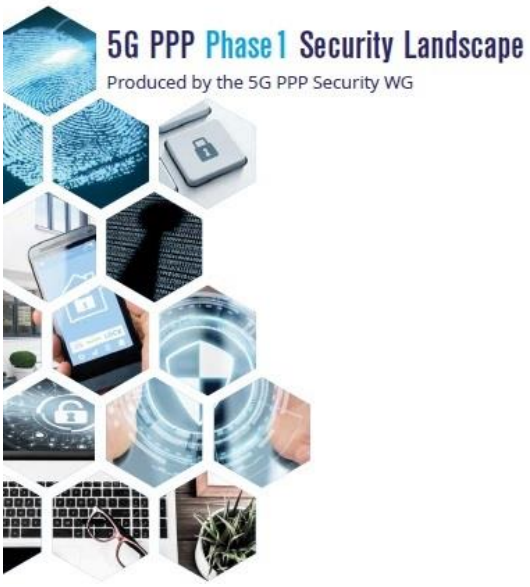
Outcomes of the workshop "**5G Security: Phase 1 landscape and foreseen evolutions**" took place at Oulu, on 12-of June.

EuCNC - the best venue to present the work of the Security WG after one year of activities.

Pascal Bisson, technical coordinator of 5G-ENSURE and also one of the chairs of the Security WG, opened the workshop providing an overview of the working group. The main objective that motivated its constituency - according to what reported by Pascal - is to reach a view on priority security aspects of 5G network that is coherent and consistent across the 5G PPP Phase I projects.

The result is the Security Landscape whitepaper launched on the occasion of the EuCNC workshop, produced with the co-operation work of several 5G PPP phase I projects.

This white paper looks like a must-read for 5G security folks, **Patrick Donegan, HardenStance**



The first session of the workshop was devoted to sharing the main findings of the whitepaper with ad-hoc presentations targeting specific security aspects selected as priorities for 5G.
The major *5G security risks and requirements* as foreseen by the 5G PPP Phase 1 projects were presented. As reported during the workshop, these are findings. They do not claim to be final but representatives of Phase 1 projects and that aim to be completed by other projects (starting first from 5G-PPP Phase 2, then Phase 3) to cover all important aspects would they be generic or specific (e.g. related to some vertical markets).
The high-level *Security Architecture for 5G network* was illustrated. The logical characteristic of the 5G network, the support of multi domains and the management aspects are only a subset of the design principles reported as building factors for the architecture design. They resulted from an agreement vision between the projects involved. The architecture was presented in its first "iteration" and highlighted some of the work on-going regarding second iteration to come.
Privacy is also another aspect covered during the workshop, where concerns were reported considering the perspective of various 5G stakeholders (users, service providers and law enforcement). While the list of these concerns does not claim to be exhaustive, it is a good illustration of the many facets of privacy in 5G, together with the main challenges. Some suggestions on how to address privacy issues were also provided as part of the workshop. The important message is that a Privacy by design framework should be established and applied over the 5G infrastructure (operator under regulation) but at the same time over services from vertical industries, with each potential actor contributes to the entire E2E delivery of 5G services.
Another discussion point was *Trust* aspects of 5G network. 5G faces a complex trust issue because of the different roles played by the stakeholders. According to the view of the Security WG trust assumptions should be an explicit part of the security architecture and trust concepts also have to evolve to liability concepts between actors of the 5G ecosystem.
Security monitoring and management was another point raised as being important and should be included by design. Several questions were shared with the attendees, such as: How to combine the needs for end to end security monitoring with the request for strong isolation between slices, How to adapt in real time an end to end security monitoring system. These are some of the key challenges highlighted for future research to further advance 5G security.
Security standardization plays a key role in 5G PPP projects. As presented during the workshop some actions have been performed by each single project to help ensure security, privacy and liability issues natively addressed in the standardisation processes according to the "Security by Design" approach. The next step for the 5G PPP Security WG is to encourage co-signed contributions to be elaborated by the H2020 projects and presented to the relevant standardisation organisations/groups considered to be the most applicable.

Pascal Bisson concluded the first session of the workshop indicating the next objective for the Security WG, which *is ensuring further advances of the 5G Security Vision and also its realisation by taking advantage not only of the findings but also of assets coming from Phase 1 projects*. The concrete action in this respect is taking 5G-PPP Phase 2 projects on-board, with a face-to-face meeting planned in the Autumn as the opportunity to update the work pan also with the engagement of Phase 2 projects.

Emmanuel Dotaro, head of ICT & Security labs at Thales Secure Communications & Information Systems, gave an interesting keynote on 5G and Security Transformation.

The workshop panel discussion on "5G Security Perspectives" brought together key invited speakers as representatives from SMEs, manufacturers, researchers and verticals.

Gabriele Rizzo explained the vision on 5G security as head of Strategic Innovation within Leonardo, where he is CTO, and also as professional futurist advisor to NATO ACT, and NATO expert for Cyberspace and Cyber Defence. Tommi Parnila, gave his perspective as Senior Security Consultant at Nixu cyber security company. Raimo Kantola provided his view as professor of Networking Technology at Aalto University, Communications and Networking, in Finland. Finally, Olav Queseth provided his perspective as both researcher at Ericsson and project leader of the METIS-I and II projects.

The panel was an opportunity to discuss 5G specific security needs/requirements, especially related to vertical domains. Based on their knowledge of the "security" eco-system and on the insights gathered from the work done and presented during the Security WG workshop, the invited speakers provided suggestions on security aspects not covered or requiring further investigation in future work

Gabriele Rizzi is Head of Strategic Innovation withn the CTO of Leonardo.

Olav Queseth is master researcher at Ericsson

Tommi Parnila is Senior Security Consultant with Nixu.

Raimo Kantola is full professor of Networking Technology at Aalto University, Communications and Networking, Finland.

5G-ENSURE exhibition stand at EuCNC

The EuCNC event gives also an opportunity for many Phase 1 projects to host a booth in the exhibition area and showcase their main achievements.

5G-ENSURE partners VTT, Thales, NIXU and SICS were hosts and played a key role in providing and showing the demos and videos on display. The EuCNC exhibition was an important opportunity to show in action some of the security and privacy enablers developed within 5G-ENSURE.

The demo presented by VTT was in two parts. The first part showed how the enablers can detect anomalies from a substantial network attack, thereby blocking suspicious users.

The second part featured an end-to-end connection between VTT and b<>com testbed. The demonstration basically showed how to gain the access to a website running in the microsegment at b<>com premises using IMSI.

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

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

Sample of our photo gallery

Figure 1: Visitors at our EuCNC Stand

Figure 2: Pavlos Fournogerakis, EC visits the stand

Figure 3: Jean-Pierre Bienaimé, Secretary General 5G IA

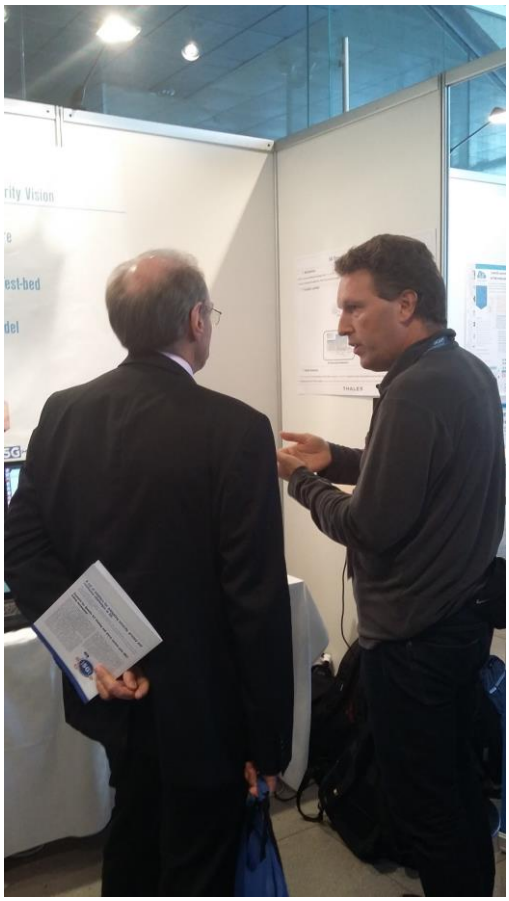


Figure 4: Special Thanks to the Team