1st International Workshop on 5G Security Standardisation

"Bringing together international standards groups, security experts and 5G stakeholders to coordinate work on 5G standardisation".

5G-ENSURE, one of the projects funded under Horizon 2020 phase 1 of the 5G PPP, drives the vision for a viable 5G network that is secure and trustworthy. 5G-ENSURE will deliver a 5G security architecture to expand the mobile ecosystem and enable entirely new business opportunities. It will provide an initial set of security and privacy enablers for the core 5G Reference Architecture, a test bed to demonstrate the enablers, and make early contributions to relevant standards bodies.

5G-ENSURE organised a one-day workshop in Sophia Antipolis, France on 16 June 2016. This proved to be the right forum to discuss and share technical insights into the security of 5G emerging from preliminary findings from 5G-ENSURE. It also and offered an opportunity to exchange European perspectives on security work and related standardisation actions within the project.

These discussions are helping to chart a course for coordinated work on 5G security with the involvement of 5G PPP projects, standards groups, international initiatives, and the 5G PPP Security Work Group.

OPENING KEYNOTE

Pavlos Fournogerakis, Programme Officer - EU Policies, Network Technologies, DG CONNECT, EC

"5G Standardisation and Security: Supporting the DSM Objective"

5G is an enabler of the digital economy. Common standards will ensure interoperability, guarantee that technologies work smoothly and reliably together, provide economies of scale, foster research and innovation and keep markets open. Europe must play a leading role in the drive towards 5G standardisation, help avoid a fragmented 5G by smoothly collaborating with all regions of the world through the joint declaration collaboration agreement signed with China, South Korea, Japan, and Brazil. The communication of the Digital Single Market on the ICT priorities on standardisation that the EU commission adopted in April 2016 indicates the importance of active participation of all the national players, standards groups and key stakeholders in definiting 5G standardisation from the very beginning. Bringing the vertical industry in the game from the onset is also very important in terms of standardisation for 5G to ensure compatibility with innovative use cases and their requirements.

Business verticals drive the 5G vision by introducing new and complex requirements in terms of softwarisation of the core network to support enhanced mobile broadband, massive machine type communication, and ultra-reliable and low latency communication, and in terms of security, which is transversal to many verticals. Another important aspect to consider is regulations and the impact on previous technologies. The EC is currently working on a manifesto for the industrial sector to indicate how to proceed for the deployment of 5G in key areas.

5G-ENSURE is the first 5G PPP project that deals with the horizontal area of security. In that respect, 5G-ENSURE will provide inputs to other 5G projects in defining the 5G security architecture, contributing significantly to the standardisation process in this area through participation in the most relevant standardisation bodies.

Session 1 - 5G ENABLERS FOR NETWORK AND SYSTEM SECURITY AND RESILIENCE

5G-ENSURE has a strong focus on 5G security needs with the aim of advancing 5G architecture, and the planned rollout of 5G security and privacy enablers, which will be validated in a security test bed. 5G-ENSURE drives the 5G PPP security vision as a pre-standardisation consensus builder. In practical terms, 5G-ENSURE will roll out two releases of the 5G enablers with open specifications, a software release and documentation. From a standards perspective, 5G-ENSURE aims to help shape implementation of the security architecture.

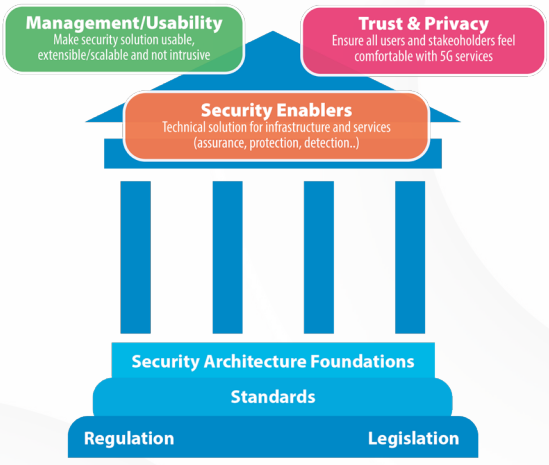
In early 2017, 5G-ENSURE will have results from its test bed, contributing to the global 5G-ENSURE position and push for standardisation. The plan is to map the security enablers at the network or protocol level for an enhanced version of the 3GPP-ETSI security architecture by working with other stakeholders, including 5G PPP projects in order to support all relevant 5G use-cases and business models.

Clearly, there has to be greater co-operation on security aspects. No single entity will have the solution and consensus for the global ecosystem. To deal with the complexity of 5G, we need a research road map and a security landscape at the EU level. Key concerns around network softwarisation include trust and liability.

5G-ENSURE is making direct contributions to the most relevant standards groups, through partner participation. The 3GPP is the main target, in particular the SA3 WG with its work on the security aspects of the next generation system and 3GPP RAN WG responsible for requirements and design of the new radio.

5G-ENSURE also contributes to ETSI TC CYBER on access control enforcement mechanisms and policy rules for PII protection on smart devices, cloud and Mobile Service with a proposed extension on specific 5G Privacy needs. 5G-ENSURE reviews its standardisation plan based on the outcomes of the workshop and public consultation with peers from the 5G PPP and other relevant stakeholders.

Key findings of the public consultation cover both security and privacy. Trust, AAA, Privacy, Security Monitoring, Network Management and virtualisation are all relevant areas for 5G security. Privacy in 5G should provide end-to-end data confidentiality and enable user control. Security certification is required to provide security assurance in 5G networks. Security in multi-tenant virtualisation scenarios requires isolation and monitoring mechanisms to avoid abuse.



5G -ENSURE pillars

SESSION 2: 5G THREATS AND CHALLENGES

Keynote by Adrian Belmonte, ENISA.

"ENISA Thematic Threat Landscape SDN & 5G"

5G is going to be a very important driver in implementing different technologies, like IoT and smart cities, and in enabling seamless communication between different layers. It is important to be prepared for current and new threats in cyber space. SDN/NFV is a key actor to improve security on 5G. ENISA is starting a new expert group to focus on security aspects of virtualisation. 5G is also an opportunity to implement security- and privacy-by-design. This requires the implementation of different actions to identify threats and attacks. Moreover, it is important to investigate the right trade-off as part of the debate about user surveillance. The work that ENISA is doing on Internet of Things could be very relevant to 5G. The EC is very interested in this discussion and results of the work in IoT and can bring to the table experts in this area.

Towards More Security and Privacy in the Digital World was the focus of the keynote from EIT Digital, whose action line on Privacy, Security and Trust pushes for security by design and privacy by design. Despite the many challenges, we need to turn data privacy and security into a business opportunity. 5G-ENSURE considers 5G privacy to be a key enabler for 5G. Homomorphic encryption could be one of the viable opportunities to protect data while not revealing the keys to untrusted parties. Several privacy enablers have been identified and specified in the first part of the project, taking into account the expertise of the partners in this area. The focus should be on constrained devices and understanding their actual capacity and limits in terms of processing capabilities and battery power to perform cryptographic operations.

SESSION 3: STANDARDS PANEL

EG-ENSURE is a timely project for security standardisation. However, it is important to move swiftly and push security aspects in standardisation. Security must be guaranteed both from the end-user's standpoint and the provider's, overcoming the false/wrong belief that the final user's interest may contrast with the correct management of information from a public interest perspective, for example, privacy. However, 5G security is not just a technical issue but also a business opportunity, as well as an opportunity to educate on social risk management. We need to ensure a minimal security baseline based on consistent technology and procedures.

ETSI ISG NFV has Working Groups to investigate a new NFV Management and Orchestration (MANO) Framework that has impact on others including Interfaces and Architecture (IFA), Security (SEC) and Reliability (REL) WG. NFV enables Network Functions to run on commodity servers as pure software entities with high impact on rises in revenue and CAPEX/OPEX saving.
In the area of security, it is key to analyse the threats to security in virtualised environments and derive service and security requirements.

The role of DevOps with continuous integration and deployment might be the source of more threats. While this brings several additional challenges, it also a chance for Telco operators to reduce time-to-market. The important areas of activity concern the definition of appropriate measures for operational efficiency and features to support regulatory requirements, e.g. Lawful

Intercept, Privacy and Data Protection. Close monitoring of de-facto standards for virtualisation, like OpenStack and Dockers, is important as the time to the market is reduced compared to standardisation solutions that require time to reach wide consensus.

On-going work within 3GPP SA3 illustrates the importance of taking action now on standardisation, with the initial results expected by the end of 2016. The 5G standardisation process has just begun and new use cases still under development, so potential impact on new security requirements is still an open book.

A lot of security aspects are being analysed at the moment, such as authentication and subscriber privacy, presenting opportunities for 5G-ENSURE to make contributions.

5G increases the need for lawful interception mechanisms. Given the many overlapping contributions, co-operation is key to delivering co-sourced contributions. The 5G PPP Pre-Standardisation Work Group also see co-operation as the way forward to reach a common agreement and provide co-signed contributions to SDOs.

Most 5G applications bring a variety of players with different interests and new market openings will bring many new roles. Regulation plays a very important role.

5G-ENSURE Research Topics	Targeted Standards Groups
5G Security specific use cases **5G Trust Model** **5G Security requirements** **5G Security architecture** **AAA GE & Privacy GE**	TSG Service and System Aspects (TSG-SA) group SA WG2 Architecture SA WG3 – Security RAN – Radio Access Network
Network Management & Virtualisation isolation GE **Security Monitoring GE** **AAA GE** **Privacy GE**	Network Functions Virtualisation (NFV ISG) Technical Committee (TC) Cyber Security (CYBER) Technical Committee Smart Card Platform (TC SCP)
Network Management & Virtualisation isolation GE	OpenFlow™ and SDN
AAA GE **Network Management & Virtualisation isolation GE**	Authentication and Authorization for Constrained Environments (ACE) Network Function Virtualization Research Group (NFVRG)
5G trust model **5G Security requirements**	Security & Fraud Risk Assessment (SFRA)

Open Consultation Services & WG Security

CONSENSUS BUILDING

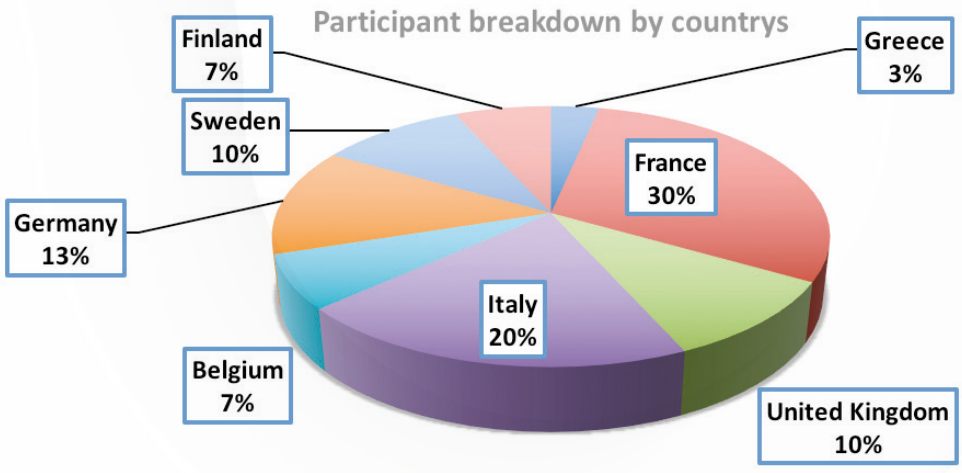
WRAP UP and CONCLUDING REMARKS

The main recommendations from the audience in the concluding session will help in the drive towards a future 5G-connected digital society based on a secure-by-design approach, where security is an integral component of the architecture design.

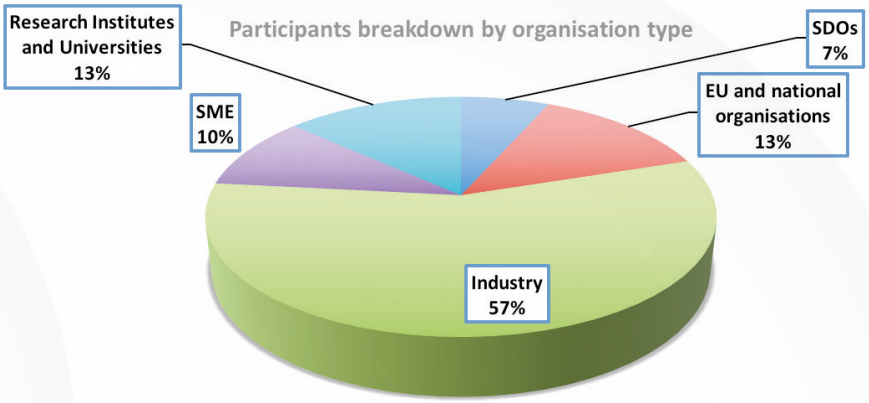
- It is important to associate a value to security and privacy and define the right balance from a social perspective to ensure that security does not come at the expense of privacy. Minimum security is not always a bad choice and several security levels should be defined to support a wide range of scenarios.
- Privacy is a very challenging topic in the coming years.
- Accounting is the important factor missing of the AAA solutions for 5G. Access management is also very challenging for the future.
- Security aspects in bringing DevOps operations to the ecosystem should be investigated further to understand the impact on potential threats to 5G networks.
- Liability is one of the most important factors and more work should be done to connect the legal and technical aspects and find the best solution to transfer the outcome into the legislation framework.
- It is important to define a-priori the minimum level of security and minimum and maximum tolerable level of trusted infrastructure that 5G network needs to deliver in order to implement a single access of digital services without compromising the security against attacks and with no impact on the freedom of users.
- 3GPP and ETSI have been confirmed as the most relevant SDO for the security aspect of the 5G.

Who attended?

Around 30 international stakeholders participated to the 5G-ENSURE 1st workshop on security standardisation and a total of 8 countries were represented. The largest regional grouping came from France with 30%, much to be expected given the location of the meeting in Sophia Antipolis. Italy represented 20% of the participants, Germany 13%, and Sweden 10%.



Representation from the industry was the highest, followed by funding agencies and government, which reflect perfectly the main 5G-ENSURE target audience.



Programme:

The detailed programme, the speaker profiles and presentations are available at:

http://www.5gensure.eu/agenda-1st-international-workshop-5g-security-standardisation and reported below

	Agenda for the 1st EG-ENSURE Workshop on 5G Standardisation
9:00 - 10:00	Registration and Welcome Coffee
10:00 - 10:30	***Opening and Welcome***
	Welcome Speech - *Petteri Mannersalo, VTT and 5G-ENSURE project coordinator* **Keynote**: *5G standardisation and security: supporting the DSM Objectives* *Pavlos Fournogerakis, Programme Officer – EU Policies, Network Technologies, DG CONNECT, EC*
	SESSION 1: 5G ENABLERS FOR NETWORK AND SYSTEM SECURITY AND RESILIENCE
10:30 - 11:45	*"Security must be built into the 5G architecture right from the start!" What is the security vision of 5G-ENSURE? What are the key enablers for security and privacy? What are the standardisation priorities to ensure the necessary trust and confidence and release the full potential of 5G networks?* *The session will provide answers to these questions with technical insights on preliminary results of the 5G-ENSURE project.* *5G-ENSURE Project* *Petteri Mannersalo, 5G-ENSURE coordinator, VTT* *Security enablers for 5G network* *Pascal Bisson, Thales Services* *Security in 5G standardisation* *Paolo De Lutiis, TIM IT* *The importance of co-operation: 5G-ENSURE approach* *Jean-Philippe Wary, Orange* *Findings from 5G-ENSURE open consultation* *Luciana Costa, TIM IT* *Open discussion*

11:45 - 12:15	*Networking Coffee Break*
12:15 - 13:15	**SESSION 2: 5G THREATS AND CHALLENGES - Moderator: Nina Olesen, EOS & CYSPA**
	"Having a clear understanding of the new threats and security issues to build secure 5G network" What are the main security challenges? How the threats landscape is evolving? *The session provides the perspectives from security experts on security and privacy challenges and an overview on the emerging security threats raised by the adoption of new technology in the next generation network.* **Keynote**: *Towards More Security and Privacy in Digital World* *Jovan Golic, TIM IT & EIT Digital – Presented by Luciana Costa, TIM* **Keynote**: *ENISA Thematic Threat Landscape SDN & 5G* *Adrian Belmonte, ENISA*
13:15 - 14:30	*Networking Lunch*
14:30 -	**SESSION 3: STANDARDS PANEL - Moderator: Bengt Sahlin, Ericsson**
16:00	*"Creating a collaborative standards organisation ecosystem is vital for the success of 5G Security" How do we set the standards for a secure 5G? No single standards organisation (e.g. ETSI, ITU, 3GPP, oneM2M, etc.) will be able to standardise 5G security. How can ITU, 3GPP, ETSI, 5GPPP, and others contribute to creating the standard for 5G?* *The section provides a focus on some of the hot security topics, on the on-going study items and work required.* *A Technology Enabler for 5G NFV aspect* *Zarrar Yousaf, NEC Laboratories Europe* *3GPP Security in 5G* *Alf Zugenmaier, Munich University of Applied Sciences & Vice-Chairman 3GPP SA3* *Security and privacy issues for present and 5G communications: a use case on user localisation* *Luca Pesando, TIM* *5G Security and Standardization* *Hugo Tullberg, Ericsson, chair of the 5G PPP Work Group Pre-standardization* **Round table**: *How do we make sure standards have security by design/default? What we can drive security in 5G specification?*
16:30	**Wrap-up and Close of Workshop**

Authors

Stephanie Parker, Trust-IT Services (UK)
Roberto G. Cascella, Trust-IT Services (UK)

Acknowledgements

Luciana Costa, TIM (IT)
Paolo De Lutiis, TIM (IT)

5G ENSURE receives funding from the EU Framework Programme for Research and Innovation H2020 under grant agreement No 671562. Duration November 2015 - October 2017.

The 5G Infrastructure Public Private Partnership (5G PPP)