

D7.4

Second Period Dissemination, Standardization and Outreach Report

This deliverable presents the second results of the ANASTACIA Task 7.1 which aims to identify the metrics in order to raise awareness thanks to the presentations, workshops and conferences.

Distribution level	PU
Contractual date	14.11.2019 [M35]
Delivery date	02.12.2019 [M36]
WP / Task	WP7 / T7.1
WP Leader	THALES
Authors	Zinelaabidine Nadir (Aalto University), Othmane Hireche (Aalto University), Aiman Nait Abbou (Aalto University), Miloud Bagaa (Aalto University) and Tarik Taleb (Aalto University), Adrian Quesada Rodriguez (Mandat International), Bojana Tosic Bajic (Archimede Solutions), Dallal Belabed (THALES), Kristian Slavov (Ericsson)
EC Project Officer	Carmen Ifrim carmen.ifrim@ec.europa.eu
Project Coordinator	SoftecoSismatSpA Stefano Bianchi Via De Marini 1, 16149 Genova – Italy +39 0106026368 stefano.bianchi@softeco.it
Project website	www.anastacia-h2020.eu

ANASTACIA has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement N° 731558 and from the Swiss State Secretariat for Education, Research and Innovation.

This document only reflects the ANASTACIA Consortium's view.
The European Commission is not responsible for any use that may be made of the information it contains.



Table of contents

PUBLIC SUMMARY	3
1 Introduction.....	3
1.1 Aims of the document.....	3
1.2 Applicable and reference documents	3
1.3 Revision History.....	3
1.4 Acronyms and Definitions	4
2 Dissemination.....	5
2.1 Publications.....	5
2.2 Dissemination and promotional activities	6
3 Standardization	15
3.1 Standardization activities in IETF	15
3.2 Standardization activities in ETSI	17
3.3 Standardization activities in 3GPP.....	17
3.4 Standardization activities in OASIS.....	18
3.5 Standardization activities in ITU.....	18
3.6 Standardization activities in TM Forum	18
4 Online presence.....	19
4.1 Website	19
5.2 Twitter	26
5.3 YouTube.....	29
5 Conclusions.....	30
6 References.....	30

Index of figures

Figure 1: ANASTACIA's booth during the IoT Solutions World Congress event 2018- Barcelona.....	7
Figure 2: AS and MI team during the The Ibero-American Meeting Of Data Protection	8
Figure 3: Official picture from IAPP 2018	9
Figure 4: ANASTACIA's Booth IAPP 2018.....	9
Figure 5: ANASTACIA's Booth WSIS conference 2019.....	10
Figure 6: ANASTACIA's BoothAI for Good Summit Geneva.....	11
Figure 7: ANASTACIA's booth during the European data protection day in Berlin	11
Figure 8: ANASTACIA's Booth IoT Week Aarhus 2019.....	12
Figure 9: Anastacia booth at CEATEC JAPAN 2019	13
Figure 10: ANASTACIA booth at Computer Science Workshop 2019.....	14
Figure 11: TIMELINE section of the ANASTACIA project's website	20
Figure 12: RESULTS section of the ANASTACIA project's website	21
Figure 13: Audience Overview for the ANASTACIA project's website (Source: Google Analytics)	22
Figure 14:Acquisition Overview for the ANASTACIA project's website (Source: Google Analytics).	23
Figure 15: Visitors' geographical distribution – world map view (Source: Google Analytics).....	24
Figure 16: Visitors' geographical distribution – table view, up to position 20 (Source: Google Analytics).....	25
Figure 17: ANASTACIA project's Twitter account - home page.....	26
Figure 18 : ANASTACIA project's Twitter account Activities in September 2019 (Source: Twitter Analytics). 26	
Figure 19: ANASTACIA project's Twitter account Activities in April 2019 (Source: Twitter Analytics).	27
Figure 20: ANASTACIA project's Twitter account Audience insights (Source: Twitter Analytics).	28
Figure 21: ANASTACIA Project's YouTube account/channel.	29

PUBLIC SUMMARY

This document outlines the standardization, dissemination and promotional activities during the second period of ANASTACIA project. It also identifies the main metrics to raise awareness through presentations, workshops, conferences, and other events.

1 INTRODUCTION

1.1 AIMS OF THE DOCUMENT

This document represents the second results of ANASTACIA's WP7. It presents the main dissemination activities and events held to raise awareness on the project achievements within the community of researchers and industrials. These events consist of workshops, presentations and conferences.

WP7 is responsible for the dissemination and outreach activities while receiving contributions from other work packages [1].

This document is structured as follows. Section 2 presents the dissemination activities of the project partners and promotional activities. Section 3 presents the different standardization activities conducted in ANASTACIA, Online presence and Conclusions are drawn in Sections 4 and 5 respectively.

1.2 APPLICABLE AND REFERENCE DOCUMENTS

This document refers to the following documents:

- ANASTACIA project deliverable D7.1 - Initial Dissemination, Standardization, and Outreach Strategy Plan

1.3 REVISION HISTORY

Version	Date	Author	Description
0.1	21.11.2019	Zinelaabidine Nadir	Content of Chapter 5
0.2	21.11.2019	Aiman Nait Abbou	Content of chapter 2, 3, 6
0.3	21.11.2019	Othmane Hireche	Content of chapter 2
0.4	22.11.2019	Miloud Bagaa	Editorial corrections of chapter 1-6
0.5	22.11.2019	Kristian Slavov	Standardization
0.6	04.12.2019	Adrian Quesada Rodriguez, Bojana Bajic	Standardization and Dissemination
0.7	11.12.2019	Dallal Belabed	Section 2 and 5 and general revision of the document
0.8	15.12.2019	Zinelaabidine Nadir, Aiman Nait Abbou, Othmane Hireche	Update and correction of chapter 1-6
0.9	17.12.2019	Miloud Bagaa	Update and correction of chapter 1-6
1.0	27.12.2019	Stefano Bianchi	Final proofreading

1.4 ACRONYMS AND DEFINITIONS

Acronym	Meaning
CGA	Cryptographically Generated Address
EAP	Extensible Authentication Protocol
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IoT	Internet-of-Things
LWIG	Light Weight Implementation Guidance
T2TRG	Thing-to-Thing Research Group
SDO	Standards Development Organization
GIoTS	Global Internet of Things Summit
IRSG	Internet Research Steering Group
EVE	Evolution & Ecosystems
ISG	Industry Specification Group
LI	Lawful interception
SBA	Service Based Architecture
ONAP	Open Network Automation Platform
ADMF	administrative function
SDNs	Software Defined Networks
NFVs	Virtual Network Functions
AAF	Application Authorization Framework
SEC	Security Subcommittee
STIX	Structured Threat Information Expression
SDOs	STIX Domain Objects
SROs	STIX Relationship Objects
SOL	solution

2 DISSEMINATION

In this section, we present the different publications, dissemination and promotional activities conducted by the project partners.

2.1 PUBLICATIONS

1. S. Ziegler, A. Skarmeta, J. Bernal, E. E. Kim and S. Bianchi, "ANASTACIA: Advanced networked agents for security and trust assessment in CPS IoT architectures," 2017 Global Internet of Things Summit (GloTS), Geneva, 2017, pp. 1-6.
2. S. Lal, T. Taleb and A. Dutta, "NFV: Security Threats and Best Practices," in IEEE Communications Magazine, vol. 55, no. 8, pp. 211-217, Aug. 2017
3. S. Lal, S. Ravidas, I. Oliver and T. Taleb, "Assuring virtual network function image integrity and host sealing in Telco cloue," 2017 IEEE International Conference on Communications (ICC), Paris, 2017, pp. 1-6
4. H. Sedjelmaci, S. M. Senouci and T. Taleb, "An Accurate Security Game for Low-Resource IoT Devices," in IEEE Transactions on Vehicular Technology, vol. 66, no. 10, pp. 9381-9393, Oct. 2017.
5. M. Bouet, V. Conan "Geo-partitioning of MEC Resources" In Proceedings of the Workshop on Mobile Edge Communications (MECOMM '17), ACM, New York, NY, USA, 2017, pp. 43-48.
6. E. Cambiaso, G. Papaleo, M. Aiello, "Slowcomm: Design, development and performance evaluation of a new slow DoS attack", Journal of Information Security and Applications, Vol 35, pp. 23-31, 2017.
7. I. Farris et al., "Towards provisioning of SDN/NFV-based security enablers for integrated protection of IoT systems," 2017 IEEE Conference on Standards for Communications and Networking (CSCN), Helsinki, 2017, pp. 169-174.
8. S. Lal, A. Kalliola, I. Oliver, K. Ahola and T. Taleb, "Securing VNF communication in NFVI," 2017 IEEE Conference on Standards for Communications and Networking (CSCN), Helsinki, 2017, pp. 187-192.
9. Y. Khettab, M. Bagaa, D. L. C. Dutra, T. Taleb and N. Toumi, "Virtual security as a service for 5G verticals," 2018 IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, 2018, pp. 1-6.
10. A. M. Zarca, D. Garcia-Carrillo, J. B. Bernabe, J. Ortiz, R. Marin-Perez and A. Skarmeta, "Managing AAA in NFV/SDN-enabled IoT scenarios," 2018 Global Internet of Things Summit (GloTS), Bilbao, 2018, pp. 1-7.
11. D. Mehta, A. Mady, M. Boubekur, D. M. Shila, "Anomaly-Based Intrusion Detection System for Embedded Devices on Internet" in Proceedings of the Tenth International Conference on Advances in Circuits, Electronics and Micro-electronics, Venice, Italy. 2018. p. 16-20
12. A. Mady, R. Trapero, A. Skarmeta, S. Bianchi, "Towards Secure Building Management System based on Internet of Things" in Proc. CENICS. 2017. p. 61-644
13. I. Vaccari, E. Cambiaso, M. Aiello, "Remotely Exploiting AT Command Attacks on ZigBee" in Networks. Security and Communication Networks, 2017, pp 1-9.
14. M. Zarca, J.B. Bernabe, I. Farris, T. Taleb, A. Skarmeta, and Y. Khettab, "Enhancing IoT Security through Network Softwarization and Virtual Security Appliances" in ACM Int'l J. of Network Management, 2018
15. M. Bouet and V. Conan, "Mobile Edge Computing Resources Optimization: A Geo-Clustering Approach," in IEEE Transactions on Network and Service Management, vol. 15, no. 2, pp. 787-796, June 2018.
16. A.M. Zarca, J.B. Bernab , Skarmeta, J.M Alcaraz, "Virtual IoT Honeynets to mitigate cyberattacks in SDN/NFV-enabled IoT networks" in IEEE Journal on Selected Areas in communications,
17. A. Molina Zarca et al., "Security Management Architecture for NFV/SDN-Aware IoT Systems," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8005-8020, Oct. 2019.
18. P. Salva, et al , "5G NB-IoT: Efficient network traffic filtering for multi-tenant IoT cellular networks" in Security and Communication Networks , 2018

19. A.M. Zarca et al. "Enabling Virtual AAA Management in SDN-Based IoT Networks." *Sensors* (Basel, Switzerland) vol. 19,no.2, Jan. 2019.
20. I. Vaccari, E. Cambiaso, L. Patti, M. Aiello, "Darknet Security: A Categorization of Attacks to the Tor Network" in *ITASEC 2019*, 2019
21. E. Cambiaso, G. Chiola, M. Aiello, "Introducing the SlowDrop Attack" in *Computer Networks*, Vol 150,pp 234-249,2019.
22. D. Mehta, B. Andrea, A. Mady, S. Vuppala, S. Piotr," Constraint Programming Model for Anomaly Detection" in *European Conference on Operational Research* Dublin, Ireland, June, 2019.
23. S. Vuppala, A. E. Mady and D. Mehta, "A Novel Asset Authentication Scheme for Cyber Physical Systems," 2019 Global IoT Summit (GloTS), Aarhus, Denmark, 2019, pp. 1-5.
24. D. Mehta, B. Andrea, A. Mady, S. Vuppala, S. Piotr, "Learning Constraint-based Model for Detecting Malicious Activities in Cyber Physical Systems" in *International Conference on Advanced and Trusted Computing*, Leicester, UK, Aug., 2019.
25. J L. Hernández-Ramos et al,"Protecting personal data in IoT platform scenarios through encryption-based selective disclosure" in *Computer Communications*, Vol 130, pp 20-37, 2018.
26. A. Boudi, I. Farris, M. Bagaa, and T. Taleb, "Assessing lightweight virtualization for security-as-a-service at the network edge" in *IEICE Transactions on Communications*, 2019, vol. 102, no 5, p. 970-977.
27. I. Farris, T. Taleb, Y. Khettab, and J. Song, "A Survey on Emerging SDN and NFV Security Mechanisms for IoT Systems" *IEEE Communications Surveys & Tutorials*, 2018, vol. 21, no 1, p. 812-837.
28. A. Boudi, I. Farris, M. Bagaa, and T. Taleb, "Lightweight Virtualization based security framework for Network Edge" in *2018 IEEE Conference on Standards for Communications and Networking (CSCN)*. IEEE, 2018. p. 1-6
29. V Casola, et al. "A security monitoring system for internet of things." *Internet of Things 7* (2019) vol. 7, p. 100080.
30. I. Vaccari, E. Cambiaso, M. Aiello, "Evaluating Security of Low-Power Internet of Things Networks" in *International Journal of Computing and Digital Systems*, 2019, vol. 8, no 02, p. 101-114.

2.2 DISSEMINATION AND PROMOTIONAL ACTIVITIES

The International Event on IoT Solutions World Congress (www.iotsworldcongress.com) is one of the leading international events that links the Internet of Things with industry. The last edition took place in Barcelona on the period between October 16th -18th 2018 and was attended by more than 13,000 visitors and 279,700 web visits during the month of the event. 252 media & press registered for the event. During its three days period, the ANASTACIA project was presented in an exhibition panel. Visitors were very interested in security and privacy solutions in order to obtain seals or certifications for private clients and IoT deployments.

The Figure 1 presents ANASTACIA's booth during the event.



Figure 1: ANASTACIA's booth during the IoT Solutions World Congress event 2018- Barcelona

The Ibero-American Meeting for the Protection of Personal Data 2018

During this meeting in Costa Rica we have promoted ANASTACIA within the ecosystem of privacy and security professionals. We had the opportunity to meet with more than 400 privacy experts and stakeholders from private and public sector from Latin America and Europe, such as representatives of data protection authorities of Spain, Mexico, Uruguay, Colombia, Chile, Argentina, the Federal Trade Commission of the United States, Google, Facebook and Microsoft. We promoted Privacy and Cyber-security Tools in relation with ANASTACIA project and exchange different ideas regarding privacy and Cyber security.



Figure 2: AS and MI team during the The Ibero-American Meeting Of Data Protection

The **IAPP Europe Data Protection Congress 2018** edition took place in Brussels – Belgium and was attended by more than 2000 visitors.

Main event in data protection, law and policy with wide-ranging discussions of strategic developments in regional and international data protection, plus training classes and a deep-dive workshop day.

ANASTACIA participated with a conference booth. In the addition to promoting the Project to the experts and professionals of security and privacy, many visitors and enthusiasts had the chance to discover the project and our vision toward the emerging technologies related to ANASTACIA from a different angle. Figure 3 and 4 provide pictures from the event.



Figure 3: Official picture from IAPP 2018



Figure 4: ANASTACIA's Booth IAPP 2018

IAPP world summit in Washington (April 2019)

IAPP summit in Washington is privacy and data protection conference that focuses on international topics, policy and strategy. Recognized as a leading forum for discussion, the Summit features expert speakers and top regulators, and delivers unmatched education and networking opportunities. MI promoted the project ANASTACIA during this conference reaching the most important stakeholders from the privacy domain.

ITU WSIS Forum in Geneva, (April 2019)

World Summit on the Information Society (WSIS) Forum is a global United Nations (UN) multistakeholder platform facilitating the implementation of the WSIS Action Lines for advancing Sustainable Development Goals (SDGs). It is co-organized by ITU, UNESCO, UNDP and UNCTAD, in close collaboration with all WSIS Action Line co-/facilitators and other UN organizations (UNDESA, FAO, UNEP, WHO, UN Women, WIPO, WFP, ILO, WMO, ITC, UPU, UNODC, UNITAR, UNICEF and UN Regional Commissions). MI and AS presented the Anastacia project with the booth during the 4 days of the conference and used the opportunity to receive the feedback regarding the DSPS thanks to the Survey made to engage the end-users in development of the DSPS. With more than 1000 visitors WSIS is one of the most important conferences in the domain of internet technologies.



Figure 5: ANASTACIA's Booth WSIS conference 2019

ITU AI for Good global summit in Geneva, (May 2019).

AI for Good is a United Nations platform, centered around annual Global Summits, that fosters the dialogue on the beneficial use of Artificial Intelligence, by developing concrete projects. MI and AS had the opportunity to present the Anastacia project during the conference and to disseminate the Survey for end-user engagement in the development of the DSPS.



Figure 6: ANASTACIA's Booth AI for Good Summit Geneva

European Data Protection Day in Berlin (May 2019)

One of the largest European conference for the privacy experts where met more than 400 data protection authorities, DPOs and data protection specialists from all over the world. AS and MI promoted the Anastacia project and its relation with in privacy regulations like GDPR and ePrivacy. Furthermore, we distributed our survey in order to implement our user validation activities.



Figure 7: ANASTACIA's booth during the European data protection day in Berlin

IoT Week Aarhus (June 2019)

Europe's largest IoT conference, IoT Week was held 17 - 21 June 2019 in Aarhus, Denmark with more than 2000 visitors, 360 speakers from the worlds of research, industry, business, technology and science. The conference was complemented for the first time by a public exhibition that provided the experience of real IoT solutions and products, inspiring and showing how far IoT and digitization have come today. Anastacia was presented at the Public Exposition place during three days of the conference.

Project and the was promoted to the experts and professionals of security and privacy but also to many visitors from universities that had the chance to discover the project and Anastacia vision toward the emerging technologies.



Figure 8: ANASTACIA's Booth IoT Week Aarhus 2019

Annual Privacy Forum 2019, Rome

ENISA, DG CONNECT, the University of Rome Tor Vergata and LUISS University organized the Annual Privacy Forum (APF) 2019 on 13 & 14 June 2019 in Italy, Rome. The event encouraged dialog with panel discussions and provided the room for exchange of ideas in between scientific sessions.

MI had the booth during the conference where Anastacia was presented to European privacy professionals.

41st International conference of data protection and privacy commissioners in Albania (Oct. 2019)

The International Conference of Data Protection and Privacy Commissioners (ICDPPC) is a worldwide annual forum at which independent regulators on privacy, data protection and freedom of information adopt high level resolutions and recommendations addressed to governments and international organisations. The Conference connects the efforts of 122 privacy and data protection authorities from across the globe.

MI promoted the project Anastacia during the conference to Data Protection and Privacy Commissioners, members, observers and European privacy community.

Combined Exhibition of Advanced Technologies, CEATEC 2019, Japan (October 2019)

Connecting CPS and IoT CEATEC creates business opportunities based on co-creation involving a wide range of industries and fields. This event brings the technologies together in one venue that is ideal for the exchange of information. This facilitates for realization of Society 5.0, the ultra-smart society designed to further economic development and the solution of social problems.

MI promoted the project Anastacia during the conference among more than 2000 visitors from IoT and CPS domain.



Figure 9: Anastacia booth at CEATEC JAPAN 2019

IAPP European summit in Brussels (Nov. 2019)

The IAPP Europe Data Protection Congress 2019 was held in Brussels, again with more than 2000 visitors. Main event in data protection, law and policy with wide-ranging discussions of strategic developments in regional and international data protection. ANASTACIA participated with a conference booth in order to explore the opportunities for the sustainability of the tools developed within the project.

Computer Science Workshop 2019 (June 2019)

<http://phd.dibris.unige.it/csse/index.php/activities-and-credits/computer-science-workshop>

The 1st edition of the Computer Science Workshop took place in Genoa (IT) at the Department of Informatics, Bioengineering, Robotics and System Engineering (DIBRIS) at the University di Genova.

As Computer Science is constantly increasing in complexity, with many and many new fields of research emerging (Virtual and Augmented Reality, Multi-Agent systems, Data Science, Computer Graphics, Security, Machine Learning, Programming Languages, Logic, Computer Vision, Software Engineering), the main goal of the workshop was discussing the many aspects of the Computer Science research fields, to present a broad perspective of this subject and look for possible (unexpected) interconnections.

SOFT was a sponsor of the event and illustrated the technical results of the project to the research community, in collaboration with CNR.



Figure 10: ANASTACIA booth at Computer Science Workshop 2019

3 STANDARDIZATION

During the project the member of the consortium have been involved in various standards organizations. The involvement spans from actively driving issues to closely monitoring and aligning the work accordingly. The standardization work requires a long-term commitment, much like open sourcing code. Simply disseminating the idea and/or code is never enough. Instead an active and long-term commitment is required for the ideas to proceed. Many of the contributions made during the project are in progress, and will not be standardized in time for the project ending. The task of pushing the ideas through will be left at partners' discretion.

ENISA (European Union Agency for Cybersecurity) has published a detailed report on threat landscape for 5G [2]. Many of the threats are generic enough to impact also non-5G related infrastructure. One of the most effective tools to combat the threats is having stronger standards. The sheer amount of threats means that they cannot all be solved within few standards. Instead, the security standardization work will always benefit from smaller inputs that make today's state of the art a bit stronger than yesterday's. In this aspect some of the mechanisms, tools and ideas, studied and evaluated within ANASTACIA, have proved to be beneficial for the standardization fora. This is evidenced by the partners' contributions that are accepted or are about to be accepted into a standard.

The main IoT security related contributions have been targeting three organizations: the Internet Engineering Task Force (IETF), the 3rd Generation Partnership Project (3GPP), and the European Telecommunications Standards Institute's Network Functions Virtualization group (ETSI NFV). Furthermore, the project has been actively following The Open Network Automation Platform (ONAP) and Organization for the Advancement of Structured Information Standards (OASIS).

Partner activity in standardization organizations has been divided in roughly three categories: *driving*, *contributing*, and *following*. The levels are defined in decreasing activity order. *Driving* is when a partner(s) push the idea/topic continuously until a final state is achieved. Reviewing and providing text and/or ideas to make the work item better is classified as *contributing*. The *following* category is reserved for any other active work.

Organization \ Activity	Following	Contributing	Driving
IETF		1	5
ETSI	3	1	2
3GPP		4	1
OASIS	1		
ITU			1
TM Forum			1

Table 1 Standardization activity

In the next subsections the topics that the partners have been driving are briefly described.

3.1 STANDARDIZATION ACTIVITIES IN IETF

IETF standardization focuses on internet protocols and network services. Within ANASTACIA, the project has been directly involved in driving and contributing to multiple security related drafts and RFCs. Here we describe some of the most essential ones to the project and the goal of the project.

Internet of Things (IoT) Security: State of the Art and Challenges

This informational standards document (RFC8576) discusses the various stages in the lifecycle of an IoT device. It documents the security threats to an IoT device and the challenges that one might face in order to protect against these threats. Finally, it discusses the next steps needed to facilitate the deployment of secure IoT systems.

One of the key challenges identified in this document was how the things in IoT networks can be securely configured before they are functional. This step is especially challenging as the number of these things may be large and they often have very limited user interfaces. The initial configuration of things may involve several sub-steps that must be completed before the thing is fully operational. Each of these sub-steps can be viewed in terms of authorization chains that need to be established.

Nimble out-of-band authentication for EAP

Secure bootstrapping is the process by which an IoT device gets the necessary configuration information and security credentials to become an operational part of the network and an IoT ecosystem.

Nimble out-of-band authentication for EAP (EAP-NOOB) is a generic bootstrapping solution for IoT devices which have no pre-configured authentication credentials and which are not yet registered on any server. EAP-NOOB performs an Ephemeral Elliptic Curve Diffie-Hellman (ECDHE) over the in-band EAP channel. The user then confirms this exchange by transferring the OOB message. Users can transfer the OOB message from the peer to the server, when for example, the device is a smart TV that can show a QR code. Alternatively, users can transfer the OOB message from the server to the peer, when for example, the device being bootstrapped is a camera that can only read a QR code. This work is still in progress.

Using EAP-TLS with TLS 1.3

EAP-TLS is specified in RFC 5216. It provides certificate-based mutual authentication and key derivation utilizing the Transport Layer Security (TLS) handshake protocol for cryptographic algorithms and protocol version negotiation, mutual authentication, and establishment of shared secret keying material. EAP-TLS is widely used for network access authentication in enterprise wireless networks. EAP-TLS is also the default certificate-based authentication method for 5G mobile networks and its usage is specified in 3GPP Technical Specification (TS) 33.501.

The most recent version of TLS, version 1.3, was published as RFC 8446. TLS 1.3 provides significantly improved security, privacy, and reduced latency when compared to earlier versions of TLS. Therefore, we are in the process of updating the EAP-TLS specification to use TLS 1.3. We not only incorporate the improved features of TLS version 1.3, but we also further improve security and privacy by mandating the use of privacy friendly identifiers and revocation checking. The work is still in progress.

EAP-based Authentication Service for CoAP

This contribution describes an authentication service for IoT devices that use EAP. The authentication service is built on top of the Constrained Application Protocol (CoAP) and allows authenticating and bootstrapping a security association between two CoAP endpoints without the need for additional protocols.

In particular, the document describes how CoAP can be used as EAP lower-layer to transport EAP between a CoAP server and a CoAP client. The CoAP client may contact a backend AAA infrastructure to complete the EAP negotiation. The work is on-going.

3.2 STANDARDIZATION ACTIVITIES IN ETSI

Standardization activities in ETSI have been focusing on Industry Specification Group for Network Functions Virtualization. From the project perspective, the most interesting working group within ISG NFV is the Security (SEC) working group. However, other working groups are also involved in defining some security aspects when they are defining the protocols. Therefore, now it is not only the SEC working group that is working with security, but other working groups such as solution (SOL) working group and interfaces and architecture (IFA) working group are also involved in defining some security requirements.

Remote attestation support for virtualized network functions

Attestation is a process of proving the environment is as was intended by the developer. It also allows repudiation in case of tampered code is executed. Attestation is a necessary step to ensure secure environment for NFV.

This work item concentrated on attestation. The work item tackles issues such as different levels of assurance, capability analysis of NFVI (NFV Infrastructure), state-of-the-art analysis of available attestation technologies and describing the operational procedures.

The work is published in ETSI GR NFV-SEC 007.

Virtualized network function (VNF) package security

Onboarding of a VNF requires a security validation check. This is critical for the successful deployment of VNFs. During the check the authenticity and integrity of the VNF package is verified against a signature provided by the VNF provider. Furthermore, some operators may choose to perform additional validation of the VNF package during the onboarding process.

The work done within this work item is defining the requirements for integrity, authenticity protection, and verification of the VNF package artefacts. Also, a process for service provider to provide confidentiality during the onboarding of the VNF is defined.

The work is published in ETSI GR NFV-SEC 021.

3.3 STANDARDIZATION ACTIVITIES IN 3GPP

With the next generation of mobile networks being specified, many new use cases are studied and covered. IoT traffic patterns is one focus point. Massive mobile communication such as, for example, Vehicle-to-Everything (V2X) create challenges especially from security point of view. The effect and management of these IoT device use cases is one of the focus points.

Privacy of users in V2X

Vehicles, i.e. UEs, are broadcasting information to other vehicles in the V2X architecture. If a UE is using the same identity in several broadcast messages, it is possible to track the vehicle and compromise the privacy of user in the vehicle.

This is being studied in 3GPP TR 33.836: Study on Security Aspects of 3GPP support for Advanced V2X Services.

URLLC security: In Ultra Reliable Low Latency Communication (URLLC)

The reliable connectivity is achieved by sending data to the UE via redundant connections called PDU sessions. The User Plane security policy for two PDU sessions used for redundant data transmission needs to have the same setting for encryption and for integrity protection. Otherwise an attack can be made against the PDU session which has weaker security.

This is being studied in 3GPP TR-33.825.

Early Small data transfer in RRC Suspend and Resume: 3GPP Cellular

IoT system has a mechanism where the RRC signaling connection from the base station to the UE can be suspended to save energy. When the UE has something to send to the network, it is possible to send the data in the first uplink (UL) RRC signaling messages to save signaling effort.

This is being studied in 3GPP TR-33.861: Study on evolution of Cellular IoT security for the 5G system.

3.4 STANDARDIZATION ACTIVITIES IN OASIS

UDG has followed the standardization activities carried out by the OASIS consortium, and has directly aligned the DSPS Agent with the STIX standard developed by the consortium (further information can be found in ANASTACIA D.5.2 and D.5.3), in order to effectively consume and generate cyber threat information with other solutions. MI is currently in the process of pursuing membership to the OASIS consortium, with the main goal of proposing an extension to the STIX standard aligned with the DSPS's privacy-related insights.

3.5 STANDARDIZATION ACTIVITIES IN ITU

As Rapporteur on Research and Emerging Technologies for the IoT and Smart Cities, ITU-T SG20, MI has introduced the ANASTACIA architecture (as part of contribution [C521](#)) for consideration as part of the upcoming Technical Report on "Unlocking Internet of Things with Artificial Intelligence: Where we are and where we could be". MI currently drives the work of Question 5 of SG20, which has led to the successful introduction of this contribution into the latest draft of the Technical Report.

3.6 STANDARDIZATION ACTIVITIES IN TM FORUM

MI is currently driving TM Forum's efforts towards the specification and standardization of diverse APIs related to the ANASTACIA project (particularly towards the integration of the DSPS with third party software). Work on this item is still confidential as per contractual agreements with TM Forum, additional information may be provided upon request.

4 ONLINE PRESENCE

In this section, we present different statistics of web access and social media of ANASTACIA's project accounts.

4.1 WEBSITE

The ANASTACIA project's website is available at: <http://www.anastacia-h2020.eu>

As a single-page site with different sections: CONCEPT, FRAMEWORK, HIGHLIGHTS, TIMELINE, RESULTS, FIGURES, TEAM, IAB, CONSORTIUM, CONTACTS.

In particular, the sections TIMELINE and RESULTS have been periodically updated to provide proper evidence of activities (meetings, events etc.) and deliveries (public deliverables, publications etc.).

























This is depicted in Figure 11 and Figure 12.





























Figure 11: TIMELINE section of the ANASTACIA project's website

RESULTS

PUBLIC DELIVERABLES

 D1.1 "Holistic Security Context Analysis" DOWNLOAD	 D1.2 "User Centred Requirements Initial Analysis" DOWNLOAD	 D7.1 "Initial Dissemination Standardization and Outreach Strategy Plan" DOWNLOAD
 D1.3 "Initial Architectural Design" DOWNLOAD	 D2.1 "Policy-Based Definition And Policy For Orchestration - Initial Report" DOWNLOAD	 D5.1 "Dynamic Privacy And Security Seal Model Analysis" DOWNLOAD
 D2.2 "Attack Threats Analysis And Contingency Actions - Initial Report" DOWNLOAD	 D6.1 "Initial Technical Integration and Validation Report" DOWNLOAD	 D3.1 "Initial Security Enforcement Manager Report" DOWNLOAD
 D2.3 "Privacy Risk Modelling And Contingency - Initial Report" DOWNLOAD	 D2.4 "Secure Software Development Guidelines - Initial Report" DOWNLOAD	 D3.2 "Initial Security Orchestrator Report" DOWNLOAD
 D6.2 "Initial Use Cases Implementation And Tests Report" DOWNLOAD	 D7.3 "First Period Dissemination Standardization And Outreach Report" DOWNLOAD	 D3.3 "Initial Security Enforcement Enablers Report" DOWNLOAD
 D6.3 "Initial End-User Validation and Evaluation Report" DOWNLOAD	 D4.1 "Initial Monitoring Component Services Implementation Report" DOWNLOAD	 D4.2 "Initial Reaction Component Services Implementation Report" DOWNLOAD
 D2.5 "Policy-based Definition and Policy for Orchestration Final Report" DOWNLOAD	 D4.3 "Initial Agents Development Report" DOWNLOAD	 D5.2 "Dynamic Security and Privacy Seal Monitoring Service" DOWNLOAD
 D1.4 "Final User Centred Requirements Analysis" DOWNLOAD	 D2.7 "Privacy Risk Modelling And Contingency - Final Report" DOWNLOAD	 D5.1 "Dynamic Privacy And Security Seal Model Analysis" DOWNLOAD

PUBLICATIONS - OPEN ACCESS, GREEN POLICY

 ANASTACIA Advanced Networked Agents for Security and Trust Assessment in CPS IoT Architectures DOWNLOAD	 An Accurate Security Game for Low-Resource IoT Devices DOWNLOAD	 Assessing Virtual Network Function Image Integrity and Host Sealing in Telco Cloud DOWNLOAD
 Geo-partitioning of MEC resources DOWNLOAD	 NFV Security Threats and Best Practices DOWNLOAD	 SlowComm Design Development and Performance Evaluation of a new Slow DoS Attack DOWNLOAD
 Towards Secure Building Management System based on Internet of Things DOWNLOAD	 Anomaly-Based Intrusion Detection System for Embedded Devices on Internet DOWNLOAD	 Securing VNF Communication in NFVi DOWNLOAD
 Towards Provisioning of SDN/NFV-based Security Enablers for Integrated Protection of IoT Systems DOWNLOAD	 Remotely Exploiting AT Command Attacks on ZigBee Networks DOWNLOAD	 Architecture of security association establishment based on bootstrapping technologies for enabling critical IoT infrastructures DOWNLOAD
 Enhancing IoT Security through Network Softwareization and Virtual Security Appliances DOWNLOAD	 Managing AAA in NFV/SDN-enabled IoT scenarios DOWNLOAD	 5G NB-IoT Efficient Network Traffic Filtering for IoT DOWNLOAD
 A survey on emerging SDN and NFV security mechanisms for IoT systems DOWNLOAD	 Assessing Lightweight Virtualization for Security-as-a-Service at the Network Edge DOWNLOAD	 Deinet Security A Categorization of Attacks to the Tor Network DOWNLOAD
 Enabling Virtual AAA Management in SDN-Based IoT Networks DOWNLOAD	 Introducing the SlowDrop Attack DOWNLOAD	 Lightweight Virtualization based security framework for Network Edge DOWNLOAD
 Protecting personal data in IoT platform scenarios through-encryption-based selective disclosure DOWNLOAD	 Trust-based Video Management Framework for Social Multimedia Networks DOWNLOAD	 Virtual Security as a Service for 5G Verticals DOWNLOAD
 Challenges in Cybersecurity and Privacy: the European Research landscape DOWNLOAD	 Key Innovations in ANASTACIA DOWNLOAD	

USE CASE DEMO VIDEOS






 DPS GUI demo DOWNLOAD [30x45]	 MEC.3 Use Case Demo DOWNLOAD [10x45]	 BMS.3 Use Case Demo DOWNLOAD [10x45]
 BMS.2 Use Case Demo DOWNLOAD [100x45]	 BMS.4 Use Case Demo DOWNLOAD [30x45]	

Figure 12: RESULTS section of the ANASTACIA project's website.

The website is monitored by Google Analytics tools (<https://analytics.google.com>). The data on the audience activity (website visitors) registered since the beginning of the project (Jan 2017) is summarized in Figure 13.

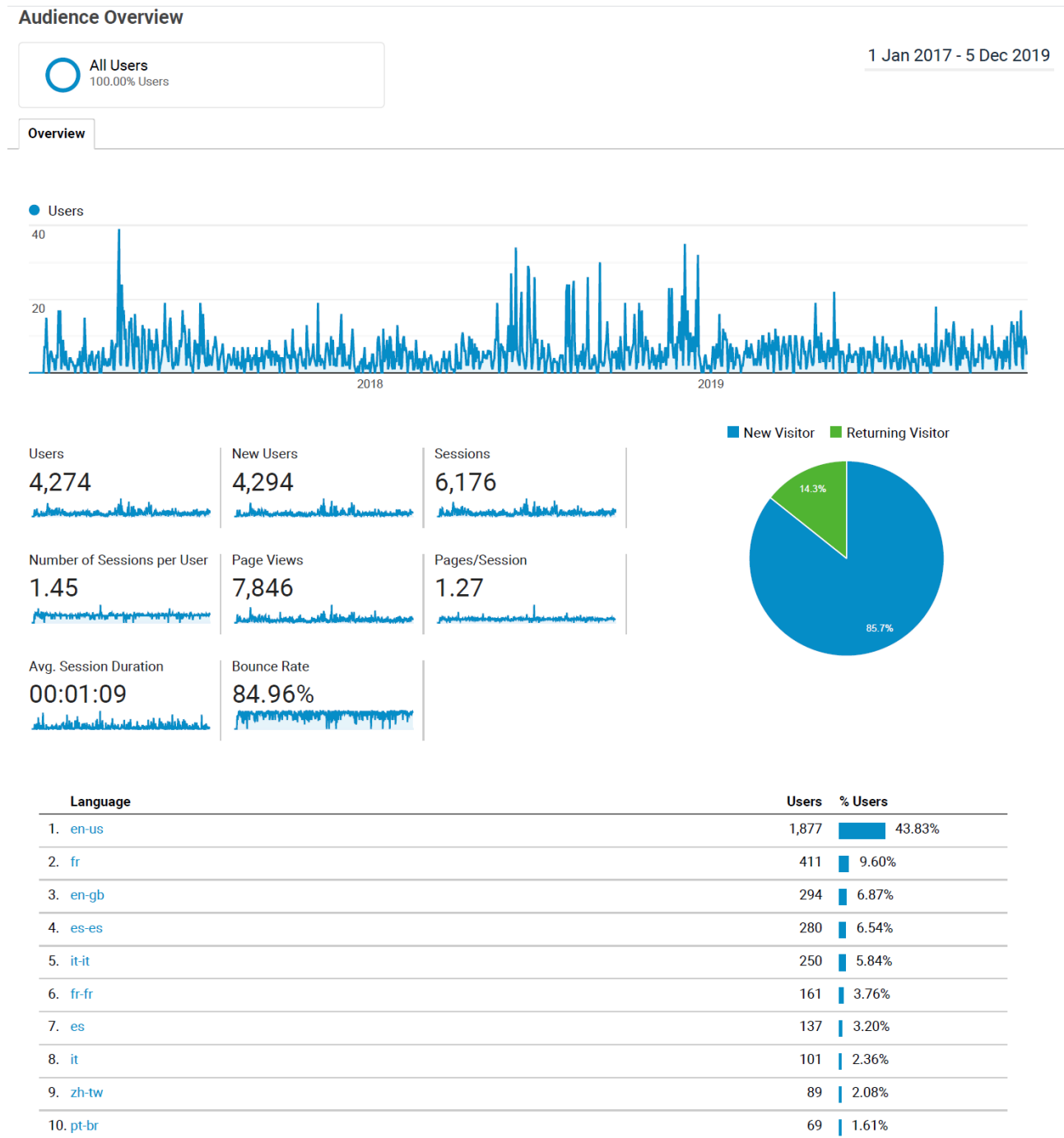


Figure 13: Audience Overview for the ANASTACIA project's website (Source: Google Analytics)

Information on acquisition modalities (i.e. ways to vehiculate user traffic on the project website) are summarized in Figure 14.

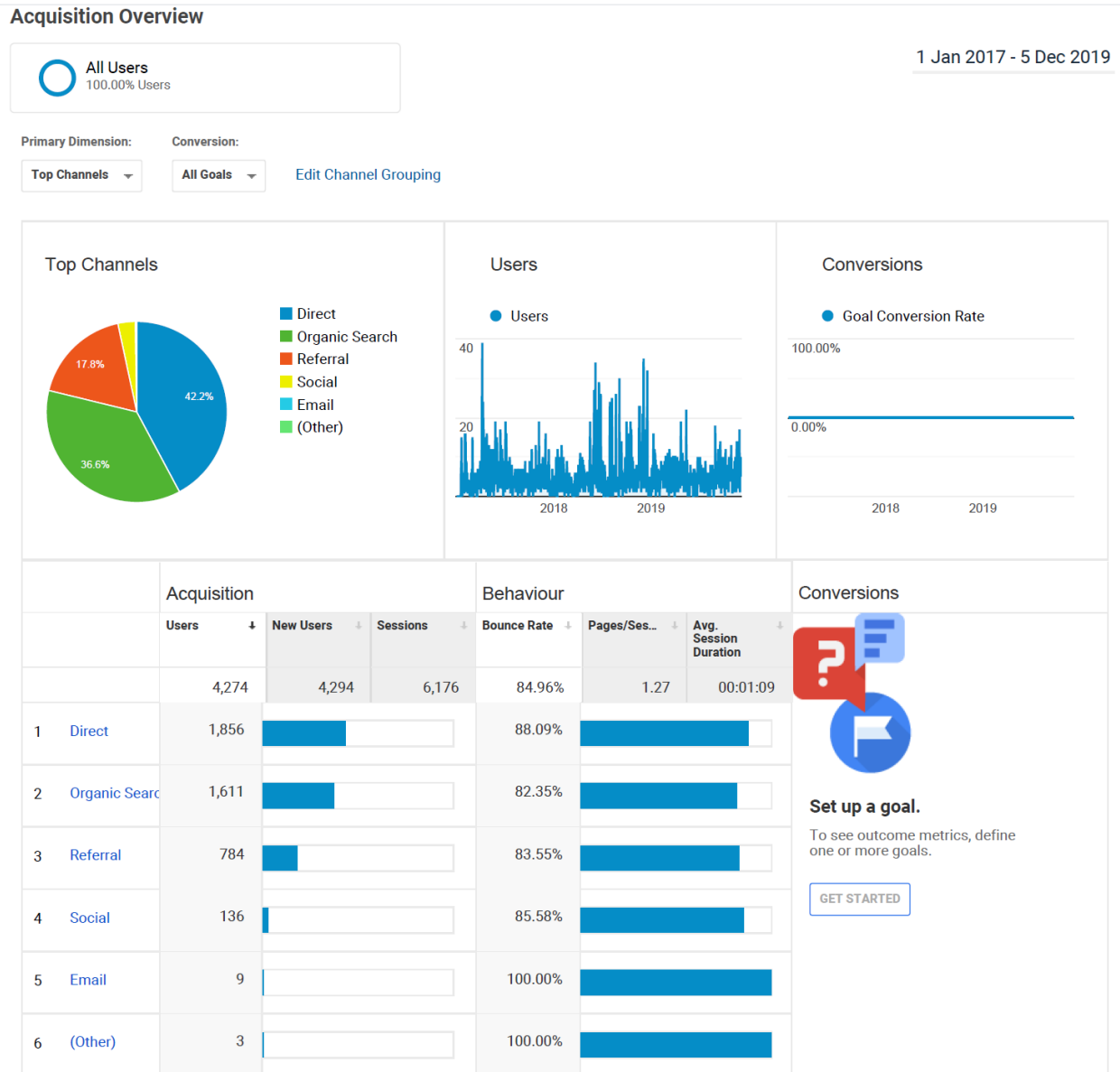


Figure 14: Acquisition Overview for the ANASTACIA project's website (Source: Google Analytics).

The geographical distribution of the website visitors is summarized in Figure 15 and Figure 16.

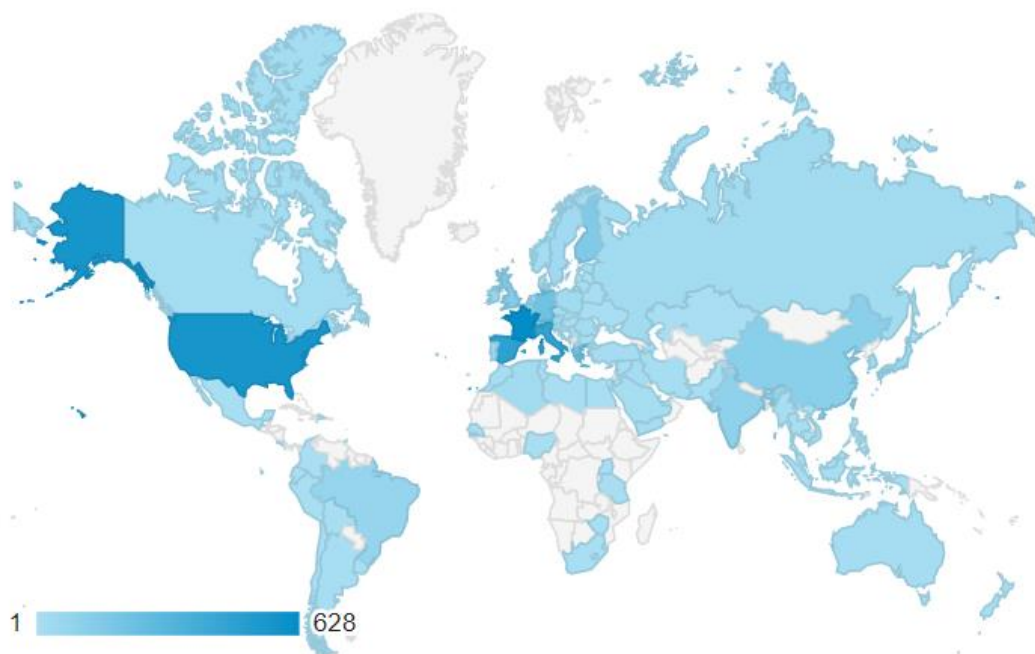



Figure 15: Visitors' geographical distribution – world map view (Source: Google Analytics).

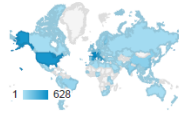
Location

 All Users
100.00% Users

1 Jan 2017 - 5 Dec 2019

Map Overlay

Summary



Country	Acquisition			Behaviour			Conversions		
	Users	New Users	Sessions	Bounce Rate	Pages/Session	Avg. Session Duration	Goal Conversion Rate	Goal Completions	Goal Value
	4,274 % of Total: 100.00% (4,274)	4,297 % of Total: 100.07% (4,294)	6,176 % of Total: 100.00% (6,176)	84.96% Avg for View: 84.96% (0.00%)	1.27 Avg for View: 1.27 (0.00%)	00:01:09 Avg for View: 00:01:09 (0.00%)	0.00% Avg for View: 0.00% (0.00%)	0 % of Total: 0.00% (0)	US\$0.00 % of Total: 0.00% (US\$0.00)
1. France	628 (14.35%)	622 (14.48%)	764 (12.37%)	83.77%	1.21	00:00:40	0.00%	0 (0.00%)	US\$0.00 (0.00%)
2. United States	560 (12.79%)	558 (12.99%)	627 (10.15%)	93.30%	1.10	00:00:35	0.00%	0 (0.00%)	US\$0.00 (0.00%)
3. Spain	475 (10.85%)	463 (10.77%)	720 (11.66%)	83.19%	1.28	00:01:12	0.00%	0 (0.00%)	US\$0.00 (0.00%)
4. Italy	452 (10.33%)	449 (10.45%)	793 (12.84%)	83.61%	1.34	00:01:42	0.00%	0 (0.00%)	US\$0.00 (0.00%)
5. Greece	218 (4.98%)	211 (4.91%)	338 (5.47%)	85.21%	1.31	00:01:08	0.00%	0 (0.00%)	US\$0.00 (0.00%)
6. Germany	216 (4.93%)	207 (4.82%)	276 (4.47%)	83.70%	1.33	00:01:42	0.00%	0 (0.00%)	US\$0.00 (0.00%)
7. Switzerland	193 (4.41%)	188 (4.38%)	360 (5.83%)	83.33%	1.27	00:01:17	0.00%	0 (0.00%)	US\$0.00 (0.00%)
8. Finland	153 (3.50%)	150 (3.49%)	309 (5.00%)	82.85%	1.26	00:01:09	0.00%	0 (0.00%)	US\$0.00 (0.00%)
9. United Kingdom	137 (3.13%)	132 (3.07%)	167 (2.70%)	85.03%	1.25	00:00:48	0.00%	0 (0.00%)	US\$0.00 (0.00%)
10. China	118 (2.70%)	118 (2.75%)	121 (1.96%)	93.39%	1.19	00:00:16	0.00%	0 (0.00%)	US\$0.00 (0.00%)
11. Taiwan	114 (2.60%)	114 (2.65%)	278 (4.50%)	77.34%	1.40	00:02:18	0.00%	0 (0.00%)	US\$0.00 (0.00%)
12. India	99 (2.26%)	96 (2.23%)	123 (1.99%)	89.43%	1.20	00:00:31	0.00%	0 (0.00%)	US\$0.00 (0.00%)
13. Belgium	90 (2.06%)	84 (1.95%)	118 (1.91%)	87.29%	1.35	00:01:21	0.00%	0 (0.00%)	US\$0.00 (0.00%)
14. Brazil	75 (1.71%)	76 (1.77%)	98 (1.59%)	91.84%	1.11	00:00:30	0.00%	0 (0.00%)	US\$0.00 (0.00%)
15. Ireland	63 (1.44%)	61 (1.42%)	84 (1.36%)	82.14%	1.35	00:01:11	0.00%	0 (0.00%)	US\$0.00 (0.00%)
16. Netherlands	61 (1.39%)	59 (1.37%)	82 (1.33%)	86.59%	1.20	00:01:37	0.00%	0 (0.00%)	US\$0.00 (0.00%)
17. Austria	52 (1.19%)	48 (1.12%)	68 (1.10%)	85.29%	1.26	00:00:31	0.00%	0 (0.00%)	US\$0.00 (0.00%)
18. Japan	49 (1.12%)	49 (1.14%)	56 (0.91%)	85.71%	1.20	00:00:44	0.00%	0 (0.00%)	US\$0.00 (0.00%)
19. Portugal	42 (0.96%)	39 (0.91%)	47 (0.76%)	82.98%	1.30	00:00:37	0.00%	0 (0.00%)	US\$0.00 (0.00%)
20. Sweden	31 (0.71%)	32 (0.74%)	49 (0.79%)	81.63%	1.55	00:01:37	0.00%	0 (0.00%)	US\$0.00 (0.00%)

Figure 16: Visitors' geographical distribution – table view, up to position 20 (Source: Google Analytics).

5.2 TWITTER

The Twitter account of the ANASTACIA project is available at: https://twitter.com/ANASTACIA_H2020

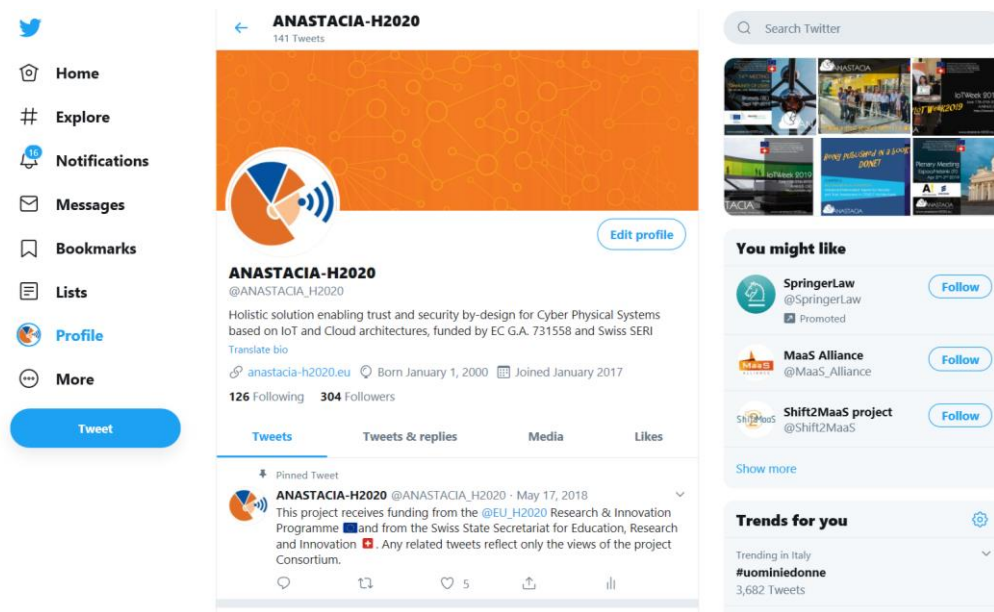


Figure 17: ANASTACIA project's Twitter account - home page

The Twitter account has been the most exploited social /online communication channel, with an intensive and constant activity focused on highlighting the main project results and dissemination events.

In its life, the project published over 150 tweets and reached more than 300 followers.

Monthly Twitter activity is illustrated in the following 4 screenshots extracted from Twitter analytics tools.



Figure 18 : ANASTACIA project's Twitter account Activities in September 2019 (Source: Twitter Analytics).

Tweet activity

Apr 1 – Apr 30, 2019

Export data

Your Tweets earned 2.3K impressions over this 30 day period



YOUR TWEETS
During this 30 day period, you earned 77 impressions per day.



Tweets Top Tweets Tweets and replies Promoted Impressions Engagements Engagement rate

ANASTACIA-H2020 @ANASTACIA_H2020 · Apr 11 Tomorrow the H2020 projects ANASTACIA (@ANASTACIA_H2020) and FINSEC (@finsec_project) will meet in GFT premises (Genoa, IT) to illustrate results, investigate mutual business and technology interests, define potential collaborations, and more! #ALLIEDFOREUCYBERSECURITY pic.twitter.com/qMzJRNwnz View Tweet activity	907	5	0.6%	Promote
ANASTACIA-H2020 @ANASTACIA_H2020 · Apr 11 Thanks to our partners in @ArchimedeSolut for (re) presenting our project! twitter.com/ArchimedeSolut... View Tweet activity	753	6	0.8%	Promote
ANASTACIA-H2020 @ANASTACIA_H2020 · Apr 11 ... #MORETHANWORDS - a big big thank you to our 250+ followers. @ANASTACIA_H2020 entered its 3rd and last year of activity - interesting & exciting results for our stakeholders to be released soon! Stay tuned! pic.twitter.com/O9Rfu1LuR1 View Tweet activity	732	8	1.1%	Promote
ANASTACIA-H2020 @ANASTACIA_H2020 · Apr 11 Did we thank @AaltoUniversity and @ericsson for hosting our plenary meeting in Espoo/Helsinki a few days ago?! Working hard on our Key Innovations, paving the road for proper exploitation of our IoT/CPS cybersecurity and privacy framework! pic.twitter.com/xsEoA9rVkn View Tweet activity	702	6	0.9%	Promote

Engagements

Showing 30 days with daily frequency



On average, you earned 0 link clicks per day



On average, you earned 0 Retweets per day



On average, you earned 0 likes per day



On average, you earned 0 replies per day

Figure 19: ANASTACIA project's Twitter account Activities in April 2019 (Source: Twitter Analytics).

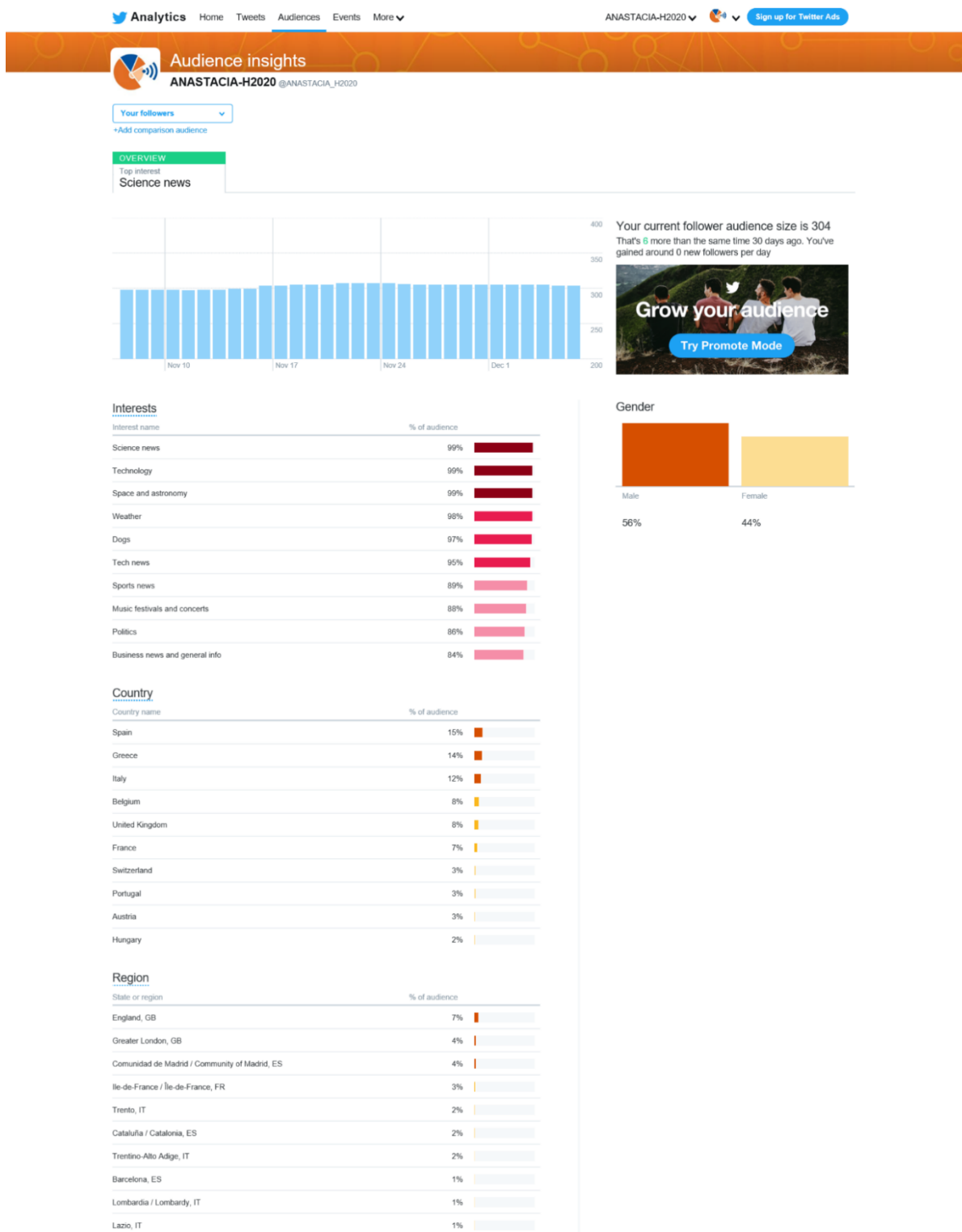


Figure 20: ANASTACIA project's Twitter account Audience insights (Source: Twitter Analytics).

5.3 YOUTUBE

The project's YouTube account/channel is available at:

<http://youtube.anastacia-h2020.eu>

which redirects to:

https://www.youtube.com/channel/UCfb6LI7eKUyE7_Ztc_utEFQ

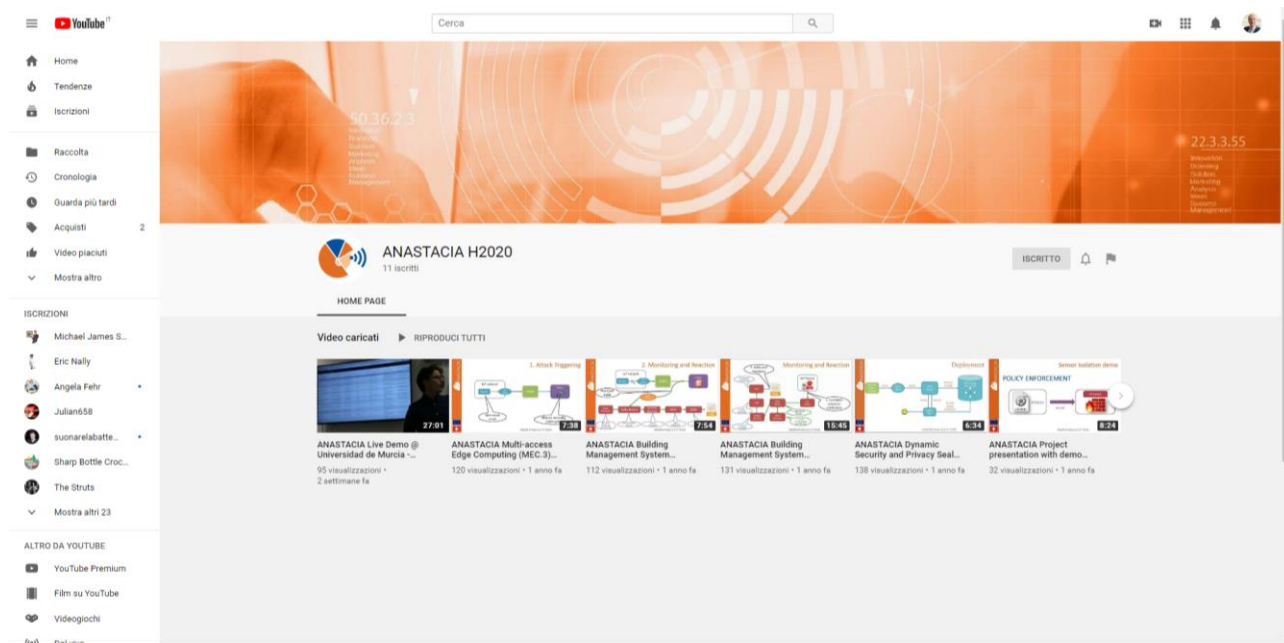


Figure 21: ANASTACIA Project's YouTube account/channel.

So far, the YouTube channel has been exploited in a limited way, since the technical results to be demonstrated/illustrated will be available starting from the beginning of project Y2. Seven short videos are available on the channel so far:

- **ANASTACIA project presentation (2:52)**
A quick introduction to the ANASTACIA project.
<https://www.youtube.com/watch?v=cQOz9SfyAc8>
- **ANASTACIA Project presentation with demo session (8:23)**
An extended video of ANASTACIA first technical results, illustrating the ANASTACIA framework cycle in a first testbed deployment with use of a firewall and IoT-Honeynet.
<https://www.youtube.com/watch?v=wHTt4zmzZWl>
- **ANASTACIA Dynamic Security and Privacy Seal (6:33)**
A short video showcasing the first implementation of the Dynamic Security and Privacy Seal (DSPS) meant to provide DPO and CIO/CISO with real time information on the security and privacy assessment of monitored IoT/CPS.
https://www.youtube.com/watch?v=opb8fWSP_-w

- **ANASTACIA Building Management System (BMS.2) (15:44)**
This video showcases the ANASTACIA platform coping with an insider attack on the fire suppression system (BMS.2).
<https://www.youtube.com/watch?v=RPByyMMfQuI>
- **ANASTACIA Building Management System (BMS.3) (7:53)**
This video showcases the ANASTACIA platform coping with a remote attack on the building energy microgrid (BMS.3).
<https://www.youtube.com/watch?v=iVKECGs2buw>
- **ANASTACIA Multi-access Edge Computing (MEC.3) (7:37)**
This video showcases the ANASTACIA platform coping with a DoS/DDoS attack using smart cameras and IoT devices.
https://www.youtube.com/watch?v=pdHBbKO_CPM
- **ANASTACIA Live Demo @ Universidad de Murcia - PEANA Labs (27:00)**
This video showcases the final ANASTACIA platform demo used for the end-user validation phase
<https://www.youtube.com/watch?v=eEQNAcGiMFE>

5 CONCLUSIONS

This document presents the results of ANASTACIA on the second phase and identifies the different metrics in order to raise awareness with presentations, workshops and conferences. It provides disseminations and standardization activities for ANASTACIA project. The participation on Promotional activities during this period were very promising, as the project emerges to its final phase, we can see the impact of this project on the security and privacy communities on both academics and industrial research field.

6 REFERENCES

- [1] ANASTACIAD7.1: <http://www.anastacia-h2020.eu/deliverables/ANASTACIA-WP7-T7.1-AALTO-D7.1-InitialDisseminationStandardizationAndOutreachStrategyPlan-v13.pdf>
- [2] M. Laurenco & L. Marinos (ed.); ENISA threat landscape for 5G networks; November 2019; <https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks>