



Grant Agreement No.: 871808
Research and Innovation action
Call Topic: ICT-20-2019-2020: 5G Long Term Evolution



INtelligent Security and Pervaslve tRust for 5G and Beyond

D6.2: Intermediate Report on dissemination, communication and standardisation activities

Version: v1.0

Deliverable type	R (Document, report)
Dissemination level	PU (Public)
Due date	30/04/2021
Submission date	14/05/2021
Lead editor	Antonio Pastor (TID)
Authors	Pol Alemany , Charalampos Kalalas , Raul, Muñoz , Ricard Vilalta(CTTC), Anastasios Kafchitsas, Sabina Sandia, Orestis Mavropoulos (CLS), Vincent Lefebvre (TAGES), Chafika Benzaid (AALTO), Ramon Sanchez, Antonio Skarmeta (UMU), Uwe Herzog, Milon Gupta (EURES), Diego Lopez (TID), Maria Christopoulou (NCSRD), Gürkan Gür (ZHAW), Edgardo Montes de Oca (MI), Pawani Porambage (UOULU), Dhouha Ayed, Geoffroy Chollon (TSG)
Reviewers	Gürkan Gür (ZHAW), Orestis Mavropoulos (CLS)
Work package, Task	WP6, T6.1, T6.2 & T6.3
Keywords	Dissemination, communication, standardisation

Abstract

This deliverable D6.2 presents a detailed statement for the outreach activities in the INSPIRE-5Gplus project. This document is the second report after the deliverable D6.1, which covers the activities' initial planning. D6.2 covers all activities accomplished up to month M18, i.e. 30/04/21. Moreover, an initial section with a summary of the target KPI figures is included, for reference.



Document revision history

Version	Date	Description of change	List of contributor(s)
v0.1	23/01/2021	First draft version	TID; UMU
v0.2	13/04/2021	Consolidated contributions	MI, UMU, TID, UOULU, CTTC, EURES, ZHAW, TSG, NCSRD
v0.3	20/04/2021	Updated contributions	MI, UMU, TID, UOULU, CTTC, EURES, ZHAW, TSG, NCSRD
v0.4	21/04/2021	Added M1-M6 contributions and communication news	UMU, EURES, TAGES
v0.5	23/04/2021	Abbreviations and editorial corrections	TID, UMU, EURES
v0.6	29/04/2021	Reviewed version	ZHAW, CLS, TID
v0.7	30/04/2021	Final editing, sending for GA approval	EURES
1.0	14/05/2021	Implement comments received during GA approval	EURES

List of contributing partners, per section

Section number	Short name of partner organisations contributing
Section 1	TID
Section 2	MI, UMU, TID, UOULU, CTTC, EURES, ZHAW, TSG, NCSRD, CLS, TAGES, AALTO
Section 3	TID, ZHAW, UMU
Section 4	TID, UMU

Disclaimer

This report contains material which is the copyright of certain INSPIRE-5Gplus Consortium Parties and may not be reproduced or copied without permission.

All INSPIRE-5Gplus Consortium Parties have agreed to publication of this report, the content of which is licensed under a Creative Commons Attribution-Non-Commercial-NoDerivs 3.0 Unported License¹.

Neither the INSPIRE-5Gplus Consortium Parties nor the European Commission warrant that the information contained in the Deliverable is capable of use, or that use of the information is free from risk, and accept no liability for loss or damage suffered by any person using the information.



CC BY-NC-ND 3.0 License – 2019-2021 INSPIRE-5Gplus Consortium Parties

Acknowledgment

The research conducted by INSPIRE-5Gplus receives funding from the European Commission H2020 programme under Grant Agreement No 871808. The European Commission has no responsibility for the content of this document.

¹ http://creativecommons.org/licenses/by-nc-nd/3.0/deed.en_US



Executive Summary

This deliverable D6.2 presents a detailed description of the project's outreach activities done until M18. The document reminds the list of KPIs defined in document D6.1 and the status of their accomplishment (Section 1). The activities are categorized in communications, dissemination (Section 2) and standardisation (Section 3). Activities in Section 2 aim to increase the impact and the visibility of the INSPIRE-5Gplus project. Meanwhile, Section 3 actions concentrate on industry standards visibility and adoption.

The main activities in communication are: 14 publications in journals, such as IEEE, ACM, or Elsevier; 12 papers/presentations in different congresses and conferences; 29 additional dissemination events (keynotes, invited talks, booths, etc.); one workshop co-organized with IEEE 5G World Forum; one white paper and collaboration in three others (two of them still in progress or to be published); one award in Spain; two iterations in the project flyer; and 24 news items via the web page.

Related to standardisation results, several contributions into documents have been made focusing on different SDO. Active participation was carried out in six groups in ETSI, three in IETF and one in IEEE. Finally, contributions have been made in two relevant industrial groups, namely GSMA and ECSC.



Table of Contents

Executive Summary	3
Table of Contents	4
List of Figures	5
List of Tables	6
Abbreviations.....	7
1 Introduction	9
2 Communication and dissemination activities	10
2.1 Goals, objectives and KPIs summary	10
2.2 Communication and dissemination results on first period	12
2.2.1 Publications.....	12
2.2.2 Other dissemination activities	18
2.2.3 Workshop Organization	20
2.2.4 White papers.....	21
2.2.5 Awards/Mentions	21
2.2.6 Flyer	22
2.2.7 Website	22
2.2.8 Social Media.....	25
3 Standardisation activities	28
3.1 Standards-related strategy summary.....	28
3.2 Standards-related results	28
3.2.1 ETSI.....	28
3.2.2 ITU-T.....	29
3.2.3 IETF/IRTF	29
3.2.4 IEEE.....	30
3.2.5 Industrial groups	31
4 Communications and Dissemination KPIs	32
5 Conclusions.....	34
Appendix A INSPIRE-5Gplus revised project flyer.....	35
Appendix B Workshop on 5G Security – Call for papers	36



List of Figures

Figure 1: 5G Rescue banner 22

Figure 2: News items 23

Figure 3: Website visitors — 1 November 2019 - 30 April 2021 24

Figure 4: Top Tweets of INSPIRE-5Gplus 26

Figure 5: INSPIRE-5Gplus activity on LinkedIn 27



List of Tables

Table 1: INSPIRE-5Gplus Target Audiences (TAs).....	11
Table 2: KPIs for communication activities	12
Table 3: KPIs for dissemination activities.....	12
Table 4: Other dissemination activities.....	20
Table 5: Agenda of organised workshop at IEEE 5G World Forum 2020	20
Table 6: Regional distribution of website visitors — 1 November 2019 - 30 April 2021	25
Table 7: KPIs and achieved results for communication activities	33
Table 8: KPIs and achieved results for dissemination activities.....	33



Abbreviations

3GPP	3rd Generation Partnership Project
5G PPP	The 5G Infrastructure Public Private Partnership
CDX	Cyber Defence Exercises
CERT/CSIRT	Computer Emergency Response Team / Computer Security Incident Response Team
COSE	CBOR Object Signing and Encryption
DGKA	Dynamic Group Key Agreement
DL	Deep Learning
DLT	Distributed Ledger Technologies
EAP	Extensible Authentication Protocol
EDHOC	Ephemeral Diffie-Hellman Over COSE
EMU	EAP Method Update
ENI	Experiential Networked Intelligence
ETI	Encrypted Traffic Integration
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
GSMA	Global System for Mobile Communications Alliance
I2NSF	Interface to Network Security Function
ICT	Information Communications Technology
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IRTF	Internet Research Task Force
ISO	International Organization for Standardisation
ITU	International Telecommunication Union
KPI	Key Performance Indicators
LPWAN	Low Power Wide Area Network
MEC	Multi-access Edge Computing
MIMO	Multiple-Input and Multiple-Output
MTC	Machine-Type Communication
NFV	Network Function Virtualisation
NFVI	NFV Infrastructure
NIS	Network and Information Systems
P2MP	Point to Multi-Point
QKD	Quantum Key Distribution
RFC	Request For Comments



RTO	Research Technology Organization
SAI	Securing Artificial Intelligence
SDN	Software-defined networking
SDO	Standard Development Organisations
SFC	Service Function Chaining
SLA	Service Level Agreement
SME	Small Medium Enterprise
SRIA	Strategic Research and Innovation Agenda
TA	Target Audiences
TEE	Trust Execution Environment
UAV	Unmanned Aerial Vehicle
V2X	Vehicle-to-everything
VNF	Virtualised Network Function
VSF	Virtual Security Function
ZSM	Zero-touch network and Service Management



1 Introduction

The Deliverable 6.2 – “Intermediate Report on dissemination, communication and standardisation activities” details on the actions done to maximize the impact of the results of the INSPIRE-5Gplus project:

- Communication that covers all the activities to increase the general visibility and impact of the project. It includes flyers, white papers, newsletter, etc. Also, several tools have been activated and improved over the M1-M18 period. This is the case of the web portal and various social media channels (Twitter, YouTube, and LinkedIn).
- Industrial and scientific dissemination. The objective is to increase the visibility to specialized groups, stakeholders, or regions and foster an interchange of knowledge that can enrich the results of the INSPIRE-5Gplus. In the area of academic dissemination, dedicated efforts have been made in publications over multiple disciplines around networks, 5G and security, as well as several workshops related activities. Industrial dissemination has not lagged, and several invited talks, keynotes and presentations have been made in the telecom and security areas.
- Standardisation actions are in progress with a particular focus on the most relevant bodies in the Telecom area (ETSI, ITU), communication (IEEE) and internet protocols (IETF). Also, a special collaboration with European Public Private Partnerships (PPP) has been pursued. This is the case for 5GPPP and ECSO.



2 Communication and dissemination activities

2.1 Goals, objectives and KPIs summary

As described in the DoW and D6.1, INSPIRE-5Gplus targets several dissemination and communication channels to raise awareness of the project's ambitions and results among the public and stakeholders.

The first phase (M1-M6) initiated awareness of the project's goals through the creation and distribution of marketing material, participation in social media and events, publication of papers and articles, and collaboration in 5G-PPP Working Groups (WGs).

The next phase (M7-M18) extended the community outreach and engagement with contributions to Standard Development Organisations (SDOs), and the definition of joint use and test cases leveraging 5GPPP facilities.

During the 2nd half of the project, these activities will be developed further to obtain global outreach and engagement.

The target audiences have been identified that include end-users (e.g., researchers, security solution providers, CSIRTs/CERTs, 5G stakeholders), administrations, policy-makers, citizens, standardisation bodies, etc. INSPIRE-5Gplus is actively contributing with the intention of informing, fostering cooperation, improving training, obtaining feedback, and advancing the state of the art related to security requirements and management. The activities that have been undertaken, and those that are planned, are presented in more detail in the Subsection 2.2.

Overall, how the different audiences have been targeted or are planned to be targeted are summarised in the following table.

End-user TA	Interest in the project	Main activities done or planned
A —Academic and RTOs	<ul style="list-style-type: none"> Advancing post-project research; Training. 	Several new research projects and training curricula are being planned. Publication of many papers and presentations in events.
B —Cyber security providers	<ul style="list-style-type: none"> Utilising project's results; Fostering cooperation. 	Collaborations established within the project (SMEs MI and TAGES, TAGES and ORANGE) and with other SMEs (e.g., R2System, Cumucore)
C —CSIRTs / CERTs and Law enforcement	<ul style="list-style-type: none"> Implementing the recommendations of the NIS directive; Advancing incident handling, response and recovery support capabilities. 	Presentations of project to law enforcement agencies (e.g., DGA in France)
D —Cyber training and CDX actors	<ul style="list-style-type: none"> Techniques and training methods; Advancing skills for professionals. 	Collaboration with SPIDER (spider-h2020.eu/) project to apply some 5G enablers in cyber exercises (TID)
E — 5G-PPP Community	<ul style="list-style-type: none"> Presenting advances in 5G Working Groups and ECSO WG6 (SRIA). 	Participation and presentations in several 5GPPP WG (e.g., 5G PPP



		Architecture WG, SME WG, TMV WG)
Other TAs	Interest in the project	Main activities done or planned
F — ECSO cPPP	<ul style="list-style-type: none"> Establishing collaborations; Co-organising events. 	Collaboration in WG6 and research challenges proposal
G —Consortia from SU calls and relevant projects	<ul style="list-style-type: none"> Sharing knowledge and tools Collaboration. 	Several planned workshops organised in prestigious conferences (e.g., Ares, EUCnC)
K —Media & General public	<ul style="list-style-type: none"> Informing; Stimulating innovation; Value of funding. 	Website, flyers, newsletters
L —Standards bodies and open-source communities	<ul style="list-style-type: none"> Developing roadmaps; Inputs for standardisation; Open-source innovation and Open science. 	Several contributions to standards (e.g., NFV SEC 024)

Table 1: INSPIRE-5Gplus Target Audiences (TAs)

The KPIs used to measure the impact of communication and dissemination activities are presented in the two tables below. These tables include updated KPI values to be reached by the project, until project end, under the changed situation of the pandemic.

Communications means	Type	Success indicator	Target # of outputs	Targeted values
Project website	Online	# of visitors	1	1000 unique visitors/year
Social Media	Online Presence	# of users	4 social media channels	300 followers in Twitter / LinkedIn / YouTube / SlideShare
Promotional videos	Online Distribution	# of views	5	> 500 views
Press releases	Online publications	# of elements	10	500 cybersecurity stakeholders
Project meetings / roundtables	Events	# of events	10	> 40 internal and invited stakeholders
Workshops/showcases	Events	# of events / attendees	5	250 participants in total
Policy-level events in Brussels	Events	# of events	2	> 60 cybersecurity policy makers
Newsletters, factsheets	Publications	# of publications	15	> 500 subscribers
White papers	Publications	# of publications	4	500 recipients
Deliverables (public)	Publications	QA standards	> 20	500 recipients



Brochure and annual report	Publications	# of stakeholders	3 ²	500 recipients
Liaison with ECSO, participation in WGs and events	Events	# attended events	> 6	> 50 participants per event
Liaison activities, common events with other H2020 projects, knowledge exchange	Networking	# of relevant projects # of joint workshops	10 3	> 100 researchers on projects
Liaison with relevant SDOs	Networking	# of active contributions to standards	5	Cybersecurity community

Table 2: KPIs for communication activities

KPIs	Targeted values
Publication in scientific journals/books	> 10
Communications in International Conferences	>15
Participation in public industry exhibitions	>5
White papers	>3
Event organisation	> 5
Deliverables	> 20

Table 3: KPIs for dissemination activities

2.2 Communication and dissemination results on first period

2.2.1 Publications

Publishing project outcomes in prestigious journals, magazines or conferences is a fundamental vehicle to disseminate the technical advances achieved in the project. In the following, we present the works published or already accepted for their publication.

M01-M06:

- INSPIRE-5Gplus Consortium. (2020) 'INSPIRE-5Gplus: Intelligent Security and Pervasive Trust for 5G and Beyond', European 5G Annual Journal. Available at: <https://bscw.5gppp.eu/pub/bscw.cgi/d356008/Full%205G%20Annual%20Journal%202020.pdf>

Contribution related to INSPIRE-5Gplus: This paper presents the vision, main objectives and expected results of the project to the 5GPPP ecosystem.

² There was an error in the "KPIs for communication activities" in D6.1. The correct value is 3 (was 300 in D6.1).



- Zhang, P. et al. (2020) 'Physical Layer Authentication for Massive MIMO Systems With Hardware Impairments', IEEE Transactions on Wireless Communications, 19(3), pp. 1563–1576. doi: 10.1109/TWC.2019.2955128.

Contribution related to INSPIRE-5Gplus: The paper proposes a new channel-based authentication scheme for massive MIMO systems with different levels of hardware impairments and investigates its authentication behaviours. False alarm and detection probabilities were theoretically analysed with hypothesis testing and matrix transformation approaches. The paper is related to work conducted in WP3.

- Benzaid, C. and Taleb, T. (2020) 'AI-Driven Zero Touch Network and Service Management in 5G and Beyond: Challenges and Research Directions', IEEE Network, 34(2), pp. 186–194. doi: 10.1109/MNET.001.1900252.

Contribution related to INSPIRE-5Gplus: The paper introduces the ZSM concept and points out the AI-based limitations and risks that need to be addressed to make ZSM a reality. The paper is related to work conducted in WP2.

- Benzaid, C. and Taleb, T. (2020) 'ZSM Security: Threat Surface and Best Practices', IEEE Network, 34(3), pp. 124–133. doi: 10.1109/MNET.001.1900273.

Contribution related to INSPIRE-5Gplus: The paper introduces the potential ZSM's attack surface and recommends possible mitigation measures along with some research directions to safeguard ZSM system security. It is related to work conducted in WP2 and WP3.

- Hewa, T. et al. (2020) 'The Role of Blockchain in 6G: Challenges, Opportunities and Research Directions', in 2020 2nd 6G Wireless Summit (6G SUMMIT). IEEE, pp. 1–5. doi: 10.1109/6GSUMMIT49458.2020.9083784.

Contribution related to INSPIRE-5Gplus: This work explores the role of blockchain enablers to address formidable challenges of B5G, future application opportunities (e.g., decentralized, and trustworthy 6G communications infrastructure and solutions) and potential research directions including security. The paper is related to work conducted in WP2 and WP3.

- Benzaid, C., Boukhalfa, M. and Taleb, T. (2020) 'Robust Self-Protection Against Application-Layer (D)DoS Attacks in SDN Environment', in 2020 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, pp. 1–6. doi: 10.1109/WCNC45663.2020.9120472.

Contribution related to INSPIRE-5Gplus: This paper proposes a robust application-layer DDoS self-protection framework. The framework empowers a fully autonomous detection and mitigation of the application-layer DDoS attacks, leveraging Deep Learning (DL) and Software Defined Networking (SDN) enablers. A key contribution of this work is to build a DL-based application-layer DDoS detection model that is robust to adversarial examples. The paper is related to work conducted in WP3.

M07-M18:

- Torroglosa-Garcia, E. M. et al. (2020) 'Enabling Roaming Across Heterogeneous IoT Wireless Networks: LoRaWAN MEETS 5G', IEEE Access, 8, pp. 103164–103180. <http://doi.org/10.1109/ACCESS.2020.2998416>.

Contribution related to INSPIRE-5Gplus: Proposal enabling interoperability between 5G network and Low Range Wide Area Network (LoRaWAN) through a novel handover roaming mechanism for



LoRaWAN that relies on the trusted 5G network to perform IoT device's authentication and key management; thereby extending the mobility and roaming capabilities of LoRaWAN to global scale. This paper is related to work conducted in WP3.

- Molina Zarca, A. et al. (2020) 'Semantic-Aware Security Orchestration in SDN/NFV-Enabled IoT Systems', *Sensors*, 20(13), p. 3622. <http://doi.org/10.3390/s20133622>.

Contribution related to INSPIRE-5Gplus: This paper presents a semantic-aware, zero-touch and policy-driven security orchestration framework for autonomic and conflict-less security orchestration in SDN/NFV-aware scenarios while ensuring optimal allocation and Service Function Chaining (SFC). It is related to work in WP3.

- Hermosilla, A. et al. (2020) 'Security Orchestration and Enforcement in NFV/SDN-Aware UAV Deployments', *IEEE Access*, 8(3), pp. 131779–131795. <http://doi.org/10.1109/ACCESS.2020.3010209>.

Contribution related to INSPIRE-5Gplus: This paper proposes a novel NFV/SDN-based zero-touch security management framework for automatic orchestration, configuration, and deployment of lightweight VSF in MEC-UAVs that considers diverse contextual factors, related to both physical and virtual conditions, to optimize the security orchestration. The paper is related to work in WP3.

- Siriwardhana, Y. et al. (2020) 'The Fight Against the COVID-19 Pandemic With 5G Technologies', *IEEE Engineering Management Review*, 48(3), pp. 72–84. <http://doi.org/10.1109/EMR.2020.3017451>.

Contribution related to INSPIRE-5Gplus: This paper discusses 5G's role in the fight against COVID-19 and integrates the 5G security and liability aspect as a key topic in addition to others such as relevant 5G use-cases. It is related to work in WP2.

- Manso, C. et al. (2021) 'End-to-End SDN/NFV Orchestration of Multi-Domain Transport Networks and Distributed Computing Infrastructure for Beyond-5G Services', *IEICE Transactions on Communications*, E104.B(3), pp. 188–198. <http://doi.org/10.1587/transcom.2020NVI0001>.

Contribution related to INSPIRE-5Gplus: This paper presents an integrated End-to-end slicing platform that allows the deployment of multiple network slices across multiple network control domains. The reported orchestration mechanisms will be the basis for demonstrating WP5 TC1 activities.

- Ortiz, J. et al. (2020) 'INSPIRE-5Gplus: Intelligent Security and Pervasive Trust for 5G and Beyond Networks', in *Proceedings of the 15th International Conference on Availability, Reliability and Security*. New York, NY, USA: ACM, pp. 1–10. <http://doi.org/10.1145/3407023.3409219>.

Contribution related to INSPIRE-5Gplus: This paper presents the INSPIRE-5Gplus' High Level Architecture. It is related to work in WP2.

- Taçyıldız, Y. B. et al. (2020) 'Dynamic Group Key Agreement for Resource-constrained Devices Using Blockchains', in *Proceedings of the 15th International Conference on Availability, Reliability and Security*. New York, NY, USA: ACM, pp. 58–76. http://doi.org/10.1007/978-3-030-61638-0_4.



Contribution related to INSPIRE-5Gplus: This paper presents a dynamic group key agreement protocol for IoT (resource-constrained devices) in 5G networks using permission-based blockchains. It is related to work in WP3.

- Alemany, P. et al. (2020) 'Peer-to-Peer Blockchain-based NFV Service Platform for End-to-End Network Slice Orchestration Across Multiple NFVI Domains', 2020 IEEE 3rd 5G World Forum (5GWF), 2020, pp. 151-156, doi: 10.1109/5GWF49715.2020.9221311.

Contribution related to INSPIRE-5Gplus: This paper presents the idea of a Blockchain network in which its peers are Network Slice Manager domains that aim to collaborate among them to deploy End-to-End Network Slices. The initial architecture and experiments in an emulated environment are presented. This paper is related to work in WP4, Task 4.1.

- Benzaid, C. and Taleb, T. (2020) 'AI for Beyond 5G Networks: A Cyber-Security Defense or Offense Enabler?', IEEE Network. New York, NY, USA: IEEE, 34(6), pp. 140–147. <http://doi.org/10.1109/MNET.011.2000088>.

Contribution related to INSPIRE-5Gplus: The paper sheds light on how AI may impact the security of 5G and its successive from its posture of defender, offender, or victim, and recommends potential defenses to safeguard from malevolent AI while pointing out their limitations and adoption challenges. The paper is related to work in WP2.

- Osorio, D. P. M. et al. (2020) 'Safeguarding MTC at the Physical Layer: Potentials and Challenges', IEEE Access. New York, NY, USA: IEEE, 8(6), pp. 101437–101447. <http://doi.org/10.1109/ACCESS.2020.2996383>.

Contribution related to INSPIRE-5Gplus: This work provides an overview on some promising physical-layer security techniques by focusing on the special requirements and design challenges for machine-type communication scenarios. This paper is related to work conducted in WP2.

- Siriwardhana, Y. et al. (2020) 'Performance Analysis of Local 5G Operator Architectures for Industrial Internet', IEEE Internet of Things Journal. New York, NY, USA: IEEE, 7(12), pp. 11559–11575. <http://doi.org/10.1109/JIOT.2020.3024875>.

Contribution related to INSPIRE-5Gplus: This work proposes a descriptive architecture for a local 5G operator which provides user specific and location-specific services in a spatially confined environment. The paper is related to work conducted in WP5.

- Hewa, T., Ylianttila, M. and Liyanage, M. (2021) 'Survey on blockchain based smart contracts: Applications, opportunities and challenges', Journal of Network and Computer Applications. New York, NY, USA: IEEE, 177(12), p. 102857. <http://doi.org/10.1016/j.jnca.2020.102857>.

Contribution related to INSPIRE-5Gplus: The survey explores the significant applications which already benefited from the blockchain based smart contracts and investigates the future research directions. The paper is related to work conducted in WP2.

- Ortiz, J. et al. (2020) 'Enforcing GDPR regulation to vehicular 5G communications using edge virtual counterparts', in 2020 IEEE 3rd 5G World Forum (5GWF). New York, NY, USA: IEEE, pp. 121–126. <http://doi.org/10.1109/5GWF49715.2020.9221248>.



Contribution related to INSPIRE-5Gplus: Development of Multi-Access Edge Computing (MEC)-based services for enabling the proper management of data considering local GDPR regulations in vehicular roaming scenarios. This paper is related to work conducted in WP5.

- Gaber, C. et al. (2020) 'Liability-Aware Security Management for 5G', in 2020 IEEE 3rd 5G World Forum (5GWF). New York, NY, USA: IEEE, pp. 133–138. <http://doi.org/10.1109/5GWF49715.2020.9221407>.

Contribution related to INSPIRE-5Gplus: This paper presents the design, building blocks and challenges of a Liability-Aware Security Management (LASM) system for 5G networks. The proposed architecture takes risk and responsibilities into account for security and liability management. It is related to work in WP4.

- Sanchez-Gomez, J. et al. (2020) 'Integrating LPWAN Technologies in the 5G Ecosystem: A Survey on Security Challenges and Solutions', IEEE Access, 8, pp. 216437–216460. <http://doi.org/10.1109/ACCESS.2020.3041057>.

Contribution related to INSPIRE-5Gplus: survey work presenting deep insights of the 5G authentication procedure as well as the related requirements and current solutions for the secure integration of LPWAN technologies within 5G architectures. Paper related to work conducted in WP2.

- Garcia, N. et al. (2021) 'Distributed real-time SlowDoS attacks detection over encrypted traffic using Artificial Intelligence', Journal of Network and Computer Applications, 173, p. 102871. <http://doi.org/10.1016/j.jnca.2020.102871>.

Contribution related to INSPIRE-5Gplus: AI-based framework that monitors in real-time 5G network traffic, analysing, processing, and aggregating packets into conversation flows, getting valuable features and statistics that are dynamically analysed in streaming for anomaly detection of Slow Denial of Service (SlowDoS) attacks. Paper related to work conducted in WP3.

- Bagaa, M. et al. (2020) 'A Machine Learning Security Framework for IoT Systems', IEEE Access, 8, pp. 114066–114077. <http://doi.org/10.1109/ACCESS.2020.2996214>.

Contribution related to INSPIRE-5Gplus: This paper presents a novel machine learning (ML) based security framework that automatically copes with the expanding security aspects related to IoT domains. Paper related to work in WP3.

- Gallego-Madrid, J. et al. (2020) 'Evaluation of a zone encryption scheme for vehicular networks', Computer Networks, 182, p. 107523. <http://doi.org/10.1016/j.comnet.2020.107523>.

Contribution related to INSPIRE-5Gplus: This work presents the implementation and evaluation of a symmetric encryption scheme based on disjoint security domains distributed in geographical areas to enable security and privacy of vehicular communications. Paper related to work in WP4.

- Vilalta, R. et al. (2020) 'Applying Security Service Level Agreements in V2X Network Slices', in 2020 IEEE Conference on Network Function Virtualisation and Software Defined Networks (NFV-SDN). IEEE, pp. 114–115. <http://doi.org/10.1109/NFV-SDN50289.2020.9289861>.

Contribution related to INSPIRE-5Gplus: This demo paper presents basic results of WP5 TC1, without enabler integration and focusing on deployment of V2X services.



- Alemany, P. et al (2020) 'Managing Network Slicing Resources Using Blockchain in a Multi-Domain Software Defined Optical Network Scenario', European Conference on Optical Communications (ECOC). pp 1-4. <http://doi.org/10.5281/zenodo.4459324>.

Contribution related to INSPIRE-5Gplus: This paper presents the work done on WP4 regarding the Blockchain-based enabler for INSPIRE-5Gplus. More specifically, the internal architecture is presented and implemented on a real testbed using real-world computing resources to deploy Network Slices. This paper is related to work in WP4.

- Alemany, P. et al. (2020) 'Transport Network Slices with Security Service Level Agreements', in 2020 22nd International Conference on Transparent Optical Networks (ICTON), 2020, pp. 1–4, doi: 10.1109/ICTON51198.2020.9248696.

Contribution related to INSPIRE-5Gplus: This paper presents the initial design of an architecture to manage and associate Security SLAs and Network Slices. The SLA model to be used is presented and the interactions among the elements within the architecture described. This paper is related to work in WP3.

- Vilalta, R., et al, (2020), 'Controlling and Monitoring Optical Network Equipment in Optical SDN Networks', European Conference on Optical Communications (ECOC). pp 1-4. <http://doi.org/10.5281/zenodo.4459180>

Contribution related to INSPIRE-5Gplus: This tutorial relates to T3.4 as it presents telemetry and notification protocols (gRPC, websockets) and monitoring for 5G infrastructure management between multiple infrastructure tenants (i.e., slices).

- Kalalas, C. and Alonso-Zarate, J. (2020) 'Lightweight and Space-efficient Vehicle Authentication based on Cuckoo Filter', in 2020 IEEE 3rd 5G World Forum (5GWF). New York, NY, USA: IEEE, pp. 139–144. <http://doi.org/10.1109/5GWF49715.2020.9221363>.

Contribution related to INSPIRE-5Gplus: This work presents the key principles and building blocks of the proposed WP3 security enabler related to vehicle authentication tailored for mission-critical vehicular scenarios. Paper related to work in WP3.

- Bagaa, M. et al. (2020) 'QoS and Resource-aware Security Orchestration and Life Cycle Management', IEEE Transactions on Mobile Computing. New York, NY, USA: IEEE, 177(12), pp. 1–1. <http://doi.org/10.1109/TMC.2020.3046968>.

Contribution related to INSPIRE-5Gplus: This paper proposes a cost-efficient optimized orchestration system that addresses the whole life-cycle management of different Service Function Chains, considering QoS, actual capacities of Virtual Network Functions (VNFs), potentially deployed across multiple Clouds-Edges, and current network security levels to ensure trusted deployments. This paper is related to work in WP3.

- Hewa, T. et al. (2020) 'Multi-Access Edge Computing and Blockchain-based Secure Telehealth System Connected with 5G and IoT', in GLOBECOM 2020 - 2020 IEEE Global Communications Conference. New York, NY, USA: IEEE, pp. 1–6. <http://doi.org/10.1109/GLOBECOM42002.2020.9348125>.

Contribution related to INSPIRE-5Gplus: This paper presents a novel Multi-access Edge Computing (MEC) and blockchain based service architecture utilizing the lightweight certificates for the realtime



data privacy, integrity, and authentication between IoT, MEC, and cloud. The work proposed in this paper is used in developing WP3 security enabler related to secure slice broker. The paper is related to work in WP3.

- Christopoulou Maria, Wissem Soussi, George Xilouris, Gürkan Gür, Edgardo Montes de Oca, Harilaos Koumaras, Burkhard Stiller (2021) 'AI-Enabled Slice Protection exploiting Moving Target Defence in 6G Networks', in EuCNC and 6G Summit 2021. Porto, Portugal (Virtual Conference), Poster Session, 6G Enabling Technologies Track (accepted)

Contribution related to INSPIRE-5Gplus: This work describes the aspects of the Test Case "Network Slice Protection with Moving Target Defence and Anomaly Detection" and highlights the use of AI as an enabler in advanced cybersecurity techniques. The paper is related with work in WP5.

2.2.2 Other dissemination activities

Activity event material type	Event name / material name	Papers / presentation title	Start Date	End Date	Venue	Responsible partner
Invited talk	Cybersecurity for Europe 2019	Participation in the panel 4: Good practices in data sharing for incident handling	2019-11-13	2019-11-15	Toulouse, France	MI
Exhibition / demo / booth	European Cyber Week	Stand Montimage to present 4G/5G/IoT monitoring tools	2019-11-18	2019-11-21	Rennes, France	MI
Moderation	1ST CYBER SECURITY JOINT PROJECT WORKSHOP	Certification tools and standards	2019-11-29	2019-11-29	Brussels	UMU
Exhibition / demo / booth	ASTech Airbus Forum	Montimage booth	2020-01-14	2020-01-14	Elancourt, Ile-de-France, France	MI
Workshop	Workshop on 5G Security: Current Trends, Challenges and New Enablers	Organization of Workshop on 5G Security: Current Trends, Challenges and New Enablers	2020-09-10	2020-10-12	Bangalore, India	UMU
Invited talk	Mobile World Congress - organised as virtual event	INSPIRE-5Gplus: Intelligent Security and Pervasive Trust for 5G and Beyond	2020-02-26	2020-02-26	Mobile World Capital	CTTC
Presentation - Webinar	ETSI Security Week Webinar/Security Challenges in 5G Multi-access Edge Computing	Security Challenges in 5G Multi-access Edge Computing	2020-06-18	2020-06-18	Sophia Antipolis, France (Webinar)	OPL
Video/Film/TV Clip	Project Video	Overview on 5G PPP project INSPIRE-5Gplus for security and trust in 5G	2020-02-13	2020-02-13	Online	EURES
Webinar	6G à l'horizon... 2030	"Nouvelles tendances pour la gestion autonome de la performance et de la sécurité"	2020-04-29	2020-04-29	Virtual	MI
Invited talk	NGIoT Workshop on "IoT and Edge Computing: Future directions for Europe"	IoT, Edge computing and AI technologies and its future impact on the next generation of IoT nodes	2020-09-11	2020-09-11	Virtual	UMU



Keynote	2nd International Workshop on Cyber-Security Threats, Trust and Privacy Management in Software-Defined and Virtualized Infrastructures (SecSoft 2020)	Dynamic Security Management on IoT through Network Softwarization	2020-07-03	2020-07-03	Virtual	UMU
Invited talk	IEEE TEMS R9 - Foro Industrial Latinoamericano virtualization for IoT in 5G	Security and virtualization in IoT and 5G	2020-10-28	2020-10-28	Virtual	UMU
Keynote	The 6th International Conference on Mobile, Secure and Programmable Networking (MSPN2020)	What Happens Next? Going Beyond Security via Liability in Future Networks	2020-10-28	2020-10-29	Virtual	ZHAW
Webinar	Webinar "5G Experimentation Facilities and Vertical Trials: Current Status and Future Perspectives"	Intelligent Security and Pervasive Trust for 5G and Beyond	2020-10-14	2020-10-14	Virtual	EURESCOM
Invited talk	IEEE Communications Society Europe, Middle East and Africa Region	Get Smart – The Challenges in Data-Driven Network Management	2020-10-02	2020-10-02	Virtual	TID
Keynote	Layer123 World Congress 2020	Data aggregation and network digital twins	2020-10-12	2020-10-15	Virtual	TID
Invited talk	ETSI Research - Boosting the Impact of Research & Innovation through Standardisation	How research projects impact security standards : the example of INSPIRE-5Gplus	2020-11-24	2020-11-25	Virtual	Orange
Keynote	The 6th International Conference on Mobile, Secure and Programmable Networking (MSPN2020)	"Cyber Threat Intelligence: the fuel for secure networking"	2020-10-28	2020-10-29	Virtual	MI
Invited talk	IEEE CloudNet 2020 - IEEE International Conference on Cloud Networking	Some Musings on the Connection of Cloud Networking, the Edge and 5G	2020-11-09	2020-11-09	Virtual	TID
Invited talk	EUCNC21 SN Workshop Telco Cloud Native: Time to Operationalise	Advancing security of softwarized networks	2021-06-01	2021-06-01	Virtual	CTTC
Poster	EuCNC & 6G Summit 2021	SFSBroker: Secure and Federated Network Slice Broker for 5G and Beyond	2021-06-08	2021-06-11	Virtual	UOULU
Keynote	LAYER123 EUROPE: 360° Network Automation Congress	Data flow aggregation for smarter network security	2021-04-13	2021-04-13	Virtual	TID
Presentation	The 1st SLICES workshop - Next Generation ICT Research Infrastructures	Twinning Networks: On the Use and Challenges of Network Digital Twins	2021-03-03	2021-03-04	Virtual	TID
Presentation	Spanish Network of Excellence on Cybersecurity Research (RENIC)	5G cybersecurity: Initiatives and challenges	2021-04-20	2021-04-20	Virtual	TID
Presentation	22nd Infocom World Conference 2020	INSPIRE-5Gplus: Intelligent Security and Pervasive Trust for 5G and Beyond	2020-11-04	2020-11-06	Virtual	NCSRD



Table 4: Other dissemination activities

2.2.3 Workshop Organization

INSPIRE-5Gplus co-organized the workshop on “5G Security: Current Trends, Challenges and New Enablers” within IEEE 5G World Forum 2020. The workshop was aimed at discussing the emerging 5G security in a holistic manner to understand the challenges, opportunities and standardisation imperatives and define the way forward and immediate next steps to ensure ubiquitous adoption of 5G globally. The call for paper can be seen in Appendix B.

The workshop received 15 paper submissions and finally 9 papers were selected. The workshop was held virtually with the following agenda and published in IEEEXplore.

Title	Authors with affiliation and country
Opening	Antonio Fernando Skarmeta Gomez (Universidad de Murcia, Spain) Sye Loong Keoh (University of Glasgow, United Kingdom (Great Britain)) Pascal Bisson (Thales, France)
5G Security Challenges and Opportunities - A System Approach	Ashutosh Dutta (Johns Hopkins University Applied Physics Labs (JHU/APL), USA); Eman Hammad (University of Toronto, Canada)
An Efficient Scheme to Secure Data Provenance in Home Area Network	Zhaohui Tang (University of Southern Queensland, Australia); Sye Loong Keoh (University of Glasgow, United Kingdom (Great Britain))
Enforcing GDPR Regulation to Vehicular 5G Communications using Edge Virtual Counterparts	Jordi Ortiz, Pedro J. Fernández, Ramon Sanchez-Iborra and Jorge Bernal Bernabe (University of Murcia, Spain); Jose Santa (Technical University of Cartagena, Spain); Antonio Fernando Skarmeta Gomez (University of Murcia, Spain)
Hybrid-Trusted Party Contract Agrees on Clients Input	Anwar Alruwaili and Dov Kruger (Stevens Institute of Technology, USA)
Liability-Aware Security Management for 5G	Chrystel Gaber and José M. Sánchez Vilchez (Orange Labs, France); Gurkan Gur (Zurich University of Applied Sciences (ZHAW), Switzerland); Morgan Chopin, Nancy Perrot, Jean-Luc Grimault and Jean-Philippe Wary (Orange Labs, France)
Lightweight and Space-efficient Vehicle Authentication based on Cuckoo Filter	Charalampos Kalalas (CTTC, Spain); Jesus Alonso-Zarate (Centre Tecnologic de Telecomunicacions de Catalunya - CTTC, Spain)
New Immersive Interface for Zero-Touch Management in 5G Networks	Ignacio Sanchez-Navarro, Pablo Salva-Garcia, Qi Wang and Jose Maria Alcaraz Calero (University of the West of Scotland, United Kingdom (Great Britain))
Peer-to-Peer Blockchain-based NFV Service Platform for End-to-End Network Slice Orchestration Across Multiple NFVI Domains	Pol Alemany, Ricard Vilalta, Raul Muñoz, Ramon Casellas and Ricardo Martinez (Centre Tecnològic de Telecomunicacions de Catalunya (CTTC/CERCA), Spain)
QKD in Support of Secured P2P and P2MP Key Exchange for Low-Latency 5G Connectivity	Argiris Ntanos, Dimitris Zavitsanos, Giannis Giannoulis and Hercules Avramopoulos (National Technical University of Athens, Greece)

Table 5: Agenda of organised workshop at IEEE 5G World Forum 2020



2.2.4 White papers

White papers are of prominent importance to disseminate projects' advances and developments to a broad audience. Although they are written from a technical perspective, using an accessible style helps to make them accessible to various readers.

During the reporting period, INSPIRE-5Gplus has released a white paper entitled "Intelligent Security Architecture for 5G and Beyond Networks". The aim of this white paper was to introduce the INSPIRE-5Gplus high-level architecture, its main functional blocks, and their role in enabling intelligent closed-loop security operations. To illustrate how the INSPIRE-5Gplus framework can be applied as a zero-touch security management solution for 5G systems, the White Paper presented a representative set of advanced security use cases. The white paper can be accessed through the following link: <https://doi.org/10.5281/zenodo.4288658>

Besides, INSPIRE-5Gplus has also collaborated on the preparation of the 5GPPP white paper entitled: "Edge Computing for 5G Networks". This white paper provides a) a brief introduction to the Edge computing concept; b) an exhaustive technology review focusing on virtualisation, orchestration, network control, and operational frameworks; c) a discussion about the role of security, and d) an analysis of several business aspects around the Edge ecosystem. Concretely, INSPIRE-5Gplus has contributed to the following technical descriptions and discussion, providing the knowledge generated during its first year: The ETSI Zero Touch network and service management (ZSM), that enables secured self-managing capabilities; Trusted Execution Environment (TEE) to elevate integrity and confidentiality to software and data of any type; Distributed Ledger Technologies (DLT) to provide with Dynamical Liability Chains and Distributed security; and Artificial Intelligence (AI) and Machine Learning (ML) to empower key security functions. The white paper can be accessed through the following link:

<https://bscw.5g-ppp.eu/pub/bscw.cgi/d397473/EdgeComputingFor5GNetworks.pdf>

INSPIRE-5Gplus has also collaborated on the preparation of the 5GPPP Technology Board white paper entitled "AI/ML – Point of Interests from XG Network View" (still in progress). This white paper discusses the potential applications of AI and ML mechanisms in 5G and B5G/6G networks from a high-level perspective. It also describes in detail the specific contributions of EU funded research projects, clustered under 5G PPP Programme, in terms of specified, designed and developed AI and ML solutions. Specifically, INSPIRE-5Gplus has contributed on two key aspects of 5G and Beyond security in terms of technical contributions and discussions, namely how Moving Target Defense (MTD) accompanied with AI/ML driven control can provide network slice protection and how robust self-protection against application layer DDoS attacks can be enabled with a security framework that empowers a fully autonomous attack detection and mitigation leveraging Deep Learning (DL) and SDN enablers.

INSPIRE-5Gplus has also contributed to the White Paper on the "European Vision for 6G Network Ecosystem" which is currently being prepared in the scope of the Vision Working Group of the 5G Infrastructure Association. The whitepaper is planned to present a European perspective on what 6G will be and what it can bring to Europe. Besides technical aspects strong emphasis will be put on political, business and societal aspects. INSPIRE-5Gplus has contributed to Chapter 6 "Architecture" with a general view about the security challenges in 6G that are coming up due to the application of new enabling technologies, e.g., AI. These new technologies are expected to create new challenges for security but at the same time these are planned to be exploited for implementing security in 6G. In addition to the general conceptual view the principals of the High Level Security Architecture defined in INSPIRE-5Gplus have been contributed. The whitepaper is planned to be published on 20 June 2021, targeting its release at the planned start of Mobile World Congress 2021 in Barcelona.

2.2.5 Awards/Mentions

The 5G Rescue use case, which is based on research done in INSPIRE-5Gplus, was selected in December 2020 as one of the ten winning proposals in the contest for the "Best Artificial Intelligence



initiatives with social and ethical impact in Spain”. The contest is supported by Telefónica, OdiselA, and the “Compromiso Empresarial” magazine. The 5G Rescue use case was presented by the project partner University of Murcia (UMU). The initiative driving the use case aimed to make the full potential of 5G technology and Artificial Intelligence available to the security and emergency services, such as fire brigades, health services, and others. The technical objective of the 5G Rescue use case was to develop and integrate a series of intelligent network management mechanisms that allow reconfiguring the 5G infrastructure in real time, in order to enable a high-definition, low-latency and secured video streaming service.

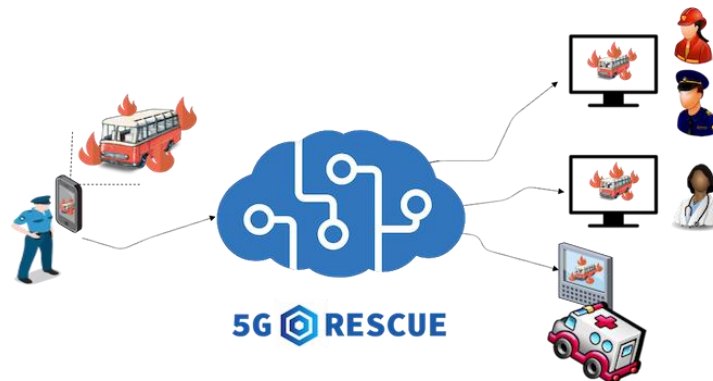


Figure 1: 5G Rescue banner

A consortium led by Montimage won the SYNAPSE Challenge (12/2020, <https://www.defense.gouv.fr/aid/actualites/challenge-synapse-les-deux-laureats>) proposed by the Ministère des Armées (MdA) and the CAP-DIGITAL cluster. The project, called CARTIMIA, was carried out together with R2CSystem and the Laboratoire ICube lab of the University of Strasbourg (UNISTRA) and proposed an initial prototype of a solution to detect anomalies in the Internet routing. The work in INSPIRE-5Gplus originated the ideas (i.e., the CTI enabler) proposed in this challenge. Even though the prize is very symbolic, it has allowed to learn about what we do and eventually will result in future contracts.

2.2.6 Flyer

As the project advances, it is necessary to update the communication material. For that reason, an updated version of the INSPIRE-5Gplus flyer has been produced, to give an overview of the most important achievements during the first half of the project. It includes a diagram of INSPIRE-5Gplus high-level architecture, the defined test-case, as well as other general information about the project. This new flyer version can be found in Appendix A.

2.2.7 Website

The INSPIRE-5Gplus website at <https://www.inspire-5gplus.eu> is the central hub for the dissemination and external communication activities of the project. It was launched in November 2019 and has been continuously updated since then. In addition to information about the project, it provides access to public deliverables, scientific publications, event dates and news items on project activities and results.



News



Figure 2: News items

News items

Since the launch of the website, INSPIRE-5Gplus has published 24 news items featuring a wide range of activities and results, from conference presentations to publications and initiatives – see the list of published news items starting with the latest:

- INSPIRE-5Gplus developments published in top-ranked journal (2021/03/26)
- INSPIRE-5Gplus presentation at ETSI ISG ZSM plenary meeting (2021/02/16)
- 5G Rescue use case among best Spanish AI initiatives (2020/12/01)
- White Paper on Intelligent Security Architecture for 5G and Beyond Networks (2020/11/24)
- IETF Internet-Draft on EDHOC authentication presented (2020/11/24)
- INSPIRE-5Gplus deliverable on 5G security test cases (2020/11/18)
- Keynote on liability concepts at MSPN 2020 (2020/11/17)
- Paper on DGKA presented at AIBlock workshop (2020/11/17)
- INSPIRE-5Gplus at first IEEE TEMS Latin American Industrial Forum (2020/10/28)
- INSPIRE-5Gplus at Online Workshop on 5G Trials in Europe (2020/10/23)
- 5G Security Workshop at 5G World Forum 2020 (2020/09/17)
- Novel E2E slicing architecture by INSPIRE-5Gplus presented at ICTON 2020 (2020/07/23)
- INSPIRE-5Gplus results presented in keynote at SecSoft 2020 (2020/07/22)
- INSPIRE-5Gplus will present its novel E2E slicing architecture at ICTON 2020 (2020/07/03)
- Successful first advisory board meeting of INSPIRE-5Gplus (2020/06/19)
- Workshop on 5G Networks Security at ARES 2020 – Call for Papers (2020/05/29)



- Survey on business requirements for security and privacy (2020/05/28)
- INSPIRE-5Gplus-related Aalto paper presented at WCNC 2020 (2020/05/28)
- INSPIRE-5Gplus Deliverable on Current Status and Future Trends of 5G Security (2020/05/27)
- The Role of Blockchain in 6G – Paper at 6G Wireless Summit (2020/05/13)
- Two INSPIRE-5Gplus partners featured in NetWorld 2020 SME brochure (2020/04/01)
- Video – Overview on INSPIRE-5Gplus (2020/02/13)
- INSPIRE-5Gplus kick-off meeting in Heidelberg (2019/11/12)

Website visitors

The website has attracted a steady number of visitors, with occasional fluctuations, since it was launched in November 2019, see Figure 3.

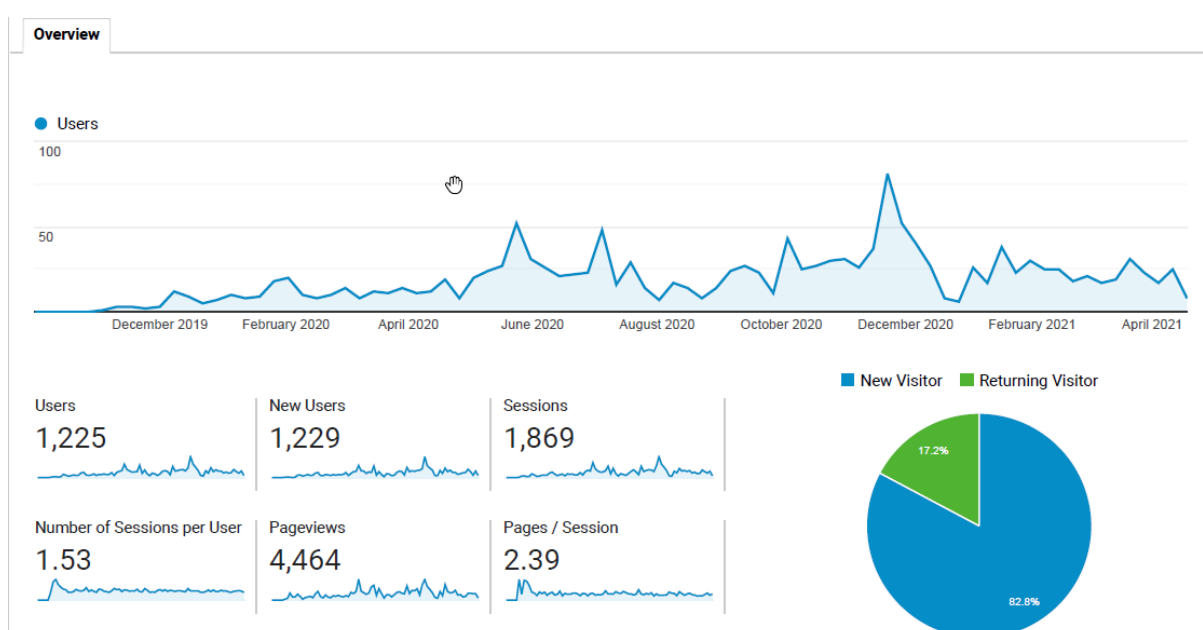


Figure 3: Website visitors — 1 November 2019 - 30 April 2021

The geographic distribution of visitors is dominated by visitors from Europe although there are also visitors from countries in other regions as e.g. India, see Table 6.



Country ?	Acquisition		
	Users ? ↓	New Users ?	Sessions ?
	1,225 % of Total: 100.00% (1,225)	1,230 % of Total: 100.08% (1,229)	1,869 % of Total: 100.00% (1,869)
1. Spain	161 (13.02%)	163 (13.25%)	264 (14.13%)
2. France	150 (12.13%)	147 (11.95%)	209 (11.18%)
3. Finland	112 (9.05%)	113 (9.19%)	188 (10.06%)
4. Greece	92 (7.44%)	90 (7.32%)	132 (7.06%)
5. Germany	71 (5.74%)	71 (5.77%)	250 (13.38%)
6. United Kingdom	64 (5.17%)	63 (5.12%)	96 (5.14%)
7. India	51 (4.12%)	51 (4.15%)	59 (3.16%)
8. Turkey	38 (3.07%)	38 (3.09%)	50 (2.68%)
9. Italy	34 (2.75%)	34 (2.76%)	43 (2.30%)
10. Canada	26 (2.10%)	26 (2.11%)	32 (1.71%)

Table 6: Regional distribution of website visitors — 1 November 2019 - 30 April 2021

2.2.8 Social Media

The focus of the project's Social Media activities has been on Twitter and LinkedIn.

Twitter

The Twitter account has grown from 75 followers (7 April 2020) to **185 followers** (27 April 2021). Between 1 December 2019 and 20 April 2021, Tweets by INSPIRE-5Gplus collectively achieved between around 1,000 and 5,000 **impressions (views) each month**. The most successful Tweet (see Figure 4) generated 2,700 impressions and 86 engagements, which means retweets, likes or other interactions.






Tweets	Top Tweets	Tweets and replies	Promoted	Impressions	Engagements	Engagement rate
	INSPIRE-5Gplus @INSPIRE_5Gplus · Feb 4			2,700	86	3.2%
	The second project meeting of INSPIRE-5Gplus is hosted by CTTC in Barcelona. It started this morning and will end on Thursday. The INSPIRE-5Gplus consortium works on advancing the security of 5G and Beyond networks. @CttcTech @5GPPP #5G #ICT #Cybersecurity #H2020 pic.twitter.com/ozVWMWyUrQc					
	View Tweet activity				Promote	
	INSPIRE-5Gplus @INSPIRE_5Gplus · Feb 14			2,537	34	1.3%
	Watch the INSPIRE-5Gplus overview video on YouTube to learn more about the project and how INSPIRE-5Gplus will improve security and trust in 5G and beyond. youtu.be/W_MMj0t2C2o #5G #ICT #Cybersecurity #H2020 @5GPPP pic.twitter.com/HPiwVG8H4h					
	View Tweet activity				Promote	
	INSPIRE-5Gplus @INSPIRE_5Gplus · Feb 25			1,727	39	2.3%
	The fastest way to learn what INSPIRE-5Gplus is all about - Watch the 2.5 min overview video on how 5G EVE will advance security and trust in 5G youtu.be/W_MMj0t2C2o #5G #ICT #Cybersecurity #H2020 @5GPPP pic.twitter.com/HWYkP8DiE2					
	View Tweet activity				Promote	




Figure 4: Top Tweets of INSPIRE-5Gplus

LinkedIn

On LinkedIn, INSPIRE-5Gplus has 81 followers (27 April 2021) and is actively contributing to the 5G PPP Group and their around 1,100 members.






Project INSPIRE-5Gplus
Horizon 2020 Project at
INSPIRE-5Gplus Project
Consortium


Followers **83**

Project's Activity

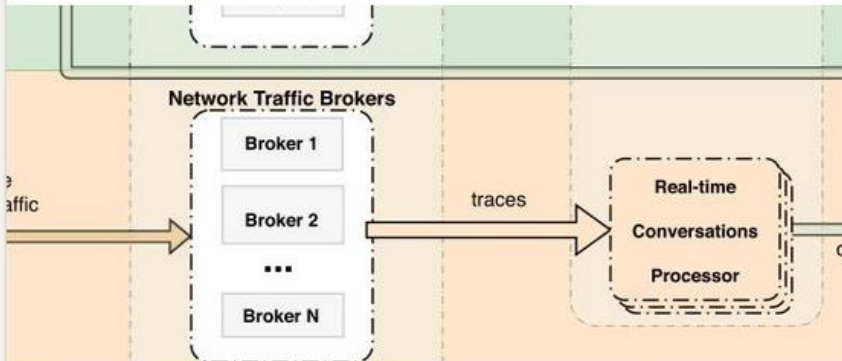
All activity Articles Posts Documents

Project INSPIRE-5Gplus posted in 5G PPP



Project INSPIRE-5Gplus
Horizon 2020 Project at INSPIRE-5Gplus Project Consortium
3w • 

The INSPIRE-5Gplus-related paper "Distributed real-time SlowDoS attacks detection over encrypted traffic using Artificial Intelligence" has been recently published in the prestigious Elsevier's Journal of Network and Computer Applications. ...see more



Tool

INSPIRE-5Gplus developments published in top-ranked journal
inspire-5gplus.eu • 2 min read

Figure 5: INSPIRE-5Gplus activity on LinkedIn

In the next period, INSPIRE-5Gplus will continue its regular activities and grow its follower base on Twitter and LinkedIn as well as expand its activities on YouTube in the course of further video production. SlideShare has been mostly abandoned, as it did not prove effective in reaching our target audiences. Instead of spending resources on maintaining this ineffective for us channel, we will engage with our target audiences via, other social media channels.



3 Standardisation activities

3.1 Standards-related strategy summary

The strategy already defined in D6.1 for standardisation activities is maintained, that is, to transform the INSPIRE-5Gplus concepts and results into open standards to encourage adoption and consensus between industry players. The focus is maintained around relevant bodies in security, Internet protocols and telecommunication industry. These are, jointly with open source initiatives, the cornerstone of 5G networks and their security.

To this end, the consortium partners with relevant roles in several standardisation bodies have continued their activity of monitoring new opportunities aligned with actual research and outcomes in the project activity. As a result, some contributions have been achieved in due time and form the following standardisation rules. All these actions will continue to be coordinated inside the Task 6.2, with the aim to maximize our impact. These actions and results are presented here.

3.2 Standards-related results

3.2.1 ETSI

ETSI is recognised as a European Standards Organisation dealing with telecommunication, broadcasting and other electronic communication networks and services. ETSI does not involve national delegates—its members are international stakeholders from industry, organisations and government.

NFV

In the Network Function Virtualisation (NFV)³ Industry Specification Group (ISG), the team activity has been mainly focused on the definition and approval of two new work items related to the project objectives:

- SEC0025, on E2E function and service security management
- SEC0026, on mechanisms for tenant isolation in NFV deployments
- SEC0027, on security assurance for NFV infrastructures

Beyond this, the project has presented a proposal on NFV SEC 024 evolution with a specific contribution on "Multiple Trust Domains and Security Managers" (NFVSEC(21)000012), aligned with activities in WP4 for trust and liability.

ETI

The team has contributed to the scope and goals of the new ETI (Encrypted Traffic Integration) ISG, including a better alignment of the ISG objectives with the requirements on privacy preservation in the analyses of encrypted traffic patterns. Active participation in the group discussions has continued since it started working.

SAI

The Securing Artificial Intelligence (SAI)⁴ ISG focuses on the security of AI, as an essential element in network management for next-generation networks. The team has participated in the definition of the SAI003 work-item on security testing. A contribution on the definition and application of Trust

³ <https://www.etsi.org/technologies/nfv>

⁴ <https://www.etsi.org/committee/sai>



Execution Environment (TEE) to secure AI was introduced as contribution SAI(20)006012, following the technologies proposed in WP3 enablers related with TEE. This has been included as part of the SAI006 draft.

ENI

The Experiential Networked Intelligence (ENI)⁵ ISG focuses on the specification of cognitive network management system, including concepts such as autonomy and closed-loop in the network. Here several discussions and contributions have been made aligned with INSPIRE-5Gplus High Level Architecture (HLA) and pointers were added, connected to specific enablers for the development of security autonomy and digital network twins in ENI 010. In addition, the group has participated in the definition and approval of a new work-item on processing and management of intent policies (ENI025).

ZSM

The Zero Touch Network and Service Management (ZSM)⁶ ISG has been taken as framework reference to define the HLA for INSPIRE-5Gplus. This approach was presented in the ZSM#14-e meeting (January 2021), as ZSM(21)000005. Feedback from delegates and additional discussions have been consolidated into a new work item to address zero-touch service management security aspects.

QKD

The Quantum Key Distribution (QKD)⁷ ISG specifies QKD system interfaces, implementation security requirements and characterization of QKD systems and their components. The experience with advance key distribution mechanisms as foundation of several of the project enablers has allowed the team to bring its experience to the definition of the SDN interfaces defined by the recently published specification QKD015.

3.2.2 ITU-T

A new Focus Group on Autonomous Networks (FG-AN) has been created within the ITU-T, with the project team participating in the definition of its scope and the initial discussions to decide on structure. The project multi-domain architecture, and its support for automation, are essential assets for future contributions to the FG-AN.

3.2.3 IETF/IRTF

The Internet Engineering Task Force (IETF) is the body acting as producer and maintainer of the core Internet specifications, from IP to HTTP, and explicitly referenced by many other bodies in their standardisation activities. IETF activity is organized in WG formed around a charter describing their objectives and plans.

NMRG

The Network Management Research Group (NMRG) focuses on the research in new technologies around network management that is not mature enough to be addressed yet in other IETF WG.

A draft⁸ has been submitted and updated, and the corresponding presentations at latest IETF 109 and

⁵ <https://www.etsi.org/committee/eni>

⁶ <https://www.etsi.org/committee/zsm>

⁷ <https://www.etsi.org/committee/qkd>

⁸ <https://tools.ietf.org/html/draft-zhou-nmr-digitaltwin-network-concepts-02>



IETF 110 meetings made, around the concept of Digital Network Twin (DTN). The work (in progress) proposes the application of the digital twin technologies, already in use by other industrial sectors, to enhance network management solutions, including the application in security verification and enforcement. This approach encompasses AI techniques, and dataset generation and collection, applying the ideas around data collection in WP3 enablers.

I2NSF

The standardisation of several interfaces for security network functions is the objective of the WG Interface to Network Security Function (I2NSF). The virtual I2NSF IPsec enabler in WP3 is based on a draft⁹ already approved to become RFC in this WG, with the enabler acting as proof-of-concept supporting the specification evolution. Beyond this, the team is participating in the discussions for extending the WG charter for two additional years to develop additional security policy mechanisms.

EMU

The IETF Internet-Draft “AAA-based assisted EDHOC Authentication”¹⁰ was presented at a meeting of the IETF Working Group on EAP Method Update (EMU). The proposal is related to the authentication process of IoT end devices in the 5G architecture. The document describes a proposal to place an Ephemeral Diffie-Hellman Over COSE (EDHOC) server in an external Authentication, Authorization and Accounting (AAA) server. The purpose is to centralize the EDHOC authentication in the AAA infrastructure. It is proposed to employ the EDHOC authentication as a new Extensible Authentication Protocol (EAP) method for the secondary authentication procedure on 5G systems.

3.2.4 IEEE

Contribution to security aspects of IEEE 1902.1 Standard for for Aerial Communications and Networking Standards.

In the first half of the project, we have contributed to the security aspects of *IEEE 1902.1 Draft Standard for Aerial Communications and Networking Standards*. IEEE 1902.1 Working Group (WG) carries out standardisation work related to an important vertical for 5G; wireless networking and communications of UAVs/drones including the security of those systems. The underlying WG premise was to render the baseline, establish connections with other SDOs/institutions like ASTM, NASA, and FAA, and have follow-up WGs to elaborate further, if possible. The work group is chaired by Prof. Kamesh Namuduri from University of North Texas. Dr. Gürkan Gür from ZHAW attended monthly group meetings (virtual) and was responsible for the security section (e.g., security analysis, threats, security controls) for the draft standard. Currently, the draft standard is going through revisions based on the comments from the technical community and IEEE. The contributions to this standard are related to WP2 work in our project.

Moreover, a new follow-up standardisation WG named *IEEE 1902.2 WG on Vehicle-to-Vehicle Communications for Unmanned Aircraft Systems*¹¹ has also recently been established. It aims to define the protocol for exchanging information between the vehicles. The information exchange will facilitate beyond line of sight (BLOS) and beyond radio line of sight (BRLOS) communications. The information exchanged between the aircraft may be for the purpose of command, control, and navigation or for any application specific purpose. ZHAW is also working to identify how to contribute to this standard from the security perspective.

⁹ <https://datatracker.ietf.org/doc/draft-ietf-i2nsf-sdn-ipsec-flow-protection/>

¹⁰ <https://tools.ietf.org/html/draft-ingles-radex-radius-edhoc-00>

¹¹ <https://sagroups.ieee.org/1920-2/>



3.2.5 Industrial groups

GSMA

GSMA Alliance is a reference as the most relevant industrial group for mobile network operators, acting as a source for specification requirements for SDOs, as well as providing operators with application recommendations on related standards. In what relates to the enablers considered in the project, the GSMA is currently working on a document on Quantum Communications within the Internet Group (IG), and the project team has contributed to the definition of the scope of this document and is participating actively in its preparation.

ECSO

The European Cyber Security Organisation (ECSO) main objective is to coordinate the European Cybersecurity Ecosystem development to protect the European Digital Single Market, conclusively contributing to European digital independence. Activities performed in this period include:

Contribution to WG6: SRIA and Cyber Security Technologies "Horizon Europe Priorities for Cyber secure future communication systems and networks"

Provided proposal on research challenges on DEH and DEP linked to project objectives of INSPIRE related to security and liability in the context of Certification on 5G.



4 Communications and Dissemination KPIs

The following two tables present a comparison between the identified communication and dissemination KPIs and their corresponding success indexes (to be achieved by project end) and the achievements of INSPIRE-5Gplus until month M18, i.e. half of the project runtime.

Communication s means	Success indicator	Target # of outputs	Outputs achievement	Target audience	Reached audience
Project website	SEO Metrics	1	1	1,000 unique visitors/year	908
Social Media	# of users	4 social media channels	4 social media channels (Twitter / LinkedIn / YouTube / SlideShare)	300 followers	278 (Twitter: 185, LinkedIn: 81; YouTube: 12; SlideShare: 0)
Promotional videos	# of views	5	5	> 500 views	122 views
Press releases	# of elements	10	0	500 cybersecurity stakeholders	0
Project meetings / roundtables	# of events	10	8	> 40 internal and invited stakeholders	50 internal and invited stakeholders
Workshops / showcases	# of events / attendees	5	4	250 participants in total	150 participants in total
Policy-level events in Brussels	# of events	2	2	> 60 cybersecurity policy makers	45 cybersecurity policy makers
Newsletters, factsheets	# of publications	15	3	> 500 subscribers	200 subscribers
White papers	# of publications	4	4	500 recipients	200 recipients
Deliverables (public)	QA standards	> 20	6	500 recipients	125 recipients
Brochure and annual report	# of stakeholders	3	1	500 recipients	200recipients
Liaison with ECSO, participation in WGs and events	# attended events	> 6	3	> 50 participants per event	50 participants per event



Communication s means	Success indicator	Target # of outputs	Outputs achievement	Target audience	Reached audience
Liaison activities, common events with other H2020 projects & knowledge exchange	# of relevant projects # of joint workshops	10 3	6 2	> 100 researchers in projects	70 researchers in projects
Liaison with relevant standardization bodies	# of active contributions to standards	5	7	Cybersecurity community	Cybersecurity community

Table 7: KPIs and achieved results for communication activities

Measure	KPI & Success Index	Achievement (M01-M18)
Publications in conferences	No. of peer-reviewed publications at conferences and workshops: ≥ 7 per year on average	M01-M06: 2 M07-M18: 12
Publications in journals	No. of peer-reviewed publications in journals: ≥ 3 per year on average	M01-M06: 4 M07-M18: 14
Participation to industrial events/exhibitions	No. of industrial events: ≥ 2 per year on average	M01-M06: 6 M07-M18: 8
Innovation workshop	No. of organized innovation workshops: At least 1 by the end of the project	1 completed (IEEE 5G World Forum 2020: Workshop on 5G Security: Current Trends, Challenges and New Enablers) 1 accepted to be organised (EuCNC&6GSummit 2021)
Seminars	No. of organized seminars: At least 2 by the end of the project	2 webinars
Academic dissemination	Average number of participants per lecture: At least ~50-70 participants per lecture	Lectures based on the INSPIRE-5Gplus' HLA in preparation
Participation and contribution to the 5G PPP programme	No. of participated/contributed 5G PPP WG's: ≥ 6	8 Working Groups
Interactions with worldwide fora and institutes	No. of interactions: ≥ 1 per year	6

Table 8: KPIs and achieved results for dissemination activities



5 Conclusions

The impact of COVID-19 pandemic has forced the consortium to adapt its strategy regarding dissemination and standardisation activities. Some of the programmed events were cancelled during the initial period of the pandemic (e.g., Mobile World Congress MWC'20), but a virtual model gradually took hold. For this reason, the consortium started to give greater weight to online events, talks, virtual conferences and virtual standardisation meetings, in order to achieve the planned dissemination and standardisation objectives.

Corresponding to that, some KPI targets have been impacted and it has become necessary to re-assess them in the light of the new situation. Nonetheless, the communication-, dissemination- and standardisation activities have progressed well, as shown in this deliverable, including the expected and achieved results.



Appendix A INSPIRE-5Gplus revised project flyer

Key Targets

INSPIRE-5Gplus makes a revolutionary shift in the 5G and Beyond security vision by progressing 5G security and by devising a smart, trustworthy and liability-aware 5G end-to-end security platform for future connected systems.

INSPIRE-5Gplus will allow the advancement of the security vision for 5G and beyond through the adoption of a set of emerging trends and technologies:

- Zero-touch security management
- Software-defined security and trust models
- Smart end-to-end security orchestration through Artificial Intelligence
- Liable and trusted security management

INSPIRE-5Gplus will ensure that the provided security level is in conformance with security requirements by legislation, standards, and verticals. Trust and liability will be fostered through integration of novel mechanisms supporting confidence between parties and compliance with regulation:

- Trust and Reputation Manager: assigns trust and reputation values to monitored entities
- Service Trust Manager: implements smart-contracts calculating trust and reliability of a cloud infrastructure or its services
- End-to-End Trust Management: provides cross-domain versions of trust functions



Project coordinator: Uwe Herzog (Eurescom, Germany)
Technical Coordinator: Dhouha Ayed (Thales, France)

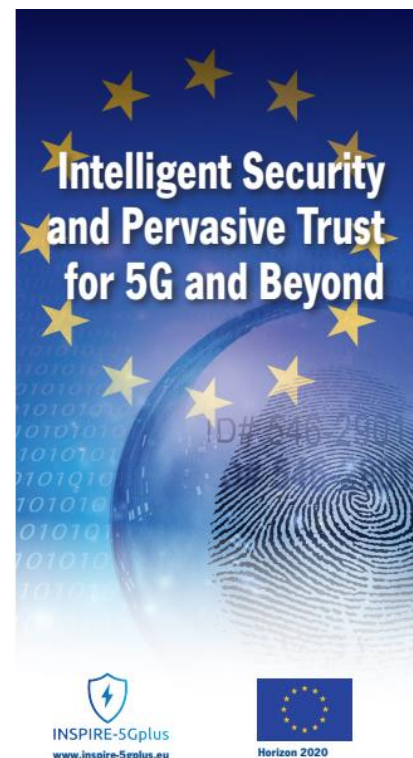
www.inspire-5gplus.eu

Twitter: @Inspire-5Gplus

www.linkedin.com/in/project-inspire-5gplus-0871961a4/



INSPIRE-5Gplus has received funding from the European Union's Horizon 2020 Research and Innovation Programme under grant agreement no. 871808.



INSPIRE-5Gplus
www.inspire-5gplus.eu



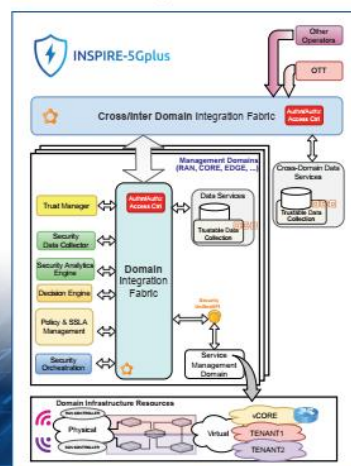
Test Cases

Test Case (TC)	High-Level Architecture Category						
	Size Management	SSLA Manager	Security Orchestrator	Security Analysis	Security Function	Security Enforcement	Security Measurement
TC1: Secured Anticipated Cooperative Collision Avoidance	*	*	*				
TC2: Definition and Assessment of Security and Service Level Agreements and Automated Remediation		*	*				*
TC3: Attack Detection over Encrypted Traffic			*				*
TC4: E2E Encryption TEE secured SECaaS	*	*	*	*	*	*	*
TC5: End-to-End Slice Protection based on Moving Target Defense and Anomaly Detection			*				*
TC6: GDPR-Aware Counterparts for Cross-Border Movement	*	*	*	*	*	*	*
TC7: Intelligent and Secure Management of Shared Resources to Prevent (D)DoS	*	*	*	*	*	*	*
TC8: Security Posture Assessment and Threat Visualization of 5G Networks							*
TC9: Secure and Privacy Enabled Local 5G Infrastructure	*						

High-Level Architecture

The INSPIRE-5Gplus architecture is designed to support fully automated end-to-end network and service security management in multi-domain 5G environments. The architecture empowers protection, trustworthiness, and liability in managing virtualized network infrastructures across multi-domains: radio, edge, and core segments.

Each Security Management Domain (SMD) is responsible for intelligent security automation of resources and services within its scope. INSPIRE-5Gplus' end-to-end SMD manages security of services that span multiple domains such as end-to-end slicing. Each SMD comprises a set of functional modules, e.g. security intelligence engine, security orchestrator, and trust manager, that operate in an intelligent closed-loop way to enable software defined security orchestration.



Main Results

- A comprehensive report on the current security landscape of 5G networks and the foreseen evolution trends of this landscape, either regarding security threats or security requirements.
- Intelligent and autonomic end-to-end cybersecurity architecture that can detect and mitigate both existing and new threats targeting 5G networks.
- Evolved and new security assets taking advantage of artificial intelligence and state-of-the-art techniques with a focus on trust and liability across 5G infrastructure and services.
- An integration and experimentation framework, with the objective of validating the project's developments in nine specific 5G security test cases.

INSPIRE-5Gplus at a Glance

Horizon 2020 Work Programme Topic:
ICT-20-2019-2020: 5G Long Term Evolution

Start Date:
1 November 2019 End Date: 31 October 2022

Consortium:
14 partners from 8 countries



Appendix B Workshop on 5G Security – Call for papers



CALL FOR PAPERS

PC Chairs

Antonio Skarmeta, *Universidad de Murcia, Spain*
 Sye Loong Keoh, *University of Glasgow, UK*
 Pascal Bisson, *Thales, France*

Programme Committee

Jordi Ortiz
Universidad de Murcia, Spain
 Edgardo Montesdeoca
Montage, France
 Xiao Yi Pan
National University of Defense Tech., China
 Chee Kiat Seow
University of Glasgow, UK
 Kok Lim Alvin Yau
Sunway University, Malaysia
 Geong Sen Poh
Singapore Telecom, Singapore
 Zhaohui Tang
University of Southern Queensland, Australia
 David Li
University of Glasgow, UK
 Forest Tan
Singapore Institute of Technology
 Ramon Ruiz
Universidad de Murcia, Spain
 Soon Yim Tan
Nanyang Technological University, Singapore
 Taleb Tarik
Aalto University, Finland
 Diego López
Telefónica I+D, Spain
 Ronny Ko
Harvard University, USA
 Ming Yao
InsightOne, China
 Antonio Pastor
Telefónica I+D, Spain

The 5G long term vision is to turn the network into an energy-efficient distributed computer that enables agile and dynamic creation, move and suppression of processes and services in response to changing customer demands and information flows, and supports interaction with humans through new communication modes, such as gestures, facial expressions, sound, haptics, etc. To make this vision a reality, a shift towards a full automation of network and service management and operation is a necessity.

However, a major challenge facing full automation is the protection of the network and system assets (i.e., services, data and network infrastructure) against potential cybersecurity risks introduced by the unprecedented evolving 5G threat landscape. Recent advances in Blockchain technology and Artificial Intelligence have opened up new opportunities in developing robust and intelligent security solutions. The fusion of 5G, Blockchain, Security and AI is anticipated to be the core technologies to realise digital transformation in the next decade.

Although work on security has been engaged throughout the successive phases of 5G-PPP Programme (e.g., 5G-ENSURE, CHARISMA, NRG-5) and some results were achieved, if not already adopted by Standards Developing Organizations (SDOs) in the field (e.g. 3GPP), addressing 5G security concerns is far from being completely resolved. Existing solutions suffer from a number of limitations.

The workshop is aimed at discussing the emerging 5G security in a holistic manner to understand the challenges, opportunities & standardization imperatives and define the way forward and immediate next steps to ensure ubiquitous adoption of 5G globally.

Within its scope, the workshop solicits research and industry papers identifying research and engineering challenges in 5G Security on following topics but not limited to:

- Security, privacy and trust in 5G
- Blockchain technology for 5G networks
- Physical and MAC layer security for 5G networks
- Current and future trends in 5G security
- Testbeds for 5G in security
- AI-driven Software-Defined Security (SD-SEC)
- Architecture and secure protocols for 5G applications
- Standardization efforts and initiatives for 5G Security
- Smart security of future connective systems
- 5G communication security
- Zero-touch management (ZTM)
- AI/ML techniques in security for 5G networks
- Verticals' and standard's security requirements
- Trust and liability in 5G

All submitted papers should follow the general paper guidelines of IEEE 5G-WF.

Submissions accepted through:

<https://edms.info/ieeePaper.php?c=26852&track=101406>

Important Dates

Paper Submission Due: **May 1, 2020**
 Acceptance Notification: **June 30, 2020**
 Camera-Ready Submission: **July 31, 2020**

Supported by:

