPP. Presenting the vision and roadmap for key standards development for 5G networks. Telecom Italia.
Stakeholder engagement	5G-PPP projects. Policy makers (EC). Representatives from business (start-ups, SMEs and large companies) and research.
5G-ENSURE role and outcomes	Attendance in the session on the 5G vision and roadmap to key standards. Direct interaction with Orange Labs and Telecom Italia, vice chair of the 3GPP RAN. Distribution of the bookmark promoting the Open Consultation and the 1st International Workshop on Standardisation.
Web links	5G-ENSURE: http://5gensure.eu/events/net-futures-2016-20-21-april-brussels Net Futures: http://netfutures2016.eu/

7 Plans and Targets for next six months

The table below provides an overview of the plans for the period May to October 2016 across the four major categories.

Content creation for the website, improvements and add-on features (e.g. surveys, registration forms) will take place in parallel to all the activities planned, including project outcomes and updated pages. In addition, the project will regularly publish items on 5G-PPP joint activities and outcomes, related Security Work Group outcomes, progress on standardisation, policy updates, as well as insights emerging on 5G and related technologies, market trends and investments. Multimedia content and web banners will be among the formats used.

KPI: Targets for a minimum number of new items have been set to ensure regular updates take place.

Table 10: Plans for May to October 2016

Communication & community | **Standardisation** | **Joint 5G-PPP activities** | **Dissemination of outputs**

5G-ENSURE - Monthly checklist May to October 2016						
Action	**M7 May 2016**	**M8 June 2016**	**M9 July 2016**	**M10 August 2016**	**M11 September 2016**	**M12 October 2016**
Website content	Min. 4	Min. 4	Min. 4	Min. 4	Min. 4	Min. 4
Dissemination of Outputs & Results		Publication & promotion of D2.2 (Trust Model)			Publication & promotion of D3.3 (5G-	Publication & promotion of D4.2 (Test Plan v1)
Dissemination of Outputs & Results	Publication & promotion of D3.2 (5G-PPP security enablers open	Publication & promotion of D2.3 (Risk Assessment Mitigation & Requirements)			Publication & promotion of D3.4 (5G-PPP security enablers documentation - v1.0)	Publication & promotion of D2.4 (Security Architecture - draft)
Twitter posts	Min. 30	Min.50	Min.30	Min. 30	Min. 30	Min. 30
PR/Media Content	Announcement on 1st International WS		1st Iteration of Standardisation Roadmap (final) shared with standardisation community		PR on 1st year major achievements	
PR/Media Content	NOKIA podcast		Article on Trust Model			
Communication Material (print & web)	Updated flier	Videos on 5G-ENSURE				Updated flier and poster
Workshop collaterals	Workshop agenda, draft of Roadmap (1st iteration)	Executive Summary of Open Consultation, roll-up banner				
Event	ETSI: From Research To Standardization	5G-ENSURE 1st International Workshop on Standardisation in conjunction with ETSI Security week			IEEE VTC Vehicular Technology Conference	SDN & OpenFlow World Congress
Event	5G Security Day, Kista (SICS, Ericsson & Royal Institute of Technology)	31st International Conference on ICT Systems Security and Privacy Protection - IFIP SEC 2016				
Event		EuCNC 2016 - Security session				
Event		5G WORLD 2016				
Event		Internet Security Days	Security & Privacy Week SPW2016			
Linkedin Updates	min.2	min. 4	min. 2	min. 2	min.2	min. 2
LinkedIn Blog Posts	min. 2	min. 2	min. 2	min. 2	min.2	min. 2
Newsletter	1st Int. WS & Takeaways from April events		Outcomes of the 1st International Workshop		5G-ENSURE Stakeholder Engagement	5G-ENSURE Outputs & Achievements
Liaison on standardisation	Open consultation	Feedback on roadmap draft via interaction with Security experts & Steering Committee Members				
Liaison on standardisation	NFV#14; 3GPPRAN1#85; NFV#14; 3GPPSA3#83;	3GPPRAN#72; CYBER#7; 3GPPSA#72				
Notes on related activities	**WP5 Flash Report (Trust-IT)**	**D1.5 Periodic Management Report (WP5 - TIIT). WP5 Flash Report (Trust-IT)**	**WP5 Flash Report (Trust-IT)**	**WP5 Flash Report (Trust-IT)**	**WP5 Flash Report (Trust-IT)**	**Submission of D5.3 (NOKIA) and D5.4 (Trust-IT). D1.6 Quarterly management report (WP5 - TIIT). D1.7 Steering Committe Report (WP5 - TIIT). WP5 Flash Report (Trust-IT)**

7.1 Liaison with Standardisation Groups

From the standardisation point of view, the main opportunity is given by the new SA3 work item "*Study on Architecture and Security for Next Generation System".* Such a deliverable, where Ericsson serves as rapporteur, will be the main target for the possible standardisation actions performed by the project for the 2016 time-line. In June 2016, 5G-ENSURE will publish two other deliverables, i.e. the D2.2 and D2.3 related to the Trust model and security requirements. These outputs will give the project a set of stable results, all of them within the scope of the new SI, ready to be presented for the discussion in the SA3 meetings. Moreover, progress achieved in the definition of the security architecture (task 2.4) and the consolidation of the enablers (WP3) are also within the scope of the SI.

Future SA3 Events	
SA3 #83	**San Jose del Cabo (Mexico)**, 9-13 May 2016
SA3 #84	**Chennai (India)**, 25th-29th July 2016
SA3 #85	**Tenerife - Santa Cruz (Spain)**, 7-11 November 2016

7.2 5G-ENSURE 1st International Standardisation Workshop

Date and venue	16 June 2016, Sophia Antipolis in conjunction with the ETSI Security Week

The workshop will provide the opportunity to discuss and gain technical insights and perspectives from security experts on security in 5G based on the preliminary findings of 5G-ENSURE. This 5G-PPP project drives the “vision” on 5G Security, to define a “Security Architecture” for 5G and specify a set “Security Enablers”, along with a (technical) road map for 5G to build the necessary trust and confidence and thus release the full potential of 5G.

5G-ENSURE encourages coordination work on 5G security with involvement of 5G-PPP projects and standards groups, where security is a key driver towards the future 5G-connected digital society. The end-goal is driving the adoption of a "Security by Design" approach, where security is an integral component of the architecture design and not just an add-on or after-thought.

An Open Consultation Survey on 5G Security and 5G-ENSURE activities will be launched as part of the workshop (See Section 9.3). The results will be presented and discussed during the workshop, offering a launch pad for an exchange on European perspectives on security work in 5G-ENSURE.

The workshops, to be held in Sophia Antipolis during the ETSI Security Week (13-17 June 2016) features two sessions:

Session 1 – provides an overview of the 5G-ENSURE project presenting the vision, achievements, the approach towards standardisation and collaboration on other projects on security aspects of 5G.

Session 2 - focuses on standardisation activities. A standards Panel will comprise leading experts working on various 5G standardisation bodies to discuss current priorities, milestones and approaches to 5G standardisation. The race is on to gather the main 5G standardisation initiatives to explore collaboration opportunities to drive the definition of 5G specifications for security.

7.2.1 Latest agenda

Session 1 – 5G-ENSURE In Focus	
(time slot)	Keynote EC - tbc
(time slot)	5G-ENSURE Project presentation – Petteri Mannersalo, VTT and 5G-ENSURE Coordinator
(time slot)	Security enablers for future network - Pascal Bisson, Thales and 5G-ENSURE Technical Coordinator

(time slot)	Security focus in 5G standardisation - Paolo De Lutiis, Telecom Italia
(time slot)	The importance of co-operation: 5G-ENSURE approach – Jean-Philippe Wary, Orange
(time slot)	Open Consultation Results – Luciana Costa, Telecom Italia
Session 2 – Standards Panel	
(time slot)	**ETSI TC Cyber:** ETSI TC Cyber: Charles Brookson, chairman; Maik Seewald, vice; Jean Pierre Quemard, vice. **ITU**: Luca Pesando (IMT-2020); Martin EUCHNER (SG17). **3GPP SA1 or SA3**: Anand Prasad; Adrian Escott; Alf Zugenmaier. **Pre-Standardisation WG**: Hugo Tullberg.
	Round Table: *How do we make sure standards have security by design? How we can drive 5G security specification?* **Moderator**: Bengt Sahlin, Ericsson
	Wrap-up and Workshop End

7.2.2 Participants Targeted

Participants are mostly targeted through personalised invites, and include the following.

European Commission	Bernardo Berani
NIST	Kevin Stine; Nelson Hastings; Murugiah Souppaya
Advisory board members (not currently in the agenda)	Francesca Bosco - **The United Nations Interregional Crime and Justice Research Institute (UNICRI)** Nina Olesen - **CYSPA, the European Cyber Security Protection Alliance** Benoit Michau - **Agence nationale de la sécurité des systèmes d'information (ANSSI)**
5G-PPP WGs and Project representatives (not currently in the agenda)	Spectrum WG - Terje Tjelta, Telenor; 5G Architecture WG - Simone Redana, Nokia; SDN / NDF WG - Josep Martrat, ATOS and Carlos Jesus Bernardos, UCIII; NetMgmt / QoS / Security WG - Robert Mullins, TSSG, Waterford; Vision and Societal Challenges WG - Jean-Sebastian Bedo, Orange SME WG - Jacques Magen, Interinnov.

7.2.3 Workshop Promotion and Collaterals

Communication material will be prepared in advance of the workshop to support promotional activities across all relevant channels:

- Web announcement banner visible on the home page.
- Twitter and LinkedIn announcement banners.
- Newsletter features.
- Announcements on external channels, e.g.5G-PPP website and project websites.

- Tweets and LinkedIn posts with agenda and speaker updates.

Workshop collaterals:

- 5G-ENSURE roll-up banner.
- Agenda (to be inserted in the badge holder).
- Flier on the main outcomes of the open consultation.
- First public draft of the Roadmap for feedback and consolidation distributed as a short booklet.
- Updated project flier.

A poster produced for the ETSI Summit on 5G includes information about the workshop, the aim of raising awareness amongst key stakeholders.

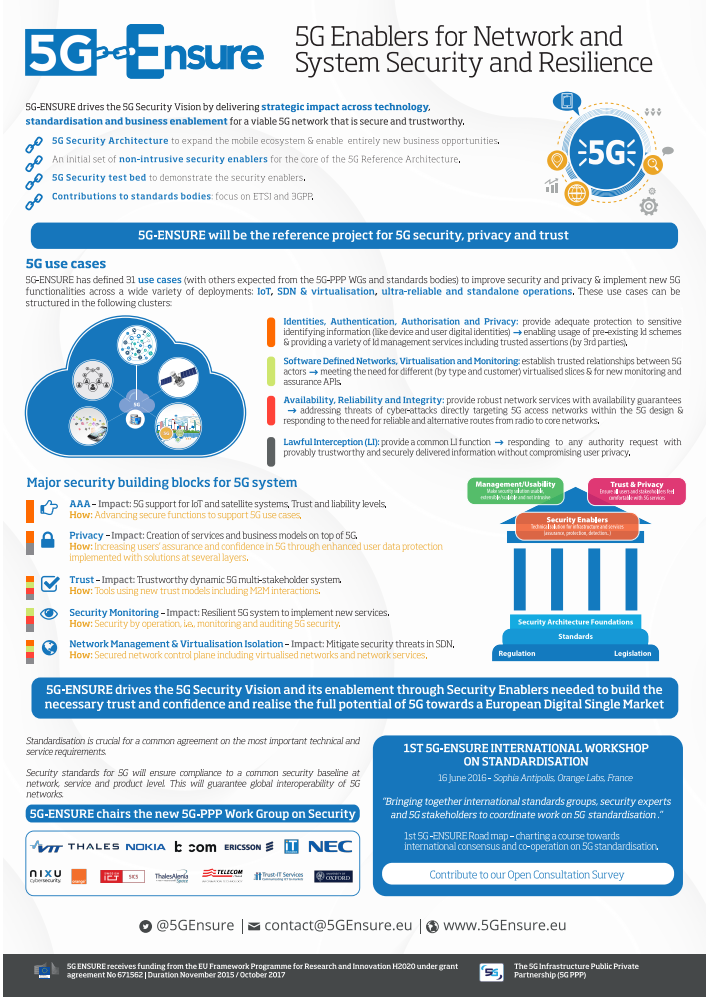


Figure 22: 5G-ENSURE Poster for ETSI Summit on 5G

7.3 Open Consultation

The objective of the 5G-ENSURE Public consultation on 5G security is to initiate and sustain constructive external relationships over time with key 5G key players on the project's security vision and priorities. In particular, it aims to create understanding about the project among anyone likely to be affected by 5G or with have an interest in 5G security.

5G-ENSURE will collect points of view, their perspectives on future technological advances in the 5G security domain, the foreseen risks, impacts, opportunities, and mitigation measures. Listening to

stakeholder concerns and feedbacks can be a valuable source of information to evaluate how the project activities are in line with the vertical market expectations and to improve project activities and outcomes. It can also form the basis for future collaboration. The outcomes of the consultation will be shared during the first international workshop on standardisations.

The open consultation will be uploaded on the 5G-ENSURE website using an in-house tool. It will be communicated to targeted audiences through announcements in the project newsletters, through the 5G-PPP, social media channels and at events attended. The three events in April 2016 – NetWorld 2020, the ETSI Summit on 5G and Net Futures, including a newly produced poster and book mark.

Figure 22: 5G-ENSURE Bookmark for 1st Workshop and Public Consultation

7.4 Community Building

7.4.1 Community Database

Community building feeds into the project database and is based on:

- Sourcing relevant members through current networks.
- Recruiting members through events and relevant business and technology associations, think tanks and media channels.

The community DB represents an important KPI for WP5 with the necessary qualitative metrics in place to measure relevance and levels of interest and engagement. Contacts are tagged based on the joint stakeholder mapping, including also professional positions, organisation size and location, as well as level of engagement achieved.

7.4.2 LinkedIn and Twitter

LinkedIn Activities will focus on:

- Building up the connections through the development of the community DB.
    - Initial focus on the 5G-PPP and Net Futures communities and standardisation stakeholders.
    - Targets: Minimum 10 new contacts/month and minimum 5 new connections.
- Creating blog posts targeting the various stakeholders, e.g.:
    - Messages for industry and vertical markets: what businesses need to know about 5G and how they can plan ahead.
    - Importance of global collaboration on standardisation and consensus building.
    - Market insights and investments in the global landscape.
    - Progress on 5G-PPP joint activities and outputs, including the outputs of 5G-ENSURE, and key technical insights emerging globally.
    - Policy announcements and communications, including relevant press conferences, blog posts, infographics, and videos.
    - Related technology news, e.g. cloud and edge computing; IoT; smart environments, etc., including, where possible, industry leader/expert opinions.
    - Open consultation: calls for action to encourage targeted stakeholders to contribute.
    - 1st International Workshop: Session overviews and main takeaway messages.

Partners will also be encouraged to contribute their own specialised knowledge, institutional/corporate strategies and investments, and insight papers.

The 5G-ENSURE profile will be regularly updated with outputs, new fliers and multimedia content, as well as press content. These will also be promoted through the LinkedIn Updates and Photos. For the **1st International Workshop on Standardisation**, the project will communicate the speakers and panellists with sneak previews on the topics covered; share agenda updates; post session overviews during the event; produce blog posts on the takeaways with multimedia material.

7.4.3 Events

The current list of events deemed relevant for the dissemination of 5G-ENSURE are included in the plan in table 8. In addition, Oxford University is planning to summit their work on the development of a Wi-Fi based IMSI catcher at Black Hat, 30 July - 4 August 2016 in Las Vegas, US [75].

7.5 Channels for Project Communications and Dissemination of Results

7.5.1 Channels for PR and Media Content

5G-ENSURE has already established relations with several key media channels moving forward. The table below lists the channels for future press releases and media content.

Table 11: Media Channels

Media Channel
TelecomTV, http://www.telecomtv.com/, @TelecomTV: daily updates on trends in telecommunications market and related technologies.
Mobile World Live, http://www.mobileworldlive.com/,
Inside 5G, @Inside5G: a blog with the latest news, articles and analysis as 5G is defined.
Telecomkh.com (English and Spanish), http://telecomkh.com/en, @telecomkhen: online magazine dedicated to telecommunications and ICT
4G-Portal.com, @4GPortal: news, videos, whitepapers, reports, jobs and much more in area of 4G Market.
4GAmericas: 4G Americas: channel for mobile operators & vendors in the Americas to provide a single voice representing LTE mobile broadband technology.
Tech Tank Talks, @techtanktalks and @techtanknews: industry think tank covering cloud, IoT and 5G.
Telecom Top News, @TelecomTopNews
Telecoms News, @TTech_News: news, comment, and analysis hub providing the latest thought leadership content from across the industry.

7.5.2 Publications for the Dissemination of Results

A detailed 5G-ENSURE dissemination plan will be defined at the end of year 1 (D5.4), following an appraisal made under WP5 and specifically T5.4 on project results and exploitation potential. For the next six months, the plan focuses mainly on identifying relevant publications for disseminating early results. As indicated in the Grant Agreement, priority is given to open access journals with a budget allocated for facilitating this approach. In disseminating its results, 5G-ENSURE targets not only technical communities and audiences through specialised repositories but also interdisciplinary research communities like the ones build around open access repositories.

Current publications

Authors: Altaf Shaik, Jean-Pierre Seifert and Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi

Title: Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems

Conference: Network and Distributed System Security Symposium (NDSS), 21-24 February 2016

Current publications planned

Authors: Heng Cui, Ghassan O. Karame, Felix Klaedtke and Roberto Bifulco

Title: Fingerprinting Software-defined Networks

Publication: IEEE Transactions on Information Forensics and Security

Targeted journals and open access repositories

Targets for disseminating early future results include: Mobile Information Systems, SpringerOpen, OpenAIRE-Zenodo, ResearchGate, Figshare.

8 Conclusion

This deliverable has reported on the outcomes of the first six-monthly plan across four key activities: communication and community building, standardisation, joint activities with the 5G-PPP and the dissemination of results. It has provided a detailed analysis of the standardisation landscape, including on-going and identified opportunities of contribution to Standards Groups, relevant to 5G-ENSURE, whose mission is to become the reference project on 5G security. It is important to note that a high number of 5G-PPP projects have an interest in the same prioritity Standards Groups as 5G-ENSURE.

We have prioritised the identified stakeholders and we have detailed the engagement plan providing tangible evidence of relations established with peer projects, the media and policy decision makers, as well as targeted actions at events. Joint activities and knowledge exchange across the 5G-PPP have been presented as an important goal of 5G-ENSURE.

As part of the engagement strategy with Standards Groups, we have presented the plan for the 1st International Workshop on Standardisation scheduled in June 2016, as well as the imminent public consultation to collect and analyse the perspectives and priorities of the 5G-ENSURE stakeholders, including 5G-PPP peer projects, in relation to 5G security. This 1st International Workshop will lead to the first iteration of a standards roadmap on 5G security.

The deliverable has also set out an initial set of KPIs (for communications and marketing) and qualitative metrics against which we have measured the impact achivied in the first six months of the project. The identified KPIs will be monitored to measure the impact and relevance of 5G-ENSURE as reference project for 5G security, and may be modified in future iterations of this report. Finally, we set out plans for the next six months.

9 References

[1] 5G-ENSURE. (2016, March) Industry panel at CeBIT 2016 calls for collaboration on 5G Security and Privacy. [Online]. http://www.5gensure.eu/news/industry-panel-cebit-2016-calls-collaboration-5g-security-and-privacy

[2] 5G-PPP. 5G-PPP, @5GPPP. [Online]. http://www.5g-ppp.eu

[3] 5G-ENSURE, "D2.1 Use Cases," Deliverable 2016.

[4] Euro-5G. [Online]. https://5g-ppp.eu/euro-5g/

[5] 5G-PPP. 5G-PPP Work Groups. [Online]. https://5g-ppp.eu/5g-ppp-work-groups/

[6] 5G-XHaul Project. [Online]. http://www.5g-xhaul-project.eu/

[7] 5G-NORMA Project, @5G_NORMA. [Online]. https://5gnorma.5g-ppp.eu/

[8] COHERENT Project. [Online]. http://www.ict-coherent.eu/

[9] FANTASTIC-5G Project, @FANTASTIC5G. [Online]. http://fantastic5g.eu/

[10] Flex5Gware Project. [Online]. http://www.flex5gware.eu/

[11] METIS-II Project, @metis2020. [Online]. https://5g-ppp.eu/metis-ii/

[12] 5G mmMagic Project. [Online]. https://5g-mmmagic.eu/

[13] CHARISMA Project, @charisma5G. [Online]. http://www.charisma5g.eu/

[14] SPEED-5G Project, @SPEED_5G. [Online]. https://speed-5g.eu/

[15] 5G-Crosshaul Project. [Online]. http://5g-crosshaul.eu/

[16] 5GEx Project. [Online]. http://www.5gex.eu/

[17] CogNet Project, @5GPPPCogNet. [Online]. http://www.cognet.5g-ppp.eu/

[18] SESAME Project, @Sesame_H2020. [Online]. http://www.sesame-h2020-5g-ppp.eu/

[19] SELFNET Project. [Online]. https://selfnet-5g.eu/

[20] SONATA Project, @sonataNFV. [Online]. http://www.sonata-nfv.eu/

[21] Superfluidity Project, @Superfluidity5g. [Online]. http://superfluidity.eu/

[22] VirtuWind Project. [Online]. http://www.virtuwind.eu/

[23] ETSI - European Telecommunications Standards Institute. [Online]. http://www.etsi.org/

[24] 3GPP - 3rd Generation partnership project. [Online]. http://www.3gpp.org/

[25] European Conference on Networks and Communications (EuCNC). [Online]. http://www.eucnc.eu/

[26] ITU. Working Party 5G - IMT systems (WP5D). [Online]. http://www.itu.int/en/ITU-R/study-

groups/rsg5/rwp5d/Pages/default.aspx

[27] ECC. ECC Project Team 1 (ECC PT1). [Online]. http://www.cept.org/ecc/groups/ecc/ecc-pt1/client/introduction/

[28] ENISA - European Union Agency for Network and Information Security. [Online]. https://www.enisa.europa.eu/

[29] Ericsson, "Mobility Report," 2015. [Online]. http://www.ericsson.com/res/docs/2015/mobility-report/ericsson-mobility-report-nov-2015.pdf

[30] 5G Forum, "5G Service Roadmap 2022," 5G White Paper 2016. [Online]. http://kani.or.kr/5g/whitepaper/5G%20Service%20Roadmap%202022.pdf

[31] ITU-T - The ITU Telecommunication Standardization Sector. [Online]. http://www.itu.int.

[32] GSMA. [Online]. http://www.gsma.com/

[33] NGMN Alliance. [Online]. https://www.ngmn.org/home.html

[34] 3GPP. Radio Access Networks (RAN). [Online]. http://www.3gpp.org/specifications-groups/ran-plenary

[35] 3GPP. Service & Systems Aspects (SA). [Online]. http://www.3gpp.org/specifications-groups/25-sa

[36] 3GPP. Core Network & Terminals (CT). [Online]. http://www.3gpp.org/specifications-groups/28-rubrique34

[37] 3GPP. GSM Edge Radio Access Networks (GERAN). [Online]. http://www.3gpp.org/specifications-groups/tsg-geran/geran-wg1

[38] 3GPP. (2015) RAN & SA plenary meetings #67 report. [Online]. http://www.3gpp.org/ftp/tsg_ran/TSG_RAN/TSGR_67/Docs/

[39] 3GPP. (2015, March) Tentative 3GPP timeline for 5G. [Online]. http://www.3gpp.org/news-events/3gpp-news/1674-timeline_5g

[40] 3GPP, "Study on New Services and Markets Technology Enablers," Technical Report TR 22.891, 2016. [Online]. http://www.3gpp.org/DynaReport/22891.htm

[41] 5G Americas. [Online]. http://www.4gamericas.org/en/resources/technology-education/5g/

[42] Chinese IMT-2020 (5G) Promotion Association. [Online]. http://www.imt-2020.cn/en/introduction

[43] 5G Forum. [Online]. http://www.5gforum.org/#!eng/cvb1

[44] 3GPP, "Feasibility Study on New Services and Markets Technology Enablers," Technical Report TR 22.891, 2016.

[45] 3GPP, "Study on Scenarios and Requirements for Next Generation Access Technologies," Technical Report TR 38.913, 2016.

[46] 3GPP, "TR for Study on New Radio Access Technology: Radio Access Architecture and Interface," Technical Report TR 38.801, 2016.

[47] 3GPP, "Study on Architecture for Next Generation System," Technical Report TR 23.799, 2016.

[48] 3GPP. SA3 - Security: Terms of reference. [Online]. http://www.3gpp.org/specifications-groups/sa-plenary/sa3-security

[49] 3GPP, "Study on the security aspects of the next generation system," Technical Report Draft TR 33.899, 2016.

[50] ETSI, "CYBER: PII Protection and Retention," Technical Report Draft TR 103 304, 2015.

[51] ETSI, "CYBER: Practical introductory guide to privacy," Technical Report Draft TR 103 370, 2015.

[52] ETSI, "CYBER: Mechanisms for privacy assurance and verification," Technical Specification Draft TS 103 485, 2015.

[53] ETSI, "CYBER: Identity management and naming schema protection mechanisms," Technical Specification Draft TS 103 486, 2015.

[54] ETSI, "CYBER: Baseline security requirements regarding sensitive functions for NFV and related platforms," Technical Specification Draft TS 103 487, 2016.

[55] ETSI, "Network Functions Virtualisation (NFV); NFV Security; Problem Statement," Group Specification GS NVF-SEC 001, 2014.

[56] ETSI, "Network Functions Virtualisation (NFV); NFV Security; Cataloguing security features in management software," Group Specification GS NFV-SEC 002, 2015.

[57] ETSI, "Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance," Group Specification GS NFV-SEC 003, 2014.

[58] ETSI, "Network Functions Virtualisation (NFV); NFV Security; Privacy and Regulation; Report on Lawful Interception Implications," Group Specification GS NFV-SEC 004, 2015.

[59] ETSI, "Network Functions Virtualisation (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration," Group Specification GS NFV-SEC 009, 2015.

[60] ITU. ITU towards "IMT for 2020 and beyond". [Online]. http://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx

[61] ITU-T, " FG IMT-2020: Report on Standards Gap Analysis" Temporary Document T13-SG13 208-PLEN".

[62] ITU-T. Study Group 13. [Online]. http://www.itu.int/en/ITU-T/studygroups/2013-2016/13/Pages/default.aspx

[63] Internet Engineering Task Force (IETF). [Online]. https://www.ietf.org/

[64] R. Peon, and M. Thomson M. Belshe, "Hypertext Transfer Protocol Version 2 (HTTP/2)," IETF RFC 7540. [Online]. https://tools.ietf.org/html/rfc7540

[65] M. Nottingham and M. Thomson, "Opportunistic Security for HTTP," IETF Internet-Draft 2016. [Online]. https://datatracker.ietf.org/doc/draft-ietf-httpbis-http2-encryption/?include_text=1

[66] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," IETF Internet-Draft 2016. [Online] https://datatracker.ietf.org/doc/draft-ietf-tls-tls13/

[67] K. Hartke, and C. Bormann Z. Shelby, "The Constrained Application Protocol (CoAP)," IETF RFC 7252, 2014. [Online] https://tools.ietf.org/html/rfc7252

[68] S. Duquennoy, and G. Selander S. Raza, "Compression of IPsec AH and ESP Headers for 6LoWPAN Networks," IETF https://tools.ietf.org/html/draft-raza-6lo-ipsec-04, Internet-Draft 2016.

[69] IEEE - The Institute of Electrical and Electronics Engineers. [Online]. https://www.ieee.org/index.html

[70] IEEE, "P802E - Recommended Practice for Privacy Considerations for IEEE 802 Technologies". [Online]. https://standards.ieee.org/develop/project/802E.html.

[71] The Open Networking Foundation (ONF). [Online]. https://www.opennetworking.org

[72] National Institute of Standards and Technology (NIST). [Online]. http://www.nist.gov

[73] NGMN, "5G White Paper". 2015. [Online]. http://www.ngmn.org/5g-white-paper.html

[74] 5G-ENSURE, "D5.1 Web platform as an interface with the umbrella 5G-PPP platform," Deliverable 2016.

[75] Black Hat. [Online]. https://www.blackhat.com/us-16/