ANASTACIA

Advanced Networked Agents for Security and Trust Assessment in CPS/IoT Architectures

D7.1

Initial Dissemination, Standardization, and Outreach Strategy Plan

Definition of dissemination plan, containing guidelines for project partners on identifying and exploiting dissemination opportunities. Report of initial dissemination activities. Analysis of standardization landscape and identification of potential contributions.

Distribution level	PU
Contractual date	30.06.2017 [M6]
Delivery date	30.06.2017 [M6]
WP / Task	WP7 / T7.1
WP Leader	THALES
Authors	T. Taleb (AALTO), I. Farris (AALTO), M. A. Bou Hanana (AALTO), S. Bianchi (SOFT), A. Skarmeta (UMU), D. Belabed (THALES), A. Mady (UTRC), L. Scudiero (AS), D. Rivera (MONT), S. Ziegler (MAND), M. Menon (MAND), R. Trapero (ATOS), B. Sahlin (ERICSSON), M. Sethi (ERICSSON), E. Cambiaso (CNR), E. Kim (DG), G. Ledakis (UBITECH), R. Marin-Perez (ODINS)
EC Project Officer	Carmen Ifrim carmen.ifrim@ec.europa.eu
Project Coordinator	Softeco Sismat SpA 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 4
1.1 Dissemination activities and Aims of the Work 4
1.2 Goals of disseminations and standardization 5
1.3 Roles and Responsibilities 5
1.4 Applicable and reference documents 7
1.5 Revision History 7
1.6 Acronyms and Definitions 8
2 Conditions for dissemination 9
3 ANASTACIA dissemination strategy plan 11
3.1 Dissemination Strategy Description 12
3.1.1 Scientific Publications and participation at international conferences, workshops, and summits 14
3.1.2 Industrial fora 14
3.1.3 Collaboration with national and European projects 15
3.1.4 Online and social network presence 16
4 Initial ANASTACIA dissemination activities 17
4.1 ANASTACIA logo 17
4.2 ANASTACIA flyer 18
4.3 ANASTACIA website 18
4.4 ANASTACIA social network presence 18
4.4.1 ANASTACIA on Twitter 19
4.4.2 ANASTACIA on LinkedIn 20
4.4.3 ANASTACIA on Youtube 20
4.5 Publications 21
5 ANASTACIA standardization strategy plan 22
5.1 Standardization landscape 22
5.1.1 Internet Engineering Task Force (IETF) 22
5.1.2 ETSI ISG NFV SEC 24
5.1.3 ITU 25
5.1.4 3GPP 26
5.1.5 IEEE 28
5.1.6 ISO 28
5.2 Standardization strategy plan 28

5.2.1 Planned contributions to IETF 28
5.2.2 Planned contributions to ETSI NFV SEC 29
5.2.3 Planned contributions to 3GPP 30
5.2.4 Planned contributions to ITU 30
5.2.5 Planned contributions to ISO 30
6 Conclusions 31
7 Annex 1 – ANASTACIA website description 32
8 Annex 2 – ANASTACIA dissemination material 35
9 Annex 3 – Initial dissemination activities list 0
10 Annex 4 – Initial publications list 5
11 Annex 5 – Dissemination work plan schedule 7

PUBLIC SUMMARY

The dissemination plan represents the main reference for communications activities related to the ANASTACIA project, containing guidelines for project partners on identifying and exploiting dissemination opportunities. Indeed, to guarantee a proper diffusion of project's results and maximize the impact, appropriate dissemination strategies should be tailored on the target audience.

Within the ANASTACIA project organization, WP7 is responsible for dissemination and outreach activities while receiving contributions from the other work packages. This document starts describing shortly the WP structure and relevant dissemination outcomes, whereas Section 2 contains the conditions for dissemination.

The dissemination plan is described in Section 3, identifying the target stakeholder groups and the different dissemination phases envisioned during the whole project. A detailed description is provided for each main communication channel, with a detailed workplan schedule of envisioned dissemination activities by ANASTACIA partners.

Section 4 presents the dissemination activities carried out since the deliverable deadline. The overview of relevant standardization activities for the ANASTACIA project, as well as potential contributions are described in Section 5.

1 INTRODUCTION

1.1 DISSEMINATION ACTIVITIES AND AIMS OF THE WORK

The ANASTACIA consortium aims at proactively disseminate project’s technical results to the main stakeholder communities expected to use or benefit from the project’s outcomes. In this vein, a significant number of dissemination activities are being planned, via several communication channels. Furthermore, the ANASTACIA consortium will also address relevant existing standards (to enable interoperability of the envisioned project’s outcomes), as well as providing contributions to the on-going development of new standards.

Within the ANASTACIA project organization, WP7 is responsible for dissemination, standardization and outreach activities. This deliverable mainly refers to the activities of the following project tasks:

Task 7.1 – Outreach and Dissemination

This task will identify the target audiences, the specific actions for their involvement in the project, and the metrics to verify the impact of relevant dissemination activities. To raise awareness around project’s outcomes, presentations will be held at fairs, workshops and conferences. This task will also take care of communications addressing the scientific community through scientific publications, including journal articles, posters and presentation at workshops and conferences. The academic partners of the project will also conduct specific educational activities related to the technologies developed. These activities will include training courses, tutorials and workshops that will be held in the universities and research centers.

Task 7.2 - Standardization

This task will coordinate the project’s standards collaboration and contributions in industry-led working groups. This task will closely monitor on going standardization activities within standardization bodies, identify the technologies or outcomes that could be standardized, and go through the engagement with the relevant standardization bodies.

According to the activities conducted in Tasks 7.1 and 7.2, the Deliverables reported in Table 1 will be released to describe dissemination and standardization plan, and to report the relevant project’s outcomes.

Table 1 – ANASTACIA deliverables plan on dissemination and standardization activities

Deliverable	Deliverable Title	Responsible	Dissemination Level	Delivery date
D7.1	Initial Dissemination, Standardization and Outreach Strategy Plan	AALTO	PU	M6
D7.3	First Period Dissemination, Standardization and Outreach Report	AALTO	PU	M18
D7.4	Second Period Dissemination, Standardization and Outreach Report	AALTO	PU	M36

WP7 deals also with the exploitation plan of the various results envisioned by the project. However, relevant activities are out of scope of this document, and will be described in deliverables D7.2 and D7.5.

The main objectives of this document are:

- to clarify roles and responsibilities for dissemination activities in the ANASTACIA consortium;
- to describe main KPIs to measure the progress of dissemination and standardization;
- to define the conditions for dissemination;

- to describe the dissemination plan and relevant communication channels;
- to identify the main target audience;
- to describe initial dissemination activities;
- to provide a solid background of relevant standardization activities;
- to define initiatives and potential contributions to relevant standards.

1.2 Goals of Disseminations and Standardization

The ANASTACIA project aims at maximizing the outcomes of its activities, by leveraging multiple communication channels. To quantitatively measure the efforts of dissemination activities and to verify the relevant progresses, the consortium has defined specific Key Performance Indicators (KPIs), reported in Table 2, addressing different areas.

Table 2 – KPIs for dissemination and standardization activities

KPIs	Target
Publications	> 30
Dissemination activities	> 80
Standardization	> 5
Deliverables	> 40

1.3 Roles and Responsibilities

In this Section, we briefly describe partners' roles and responsibilities related to dissemination activities.

- THALES is leader of WP7 Exploitation, Standardization and Dissemination and also task leader of T7.4 regarding Innovation Management.
- AALTO is leader of task T7.1 Outreach and Dissemination.
- ERICSSON is leader of task T7.2 Standardization.
- SOFT is leader of task T7.3 coping with individual/joint Exploitation Plan.

The WP leader is also responsible for:

- keeping track and reporting back to EC on the project dissemination activities;
- ensuring proper use of public dissemination materials and respect of partners' IPRs confidentiality;
- ensuring consistency of project image and published content;
- securing optimum use of the project dissemination resources.

Partners are expected to actively contribute by:

- identifying and informing the consortium about dissemination opportunities (e.g. events, publications, etc.);
- contributing content to e.g. leaflet, website, etc.;
- promoting the project results in their own organization press releases and webpages;
- submitting technical papers and presenting the project results at relevant external conferences;
- ensuring liaison with related initiatives and appropriate standardization bodies;

- helping to promote and organize ANASTACIA events (e.g., project workshops and/or displays at external events);
- sharing existing communications resources and skills within their organization (e.g. marketing & PR departments).

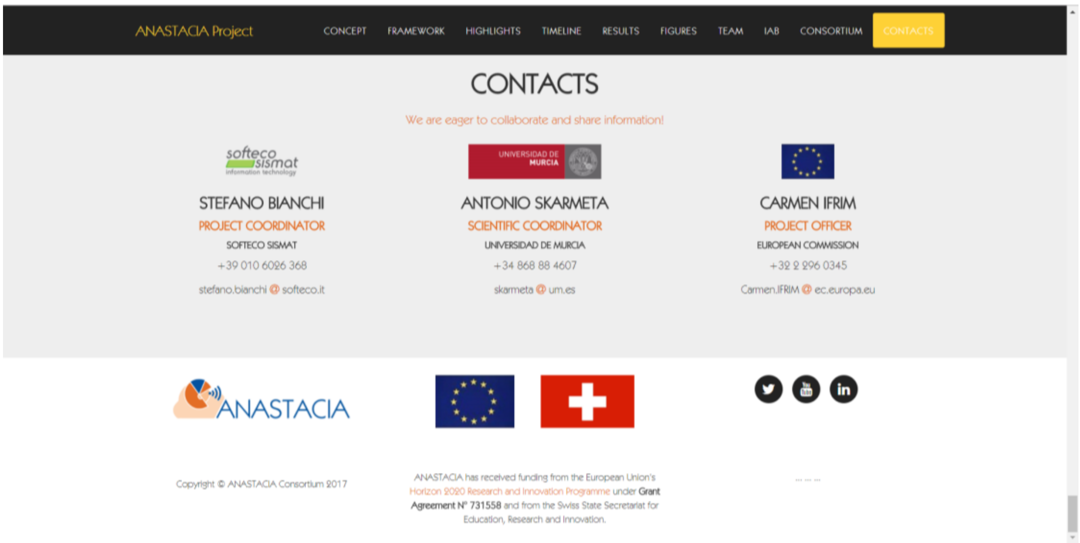
For all dissemination activities promoted and organized by beneficiaries, **Article 29.4 Information on EU funding — Obligation and right to use the EU emblem** of the Grant Agreement applies:

> *Unless the Commission requests or agrees otherwise or unless it is impossible, any dissemination of results (in any form, including electronic) must:*
>
> *(a) display the EU emblem and*
>
> *(b) include the following text:*
>
> *"This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 731558".*
>
> *When displayed together with another logo, the EU emblem must have appropriate prominence. For the purposes of their obligations under this Article, the beneficiaries may use the EU emblem without first obtaining approval from the Commission. This does not however give them the right to exclusive use. Moreover, they may not appropriate the EU emblem or any similar trademark or logo, either by registration or by any other means.*

Since the activities carried out by Swiss partners of the ANASTACIA project are not directly funded by the EC, the above required text is modified accordingly:

> *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.***

and, in addition to the EU emblem, also the Swiss flag is required:



CONTACTS

We are eager to collaborate and share information!

STEFANO BIANCHI
PROJECT COORDINATOR
SOFTECO SISMAT
+39 010 6026 368
stefano.bianchi @ softeco.it

ANTONIO SKARMETA
SCIENTIFIC COORDINATOR
UNIVERSIDAD DE MURCIA
+34 868 88 4607
skarmeta @ um.es

CARMEN IFRIM
PROJECT OFFICER
EUROPEAN COMMISSION
+32 2 296 0345
Carmen.IFRIM @ ec.europa.eu

Copyright © ANASTACIA Consortium 2017

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.

Figure 1. Use of emblems and acknowledgement on the ANASTACIA project's website.

As for publications (and possibly for all other applicable actions) it is required that partners acknowledge the EC's funding as well as the other Consortium beneficiaries, as e.g. shown below:

ACKNOWLEDGMENT

This article has been written in the context of the dissemination activities of the project ANASTACIA (www.anastacia-h2020.eu), which has received funding from the European Union Horizon 2020 Research and Innovation Programme under Grant Agreement N 731558 and from the Swiss State Secretariat for Education, Research and Innovation. This document reflects only the ANASTACIA Consortium's view. The European Commission is not responsible for any use that may be made of the information it contains.

All partners are invited to produce all dissemination material (and possibly all graphical material also for public deliverables) according to the **project identity** as defined in the following sections.

1.4 Applicable and Reference Documents

This document is strictly related to WP7 and references with other project's deliverables are restricted only to D1.1 "*Holistic Security Context Analysis*", which provides a broad overview of background on project's research areas. This document will represent also a basis for the expected following deliverables on dissemination:

- D7.3 "*First Period Dissemination, Standardization and Outreach Report*"
- D7.4 "*Second Period Dissemination, Standardization and Outreach Report*"

1.5 Revision History

Version	Date	Author	Description
1	20/02/2017	T. Taleb (AALTO)	Table of Contents
2	31/03/2017	I. Farris (AALTO)	Description of ANASTACIA dissemination organization and objectives
3	20/04/2017	T. Taleb (AALTO)	Preliminary draft of dissemination plan
4	12/05/2017	M. Sethi (ERICSSON)	Description of relevant IETF standardization activities and potential ANASTACIA initiatives
5	22/05/2017	I. Farris (AALTO)	Description of initial dissemination activities based on partners' feedback
6	23/05/2017	S. Bianchi (SOFTECO)	Definition of roles and responsibilities, conditions for dissemination, collaboration with nationals and European projects, details on online and social dissemination activities
7	24/05/2017	A. Skarmeta (UMU)	Contributions on industrial fora, collaboration with other European projects, and relevant standardization activities within IEEE
8	02/06/2017	B. Sahlin (ERICSSON)	Description of relevant ETSI NFV SEC and 3GPP standardization activities and potential ANASTACIA initiatives
9	08/06/2017	I. Farris (AALTO)	Update of dissemination activities and plan based on partners' feedback

10	14/06/2017	S. Ziegler, M. Menon (MI)	Revision and inclusion of complementary inputs related to projects and standardization activities, dissemination activities and annexes
11	20/06/2017	I. Farris (AALTO)	First consolidated version of deliverable D7.1
12	23/06/2017	D.Belabed (THALES)	Document reviewed and validated.
13	30/06/2017	S.Bianchi (SOFT)	Formal delivery of D7.1 to EC

1.6 Acronyms and Definitions

In the following Table 3, we report the list of acronyms used in this deliverable.

Table 3 – Acronyms

Acronym	Definition
3GPP	3rd Generation Partnership Project
ETSI	European Telecommunications Standards Institute
KPI	Key Performance Indicator
IETF	Internet Engineering Task Force
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
ISO	International Organization for Standardization
ITU	International Telecommunication Union
NFV	Network Function Virtualization
RFC	Request For Comments
SME	Small Medium Enterprise
SDO	Standards Developing Organization

2 CONDITIONS FOR DISSEMINATION

In addition to the obligations required by the EC in the Grant Agreement (see above), also Article 8.4 of the Consortium Agreement signed by all beneficiaries before the start of the project (January 2017) applies:

> ***8.4 Dissemination***
>
> ***8.4.1*** *For the avoidance of doubt, nothing in this Section 8.4 has impact on the confidentiality obligations set out in Section 10.*
>
> ***8.4.2*** *Dissemination of own Results*
>
> ***8.4.2.1*** *During the Project and for a period of one (1) year after the end of the Project, the dissemination of Results by one or several Parties (including but not restricted to publications and presentations) shall be governed by the procedure of Article 29.1 of the Grant Agreement subject to the following provisions. Prior notice of any planned publication shall be given to the other Parties at least fourtyfive (45) calendar days before the publication. Any objection to the planned publication shall be made in accordance with the Grant Agreement in writing to the Coordinator and to the Party or Parties proposing the dissemination within twentyone (21) calendar days after receipt of the notice. If no objection is made within the time limit stated above, the publication is permitted.*
>
> ***8.4.2.2*** *An objection is justified if the intended publication (a) would prevent patenting or other protection of the objecting Party's Results by registration; (b) includes Background, unpublished Results or Confidential Information of the objecting Party. (c) would significantly harm the objecting Party's legitimate interests in relation to the Results or Background. The objection has to include a precise request for necessary modifications.*
>
> ***8.4.2.3*** *If an objection has been raised, the involved Parties shall discuss how to overcome the justified grounds for the objection on a timely basis (for example by amendment to the planned publication consistent with requested modifications and/or by protecting information before publication) and the objecting Party shall not unreasonably continue the opposition if appropriate measures are taken following the discussion.*
>
> ***8.4.2.4*** *The objecting Party can request a publication delay of not more than in case of Sub-Section 8.4.2.2 a) ninety (90) calendar days, and in case of Sub-Section 8.4.2.2 b) thirty (30) calendar days from the time it raises such an objection. After ninety (90) or thirty (30) calendar days respectively the publication is permitted, provided that Confidential Information of the objecting Party has been removed from the Publication as indicated by the objecting Party.*
>
> ***8.4.3 Dissemination of another Party’s unpublished Results or Background***
>
> *A Party shall not include in any dissemination activity another Party's Results or Background and/or Confidential Information without obtaining the owning Party's prior written approval in accordance with Section 8.4.2, unless they are already published.*
>
> ***8.4.4 Cooperation obligations***
>
> *The Parties undertake to cooperate to allow the timely submission, examination, publication and defence of any dissertation or thesis for a degree that includes their Results or Background subject to the confidentiality and publication provisions agreed in this Consortium Agreement.*
>
> ***8.4.5 Use of names, logos or trademarks***

> *Nothing in this Consortium Agreement shall be construed as conferring rights to use in advertising, publicity or otherwise the name of the Parties or any of their logos or trademarks without their prior written approval.*

As for the general approach to follow, the Consortium agrees in trying and adhering to the EC's "Communicating EU research and innovation guidance for project participants" (http://ec.europa.eu/research/participants/data/ref/h2020/other/gm/h2020-guide-comm_en.pdf)

European Commission

The EU Framework Programme for Research and Innovation

HORIZON 2020

Communicating EU research and innovation guidance for project participants

Version 1.0
25 September 2014

Disclaimer:
This document is aimed at assisting applicants and beneficiaries for Horizon 2020 funding. Its purpose is to explain the Horizon 2020 framework programme and the procedures to be followed. Please note that the final version of this document is still under discussion and may still change.

Research and Innovation

and in particular to the included checklists and tools/resources that will be used to control advancements and results, as well as to amplify the outreach of dissemination activities.

3 ANASTACIA DISSEMINATION STRATEGY PLAN

To achieve the dissemination objectives reported in Table 2, the partners will adopt a dissemination plan which aims at establishing strong communication channels with the target audience. The proposed plan will provide guidelines on communicating the project's vision and results, with recognizable, clear and effective messages, as well as stimulate interest in the project technologies and achievements. To this aim, the ANASTACIA consortium has identified several target groups, which are described in Table 4.

Table 4 - Indication about Target groups' definition

Target Areas	Potential Users	Technical level	Main focus
Social	General public Public administration	Understandable by a large public of non-specialists	General project presentation. Economic impact and societal benefits. Personal data protection and software security awareness and measures.
Technical	System developers	Understandable by ICT systems developers and system managers.	Specific project presentation. Focus on software development cycle and end user requirements.
Scientific	Research community International forums	High level on the main scientific and technical innovation addressed by ANASTACIA	Technological presentations. Focus on scientific innovation. Journal articles and conference papers.
Business	Industry SMEs Investors	Business opportunities and potential of technology and societal benefits	Business-oriented project presentation. Scientific and technical innovations. Business opportunities identification. Societal benefits identification.
Legislative	Public administrations Policy-making	Legislative and social implications	Focus on the implementation of the new EU privacy and security legislation and cybersecurity strategy.

3.1 Dissemination Strategy Description

The ANASTACIA dissemination plan consists of different activities and is based on an iterative process to improve the effectiveness of communication activities during the project timespan. The overall view of the dissemination plan is provided in Figure 2.

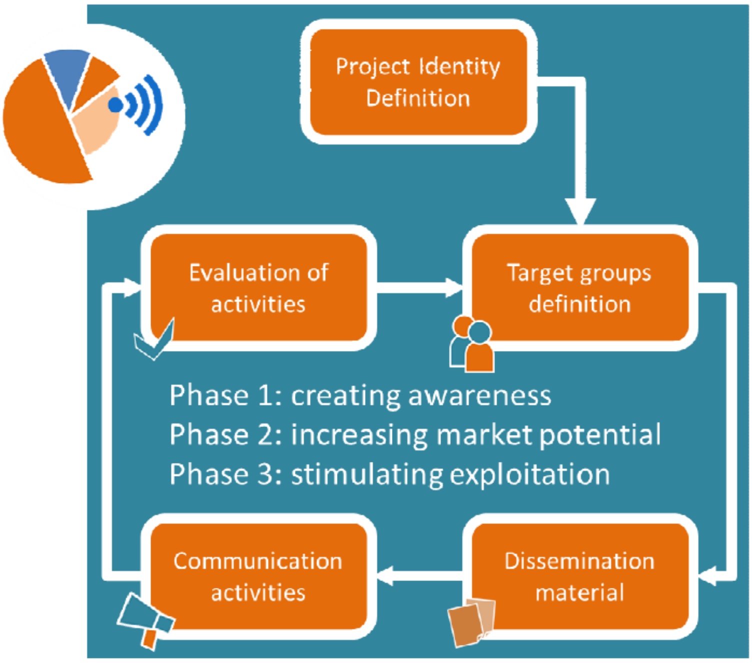

Project Identity Definition
Evaluation of activities
Target groups definition
Phase 1: creating awareness
Phase 2: increasing market potential
Phase 3: stimulating exploitation
Communication activities
Dissemination material

Figure 2 Overall view of the ANASTACIA dissemination plan

The following activities are envisioned in the ANASTACIA dissemination plan:

- **Project identity definition.** The partners intend to provide recognizable, clear and effective messages that communicate the project vision and results, as well as stimulate interest in the project technology and results. This will be pursued by defining a project "logo", including "advertising slogans", common graphical layout and look-and-feel for all dissemination material, a list of keywords and basic concepts on which to base all communication actions.
- **Target groups' definition.** Dissemination activities will be tailored to the target audience, mainly industry (entrepreneurs, software service providers and developers, IoT and smart objects designers and developers), academic and research, policy makers and the general public.
- **Dissemination material.** A broad range of dissemination material will be developed: general presentation material (such as project brochures and leaflets), and PowerPoint presentations; more specific presentations such as technology descriptions, industrial cases description, proceedings of workshops; demonstrators, such as online software, videos, and downloadable software demonstrators.
- **Selection of the appropriate communication activities.** The communication activities will be tailored to the selected target groups, to maximize the impact of project dissemination.
- **Evaluation of the communication activities performed.** Feedback, for each communication activity, will be collected including qualitative and quantitative information (number of participants, cultural background, contact established, comments and suggestions) and will be analysed to derive indications used to improve the dissemination activities. If possible, evaluation tools, such as electronic forms and questionnaires, will be adopted.

ANASTACIA dissemination will follow the three main phases of the project. During the first phase (up to *month M17 – First prototype ready for demonstration*) the main purpose will be to create general awareness about project objectives and expected results, and to establish links with stakeholders and related initiatives and projects. The second phase (up to *month M35 – Second prototype ready for demonstration*) will aim at increasing the market potential of ANASTACIA and gather feedback for driving the final development. It will be results-oriented and will involve the presentation of the tangible/exploitable results achieved. The final phase (starting from month M36) will go beyond the end of the project and will aim at stimulating the exploitation of the project achievements and the participation of other individuals, enterprises, research institutes and other organisations.

The project will exploit different communication channels to maximize its outreach with different audiences. In Table 5, we report a list of envisioned dissemination activities in the ANASTACIA project. This list can be updated and extended in the next phases of the project.

Table 5 – List of dissemination activities

Dissemination Activity Types
Organisation of a Conference
Organisation of a Workshop
Press release
Non-scientific and non-peer-reviewed publication (popularised publication)
Exhibition
Flyer
Training
Social Media
Website
Communication Campaign (e.g. Radio, TV)
Participation to a Conference
Participation to a Workshop
Participation to an Event other than a Conference or a Workshop
Video/Film
Brokerage Event
Pitch Event
Trade Fair
Participation in activities organized jointly with other H2020 projects
Other

Statistics of publications, the number of citations, submitted standard proposals, as well as the number of website visitors and reference links will be continuously collected serving as a performance metric. In **Annex 5 – Dissemination work plan schedule** we only include dissemination activities that can be time wise scheduled. Other activities may take place using channels mentioned in Table 5, when and where opportunities arise. In the following Sections, we provide detailed description of the main communication channels.

3.1.1 Scientific publications and participation at international conferences, workshops, and summits

ANASTACIA intends to disseminate its innovation results in international peer reviewed scientific journals, magazines, book chapters and conferences. The editorship of book and chapters related to the project research items will be also exploited as a means to externalise ANASTACIA work and to document the advances with reference to the state-of-the-art achievements.

Furthermore, the projects results will be also disseminated at conferences, fora and bodies which are attended by potential future users. ANASTACIA will submit and present papers in selected, highly recognized international conferences and workshops. Also, ANASTACIA researchers will provide talks and panels in international conferences.

In the following we provide a non-exhaustive list of conferences and journals of potential interest for disseminating ANASTACIA outcomes. Main target journals are also linked with previous publications of the researchers involved in ANASTACIA.

International conferences:

- IEEE International Conference on Communications (ICC)
- IEEE GLOBECOM
- IEEE Conference on Standards for Communications and Networking (CSCN)
- IEEE Wireless Communications and Networking Conference (WCNC)
- IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIRMC)
- IEEE World Forum on Internet of Things (WF-IoT)
- IEEE endorsed Global IoT Summit (GIOTS)

International journals:

- IEEE Internet of Things journal, IEEE Journal on Selected Areas in Communications, IEEE Communications letters, IEEE Wireless Communication letters, IEEE Transactions on Wireless Communications, IEEE Transactions on Vehicular Technology
- IEEE Communications Magazine, IEEE Network
- Elsevier Ad-hoc Networks, Computer Networks, Future Generation Computer Systems, Journal of Information Security and Applications

3.1.2 Industrial fora

ANASTACIA will benefit from and contribute to relevant international fora, including:

- IERC Cluster: ANASTACIA will present and disseminate its results through the IERC Cluster within the scope of the clustering efforts;
- AIOTI Alliance for the Internet of Things Innovation was launched by the European Commission and various key IoT players in March 2015. Several partners like UMU are involved and it is a fora where discussion on aspects like security and privacy related to IoT will be highly relevant to ANASTACIA, for example to focus on labelling and testing mechanism;
- IPSO alliance: ANASTACIA will work in close cooperation and will benefit from the support of the IPSO Alliance to address the IoT accessibility issues;
- IoT Forum (www.iot-forum.eu): MAND is chairing the IoT Forum, which aims at promoting international dialogue and cooperation for the Internet of Things. ANASTACIA will actively contribute to the activities of the IoT Forum, and more specifically to its yearly conference, the IoT Week;
- International Cyber Security Protection Alliance (ICSPA), the Spanish Industrial Cybersecurity Center (CCI) and the Cloud Security Alliance (CSA) where some of the partners like ATOS and UMU are participating;

- European Technology Platform NESSI (Networked European Software and Services Initiative), where ATOS is a founding member and other partners participate, like UMU and Ericsson;
- ECSO (https://ecs-org.eu) it is the cPPP on Cibersecurity and partners like ATOS, and UMU are involved on different WG related to security for IoT and industrial deployment. It will be a fora also to discuss possible impact of ANASTACIA results with industrial players.

3.1.3 Collaboration with national and European projects

Contacts will be possibly established with other projects funded in the same call[1] in order to promote the exchange of information and leverage EU funding to potentially optimize both methodological and technical results:

- **EU-SEC** - The European Security Certification Framework
  - ID: 731845, Start date: 2017-01-01, End date: 2019-12-31
- **REASSURE** - Robust and Efficient Approaches to Evaluating Side Channel and Fault Attack Resilience
  - ID: 731591, Start date: 2017-01-01, End date: 2019-12-31
- **VESSEDIA** - VERIFICATION ENGINEERING OF SAFETY AND SECURITY CRITICAL DYNAMIC INDUSTRIAL APPLICATIONS
  - ID: 731453, Start date: 2017-01-01, End date: 2019-12-31
- **SAFERtec** - Security Assurance FramEwoRk for neTworked vEhicular teChnology
  - ID: 732319, Start date: 2017-01-01, End date: 2019-12-31
- **TRUESSEC.EU** - TRUst-Enhancing certified Solutions for SEcurity and protection of Citizens' rights in digital Europe
  - ID: 731711, Start date: 2017-01-01, End date: 2018-12-31
- **certMILS** - Compositional security certification for medium- to high-assurance COTS-based systems in environments with emerging threats
  - ID: 731456, Start date: 2017-01-01, End date: 2020-12-31

At the time of reporting, ANASTACIA has already been contacted by TRUESSEC.EU, a CSA that will complement active EU-funded projects in the same areas of research, specially focusing on the associated research and innovation projects from the same cluster (e.g. those approved by the call H2020- DS-2014-2015, as well as the RIAs and IAs from the call DS-01-2016 to which this CSA will provide support). By cooperating with these, we will ensure that our work is aligned, avoid that efforts are duplicated, and foster a strong network of support. On-going projects will be contacted and invited to join the TRUESSEC.EU community, so as to develop synergies and exchange results in our proposed cooperation and support activities.

Additionally, within the context of the cluster of projects related to security, ANASTACIA will identify possible collaborations and synergies with other projects and will pursue to prepare some workshops for possible discussion. It will leverage the participation of its consortium members in other related projects such as SAINT, Privacy Flag, or Create-IoT. Also, ANASTACIA will look forward to identifying conference and meeting organized by the commission in the context of the project to communicate results to the research and industrial community.

All partners, involved in national and regional research projects, are invited in disseminating ANASTACIA results in the related Consortia, in order to identify the possibility to increase the impact of the projects' findings also in other application domains.

[1] CORDIS website http://cordis.europa.eu/search/result_en?q=contenttype=%27project%27%20AND%20/project/relations/associations/relatedCall/call/identifier=%27H2020-DS-LEIT-2016%27

3.1.4 Online and social network presence

The ANASTACIA consortium aims at creating and maintaining a comprehensive public website that will contain all relevant information about the project.

It will provide a centralized access to the various publicly available deliverables, publications and articles related to the project.

The site will be regularly updated over the lifetime of the project with project publications and public materials, such as flyers, posters and public deliverables, organized workshops, available services, etc. Also, ANASTACIA partners will also promote the project's vision and results by leveraging their academic/industrial organization websites.

The project intends to develop its presence on the social networks and media. These channels will be used both for interaction with more professional community (researchers, SMEs, large industry), and for interaction with the general public (while being cautious with personal data protection issue).

4 INITIAL ANASTACIA DISSEMINATION ACTIVITIES

To guarantee a wide spread of project results as well as to ensure a maximum impact, different dissemination activities will be carried out during the whole project lifespan of the ANASTACIA project. In this Section, we provide an overview of the initial communication activities, which have concerned scientific publications, press releases, brochures, online website, media briefings, participation at workshops. A complete list of initial activities performed so far is reported in Annex 3 – Initial dissemination activities list. As the project evolves, the table will be updated accordingly, i.e. including the new performed dissemination activities.

In the next Sections, we focus on the most important dissemination activities being carrying out in the project: logo, website, brochure and flyers, social networking, and scientific publications.

4.1 ANASTACIA LOGO

The project's logo defines the project visual identity, creates an easily recognizable "image" and helps to improve the visibility. It should be used prominently in all dissemination tools and printed materials. Figure 3 shows different versions of the ANASTACIA logo.

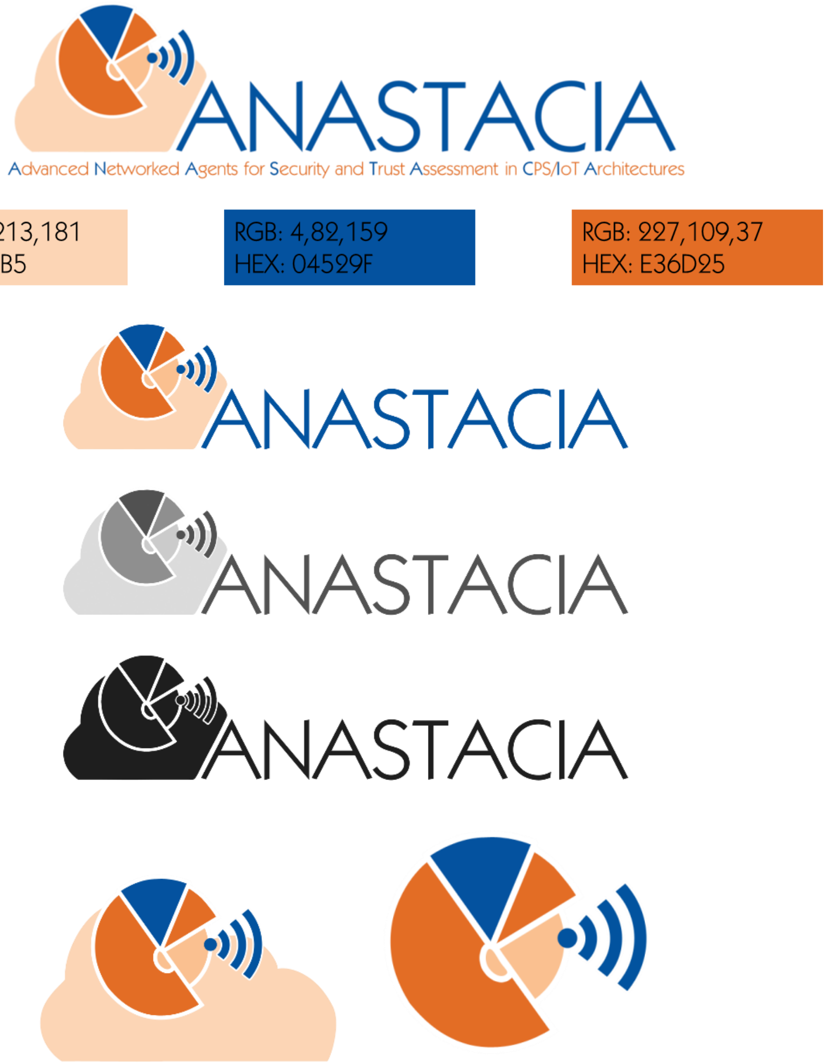


Figure 3 ANASTACIA's logo (different versions) and related graphical items

4.2 ANASTACIA FLYER

The purpose of the ANASTACIA flyer is to give an overview of the main goals, innovations, benefits envisioned by the project. The brochure is composed of two pages, describing the main objective and concepts of the project, and the framework features. For more details, the complete flyer description can be found in Annex 2 – ANASTACIA dissemination material .

4.3 ANASTACIA WEBSITE

The ANASTACIA website[2] follows the EU Project Website - Best Practice Guidelines and it is composed of the following main sections: Concept, Framework, Highlights, Timeline, Results, Figures, Team, IAB, Consortium, Contacts. Figure 4 shows a screenshot of the ANASTACIA website.

Further details about the project structure and contents can be found in Annex 1 – ANASTACIA website description.

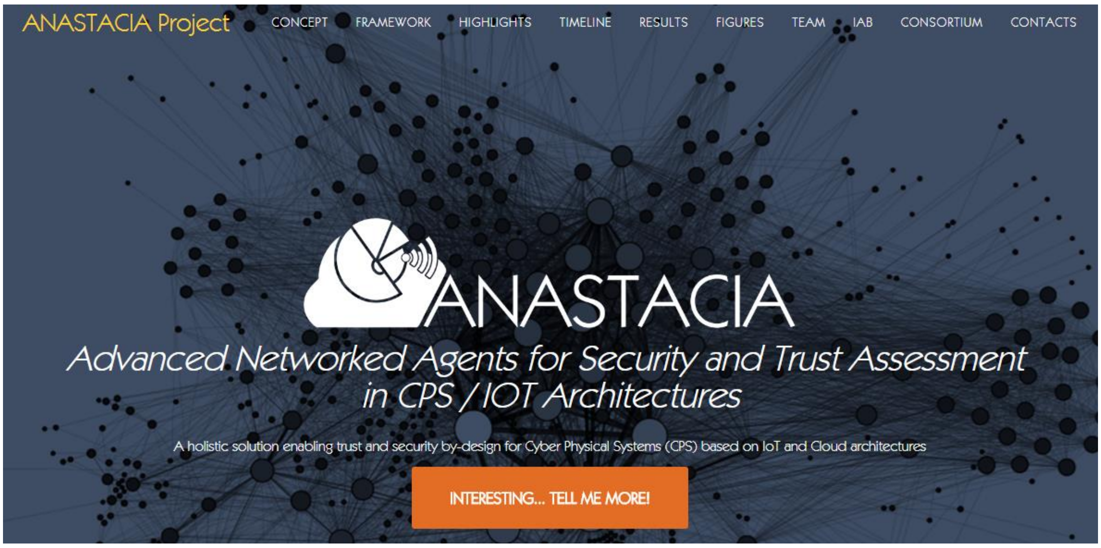

ANASTACIA Project
CONCEPT
FRAMEWORK
HIGHLIGHTS
TIMELINE
RESULTS
FIGURES
TEAM
IAB
CONSORTIUM
CONTACTS
ANASTACIA
Advanced Networked Agents for Security and Trust Assessment in CPS / IOT Architectures
A holistic solution enabling trust and security by-design for Cyber Physical Systems (CPS) based on IoT and Cloud architectures
INTERESTING... TELL ME MORE!

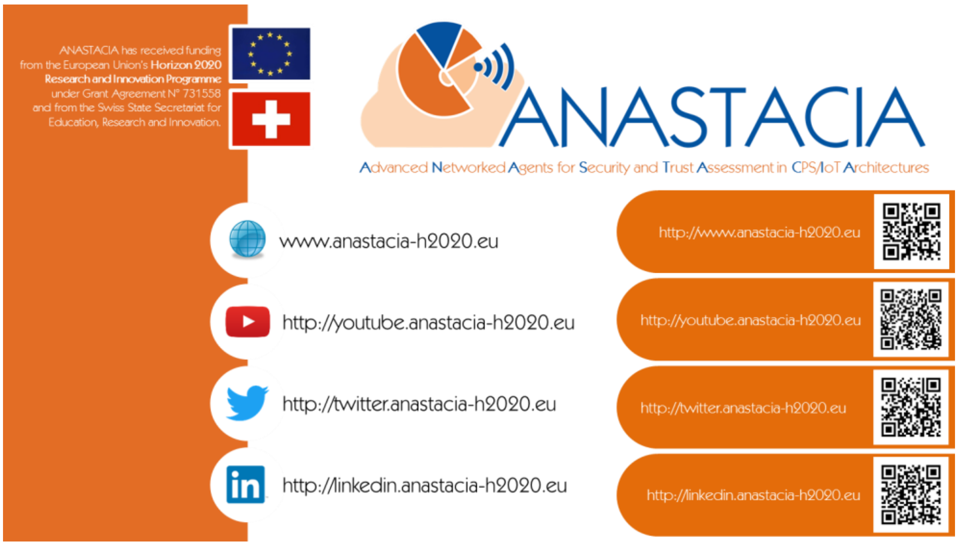
Figure 4 ANASTACIA website

4.4 ANASTACIA SOCIAL NETWORK PRESENCE

ANASTACIA aims at exploiting social media to keep a fast-moving flow of project news towards various online communities, and similarly to the project web portal, to reach the widest audience possible and especially the end users.

Proper subdomains have been established to ease connection to main channels and related dissemination:

[2] http://www.anastacia-h2020.eu/



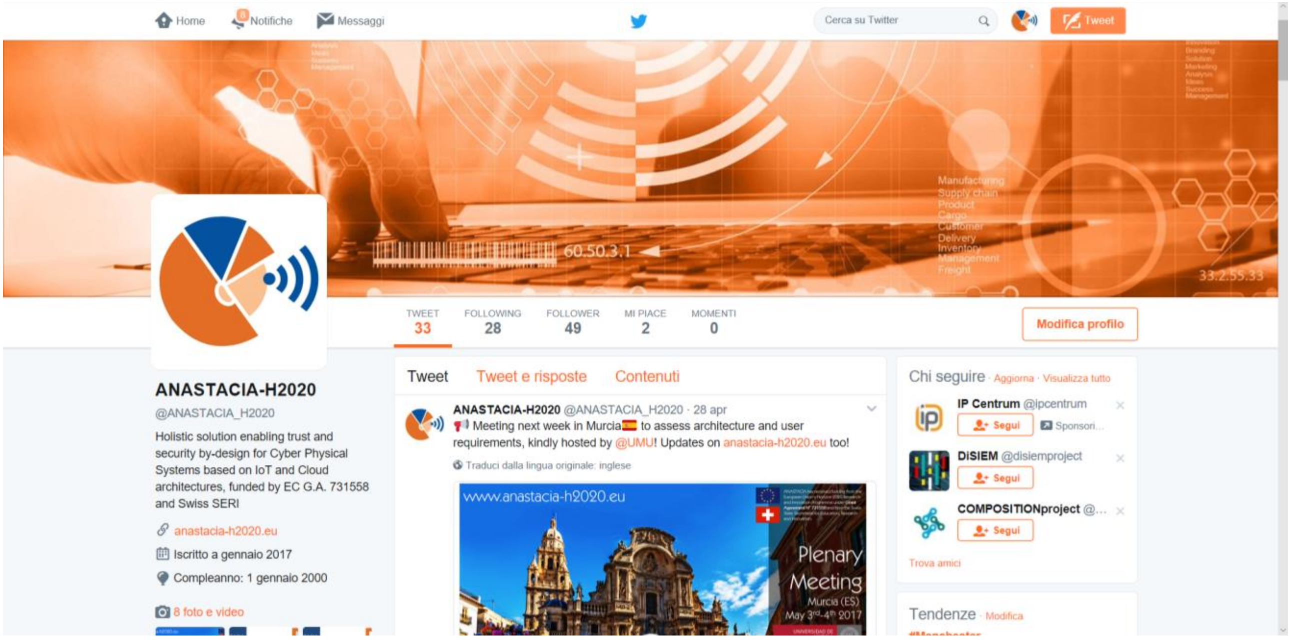
ANASTACIA has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement N° 731558 and from the Swiss State Secretariat for Education, Research and Innovation.

ANASTACIA
Advanced Networked Agents for Security and Trust Assessment in CPS/IoT Architectures
www.anastacia-h2020.eu
http://youtube.anastacia-h2020.eu
http://twitter.anastacia-h2020.eu
http://linkedin.anastacia-h2020.eu
http://www.anastacia-h2020.eu
http://youtube.anastacia-h2020.eu
http://twitter.anastacia-h2020.eu
http://linkedin.anastacia-h2020.eu

Figure 5. Subdomain policies on anastacia-h2020.eu to ease access to dissemination channels.

4.4.1 ANASTACIA on Twitter

A Twitter account has been created to spread information about the project and related topics on this emerging social network. Events and breaking news related to the ANASTACIA project are published on this media. The account of the project is https://twitter.com/ANASTACIA_H2020.



ANASTACIA-H2020
@ANASTACIA_H2020
Holistic solution enabling trust and security by-design for Cyber Physical Systems based on IoT and Cloud architectures, funded by EC G.A. 731558 and Swiss SERI
anastacia-h2020.eu
Iscritto a gennaio 2017
Compleanno: 1 gennaio 2000
8 foto e video

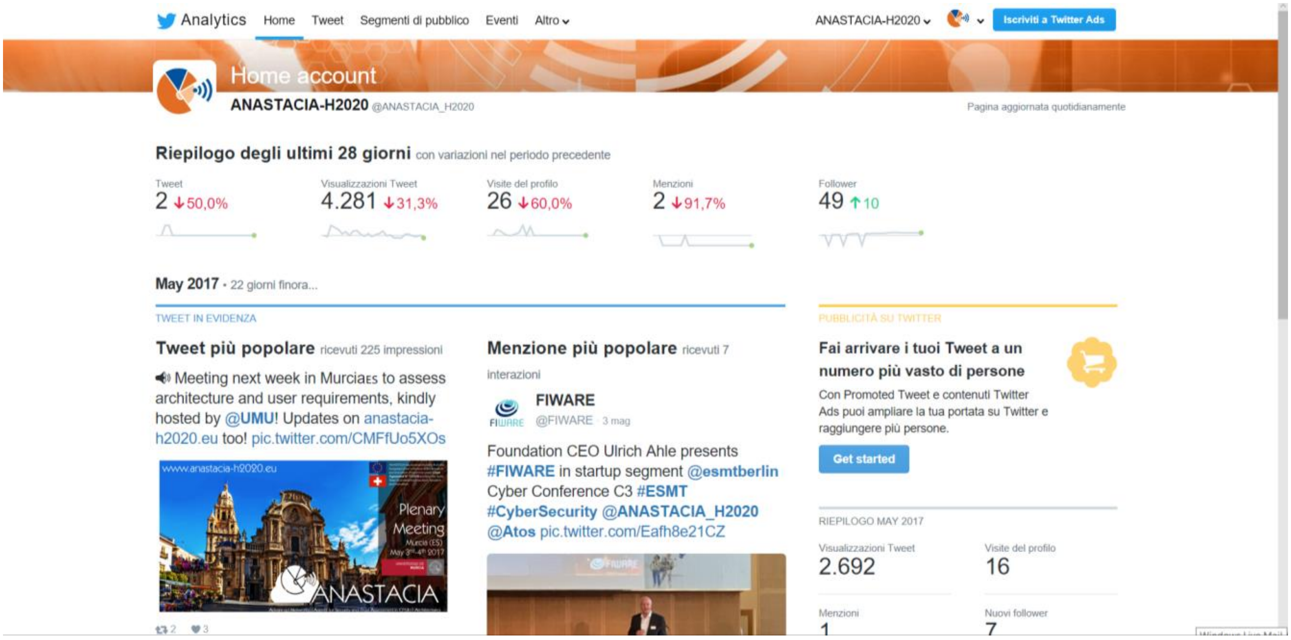
ANASTACIA-H2020 @ANASTACIA_H2020 · 28 apr
Meeting next week in Murcia to assess architecture and user requirements, kindly hosted by @UMU! Updates on anastacia-h2020.eu too!
Traduci dalla lingua originale: inglese

www.anastacia-h2020.eu
Plenary Meeting
Murcia (ES)
May 3rd-4th 2017

IP Centrum @ipcentrum
DiSIEM @disiemproject
COMPOSITIONproject @...

Figure 6. ANASTACIA project's TWITTER account – profile page

Activities on Twitter are monitored by means of the Analytics toolkit:



Home account

ANASTACIA-H2020 @ANASTACIA_H2020

Pagina aggiornata quotidianamente

Riepilogo degli ultimi 28 giorni con variazioni nel periodo precedente

Tweet	Visualizzazioni Tweet	Visite del profilo	Menzioni	Follower
2 ↓50,0%	4.281 ↓31,3%	26 ↓60,0%	2 ↓91,7%	49 ↑10

May 2017 • 22 giorni finora...

TWEET IN EVIDENZA

Tweet più popolare ricevuti 225 impressioni

Meeting next week in Murciaᴇs to assess architecture and user requirements, kindly hosted by @UMU! Updates on anastacia-h2020.eu too! pic.twitter.com/CMFfUo5XOs

Menzione più popolare ricevuti 7 interazioni

FIWARE @FIWARE · 3 mag

Foundation CEO Ulrich Ahle presents #FIWARE in startup segment @esmtberlin Cyber Conference C3 #ESMT #CyberSecurity @ANASTACIA_H2020 @Atos pic.twitter.com/Eafh8e21CZ

PUBBLICITÀ SU TWITTER

Fai arrivare i tuoi Tweet a un numero più vasto di persone

Con Promoted Tweet e contenuti Twitter Ads puoi ampliare la tua portata su Twitter e raggiungere più persone.

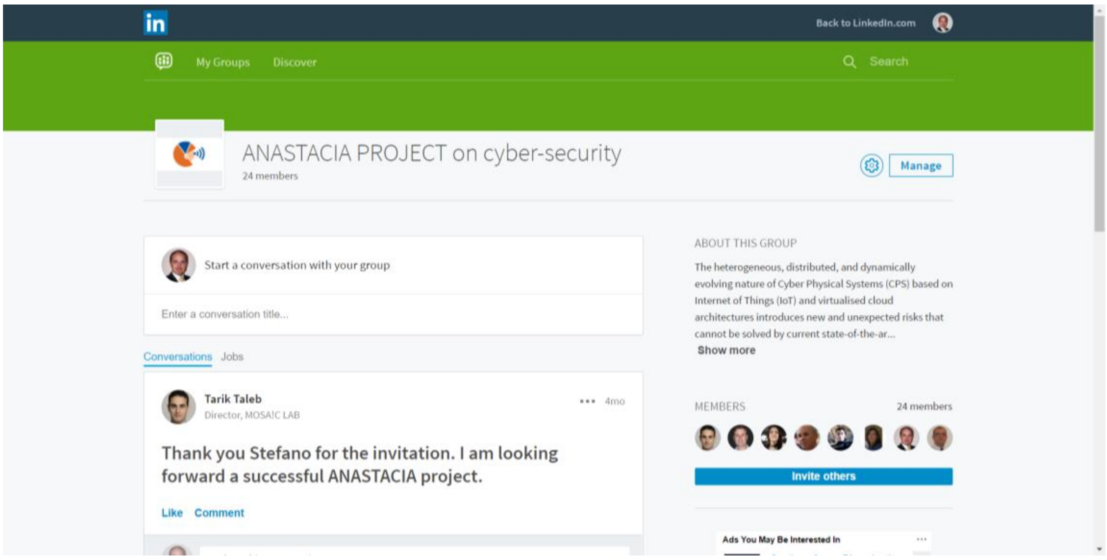
RIEPILOGO MAY 2017

Visualizzazioni Tweet	Visite del profilo
2.692	16
Menzioni	Nuovi follower
1	7

Figure 7. ANASTACIA project's TWITTER account – analytics

4.4.2 ANASTACIA on LinkedIn

To exploit the increasing networking opportunities of LinkedIn, the group "*ANASTACIA PROJECT on cyber-security*" has been established. Objectives of this communications channel is to engage potential professional stakeholders in multiple areas related to the ANASTACIA project and provide updated information about the project's progresses.



ANASTACIA PROJECT on cyber-security

24 members

Start a conversation with your group

Enter a conversation title...

Tarik Taleb
Director, MOSA!C LAB
4mo

Thank you Stefano for the invitation. I am looking forward a successful ANASTACIA project.

ABOUT THIS GROUP

The heterogeneous, distributed, and dynamically evolving nature of Cyber Physical Systems (CPS) based on Internet of Things (IoT) and virtualised cloud architectures introduces new and unexpected risks that cannot be solved by current state-of-the-ar...
Show more

MEMBERS 24 members

Figure 8. ANASTACIA project's LinkedIn group.

4.4.3 ANASTACIA on Youtube

A Youtube channel has been created to spread video contents related to the ANASTACIA project. The channel of the project is available at: https://www.youtube.com/channel/UCfb6Ll7eKUyE7_Ztc_utEFQ.

This channel will soon host non-specialist informative videos, technical and demonstration videos, interviews to ANASTACIA personnel and potential users.

4.5 Publications

The publications carried out in the scope of ANASTACIA project include so far 3 conference papers and 3 journal papers. Details on these publications are reported in Annex 4 – Initial publications list.

5 ANASTACIA STANDARDIZATION STRATEGY PLAN

ANASTACIA will leverage on members of the consortium who are active in Standards Development Organizations (SDOs), to promote and standardize technology, in line with the "2016 Rolling Plan on ICT Standardization" established by the Digital Single Market initiative launched by the EC6. The project is planning for a clear and ambitious standardisation plan, and includes in the consortium partners with specialised expertise in this field. Thanks to the heterogeneity of the consortium and to the presence of partners well-known at international level, ANASTACIA will benefit from and contribute to relevant international forums and standardisation bodies and will interact through complementary channels.

5.1 STANDARDIZATION LANDSCAPE

In this Section, we provide a brief description of the main standardization activities related to research domains of the ANASTACIA project.

5.1.1 Internet Engineering Task Force (IETF)

Background:

The Internet Engineering Task Force (IETF) is the primary standards body for the core Internet standards that comprise the Internet protocol suite. Essentially, the IETF develops and maintains standards for technologies used to provide Internet service or to provide services over the Internet. IETF standards are published as Request for Comment (RFC) documents that are free and openly accessible. Example of standards at the different layers of the Internet protocol suite include- Network layer: IPv4 (RFC 791), IPv6 (RFC2460); Transport layer: TCP (RFC 793), UDP (RFC 768); Session layer: TLS (RFC 5246), DTLS (RFC 4347); Application layer: HTTP (RFC 2616), HTTP/2.0 (RFC 7540). Anastacia partners such as Ericsson and University of Murcia actively follow and contribute to the ongoing standards work at the IETF.

Ongoing work:

In this section, we highlight the ongoing work at the IETF that is related to the targets and objectives of Anastacia. In recent years, the IETF has worked on a new version of the HTTP protocol. The new version is called HTTP/2, and it provides performance improvements by means of a binary representation of the commands. Other improvements include header field compression and support of multiple exchanges on the same connection. HTTP/2 was published as IETF RFC 7540 (May 2015). On the security side, the HTTP/2 specification states that TLS version 1.2 or a higher version must be used for HTTP/2 over TLS. The new phase of work also focuses on opportunistic encryption for HTTP. This proposal makes it possible to run HTTP over TLS and encrypt the communication, without requiring strong server authentication (17 March 2016).

The IETF is also updating the TLS protocol itself (the latest draft is for TLS is v 1.3, 21 March 2016). One of the main goals of the new version is to encrypt as much as possible of the handshake messages to reduce the amount of data available to attackers. Another major goal is to reduce the handshake to one round-trip. TLS 1.3 will also update the profiles to address known weaknesses in CBC block cipher modes and RC4.

In parallel to the update of TLS, the QUIC working group is developing a specification for a new encrypted, UDP-based, transport protocol, that relies on the implementation and deployment experience of SPDY (developed in 2009). There have been recent suggestions that HTTP/2 and QUIC might provide efficiency gains in certain IoT deployments. This proposal is documented in H2oT: HTTP/2 for the Internet of Things (*https://tools.ietf.org/html/draft-montenegro-httpbis-h2ot-00*).

Internet of Things (IoT) area in general has seen a considerable amount of contribution from various working groups at the IETF. The IETF has developed a new lighter weight version of the HTTP protocol for use in constrained devices. This protocol is called as the Constrained Application Protocol (CoAP) and it is specified in RFC 7252. CoAP is based on the same Representational State Transfer (REST) architecture and provides a generic request/response interaction model similar to the Hypertext Transfer Protocol (HTTP). However, unlike HTTP, messages in CoAP are exchanged asynchronously over the unreliable datagram-oriented transport such as UDP with optional reliability.

Datagram Transport Layer Security (DTLS) provides communications privacy for datagram protocols and is based on the standard Transport Layer Security (TLS) protocol that is used widely on the Internet. The CoAP base specification provides a description of how DTLS can be used for securing CoAP. It proposes three different modes for using DTLS, namely: Preshared key mode (where nodes have pre-provisioned keys for initiating a DTLS session with another node), Raw Public Key mode (where nodes have an asymmetric-key pair(s) but no certificates to verify the ownership) and Certificate mode (where public keys are signed in certificates by a certification authority). In addition, IETF has also specified an implementation profile for TLS version 1.2 and DTLS version 1.2 that offers communications security for resource-constrained nodes that are part of IoT.

The CoAP specification also provides an alternative approach for securing communication with Internet Protocol Security (IPSec). It argues that many constrained devices already have support for link layer encryption in hardware which can be used to make IPSec a viable option in such networks. There is work ongoing in this area with the standardization of header compression for IPSec.

There are also other communication security issues associated with resource-constrained IoT devices that sleep during their lifecycle to save energy. Such IoT devices cannot afford to stay online for large amounts of time to be polled for data or support computationally intensive security protocols. To ensure data integrity, authenticity and confidentiality in such devices, the cryptographic protection measures need to be applied directly to the application-layer message objects. This method of communication security is also referred to as “object security”. The IETF is also currently working on a specification to provide object security on top of the CoAP protocol. This is referred to as Object Security for CoAP (OSCOAP).

Access control mechanisms are a necessary and crucial design element to any application's security. Therefore, it is not surprising that IETF is also investigating how web-based access control and authorization solutions can be applied to resource-constrained devices that are part of the IoT. It is currently defining an authorization and access control framework for resource-constrained nodes based on the OAuth 2.0 framework, which is currently the de-facto standard for authorization on the web.

In many IoT deployments, the devices are connected to the Internet via a gateway that is directly reachable one hop away. For example, an IEEE 802.11 Access Point (AP) typically connects the client devices to the Internet over just one wireless hop. However, some deployments of Internet-connected devices (such as smart meters) may require routing between the devices themselves for reducing the cost of deployment and increasing the reliability of the network. The IETF has therefore defined the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) RFC6550. RPL provides support for multipoint-to-point traffic from resource-constrained smart objects towards a more resourceful central control point, as well as point-to-multipoint traffic in the reverse direction. It also supports point-to-point traffic between the resource-constrained devices. A set of routing metrics and constraints for path calculation in RPL are also specified.

JavaScript Object Notation (JSON) is a lightweight text representation format for structured data RFC7158. It is often used for transmitting serialized structured data over the network. IETF has defined specifications for encoding public keys, signed content, and claims to be transferred between two parties as JSON objects. They are referred to as JSON Web Keys (JWK), JSON Web Signatures (JWS) and JSON Web Token (JWT).

An alternative to JSON, Concise Binary Object Representation (CBOR) RFC7049 is a concise binary data format that is used for serialization of structured data. It is designed for extremely resource-constrained nodes and therefore it aims to provide a fairly small message size with minimal implementation code, and extensibility without the need for version negotiation. There is ongoing work to specify CBOR Object Signing and Encryption (COSE), which would provide services similar to JWS and JWT.

While CoAP defines a standard communication protocol, a format for representing sensor measurements and parameters over CoAP is required. The Sensor Markup Language (SenML) is a specification that is currently being written to define media types for simple sensor measurements and parameters. It has a minimalistic design so that constrained devices with limited computational capabilities can easily encode their measurements and, at the same time, servers can efficiently collect large numbers of measurements. SenML is used to communicate the dynamic data originating from the constrained devices. Sensor Markup representations can be defined with JavaScript Object Notation (JSON), eXtensible Markup Language (XML) or Efficient XML Interchange (EXI).

The IoT@Work project defines bootstrapping in the context of the Internet of Things (IoT) as the process by which the state of a device, a subsystem, a network, or an application changes from not operational to operational. Secure bootstrapping of IoT devices is another research area that currently remains open and there are several proposals being developed at the IETF to address is problem. For example, in one of the proposals, a method for configuring a resource-constrained device with an initial key when it joins an operational network is suggested. This proposal assumes that the resource-constrained devices use the Transmission Control Protocol (TCP) over IP and rely on CoAP application layer messaging. The solution requires the embedding of an initial identifier and key information to the smart object during installation before it can be reconfigured with another key while joining the network.

5.1.2 ETSI ISG NFV SEC

ETSI Industry Specification Group (ISG) for NFV is the home for developing requirements and specifications for NFV. The main goal to form ETSI ISG NFV was to produce the technical specifications to enable the development of an open, interoperable, commercial ecosystem based on virtualized network functions. The ETSI ISG NFV maintains core NFV documentation, including an architectural framework and associated technical requirements, as well as liaison relationships with other specialist SDOs and industry alliances contributing technology or applying NFV concepts within their specializations.

From Anastacia project perspective, the most interesting working group is the ETSI NFV SEC working group. This SEC WG is responsible for security considerations throughout the NFV platform. In order to achieve such a goal, NFV SEC WG is working with many different topics starting from defining a problem statement, defining the threat landscape, identifying potential areas for security vulnerabilities, hardening requirements, NFV specific use of security functionalities, etc. to name a few. After analyzing the key security issues submitted by the participants in the first ETSI NFV ISG meeting, NFV SEC WG has compiled the areas of concern into 10 domains. These are listed in the following:

1. Topology Validation & Enforcement
2. Availability of Management Support Infrastructure
3. Secured Boot
4. Secure crash
5. Performance isolation
6. User/Tenant Authentication, Authorization and Accounting
7. Authenticated Time Service
8. Private Keys within Cloned Images
9. Back-Doors via Virtualised Test & Monitoring Functions
10. Multi-Administrator Isolation

Based on the above security domains and beyond, the SEC WG has published several reports. These are publicly available for use as reference. These are:

- ETSI GS NFV-SEC 001 V1.1.1 (2014-10): Problem Statement
- ETSI GS NFV-SEC 002 V1.1.1 (2015-08): Cataloguing security features in management software
- ETSI GS NFV-SEC 003 V1.2.1 (2016-08): Security and Trust Guidance

- ETSI GS NFV-SEC 004 V1.1.1 (2015-09): Privacy and Regulation; Report on Lawful Interception Implications
- ETSI GS NFV-SEC 006 V1.1.1 (2016-04): Report on Security Aspects and Regulatory Concerns
- ETSI GS NFV-SEC 009 V1.2.1 (2017-01): Report on use cases and technical approaches for multi-layer host administration
- ETSI GS NFV-SEC 010 V1.1.1 (2016-04): Report on Retained Data problem statement and requirements
- ETSI GS NFV-SEC 012 V3.1.1 (2017-01): Network Functions Virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components
- ETSI GS NFV-SEC 013 V3.1.1 (2017-02): Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring specification

5.1.3 ITU

Background:

One of the oldest United Nations entities, the International Telecommunication Union (ITU) is the United Nations specialized agency for information and communication technologies (ICTs). In addition to being a United Nations agency, ITU also serves as one of the three international standards developing organizations (as designated by the World Trade Organization). Since its inception, ITU operations are premised upon public private partnership. It currently has a membership of 193 countries and 800 private-sector entities and academic institutions.

The ITU Telecommunication Standardization Sector (ITU-T) functions as the standards wing of the ITU. The standardization work within the ITU-T is conducted through designated Study Groups, which are responsible for developing ITU-T Recommendations (international standards) on specific fields of international telecommunications and ICTs. As of May 2017, ITU-T has 11 active Study Groups.

Ongoing work:

In this section, we highlight the ongoing work at the ITU that is related to the targets and objectives of ANASTACIA[3] . The most relevant Study Group is ITU-T Study Group 20 on Internet of Things and Smart Cities and Communities. Created in June 2015, ITU-T Study Group 20 is responsible for developing international standards which will enable the coordinated development of IoT-related technologies, including machine-to-machine communications and ubiquitous sensor networks. In line with its mandate, the ITU-T Study Group 20 also develops standards that leverage IoT technologies to address urban challenges. ITU-T Study Group 20 also explores the standardization of end-to-end architectures for IoT and mechanisms for the interoperability of IoT applications and datasets employed by various vertically oriented industry sectors.

Within the ITU-T Study Group 20, Question 6/20 on “Security, privacy, trust and identification” specifically deals with the security and privacy issues associated with large numbers of interconnected devices within the IoT ecosystem along with linked scalability issues. Some of the study items under this Question include:

- What are the possible threats against the compromise of authenticity, confidentiality, integrity, non-repudiation, and availability of IoT and smart cities and communities (SC&C) devices, systems, applications, protocols, platforms, and services?
- What is needed to mitigate and counteract the risks and threats identified in IoT and SC&C systems, and services?

[3] Information on ITU’s work in this area has been sourced from https://www.itu.int/en/ITU-T/studygroups/2017-2020/Pages/default.aspx

- What are the identification systems capable of fulfilling the requirements of IoT and SC&C including security, privacy and trust?
- What are the requirements and mechanisms for protecting, and preventing disclosure of things' information?

Other security and privacy issues related to the data streams generated within the IoT framework are being explored under the Focus Group on Data Processing and Management to support IoT and Smart Cities & Communities (FG-DPM). This provides an open platform and alternative working environment for development of guidelines, policies and specifications linked to data processing and management and establishment of IoT ecosystem solutions for cities. The Focus Group itself cannot approve international standards. ITU-T Study Group 20 serves as the parent group of the FG-DPM.

ITU-T Study Group 13 on Future networks, with focus on IMT-2020, cloud computing and trusted network infrastructure could also be considered as relevant for ANASTACIA. ITU-T Study Group 13 is responsible for the standardization work on next-generation networks, including the evolution trends of NGNs, while focusing on future networks and network aspects of mobile telecommunications. This Study Group also develops international standards on the requirements and functional architectures of the cloud computing ecosystem, covering inter- and intra-cloud computing. Within the ITU-T Study Group 13, Question 19/13 on "End-to-end cloud computing management and security" deals with cloud service and infrastructure management and the management of composite cloud services and components that use a variety of telecom and IT infrastructure resources.

5.1.4 3GPP

Background:

The 3rd Generation Partnership Project (3GPP) is the primary standards body for the mobile network standards that comprise the 3GPP system. Essentially, 3GPP develops and maintains standards for technologies used to provide connectivity to mobile networks and their services as well as to provide connectivity over mobile networks to various packet data networks (PDNs) such as the Internet and the services provided by those PDNs. 3GPP is a global standards development organization that produces standards specifications, which are then endorsed by regional standards organizations, such as European Telecommunication Standards Institute (ETSI). 3GPP standards are published as Technical Specifications (TS) documents that are publicly accessible. 3GPP has different series of Technical Specifications for different parts of the 3GPP system. E.g. 23-series is for system architecture specifications such as 3G/UMTS system (3GPP TS 23.060), 4G/EPS system (3GPP TS 23.401 and TS 23.402), and the ongoing work for 5G system (3GPP TS 23.501 and 23.502). 36-series is for 4G LTE radio networks, and 33-series is for security specifications such as 3G/UMTS security (3GPP TS 33.102), 4G/EPS security (3GPP TS 33.401 and TS 33.402), and 5G security (3GPP TS 33.501). In addition to access level functionality, 3GPP has also specified standards e.g. for service level communication such as IP Multimedia System (IMS) and Mission Critical Communication. Anastacia partners such as Ericsson actively follow and contribute to the ongoing standards work at the 3GPP.

Ongoing work:

In this section, we highlight the ongoing and recent work at the 3GPP that is related to the targets and objectives of Anastacia.

Due to its wide deployment in some regions, GSM and GPRS networks are a promising and already used technology for many IoT use cases. For this purpose 3GPP has developed a new radio interface for GSM called Enhanced Coverage GSM (EC-GSM). At the same time, the security of EC-GSM was enhanced considerably by adding integrity protection to control plane signalling and adding also possibility to use integrity protection also for the user plane. GSM networks are already able to use 3G authentication and key agreement (3G AKA) with mutual authentication instead of 2G AKA, and 3G AKA was mandated for EC-GSM.

3GPP has also worked on enhanced Machine Type Communication (eMTC), which is an optimization of LTE technology to support IoT use cases by simplifying functionality and cutting down device complexity and cost. Security-wise eMTC is equivalent to 4G networks.

To further optimize the 3GPP networks for IoT, 3GPP developed a new radio technology called Narrow-band IoT (NB-IoT). The new radio technology is based on LTE, but is considerably simpler with less bandwidth, which has also allowed to strip-down device complexity and cost and allow extended battery lifetime. To support NB-IoT, two specific optimizations were designed. The first is so called Control Plane Cellular IoT EPS optimization, which allows to send a small amount of user data, e.g. an IP packet, in the Non- Access Stratum (NAS) signalling between the UE and the core network. Therefore, the functionality is also known as Data over NAS (DoNAS). The intention of DoNAS is to save signalling as the user data can be sent already in the early NAS signalling message and there is no need to set-up dedicated radio bearers. Security-wise, only the user data part in the NAS message is encrypted since the rest of the message might be only integrity protected. In DoNAS, security is not set-up at all in the radio network layer, i.e. in so called Access-Stratum (AS) layer. The second optimization is called User Plane Cellular IoT EPS optimization, which is based on caching the AS layer UE context, including security context, in the base stations. This allows the radio layer connection, and also the security of that connection, to be quickly suspended and resumed, thus saving signalling.

In 3GPP networks, the user plane security from the UE is terminated in the serving network, and there can be another secure connection from the serving network to the home network. In order to enable efficient secure connection for IoT from the UE all the way to the home network, or beyond the home network to an application server, a mechanism called Battery Efficient Security for very low Throughput Machine Type Communication Devices (BEST) is being finalised in 3GPP. The purpose of BEST is to provide keys for the UE and the home network based on 3G AKA. The work also includes a design of a new security protocol intended for low-throughput IoT devices, but the keys can also be used with other security protocols, such as DTLS.

Currently the most activities in 3GPP are focusing on the ongoing 5G work, and especially on the first phase of 5G. While 4G networks were originally designed for mobile broadband (MBB) and were then later enhanced to better support e.g. IoT and mission critical use cases, the design of the 5G network tries to take requirements from different use cases into account from the beginning. The work includes among other things a new network architecture, new radio interface, separation of mobility and session management, support for network slicing and unified approach to different access network types, etc.

New security mechanisms are being defined for 5G. Some of the main security enhancements harmonised authentication for all access types, including support of the EAP framework, which allows to use also other authentication methods than 3GPP defined AKA mechanism. Another one is enhanced user privacy.

5.1.5 IEEE

UMU and MAND are vice-chairing the IEEE Communication Society Internet of Things Technical Committee, facilitating the development of standards, white papers, and other initiatives. In that sense, IEEE will serve as a fora where we can use the IEEE IoT Initiative http://iot.ieee.org/ channels like the newsletter and the WF-IoT conference for communication and dissemination activities.

5.1.6 ISO

Background:

The International Organization for Standardization (ISO) is one of the three international standards developing organizations along with IEC and ITU. Its members include the national standards bodies of 163 countries. The ISO develops voluntary, consensus-based standards that are often adopted by member countries. The standardization work with ISO is conducted through technical committees that are responsible for specific areas. These technical committees are composed of experts nominated by members.

Ongoing work:

ISO already has numerous standards, which can supplement the work conducted in ANASTACIA. The standards relevant for ANASTACIA include:

- ISO/IEC 27000 family - Information security management systems: These standards help manage the security of assets including financial information, intellectual property, employee details or information entrusted by third parties.
- ISO/IEC CD 30141 “Internet of Things Reference Architecture (IoT RA)” (under development).

The technical committee relevant for ANASTACIA is the ISO/IEC JTC 1 on “Information technology”. Within this technical committee, the work of Sub-committee ISO/IEC JTC 1/SC 38 on “Cloud Computing and Distributed Platforms” and Working Group ISO/IEC JTC 1/WG 10 on “Internet of Things” would be beneficial for ANASTACIA[4].

5.2 STANDARDIZATION STRATEGY PLAN

Based on the analysis of on-going standardization activities, in this Section we illustrate potential contributions related to ANASTACIA research and innovation areas.

5.2.1 Planned contributions to IETF

We plan to make IETF contributions based on the components of the ANASTACIA architecture and results from the rest of the work done during the project. Concretely we plan to work on the following:

1. An overview document that first discusses the various stages in the lifecycle of an IoT device. It will then look at the building blocks available for securing the different layers of the Internet protocol suite. It will also document the various security threats to an IoT device and the challenges that one might face in order

[4] More information on the ISO technical committee ISO/IEC JTC can be found here: https://www.iso.org/committee/45020.html

to protect against these threats. Lastly, the contribution would also discuss the concept of security profiles necessary for a successful roll-out of secure IoT applications.

2. A contribution on secure neighbour discovery for resource-constrained devices. This contribution would look at defining an extension to existing neighbour discovery mechanism specified in RFC 6775 to provide additional security. Nodes supporting this extension would rely on cryptographic addresses instead of EUI-64 addresses that are specified in RFC 6775.

3. A draft contribution for secure bootstrapping of IoT devices. This contribution would extend the Extensible Authentication Protocol (EAP) framework and define a method for out-of-band (OOB) authentication and key derivation. This EAP method is intended for bootstrapping all kinds of Internet-of-Things (IoT) devices that have a minimal user interface and no pre-configured authentication credentials.

4. An informational document describing a method for enabling and configuring network access for IoT devices that are first authenticated at a server. This method is needed because many of these devices have only limited user interfaces that can be used for configuring the security credentials. The device configuration is also made more challenging by the fact that the devices may exist in large numbers. Therefore, this contribution would allow users to easily enable network access for their IoT devices using existing protocols and technologies.

5. An informational draft documenting implementation experiences of public-key cryptography on small devices. It is often incorrectly assumed that resource-constrained IoT devices cannot perform cryptographic operations needed for strong security. This draft would document our experiences of implementing RSA and Elliptic Curve Cryptography on small micro-controllers and present them to the Light Weight Implementation Guidance (LWIG) working group of the IETF.

6. As more IoT devices are connected to the network, strong network isolation becomes a critical requirement. To aid this network isolation, we would work on a contribution that describes how existing RADIUS attributes can be used for fine-grained access control in enterprise environments.

7. We will actively follow the ongoing security standards work at Authentication and Authorization for Constrained Environments (ACE), IPv6 over the TSCH mode of IEEE 802.15.4e (6ticsh), IPv6 over Networks of Resource-constrained Nodes (6lo), Constrained RESTful Environments (CoRE), Firmware Updating Description (FUD), A Protocol for Dynamic Trusted Execution Environment Enablement (TEEP), Thing-to-Thing (T2TRG) working and research groups of the IETF/IRTF. The work would serve as input for the ANASTACIA architecture and project goals.

However, it should be noted that the ANASTACIA architecture and other work items are still being developed. Therefore, certain envisioned contributions may have to be changed during the course of the project. Additionally, the standardization process is quite dynamic and the progress of our contributions is also dependant on the market and community dynamics.

5.2.2 Planned contributions to ETSI NFV SEC

There are several work items currently planned for delivery within one year. Most of these work items are normative specifications while some being informative. These work item names are listed in the following:

- DGS/NFV-SEC005 (GS): Certificate management report
- DGR/NFV-SEC007 (GR): NFV Attestation report
- DGS/NFV-SEC011 (GS): LI Architecture report
- DGS/NFV-SEC014 (GS): MANO Security Spec
- DGS/NFV-SEC015 (GS): MANO Security spec
- DGR/NFV-SEC016 (GR): Location, locstamp and timestamp

While the above list only shows a planned landscape for upcoming deliverables by this group, it does not stop here. There are many other security issues remains to be investigated such as security impacts of network slicing from NFV perspective, implications of multiple domains on NFV security, implications of geography on management and monitoring, etc. The potential areas for contribution are quite large at this moment. Since, most of the technical specifications are currently under development, it is high time for a contribution and to have an impact towards further development of this technology in the right direction.

5.2.3 Planned contributions to 3GPP

We plan to make 3GPP contributions based on the components of the ANASTACIA architecture and results from the rest of the work done during the project. The work for 3GPP includes contributions to develop the 5G system, including specific enhancements taking into account IoT specific requirements.

5.2.4 Planned contributions to ITU

Accounting for WP5 ANASTACIA actitivies, it is foreseen that we could prepare contributions based on D5.1 "Dynamic Security and Privacy Seal Model Analysis Report" and D5.2 "Dynamic Security and Privacy Seal Monitoring Service Demonstrator" for submission to ITU-T Study Group 20 next year.

Another Contribution based on D2.3 "Privacy Risk Modelling and Contingency Initial Report" could be submitted to ITU-T Study Group 13.

Further, based on the progress of ANASTACIA deliverables in the realm of data security and privacy, contributions could also be made to the FG-DPM. Device Gateway and Mandat International have already been invited to participate in the work of this Focus Group, which will hold its first meeting in July 2017.

5.2.5 Planned contributions to ISO

We could consider the possibility of sharing relevant results of ANASTACIA related to the dynamic and privacy seal with ISO, especially with the technical committee ISO/IEC JTC.

6 CONCLUSIONS

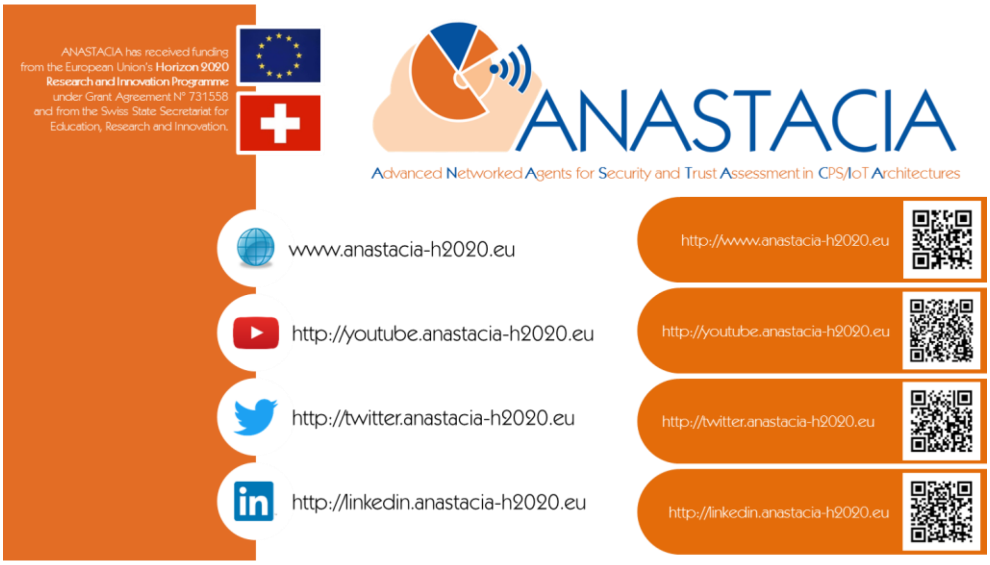
This deliverable includes the dissemination plan of the ANASTACIA project, providing the main guidelines for the widespread diffusion of project vision and results. To this aim, the main target groups are identified and a broad range of potential dissemination activities have been defined to increase the awareness and stimulate interest in the project technologies and achievements. A detailed schedule of the dissemination activities envisioned by ANASTACIA partners is reported in ANNEX 5.

This dissemination plan is based on an iterative process to improve the effectiveness of communication activities during the project timespan. Indeed, the dissemination strategies will be updated on the successive versions of this deliverable, i.e., D7.3 and D7.4, taking also into account the dissemination activities effectively carried out during the periods covered by these deliverables.

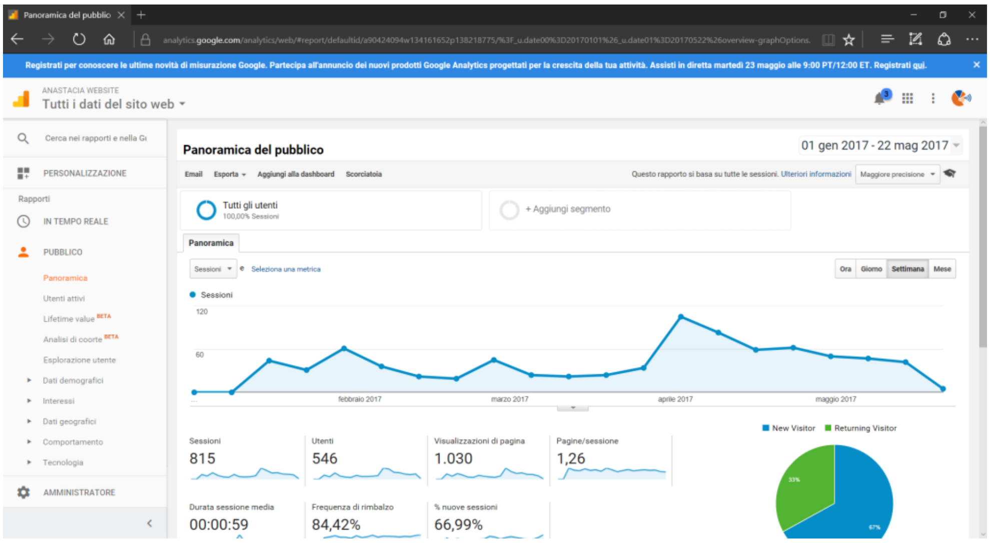
As main initial results, the project host a public accessible website (ANNEX 1), different social media channels, a brochure and a baseline presentation (ANNEX 2), 3 conference papers and 3 journal publications (ANNEX 4), and more than 20 dissemination activities already performed by ANASTACIA partners (ANNEX 3) in manifold national and international events. Furthermore, a comprehensive analysis of standardization activities relevant to ANASTACIA research and innovation areas has been conducted. In this vein, several potential contributions to standardization bodies are envisioned.

7 ANNEX 1 – ANASTACIA WEBSITE DESCRIPTION

The ANASTACIA website is available at www.anastacia-h2020.eu. The domain name has been selected to recall the project acronym and give proper evidence of the funding received by the EC within the Horizon 2020 programme. Subdomains have been created on the anastacia-h2020.eu domain to ease accessing other dissemination tools and channels, as depicted below:


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.
ANASTACIA
Advanced Networked Agents for Security and Trust Assessment in CPS/IoT Architectures
www.anastacia-h2020.eu
http://youtube.anastacia-h2020.eu
http://twitter.anastacia-h2020.eu
http://linkedin.anastacia-h2020.eu
http://www.anastacia-h2020.eu
http://youtube.anastacia-h2020.eu
http://twitter.anastacia-h2020.eu
http://linkedin.anastacia-h2020.eu

The website is monitored by Google Analytics, using the account registered to manage the Google tool suite and the YouTube account:



Registrati per conoscere le ultime novità di misurazione Google. Partecipa all'annuncio dei nuovi prodotti Google Analytics progettati per la crescita della tua attività. Assisti in diretta martedì 23 maggio alle 9:00 PT/12:00 ET. Registrati qui.

Panoramica del pubblico

01 gen 2017 - 22 mag 2017

Questo rapporto si basa su tutte le sessioni. Ulteriori informazioni

Tutti gli utenti
100,00% Sessioni

+ Aggiungi segmento

Sessioni
815

Utenti
546

Visualizzazioni di pagina
1.030

Pagine/sessione
1,26

Durata sessione media
00:00:59

Frequenza di rimbalzo
84,42%

% nuove sessioni
66,99%

Figure 9. Google Analytics dashboard for www.anastacia-h2020.eu.

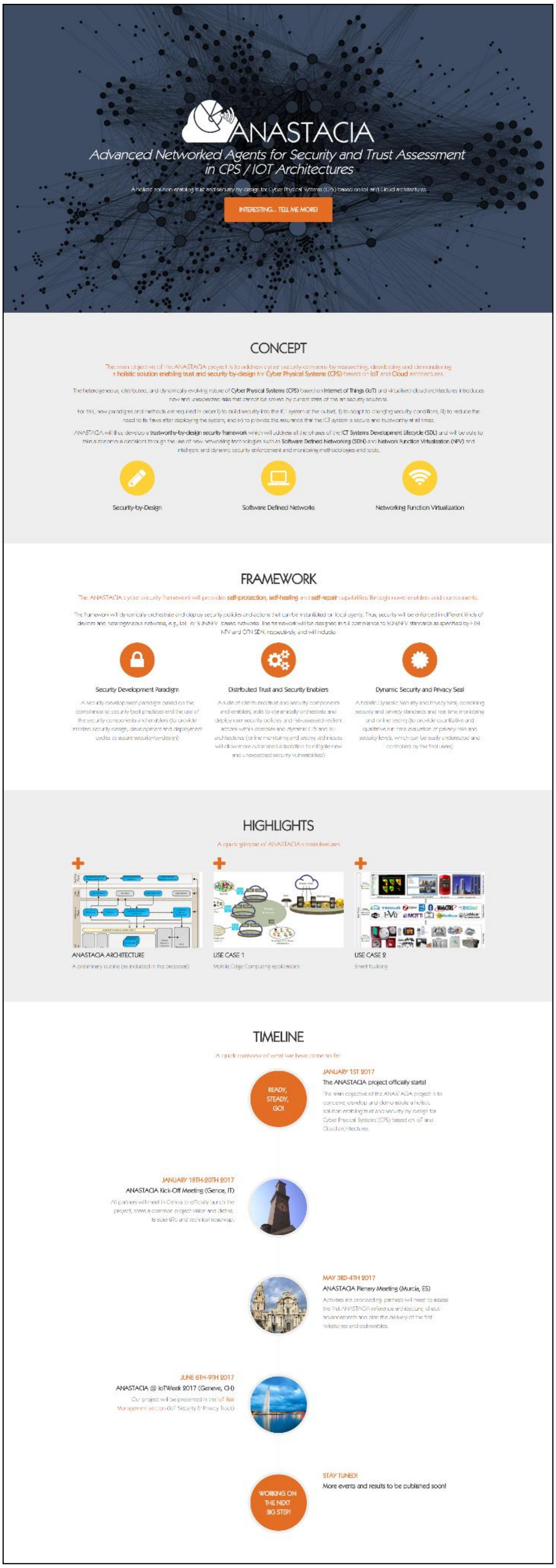
The website is a simple one-page website with an adaptive layout based on Bootstrap and customized starting from the free template **Agency** by **StartBoostrap.com** (https://startbootstrap.com/template-overviews/agency/) to match the requirements of the project.

The contents of the website have been structure so far to provide an overview of the methodological approach, of the ongoing project activities, of participating people and of involved third parties.

The sections that can be accessed from the HOME view are:

- CONCEPT: a brief introduction on the context and problems addressed by the project;
- FRAMEWORK: a summary of the solution proposed by the project;
- HIGHLIGHTS: a set of insights on methodological and technical approaches;
- TIMELINE: a summary of main project activities and initiatives;
- RESULTS: a work-in-progress section meant to host main public/reusable results, including publications and public deliverables as soon as available;
- FIGURES: ANASTACIA project in figures (e.g. summarized information);
- TEAM: Who's who in ANASTACIA, people and roles;
- IAB: the members of the Innovation Advisory Board;
- CONSORTIUM: the group of beneficiaries;
- CONTACTS: project administrative and technical coordination's contact details.

Direct links to Twitter, LinkedIn and YouTube are available too in the page footer.



ANASTACIA

Advanced Networked Agents for Security and Trust Assessment in CPS / IOT Architectures

A holistic solution enabling trust and security by design for Cyber Physical Systems (CPS) based on IoT and Cloud architectures

INTERESTING... TELL ME MORE!

CONCEPT

The main objective of the ANASTACIA project is to address cyber security concerns by researching, developing and demonstrating a **holistic solution enabling trust and security by-design** for **Cyber Physical Systems (CPS)** based on **IoT** and **Cloud** architectures.

The heterogeneous, distributed, and dynamically evolving nature of **Cyber Physical Systems (CPS)** based on **Internet of Things (IoT)** and virtualised cloud architectures introduces new and unexpected risks that cannot be solved by current state of the art security solutions.

For this, new paradigms and methods are required in order i) to build security into the ICT system at the outset, ii) to adapt to changing security conditions, iii) to reduce the need to fix flaws after deploying the system, and iv) to provide the assurance that the ICT system is secure and trustworthy at all times.

ANASTACIA will thus develop a **trustworthy-by-design security framework** which will address all the phases of the **ICT Systems Development Lifecycle (SDL)** and will be able to take autonomous decisions through the use of new networking technologies such as **Software Defined Networking (SDN)** and **Network Function Virtualisation (NFV)** and intelligent and dynamic security enforcement and monitoring methodologies and tools.

Security-by-Design

Software Defined Networks

Networking Function Virtualization

FRAMEWORK

The ANASTACIA cyber security framework will provide **self-protection**, **self-healing** and **self-repair** capabilities through novel enablers and components.

The framework will dynamically orchestrate and deploy security policies and actions that can be instantiated on local agents. Thus, security will be enforced in different kinds of devices and heterogeneous networks, e.g., IoT- or SDN/NFV- based networks. The framework will be designed in full compliance to SDN/NFV standards as specified by ETSI NFV and ONF SDN, respectively, and will include:

Security Development Paradigm

A security development paradigm based on the compliance to security best practices and the use of the security components and enablers (to provide assisted security design, development and deployment cycles to assure security-by-design)

Distributed Trust and Security Enablers

A suite of distributed trust and security components and enablers, able to dynamically orchestrate and deploy user security policies and risk-assessed resilient actions within complex and dynamic CPS and IoT architectures (online monitoring and testing techniques will allow more automated adaptation to mitigate new and unexpected security vulnerabilities)

Dynamic Security and Privacy Seal

A holistic Dynamic Security and Privacy Seal, combining security and privacy standards and real time monitoring and online testing (to provide quantitative and qualitative run-time evaluation of privacy risks and security levels, which can be easily understood and controlled by the final users)

HIGHLIGHTS

A quick glimpse of ANASTACIA's main features

ANASTACIA ARCHITECTURE

A preliminary outline (as included in the proposal)

USE CASE 1

Mobile Edge Computing applications

USE CASE 2

Smart building

TIMELINE

A quick overview of what we have done so far

READY, STEADY, GO!

JANUARY 1ST 2017

The ANASTACIA project officially starts!

The main objective of the ANASTACIA project is to conceive, develop and demonstrate a holistic solution enabling trust and security by design for Cyber Physical Systems (CPS) based on IoT and Cloud architectures.

JANUARY 18TH-20TH 2017

ANASTACIA Kick-Off Meeting (Genoa, IT)

All partners will meet in Genoa to officially launch the project, share a common project vision and define its scientific and technical roadmap.

MAY 3RD-4TH 2017

ANASTACIA Plenary Meeting (Murcia, ES)

Activities are proceeding: partners will meet to assess the first ANASTACIA reference architecture, check advancements and plan the delivery of the first milestones and deliverables.

JUNE 6TH-9TH 2017

ANASTACIA @ IoTWeek 2017 (Geneve, CH)

Our project will be presented in the IoT Risk Management section (IoT Security & Privacy Track)

WORKING ON THE NEXT BIG STEP!

STAY TUNED!

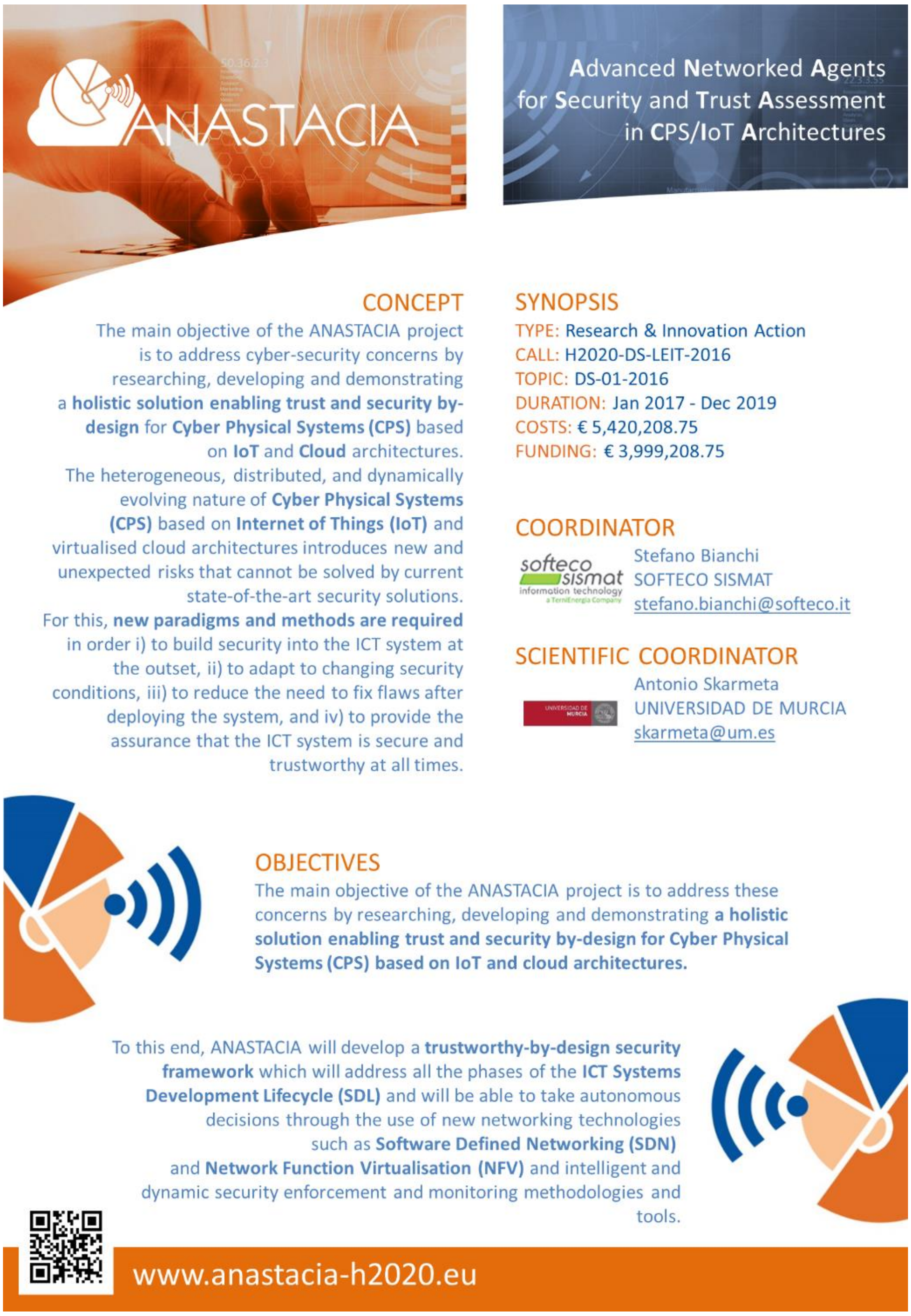
More events and results to be published soon!

Figure 10. ANASTACIA single-page website – overall view and details

8 ANNEX 2 – ANASTACIA DISSEMINATION MATERIAL

The ANASTACIA consortium aims at boosting the dissemination of project's vision and results exploiting multiple channels and events. To achieve this goal, different dissemination materials, such as a project leaflet and a project presentation, have been developed so far. Further dissemination materials developed during the project will be reported in this Annex.

The ANASTACIA project leaflet provides interested parties with basic information about the project objectives and technical concepts, as well as the Consortium members, the Advisory Board and the contact points. The first page of the leaflet is shown in Figure 11, while the second page is shown in Figure 12.



ANASTACIA

Advanced Networked Agents for Security and Trust Assessment in CPS/IoT Architectures

CONCEPT

The main objective of the ANASTACIA project is to address cyber-security concerns by researching, developing and demonstrating a **holistic solution enabling trust and security by-design** for **Cyber Physical Systems (CPS)** based on **IoT** and **Cloud** architectures.

The heterogeneous, distributed, and dynamically evolving nature of **Cyber Physical Systems (CPS)** based on **Internet of Things (IoT)** and virtualised cloud architectures introduces new and unexpected risks that cannot be solved by current state-of-the-art security solutions.

For this, **new paradigms and methods are required** in order i) to build security into the ICT system at the outset, ii) to adapt to changing security conditions, iii) to reduce the need to fix flaws after deploying the system, and iv) to provide the assurance that the ICT system is secure and trustworthy at all times.

SYNOPSIS

TYPE: Research & Innovation Action
CALL: H2020-DS-LEIT-2016
TOPIC: DS-01-2016
DURATION: Jan 2017 - Dec 2019
COSTS: € 5,420,208.75
FUNDING: € 3,999,208.75

COORDINATOR

Stefano Bianchi
SOFTECO SISMAT
stefano.bianchi@softeco.it

SCIENTIFIC COORDINATOR

Antonio Skarmeta
UNIVERSIDAD DE MURCIA
skarmeta@um.es

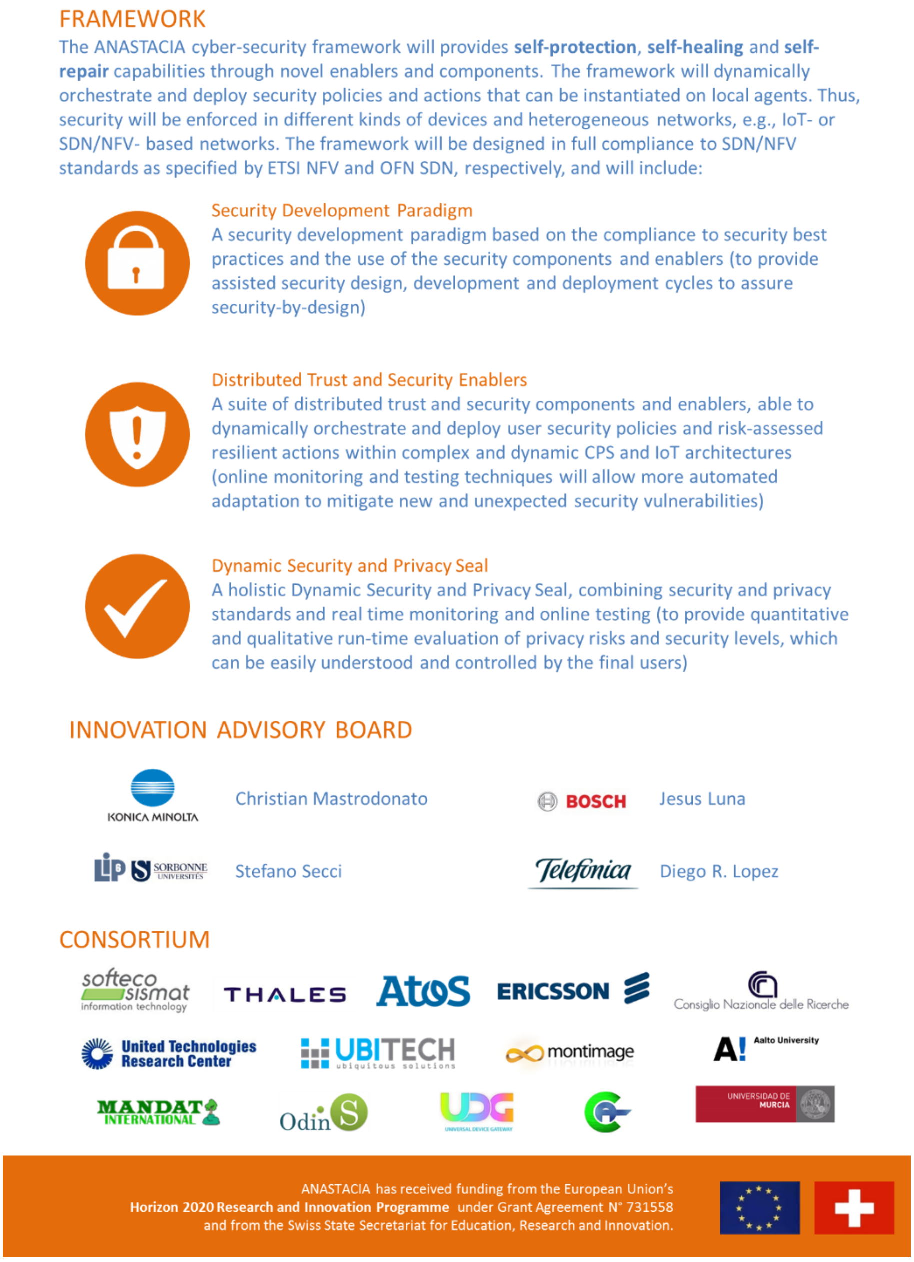
OBJECTIVES

The main objective of the ANASTACIA project is to address these concerns by researching, developing and demonstrating **a holistic solution enabling trust and security by-design for Cyber Physical Systems (CPS) based on IoT and cloud architectures.**

To this end, ANASTACIA will develop a **trustworthy-by-design security framework** which will address all the phases of the **ICT Systems Development Lifecycle (SDL)** and will be able to take autonomous decisions through the use of new networking technologies such as **Software Defined Networking (SDN)** and **Network Function Virtualisation (NFV)** and intelligent and dynamic security enforcement and monitoring methodologies and tools.

www.anastacia-h2020.eu

Figure 11. First page of the ANASTACIA leaflet



FRAMEWORK

The ANASTACIA cyber-security framework will provides **self-protection**, **self-healing** and **self-repair** capabilities through novel enablers and components. The framework will dynamically orchestrate and deploy security policies and actions that can be instantiated on local agents. Thus, security will be enforced in different kinds of devices and heterogeneous networks, e.g., IoT- or SDN/NFV- based networks. The framework will be designed in full compliance to SDN/NFV standards as specified by ETSI NFV and OFN SDN, respectively, and will include:

Security Development Paradigm

A security development paradigm based on the compliance to security best practices and the use of the security components and enablers (to provide assisted security design, development and deployment cycles to assure security-by-design)

Distributed Trust and Security Enablers

A suite of distributed trust and security components and enablers, able to dynamically orchestrate and deploy user security policies and risk-assessed resilient actions within complex and dynamic CPS and IoT architectures (online monitoring and testing techniques will allow more automated adaptation to mitigate new and unexpected security vulnerabilities)

Dynamic Security and Privacy Seal

A holistic Dynamic Security and Privacy Seal, combining security and privacy standards and real time monitoring and online testing (to provide quantitative and qualitative run-time evaluation of privacy risks and security levels, which can be easily understood and controlled by the final users)

INNOVATION ADVISORY BOARD

KONICA MINOLTA	Christian Mastrodonato	BOSCH	Jesus Luna
LIP SORBONNE UNIVERSITÉS	Stefano Secci	Telefónica	Diego R. Lopez

CONSORTIUM

softeco sismat information technology
THALES
Atos
ERICSSON
Consiglio Nazionale delle Ricerche
United Technologies Research Center
UBITECH ubiquitous solutions
montimage
A! Aalto University
MANDAT INTERNATIONAL
OdinS
UDG UNIVERSAL DEVICE GATEWAY
UNIVERSIDAD DE MURCIA

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.

Figure 12. Second page of the ANASTACIA leaflet

The ANASTACIA presentation can be used as a baseline in dissemination events to provide a broad overview of the project, pointing out the main following aspects:

- Rationale
- Mission
- Framework concepts
- ANASTACIA objectives
- WP structure
- Use cases
- Innovation Advisory Board
- Contacts
- Project website and social media
- Consortium

In Figure 13, the slides of the ANASTACIA PowerPoint presentation are illustrated.

1

ANASTACIA

Project overview

<presenter>
<affiliation>
<event details>

2

ANASTACIA

TYPE: Research & Innovation Action
CALL: H2020-DS-LEIT-2016
TOPIC: DS-01-2016 Assurance and Certification for Trustworthy and Secure ICT systems, services and components
DURATION: 36 MONTHS (Jan 2017 → Dec 2019)
COSTS: € 5,420,208.75
FUNDING: € 3,999,208.75
G.A.: 731558

3

Rationale

- ANASTACIA will deliver paradigms and methods that
  - build security into the system at the outset;
  - adapt to changing conditions;
  - reduce the need of finding flaws and repairing them when the system is already deployed;
  - provide the assurance that ICT systems are secure and trustworthy at all times.

4

Mission

- To develop a trustworthy-by-design autonomic security framework which will address all the phases of the ICT Systems Development Lifecycle (SDL) and will be able to take autonomous decisions through the use of new networking technologies such as Software Defined Networking (SDN) and Network Function Virtualisation (NFV) and intelligent and dynamic security enforcement and monitoring methodologies and tools
- holistic solution enabling trust and security by-design for Cyber Physical Systems (CPS) based on IoT and cloud architectures

5

The ANASTACIA framework includes

1 Security development paradigm
2 Distributed trust and security components and enablers
3 Holistic Dynamic Security and Privacy Seal (DSPS)

6

The ANASTACIA framework provides

1 Self-protection capabilities
2 Self-healing capabilities
3 Self-repair capabilities

7

ANASTACIA's sub-objectives

8

Summarizing...

Security development paradigm
Distributed trust and security components and enablers
Holistic Dynamic Security and Privacy Seal (DSPS)
Self-protection capabilities
Self-healing capabilities
Self-repair capabilities
VALUE CHAIN

9

WP structure

WP 0 Coordination and Management
WP 1 Requirements and Architecture Design
WP 2 Security and Trust by Design Enablers
WP 3 Policy Enforcement and Run-Time Enablers
WP 4 Monitoring and Alert Reacting Enablers
WP 5 Dynamic Security and Privacy Seal
WP 6 Integration and Use Cases Validation
WP 7 Exploitation, Standardization and Dissemination

10

Use Cases

- Mobile Edge Computing applications
  - **Test Case**: MEC on video cameras
  - **Scenario**: Spoofing attack on the security camera system
- Smart Building Management Systems applications
  - **Test Case**: Resilient cyber-physical systems in smart buildings
  - **Scenario**: Cyber attack at a hospital building

11

Innovation Advisory Board (IAB)

To support the Consortium in the identification and implementation of the strategy to maximize the impact of results, overviewing and aligning the relevant outcomes with the industry's and standardization bodies' requirements.

12

IAB members

13

Contacts

- Project Coordinator
  Stefano BIANCHI (Softeco Sismat)
  stefano.bianchi@softeco.it
- Scientific and Technical Project Manager
  Antonio SKARMETA (Universidad de Murcia)
  skarmeta@umu.es

14

ANASTACIA

www.anastacia-h2020.eu
http://youtube.anastacia-h2020.eu
http://twitter.anastacia-h2020.eu
http://linkedin.anastacia-h2020.eu

15

ANASTACIA

Figure 13. ANASTACIA basic powerpoint presentation

9 ANNEX 3 – INITIAL DISSEMINATION ACTIVITIES LIST

In the following Table we report the initial dissemination activities related to the ANASTACIA project. This table will be updated in the following Deliverables D7.3 and D7.4.

Number	Date	Location	Typology	ANASTACIA partner	Organizer	Host	Number of persons reached	Short description of the activity
1	19/01/2017	ubitech.eu website	Website	UBITECH	UBITECH	https://www.ubitech.eu/ubitech-undertakes-the-technical-integration-lead-of-the-anastacia-research-project-on-security-and-trust-assessment-in-cps-and-iot-architectures/	1000+	Announcement of the ANASTACIA project on the company website. Description of the project vision and the role of UBITECH in the project
2	23/01/2017		Press release	SOFTECO	TerniEnergia	http://www.ternienergia.com/index.php/ternienergia-entra-nel-settore-cybersecurity-e-rafforza-lattivita-sulle-smart-grid/ http://www.ternienergia.com/wp-content/uploads/2017/01/TE-COS_CYB-23-01-2017IT.pdf http://www.ternienergia.com/wp-content/uploads/2017/01/TE-COS_CYB-23-01-2017EN.pdf	*[1]	TerniEnergia enters into the cybersecurity industry and strengthens the activity on smart grids
3	01/02/2017	Murcia	Communication Campaign	UMU	UMU	http://www.etsi.org/etsi-security-week-2017/nfv-security	2000	Press release related to ANASTACIA from the press unit of UMU
4	02/03/2017	Rome, Università La Sapienza	Participation to a Conference	SOFTECO	Università La Sapienza / Cyber Security National	Presentation of the "ITALIAN CYBERSECURITY REPORT 2016" https://www.cis.uniroma1.it/node/5935	500	Networking activities, monitoring of ongoing relevant initiative in the Cyber-Security sector

					Lab / CIS-Sapienza			
5	06-07/03/2017	Brussels	Brokerage Event	SOFTECO	SEREN3 project	Secure Societies Info day and Brokerage event https://www.b2match.eu/seren3brussels2017	250+	Contacts established with potential Innovation Advisory Board members, contacts established with the network of National Contact Points on Secure Societies for possible collaboration in dissemination activities
6	22/03/2017	Milan	Participation to a Workshop	SOFTECO	Orrick, Kroll & CIV	Workshop "Cyber Security and Data Protection"	50+	Networking activities, monitoring of legal approached on cyber security and data protection (GDPR in particular)
7	27/03/2017	Milan	Participation to a Workshop	SOFTECO	Osservatori Digital Innovation	Kick-Off Meeting "Information Security and Privacy"	75+	Networking activities, monitoring of legal approached on cyber security and data protection (GDPR in particular)
8	28/03/2017	Genova	Participation to a Workshop	SOFTECO	CTI Liguria	CyberSecurity & GDPR	50+	Networking activities, monitoring of legal approached on cyber security and data protection (GDPR in particular)
9	06/04/2017	Paris	Press release	ATOS	ATOS	A press note was published by Atos. https://atos.net/en/2017/press-release/general-press-releases_2017_04_06/atos-partners-european-project-anastacia-iot-security.	International scope	The press note was widely republished to other news portals, as detailed in *[2]

10	06-07/04/2017	Paris	Social Media (Facebook and Tweeter)	ATOS	ATOS	Twitters: https://twitter.com/AtosFR/status/850265574919643136 (French) https://twitter.com/AtosES/status/850356498693750788 (Spanish) Facebook page: https://www.facebook.com/Atos/posts/1481839438514567?comment_tracking=%7B%22tn%22%3A%22O%22%7D	Around 6000 followers	Anastacia outlines with pointers to detailed information. Twitters are available either in French and Spanish
11	11/4/2017	Roma	Participation and networking	AS	Cyber Criminality conference	http://www.tecnaeditrice.com/eventi/cyber_crime_conference_2017/presentazione	Cybersecurity audience	Liaising and networking
12	24/05/2017	Madrid	Communication Campaign (RV)	ATOS	RTVE (Spanish National Radio Broadcasting)	http://www.rtve.es/alacarta/audios/marca-espana/marca-espana-atos-empresa-encabeza-revolucion-digital/4034694/ (Spanish)	Global Spanish National audience	An interview for the national radio station in Spain was conducted, where Anastacia was described
13	29/05/2017	Murcia	Website	ODINS	ODINS	www.odins.es https://twitter.com/odinsolutions https://www.linkedin.com/in/odinsolutions	1000+	Diffusion of the ANASTACIA projects among our contacts networks of Clients, Suppliers, Partners and Developers of IoT products.
14	31/05/2017	Madrid	Exhibition	UMU	Network Virtualization Europe	https://tmt.knect365.com/virtualization-sdn-europe/	50+ Individual operator companies in attendance, 30+ Exhibitors	Presentation of ANASTACIA project, and how SDN/NFV security can be applied for IoT based on ANASTACIA framework.

15	14/06/2017	Sofia Antipolis	Participation to a Conference	UMU	ETSI	http://www.etsi.org/etsi-security-week-2017/nfv-security	200	Presentation of ANASTACIA project. Topic: Policy Based Security Management System for NFV-SDN and IoT Scenarios
16		Lausanne	Website	DG	DG	www.devicegateway.com	DG's stakeholders and potential customers	We will include ANASTACIA intro and link to the project website in DG's website
17	7/6/2017	Geneva	Article presentation	MI, DG, Softeco, UMU	Global IoT Summit	GIoTS "2nd Workshop on User centric security, privacy and data governance in smart cities (USP4SC)" https://sites.grenadine.co/sites/iot/en/iot-week-2017/items/802	>800	Presentation of ANASTACIA
18	6-9/6/2017	Geneva	Session on IoT Security and Privacy	MI	IoT Week 2017	http://iot-week.eu/programme-2017/	>800	Discussing data protection challenges for IoT deployments
19	6-9/6/2017	Geneva	Session on IoT Risk Management	MI, Softeco, AS	IoT Week 2017	http://iot-week.eu/programme-2017/	>800	Presentation of ANASTACIA
20	6-9/6/2017	Geneva	Session on GDPR & IoT	AS	IoT Week 2017	http://iot-week.eu/programme-2017/	>800	Discussing IoT deployment compliance with the GDPR
21	12/06/2017	Spain	Outline in outreach magazine	ATOS	Codasic	https://revistasic.es/index.php?option=com_content&view=article&id=1837&Itemid=1409	Security-related Technical Spanish audience	A brief outline of ANASTACIA was published in the printed version of the magazine. The link specified before shows the highlight of the publication done in the printed version.

*[1] Targets of SOFTECO pressrelease: Ansa; Reuters; Radiocor; ADN Kronos; Wind Press (Eco della Stampa group – 1500 journalists); Soldionline; Abc Risparmio; Borsa Expert; Money Report; Soldi Expert; Gazzetta dell'Economia; Soldiweb; Bluerating; Azienda Banca; Italpress; Forex Info; Business Community; MF Dow Jones; Sole 24 Ore; MF; Italia Oggi; Corriere della Sera (+ ed. locali); Repubblica (+ ed. locali); La Stampa; Il Messaggero; Libero; Il Giornale; Il Fatto Quotidiano; Avvenire; Corriere dell'Umbria; La Nazione; Il Giorno.

*[2] A press note was published by Atos. https://atos.net/en/2017/press-release/general-press-releases_2017_04_06/atos-partners-european-project-anastacia-iot-security. The press note was widely republished to other news portals translated to d+H7ifferent languages in some cases:

English:

- https://globenewswire.com/news-release/2017/04/06/955018/0/en/Atos-partners-in-the-European-project-ANASTACIA-for-IoT-security.html
- https://www.telecompaper.com/news/atos-joins-eu-funded-anastacia-project-on-iot-architectures--1191391

Spanish:

- http://www.economiadehoy.es/noticia/16304/tecnologia/atos-participa-en-anastacia-un-proyecto-de-la-union-europea-que-garantizara-la-seguridad-del-internet-de-las-cosas.html
- http://www.dealerworld.es/tendencias/atos-participa-en-el-proyecto-de-seguridad-iot-de-la-union-europea
- https://www.esmartcity.es/2017/04/07/anastacia-proyecto-horizonte-2020-seguridad-servicios-iot

French:

- http://www.euroinvestor.fr/actualites/2017/04/06/atos-partenaire-du-projet-europeen-anastacia-pour-la-securite-de-linternet-des-objets/13570195
- https://www.boursedirect.fr/fr/actualites/categorie/divers/atos-est-partenaire-du-projet-europeen-anastacia-boursier-493809270a858086b7088aadf06ef63cefde780f
- https://www.abcbourse.com/marches/atos-partenaire-du-projet-europeen-anastacia_394441_ATOp.aspx
- http://www.boursorama.com/actualites/atos-partenaire-du-projet-europeen-anastacia-16fb908a878a1959ed2c4c89848b37ff

Portuguese:

- https://www.abcbourse.com/marches/atos-partenaire-du-projet-europeen-anastacia_394441_ATOp.aspx

10 Annex 4 – Initial publications list

In the following table, we report the details of the initial scientific publications related to the ANASTACIA project. This table will be updated in the following Deliverables D7.3 and D7.4.

Number	DOI	Type of publication	Repository link	Title	Authors	Title of the journal/ Proceedings/ Books series	Number, date or frequency	Relevant pages	Publisher	Place of publication	Year of publication	Open-Access, or will it be made available?
1		Conference		**ANASTACIA, Advanced Networked Agents for Security and Trust Assessment in CPS IoT Architectures**	S. Ziegler, A. Skarmeta, J. Bernal, E. E. Kim, S. Bianchi	The Global Internet of Things Summit (GIoTS 2017)			IEEE	IEEE Xplore	2017	NO
2	10.1109/ MCOM. 2017.16 00899	Journal	http://ieeexplore.ieee.org /document/7 927935/	**NFV: Security Threats and Best Practices**	S. Lal, T. Taleb, and A. Dutta	IEEE Communications Magazine			IEEE	IEEE Xplore	2017	NO
3		Conference		**Assuring Virtual Network Function Image Integrity and Host Sealing in Telco Cloud**	S. Lal, I. Oliver, S. Ravidas, and T. Taleb	IEEE ICC 2017			IEEE	IEEE Xplore	2017	NO
4	10.1109/ TVT.20 17.2701 551	Journal	http://ieeexplore.ieee.org /document/7 920414/	**An Accurate Security Game for Low-Resource IoT Devices**	H. Sedjelmaci, S.M. Senouci, and T. Taleb	IEEE Transactions on Vehicular Technology			IEEE	IEEE Xplore	2017	NO
5		Workshop		**Geo-partitioning of MEC resources**	M. Bouet and V. Conan	Workshop on Mobile Edge Communications (MECOMM' 2017), co-located with ACM SIGCOMM			ACM	ACM Digital Library	2017	No

6	10.1016/j.jisa.2017.05.005	Journal	http://www.sciencedirect.com/science/article/pii/S2214212616300680	**Slowcomm: Design, development and performance evaluation of a new slow DoS attack**	E. Cambiaso, G. Papaleo, M. Aiello	Journal of Information Security and Applications	35	23-31	Elsevier	www.sciencedirect.com	2017	NO

11 ANNEX 5 – DISSEMINATION WORK PLAN SCHEDULE

In the following table, we include the plan of dissemination activities that can be time-wise scheduled. Other activities may take place using channels mentioned in Section 3, when and where opportunities arise. This table will be updated in the following Deliverable D7.3.

Type	ANASTACIA partners	Target audience	Expected Period	Description
Website and Social Media (Facebook, Twitter, LinkedIn)	UBITECH	Public Web (Companies and ISVs working with IOT segment or utilizing SDN technologies, private and public sector)	Whole duration of the project	UBITECH will disseminate the ANASTACIA outcomes on the company website and social media accounts, in order to reach people in the network of the company and possible customers in both private and public sector
	ODINS	Our contacts networks of Clients, Suppliers, Partners and Developers of IoT products.	2017	Diffusion of security and privacy framework of the ANASTACIA project among public and private entities related with OdinS.
	AALTO	Website visitors	Whole duration of the project	Mentioning of the project's vision and results in the research group website
	ATOS	ATOS Social Media (Twitter, LinkedIn, and Facebook)	2017-2018	Atos counts with a stable presence in social Media, with a noteworthy relevance. Atos plans to continue publishing regular outlines about the ongoing progress of ANASTACIA in its corporative Facebook, Twitter and LinkedIn accounts.
	MONT	Website visitors	Whole duration of the project	Montimage will disseminate the ANASTACIA activities in its website and Social Network accounts.
	CNR	Website visitors	Whole duration of the project	Mentioning of the project in the research group website
	DG	Website visitors	Whole duration of the project	DG will include ANASTACIA intro and link to the project website in DG's website
	AS	Website visitors	Whole duration of the project	AS will promote ANASTACIA through its website.

	MI	Website visitors	Whole duration of the project	MI will promote ANASTACIA through its website.
	SOFTECO	Other cyber-security research projects, institutions, researchers, students, cybersecurity professionals	Whole duration of the project	Extensive use of Twitter.com to tweet on project activities and achievements, to create expectations on results to be delivered and inform the community of cyber-related professionals and researchers.
Training	UMU	Master Degree	Academic Year	Inclusion of results of ANASTACIA in different courses of the Master on New Technologies on Informatics
	AALTO	Master Degree	Academic Year	Inclusion of results of ANASTACIA in different courses of Master's Programme in Computer, Communication and Information Sciences (CCIS)
	MI	Master Degree	Academic Year	Inclusion of relevant ANASTACIA results in the Master in Advanced Studies on IoT of the University of Geneva, codirected by MI.
	SOFTECO	ICT professionals	Second half of the project	Among side exploitation activities, vocational training on cybersecurity aspects investigated in ANASTACIA will be designed and proposed to ICT staff of other companies in the Italeaf group (www.italeaf.com) - to be planned
Press Release	UMU	Second press release	2018	Provision of a second press release with results of the project
	SOFTECO	Press releases	Second half of the project	Following the initial press release, an update on methodological and technical results achieved will be issued for interested stakeholders.
	UBITECH	Mail campaign to targeted contacts and possible press release	2019	After having concrete results and a stable platform that can be presented to external audience

Organization of a Workshop	UMU	Workshop to be proposed on EuCNC 2018 in Slovenia	June 2018	Proposal for a workshop organization
	MONT	Research Comunity and PhD Students	26/06/2017 - 30/06/2017	Poster presentation at TAROT Summer School 2017
	SOFTECO	ICT Students	Second half of the project	A workshop on ANASTACIA technical and methodological approach as well as results will be proposed to the Cybersecurity Master in the University of Genoa (http://www.mastercybersecurity.it/)
Organization of a Conference	UTRC	Research community	10/09/2017	CENICS 2017 The special track CYPHYS: Cyber-Physical Security (https://www.iaria.org/conferences2017/filesCENICS17/CYPHYS.pdf) has been proposed to match ANASTACIA interest and to discuss many novel aspects of cyber-physical security
Participation in activities organized jointly with other H2020 projects	UBITECH	Research community, Research-focused industrial partners	2018-2019	Participation at joint events with other H2020 projects for the dissemination of innovative ANASTACIA outcomes
	SOFTECO	Other EU-funded projects, researchers	Whole duration of the project since M6	By cooperating with TRUESSEC.EU, we will ensure that our work is aligned, avoid that efforts are duplicated, and foster a strong network of support.
Participation to a Workshop	UMU	TBD	June 2018	TBD
	SOFTECO	Industry, research community	To be defined	Contacts with cybersecurity NCP have been established to organize a workshop on best practices for EU-funded project management and best practices in the cyber-security domain
	MONT	Research Community, Research-centered industrial partners	2017-2018	Participation at Workshops with ANASTACIA innovations published as workshop papers.
	ATOS	Technical audience and research community	2017-2018	Atos will participate in technical workshops (including those organized by Anastacia) and mainly derived from scientific publications, invitations to round tables, or distinguished seminars.
	THALES	Industry, research community	2017-2019	Participation at workshops for the dissemination of innovative ANASTACIA outcomes as workshop papers and at workshops organized by Anastacia.
	UBITECH	Research community, research-focused industrial community	2018-2019	Participation at workshops will be performed for the dissemination of innovative ANASTACIA outcomes

Participation to a Conference	UMU	IEEE WF-IoT 2018, IEEE CCNC, IEEE Conference on Network Function Virtualization and Software Defined Networks	January-February 2018	Paper presentations and talks
	AALTO	IEEE CSCN, IEEE ICC, IEEE GLOBECOM, IEEE WCNC	2017-2019	Paper presentations and talks
	SOFTECO	Cybersecurity professional, stakeholders, operators	2018	Participation in the ITASEC'18 conference (Jan-Feb 2018), SAFE 2017 - 7th International Conference on Safety and Security Engineering - TO BE EVALUATED, Security Summit (https://www.securitysummit.it/)
	CNR	Research and academics	4-8 September 2017	Participation to the ITC29 conference
	UTRC	Research community, cybersecurity professional, stakeholders, operators	4-7/12/2017	Participation to Black Hat Europe 2017, the most technical and relevant global information security event series in the world.
	MI	Research community, cybersecurity professional, stakeholders, operators	2017-2019	Paper presentations and talks

	DG	Research community, cybersecurity professional, stakeholders, operators	2017-2019	Paper presentations and talks
	AS	Research community, cybersecurity professional, stakeholders, operators	2017-2019	Paper presentations and talks
	THALES	IEEE and ACM Conferences based on Network Function Virtualization, Software Defined Networks and Multi-access Edge computing	August 2017, January-February 2018	Paper presentations and talks
	UBITECH	IOT related companies, industrial community	2018-2019	Presenting ANASTACIA results to conferences in order to attract possible customers
Exhibition	ODINS	IoT World Congress	October 2017	Show the first developments of the ANASTACIA project for attendees of IoT world
			2018	Show the ANASTACIA results to find commercial collaborations to introduce security framework in the world of IoT market.
		Advanced Factories Expo & Congress	2018	Show the ANASTACIA results to find commercial collaborations to introduce security framework in the world of Advanced Factories and Industry 4.0.
Trade Fair	ODINS	Smart City Expo World Congress	November 2017	Show the first developments of the ANASTACIA project for attendees of the world of SmartCities
			2018	Show the ANASTACIA results to find commercial collaborations to introduce security framework in the world of SmartCities market.
Participation to an Event other than a Conference or a Workshop	SOFTECO	ICT professionals	Several possible events, whole duration of the project, according	Local technical dissemination events promoted by CTILiguria (http://www.ctiliguria.it) focusing on initiatives by industry based in Genoa (IT)

			the the schedule provided by the organizers	
	ATOS	Digital security experts and IoT developers	September 2017	Atos is evaluating its participation in the Connect Security World, Embedded Trust in IoT Systems and Connected Hardware www.connectsecurityworld.com
Communication Campaign (e.g. National Confederation of SMEs, Regional Governments, Municipalities)	SOFTECO	ICT professionals, stakeholders, SMEs	Second half of the project	As founding active member of SIIT, Intelligent Integrated Systems and Technologies, the Technology District of the Liguria Region (http://www.siitscpa.it/), promotion of ANASTACIA initiative among the industrial and academic members active in ICT and cybersecurity domains
	ATOS	General public	2017-2018	Atos will continue with its successful strategy of dissemination to large audience media through press notes and interviews targeting mainly general public, such as interviews at radio stations, newspapers or magazines (general purpose, economic, etc).
	MONT	Parisian SMEs	2017-2018	As member of the Systemic SME Cluster, Montimage will disseminate the technologies and results of ANASTACIA among the community of Parisian SMEs.
Dissemination to other EU co-funded projects	UBITECH	Research community, Research-focused industrial partners	2017-2019	ANASTACIA will be presented to related EU co-funded research projects and liaisons will try to be established
	ATOS	Technical audience	2017-2018	Atos will present the Anastacia outcomes and ongoing activities to the related projects where it is participating. Some of these projects are CIPSEC, WITDOM, WISER, TREDISEC, COMPOSITION and DISIEM
Other	DG	Research community, Research-focused industrial partners	2017-2019	DG introduces and will introduce ANASTACIA whenever we meet relevant DG's stakeholders including other EU project partners where DG is involved.
	ODINS	Regional and National Associations of Innovative Technologies Companies such as CENTIC, CEEIM, SmartLivingPlat, Planetic, Secartys.	2018	Presentation of ANASTACIA results to promote the security and privacy framework among technological SMEs and national operators

ANASTACIA