

Deliverable D8.5 Final communication plan and activities progress reports

Review of mid-term Communication plans and description of the Communication activities achieved during the project life

WP8

Periodic Activity and Management Report

Contract Number:	731711
Project Acronym:	TRUESSEC.EU
Project Title:	"TRUst-Enhancing certified Solutions for SEcurity and protection of Citizens' rights in digital Europe"

Document Identifier:	D8.5
Status:	Draft

Title of Document:	D8.5 Final communication plan and activities progress reports
Dissemination Level:	Public

Author(s):	Ali Anjomshoaa (KTN)
Reviewed by:	Pablo López-Aguilar Beltrán (APWG)

Created on:	20/11//2018
Last update:	03/12/2018

Grant agreement number:	731711
Project Acronym:	TRUESSEC.EU
Project Title:	“TRUst-Enhancing certified Solutions for SEcurity and protection of Citizens’ rights in digital Europe”.
Start date of the project:	01/01/2017
Duration of the project:	24 months
Period covered by the report:	Jan-Dec 2018
Periodic report:	N/A
Date of submission of the periodic report:	31/12/2018
Version:	V1.0
Project website address:	http://truessec.eu/
The report is elaborated on the basis of the:	N/A

CHANGE HISTORY

Date	Change	Author
30/11/2018	First draft	A. Anjomshoaa (KTN)
03/12/2018	Added sub-sections 3.4 and 3.5	A. Anjomshoaa (KTN)
19/12/2017	Comments	M.Medina & Pablo López-Aguilar (APWG)

Table of Contents

1. Executive summary	7
2. Introduction	8
2.1. TRUESSEC background	8
2.2. Relationship with other Work Packages and deliverables	9
2.3. General Objectives	10
3. Communication Plan	11
3.1. Target Stakeholders	11
3.2. Key Messages	11
3.3. Campaigns	11
3.4. Communication Plan Response Following European Commission Review in 2018	12
3.5. Advisory Board	13
4. Communication Tools	15
4.1. Visual identity	15
4.1.1. Project logo	15
4.1.2. Presentation	15
4.1.3. Letters	16
4.2. Information tools:	16
4.2.1. Social Media	16
4.2.1.1. Twitter	16
4.2.1.2. LinkedIn	17
4.2.1.3. YouTube	17
4.2.2. Project Web Platform (SHOP)	17
4.2.2.1. Operational structure	17
4.2.2.2. Recruitment	19
4.2.2.3. Roles	20
4.2.2.4. Populating the SHOP	21
4.2.3. Project Web Platform (for internal project exchanges, i.e. not the SHOP)	21
4.2.3.1. Internal Project Meetings	21
4.3. Common promotional material	22
4.3.1. Brochure	22
5. Events	24
6. Communication activities and progress summary	25

7. Annexes.....	26
7.1. Annex 1	26
7.2. Annex 2	28

DRAFT

List of Figures

Figure 1. Interrelation of WP8 and the other WPs.	9
Figure 2. TRUESSEC official project logo.	15
Figure 3. Screenshot of YouTube page hosting audio file from the debate at Cybersec 2018, Krakow, Poland.	17
Figure 4. process of recruiting members to SHOP, for a given Campaign.	19
Figure 5. Internal communication file structure.	21
Figure 6. TRUESSEC.eu Brochure.	22
Figure 7. TRUESSEC.eu Brochure.	23

DRAFT

List of Tables

Table 1. Responsibilities for activities.20

DRAFT

1. Executive summary

This document contains reviews of the communication plans expressed in part B of the TRUESSEC.eu Grant Agreement (GA) and the first version of the communication and activities plan and progress report for the project submitted in M12, and is an update of the latter. This report covers the plan and activities progress for project communication spanning M1-24. The report is divided into three main sections, firstly an outline of the project's overall objectives and approach to communication, secondly an overview of the tools that were utilised to support the communication plan and a final section is dedicated to a summary of progress against plan.

DRAFT

2. Introduction

In this section, we provide an overview of TRUESSEC.eu and the general objectives of the communication and activities plan.

2.1. TRUESSEC background

TRUESSEC.eu is a Coordination and Support Action on certification and labelling of trustworthiness properties from a multidisciplinary SSH- (Social Sciences and Humanities) ICT perspective and with emphasis on human rights. The current complexity of ICT products and services makes it difficult to appraise their trustworthiness. Thus, certification becomes a must to restore transparency and trust.

TRUESSEC.eu aims at exploring:

- The current situation;
- The barriers to trustworthiness, and
- The benefits of security and privacy labels;
- Engaging stakeholders in the discussions, and
- Issuing recommendations that seek to foster the adoption and acceptance of labels.

With these aims, TRUESSEC.eu work and results are sustained by three pillars:

- 1) A Stakeholders' Online Platform (SHOP), where associated cluster projects and stakeholders from industry, academia, governments and civil society can gather, participate in debates, be informed, and provide their opinions and feedback on the topics of the project.
- 2) A series of Support Analysis and Studies (SUPPA) from multidisciplinary perspectives on issues of trustworthiness certification and assurance, to study the situation of trust-enhancing labels, barriers to / incentives for industry adoption and consumer acceptance. Information will be gathered from both public sources and the interactions with stakeholders through the SHOP.

Four different approaches will be applied:

1. Socio-cultural;
 2. Legal & ethical;
 3. Technological; and
 4. Business.
- 3) A set of Recommendations on European Trust-Enhancing Labels (ETEL) dealing with:
 1. Methodological aspects of certification and assurance;
 2. A catalogue of criteria (Criteria Catalogue) for labels and certifications, and
 3. Regulatory aspects to foster their adoption, plus a strategic agenda.

These recommendations reflect the conclusions obtained from the support analysis and from the stakeholders.

The main goal of WP8 is to manage dissemination of the knowledge and results generated and achieved throughout the duration of the project to the academic and industrial communities, and communication to

society. In close collaboration with the project's partners and using the online SHOP platform developed in WP2, the work carried out in WP8 is intended to generate awareness of the TRUESSEC.EU project with stakeholders, including Internet-based providers and the cybersecurity and privacy industry, data protection authorities, cybersecurity agencies, European institutions and policy makers.¹

To support these goals project communications will focus on reaching the broadest audience possible via multiple channels, including web, social media, and face-to-face at conferences, workshops and appropriate events at both the national and international levels, engagement with those project partners that represent stakeholder networks, and the network of H2020 projects within the same cluster.

2.2. Relationship with other Work Packages and deliverables

Figure 1 highlights the role of WP8, and its support of other WPs.

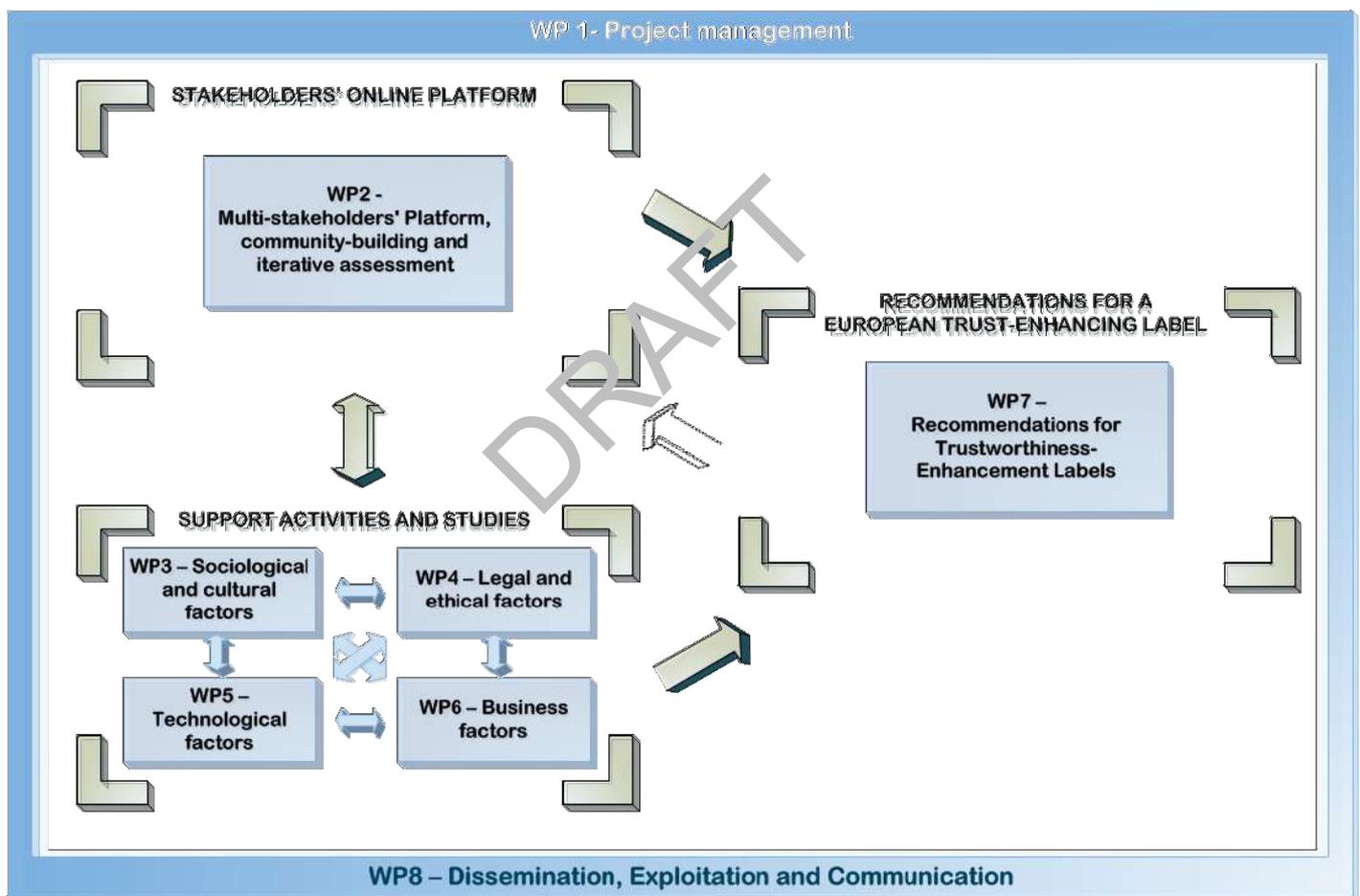


Figure 1. Interrelation of WP8 and the other WPs.

¹ EU Publications Office. 2017. *CORDIS*. [ONLINE] Available at: http://cordis.europa.eu/project/rcn/207202_en.html. [Accessed 12 December 2017].

2.3. General Objectives

The purpose of this communication plan has been to set out the measures that were planned and taken to promote the TRUESSEC project, its activities, achievements and dissemination of results.

The general aims of project communications are as follows:

- Promote awareness of TRUESSEC and its mission;
- Ensure adoption of the responsibilities and actions assigned to each project partner; and
- Encourage two-way communication, (particularly on the SHOP) between identified stakeholder groups and individuals, sister projects and relevant policy influencers.

WP8 leader APWG is responsible for coordinating the execution of the communication activities outlined within this plan, with close support from DigiCat as lead for T8.3. It should be noted that the engagement responsibilities of WP8 were transferred from DigiCat to KTN in the last quarter of the project. All other consortium members have been actively involved in this task, with each partner taking responsibility for ensuring promotion of the project, as defined in the GA.

DRAFT

3. Communication Plan

3.1. Target Stakeholders

The target stakeholders differed depending on the nature of the message to be communicated and appropriate tools were used to reach and engage each audience. The target audience for project activity comprised representatives of one or more of the following groups:

• CERT	• NGOs
• City	• Public Authority
• Community	• RTO
• Consortium	• SME
• Consumer	• Standard body
• Enterprise	• Strategy Body
• Financial Institution	• Trade org
• Government Body	• Union
• Key Prime	• University
• Law Enforcement Agency	

3.2. Key Messages

Communications from the project were made in the context of a unified set of key messages, which extended as the project and its findings became more refined. Communications associated with research publications summarised the abstract of the associated paper, poster or presentation. In the latter phase of the project, messages have focused on summarising project findings and achievements, which were posted on the SHOP and communicated via Twitter and emails.

During the initial phase of the project, key messages echoed mission, goals and values, focusing specifically on recruitment of participants for SHOP. Recruitment to the SHOP has been extremely challenging. We believe this to be due to the large body of cybersecurity work and the substantial amount of global and European activity, particularly European Commission funded projects, which have had to compete for the attention of researchers, policy makers, industrialists and the private sector, and other projects. Even though we had anticipated this large amount of activity to be a substantial opportunity for outreach and engagement, it would appear that the competition for attention and some of the confusion around the roles of EC projects in this area have combined to work against us in recruiting participants to the SHOP platform.

3.3. Campaigns

Communication campaigns generally aligned with the project phases supported content generation for both the SHOP and social media. The proposed project campaigns were:

Dissemination level: PUBLIC

- Sharing the mission, goals and values;
- Recruitment of the Advisory Board;
- Notifying target stakeholders and established networks of activities throughout the phases of the project;
- Promotion / validation of project findings via the SHOP and social media;
- Event promotion, including that of debates specifically tasked with enhancing the findings of TRUESSEC; and
- Announcing deliverables to encourage adoption of their findings.

3.4. Communication Plan Response Following European Commission Review in 2018

At the TRUESSEC 2018 interim review by the European Commission's reviewers, feedback was provided on the project's lower than expected levels of stakeholder engagement, in particular, the lack of stakeholder activity on the SHOP. As a result, APWG and the project coordinator, DigiCat, together with project partners, revisited the communication plan. This was summarised in a response to the Head of Unit at the Commission and is copied below.

It is generally acknowledged within the project that the stakeholder platform (SHOP) has not received enough public attention, and that the organic approach to engagement via the SHOP within the first 18 months of the project has been suboptimal.

As a result, starting in project month 19, the TRUESSEC.eu Project Coordinator, Digital Catapult (UK), has undertaken a new approach to engagement activities, with a more focussed engagement strategy, through dedicated full-time engagement effort in the final quarter of the project. This has resulted in a contract amendment that sees this activity transferred to Dr. Ali Anjomshoaa at the Knowledge Transfer Network (UK), Ali having worked on FP5-FP7 and Horizon2020 projects with specific experience in engagement in various technical fora.

The updated multi-channel approach instigated by Ali Anjomshoaa includes the following actions:

1. General dissemination and public engagement through the project's and partners' Twitter accounts – this has already led to increased traction and relationships with sister and related European Commission projects;
2. A reorganisation of the SHOP website to ensure debates are clearly debates and other posts moved to a News section;
3. Reinvigorating an internal partner programme of individual, named Debate Champions, who are experts having worked on project deliverables, and who will own and engage in debates on the SHOP according to their expertise;
4. Dissemination of deliverables and debate activity via Twitter and by direct email to known interested parties;
5. Continued engagement with the project's Advisory Board (see list below) with increased specific requests for **feedback on specific deliverables, general guidance and help in stakeholder engagement**, especially as in this final quarter of the project all earlier works are culminating in critical results and outputs, i.e. the Criteria Catalogue and indicators, and leading to solutions recommendations for trust enhancing labels and certification;
6. A push to increasing dissemination of key project outputs, starting with the Draft Criteria Catalogue D4.3 by:

- a. Directly engaging key stakeholders on an individual basis: Advisory Board members, and sister and related projects' liaisons and Coordinators; and
- b. Disseminating at upcoming conferences and seeking engagement with the SHOP, such as:
 - i. **European projects Clustering workshop On Cybersecurity and Privacy (ECoSP 2018) at the ARES Conference, August 27–30, 2018, Hamburg, Germany** – Talk by Prof. Manel Medina, Head esCERT-inLab-UPC, Universitat Politècnica de Catalunya
 - ii. **MyData 2018, August 29–31, Helsinki, Finland** – Talk by Stefan Reichmann, UniGraz
 - iii. **EU Symposium on Electronic Crime Research (eCrimeEU 2018), September 17–19, 2018, Krakow, Poland** – Poster and presentation by Pablo López-Aguilar Beltrán, APWG.EU, and Valentin Gibello, Ceraps, Center for European Research on Administration, Politics, and Society
 - iv. **CYBERSEC Forum, October 8-9, 2018, KRAKOW, Poland** – TRUESSEC Panel Discussion: “Labelling and Certification Landscape – Building Trustworthy ICT Industry” organised by Iwona Wilk, KTN, and chaired by Jon Kingsbury, Head of Digital Economy & Creative Industries, Knowledge Transfer Network
7. Launching a series of stakeholder and public surveys, e.g.: <https://r1.dotmailer-surveys.com/9b2vfu0b-6837sl9f> the results from which will be reported through the SHOP and in a Project Engagement Report as part of WP8.

It should be acknowledged that a natural ramp up of activity was expected within the project, where in the earlier parts of the project engagement was a lower profile activity until some traction was achieved through the project's deliverables, particularly the Support Active Analysis and Studies (SUPPA) work package and deliverables, which in this final quarter of the project are providing the assets and information needed to engage key stakeholders and the public. For example, with the publication of D4.3 First Draft Criteria Catalogue at the end of June 2018, it is now possible to explain the project's approach to stakeholders and gain their feedback and buy-in into the project's approach.

3.5. Advisory Board

The TRUESSEC Advisory Board (AB) was engaged as follows:

1. We asked AB members to read and give general feedback and specific feedback, according to their expertise, on specific key deliverables. Specifically, we will ask the AB members to review and provide feedback on:
 - a. **D4.3 First draft Criteria Catalogue and regulatory recommendations** – July 2018
 - b. **D7.2 Cybersecurity and Privacy Criteria Catalogue for Assurance and Certification** – August 2018
 - c. **D6.3 Recommendations for standardization initiatives** – September 2018
 - d. **D7.3 Perceived levels of security & privacy** – November 2018
 - e. **D7.4 Methodological guidelines for assurance and certification of security and privacy level** – November 2018

2. With the help of the AB and their feedback on the above deliverables, we will publish a document, for use by the European Commission, which **provides guidance and recommendations on labeling for trustworthiness in ICT products and services – the AB members will be named on this document.**
3. We aimed to engage the AB to participate in a number of surveys targeting stakeholders and the public, to provide rapid, summary feedback on the work and output of TRUESSEC project. However, the first survey (<https://r1.dotmailer-surveys.com/9b2vfu0b-6837sl9f>) did not generate sufficient response to follow up with additional surveys and AM members with engaged individually and collectively by email.
4. We engaged AB members on a one-to-one basis to ask them to initiate, champion and participate in a number of debates, according to their expertise, on the SHOP platform – this engagement was led by the Knowledge Transfer Network and DigiCat.

Name	Type of Organisation	Expertise	Country
David Alexander	University	Disaster Risk	UK
Harry Armstrong	R&D Organisation	Policy	UK
Georg Borges	University	Law	DE
Jacques Bus	Consultancy	Privacy, Identity and Trust in the Digital Environment	LU
Laurent Caron	Law Firm	Data Protection	FR
Robert von den Hoven von Genderen	Law and Internet	Certification	NL
Ludmilla Georgieva	European Body	IT Law and Cybersecurity	AT
Tracy Harwood	University	Consumer Behaviour	UK
Laura James	Consultancy	Knowledge and IT	UK
Mar Espana Marti	Government Body	Data Protection Authority	ES
Antonio Ramos	SME	Security	ES
Bruno Rasle	Civil Society	Protection of Personal Data	FR
Reinhard Riedl	University	E-government expertise	CH
Burkhard Schafer	University	IT and IP Law	UK
Maximilian Schubert	Internet Service Providers Association	The Internet and IT Law	AT
Andrea Servida	European Body	Legislation	BE
Dan Sutch	University	Social Change Through Digital Technology	UK
Andrej J. Zwitter	University	Internal Relations and Law	NL

4. Communication Tools

The tools for the implementation of the communication plan have been divided into three groups according to their specific objective, as detailed in the following sections:

- A unified and compelling *visual identity* and associated branding;
- *Information tools* to facilitate and scale communication; and
- *Common promotional materials* specially to support face-to-face interactions.

4.1. Visual identity

4.1.1. Project logo

A Project logo was created in M4 by UPM using the Inkscape programme and is shown in Figure 2. The logo can be imported by any vector image editing program, e.g. Adobe Illustrator, and from there, PNG versions or other formats can be created to allow for flexibility of use.

The agreed logo was supplied to each partner in 6 variations, each to be used when it is deemed appropriate (e.g. horizontal versions for a title bar, grayscale version for black and white material).



Figure 2. TRUESSEC official project logo.

Regarding the use of the EU emblem, the project has adhered to usage guidelines published in the following:

- <http://eacea.ec.europa.eu/about/logos/eu-emblem-rules-hr.pdf>
- https://europa.eu/european-union/abouteuropa/legal_notices_en#use-of-the-eu-emblem-by-third-parties

4.1.2. Presentation

To support partners in communication, a standard presentation slide template was created and distributed to ensure consistent stylistic approach and coherence of messages. All presentations should contain information on the project objectives and relevant information about the Consortium. This information will be updated and maintained as the project progresses to summarise the growing set of findings and suitability for the audience.

Partners may include slides from this presentation in their own slide-sets, and customise it to their needs, provided that:

- The essential messages are not materially changed; and
- The project branding is retained, with any copyrights respected.

An example of this template can be found in [Annex 1](#).

4.1.3. Letters

A standard letter head was created to support the requirement for any official written communication, such as the agreement between Advisory Board members and the TRUESSEC consortium. A copy of this letter can be seen in [Annex 2](#).

4.2. Information tools:

4.2.1. Social Media

Social media channels were used for publishing project information, such as events, publicly available deliverables and findings, as well as disseminating news on digital trust and related topics. The primary objective of social media activity has been to generate the interest of a wide range of stakeholders through additional communication and dissemination channels.

4.2.1.1. Twitter

DigiCat created and was responsible for management of the project's Twitter account. The Twitter handle @TRUESSECeu went live at the beginning of the project live and all partners were asked to contribute relevant content that can be shared and / or reviewed.

The account has been used for the promotion of project messages and monitoring social engagements. Furthermore, where appropriate, each partner promoted project activity through their own organisations' Twitter accounts to enable a greater audience to be reached through established networks and followers. The following accounts were used to do this to varying degrees:

- @apwg_eu
- @UniGraz
- @DigiCat
- @KTN_UK
- @telecoupm, @la_upm, @dit-etsit-upm
- @usuariosdeinter, @diadeinternet

In addition to using the organisational Twitter accounts of project partners, individual project members, e.g. Valentin Gibello, Lille; Iwona Wilk and Jon Kingsbury, KTN; Manel Medina, APWG; etc., used their own social media accounts on Twitter and LinkedIn to communicate with their followers.

The project's main channel for communication has been the Twitter platform as it offers a more efficient network effect and lower cost per engagement. Since a step change was made in the use of Twitter in WP8 in the last quarter of the project, Twitter followers have doubled in number, with a related increase in engagements with @TRUESSEC.eu Tweets and click-throughs to the SHOP platform. Using Twitter has proved effective in engaging sister projects and other EU initiatives in the TRUESSEC domain.

4.2.1.2. *LinkedIn*

The proposed approach for project promotion via LinkedIn was designed to utilise each partner's organisation's existing LinkedIn accounts, where they exist, to achieve the good traction and results. A TRUESSEC LinkedIn group² was created for communication of the project achievements to our stakeholders.

In the end, less emphasis was put on the use of LinkedIn than on the use of Twitter and direct emails for communication purposes. The main reasons for this were the lack of engagement amongst academia with the LinkedIn platform and the higher effort cost per user reached, of using the LinkedIn group. It was recognised by the TRUESSEC engagement team that Twitter offers a broader bandwidth for engagement with the whole community and is a lower cost option for communication as it exhibits a more efficient network effect.

4.2.1.3. *YouTube*

YouTube was used to host any large media files needed for dissemination, for example debate recordings. Figure 3 Shows a screenshot of the YouTube page³ hosting the audio file from the debate at Cybersec 2018 in Krakow, Poland, details of which can be found in TRUESSEC deliverable "D2.4 Community Building and Awareness Raising Material"⁴.



Figure 3. Screenshot of YouTube page hosting audio file from the debate at Cybersec 2018, Krakow, Poland.

4.2.2. Project Web Platform (SHOP)

4.2.2.1. *Operational structure*

APWG launched and operates the project website, known as the SHOP (StakeHolder Online Platform), in collaboration with all project partners. The SHOP became operational in M6 of the project. Its content is periodically updated to facilitate better communication, dissemination and outreach of the project outcomes, and to stimulate collaboration with our stakeholders.

The selected website URL: <https://truessec.eu/>, and the domain name TRUESSEC.eu have been purchased by APWG for use by the project.

² <https://www.linkedin.com/groups/8610462>

³ <https://www.youtube.com/watch?v=5LpgyyyQPWY&feature=youtu.be>

⁴ Can be found at: <https://truessec.eu/library>

A detailed description of the operational guide for the SHOP was produced and published as TRUESSEC deliverable “D2.1 Multi-stakeholders platform – Online Platform: SHOP”. Herein follows a short summary of the platform structure and rationale.

4.2.2.1.1. Landing page (<https://truessec.eu/>)

The website’s landing page includes a brief description of the project and summarises the latest activities from across the platform to help visitors identify new content and to provide contributions to the topics of their interest. In order to increase engagement with the SHOP, the landing page was significantly improved in the second year of the project so that it could host media files and to remove some unnecessary elements in order to help make the debates and blog lists more prominent.

4.2.2.1.2. Work packages structure (<https://truessec.eu/about#wpstructure>)

The platform also maintains a section for information specific to work packages where they and their main achievements will be described.

4.2.2.1.3. Events (<https://truessec.eu/events>)

A section specific to events allows all registered users to publish, comment on and keep up with events that may be of interest to them.

4.2.2.1.4. TRUESSEC.eu Debates (previously called Futures) (<https://truessec.eu/futures>)

This is the section where debates about the proposals to assess the trustworthiness of digital applications are hosted. The presentation of outcomes and dissemination of results obtained by the project on the studies about assurance, certification and recommendations for trustworthiness labels, as key project successes, will be presented and debated in this section. This section is not only the home to debate the outcomes and results of the project and for comments about them, but also a way to receive feedback from the community towards adopting the recommendations produced.

We acknowledge that, given the difficulty in recruiting stakeholders to the SHOP platform as described in section 3.2 above, the idea of using the debates section of the SHOP has not been fruitful. Instead, direct contact with sister projects and Advisory Board members has been used to elicit feedback on key project outputs in WPs 4, 5, 6, and 7.

In addition to direct contact with sister projects and the Advisory Board members, we designed and used an online survey to get feedback on the TRUESSEC Criteria Catalogue as described in deliverable “D4.3 First draft Criteria Catalogue and regulatory recommendations”. This survey was promoted to a wide audience through the project’s Twitter account as well as by direct contact within the partners’ networks. However, although we are confident that the survey reached a wide audience, completed responses were much lower than expected and numbered about 20. As a result, further surveys towards the end of the project have not been implemented yet, but once the project results are final, the TRUESSEC recommendations on labelling may be summarised and sent out to stakeholders, particularly policy makers and businesses, for feedback using a short survey.

4.2.2.1.5. Community Projects' Blog (previously called Ideas) (<https://truessec.eu/ideas>)

In this section, members of TRUESSEC and other projects can create references to ongoing activities and initiatives related with the goals of TRUESSEC. This section was created to allow the SHOP platform’s community to publish and debate aspects related to trust-enhancing labels and various certification and trust mechanisms. This section allows participants to initiate debates, through posting on the site, and to carry on debates, through commenting on posts.

4.2.2.1.6. News

In the second year of the project, a new News section⁵ was created aimed at posting any articles related to the project that do not fit in the Debates or the Blog sections of the SHOP.

4.2.2.1.7. Library (<https://truessec.eu/library>)

This section will act as a library of TRUESSEC deliverables and other documents of any kind related to the TRUESSEC project and our mission, whether generated internally or externally by others, e.g. those referenced in the Community Projects' Blog section.

As a way of keeping the SHOP platform simple and clean, but resourceful, the Library section will be used to store all TRUESSEC generated or related material, so they can be referenced across the SHOP platform and provide support to visitors. Material in the Library can also be referenced externally in other sites and publications.

4.2.2.2. Recruitment

The strategy for recruitment of members to the SHOP platform can be seen in Figure 4. Table 1 shows which Project WPs and / or people were responsible for each Process.

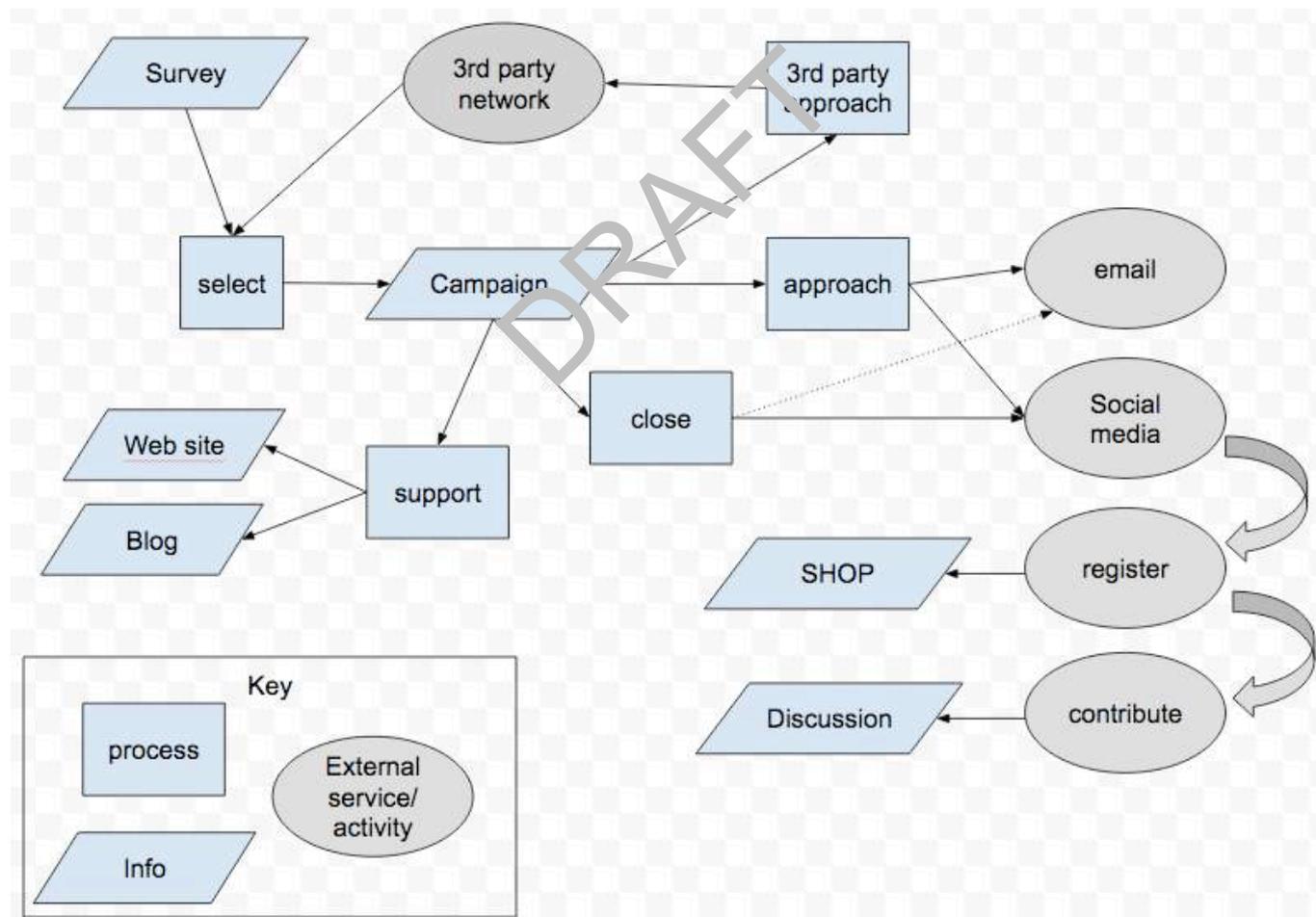


Figure 4. process of recruiting members to SHOP, for a given Campaign.

⁵ <https://truessec.eu/news>

<i>Activity</i>	<i>Project</i>
Manage Campaign	WP2/T2.2
Select Distribution List	WP2/T2.2 with input from most relevant WPs
Support Campaign	WP9
Manage 3 rd party	WP with link to 3 rd party n/w
Manage Pipeline	WP2/T2.2
Approach Contact	WP2/T2.2
Close Prospect	Allocated WP person

Table 1. Responsibilities for activities.

Again, as discussed in section 3.2, recruitment to the SHOP platform has met with considerable difficulty. As well as the reasons provided in that section, the need to log in to the SHOP platform may have been a barrier to engagement with the platform. However, a completely open access to post and comment on the site would not have been a practical solution to ensuring the quality of content and debate. This is, of course, a moot point.

4.2.2.3. Roles

Roles are described in more detail in TRUESSEC deliverable “D2.1 Multi-stakeholders platform – Online Platform: SHOP”⁶.

As well as anonymous, unregistered visitors, the SHOP platform supports three roles:

1. Authenticated user,
2. Moderator; and
3. Administrator.

So that:

- Once a visitor registers on the SHOP, they become a registered user. The system then authenticates a registered user each time they log on to the SHOP, where they are then considered an *Authenticated user*. Authenticated users are allowed to introduce comments, interacting with the platform.
- A *Moderator* role is reserved for Project Members who are allowed to create new content aimed to communicate with stakeholders and to stimulate interaction with them.

⁶ https://truessec.eu/sites/default/files/evidence/d2.1_multi-stakeholders_platform_-_online_platform_shop_v1.pdf

- A *Moderator* role will be assigned by an *Administrator* after authenticating the identity of the registered user as one with moderator privileges.
- An *Administrator* is responsible for managing users' roles on the SHOP and publishing content introduced by *Moderators* and *Authenticated users*. Administrators are also responsible for removing content reported as inadequate for the TRUESSEC website.

4.2.2.4. Populating the SHOP

The process for populating the SHOP can be found in TRUESSEC deliverable “D2.1 Multi-stakeholders platform – Online Platform: SHOP”, which details the platform’s description and user guidelines.

4.2.3. Project Web Platform (for internal project exchanges, i.e. not the SHOP)

To support confidential internal project communication among consortium members, the CyberConnector platform (<https://cyberconnector.eu/>) has been used. This opportunity was identified through collaboration with a sister project, HERMENEUT.

CyberConnector is a platform open for private organisations, public administrations, CERTs, law-enforcement agencies and individuals to create and enhance collective knowledge and encourage communication. The platform facilitates the sharing of all types of internal project communications, including discussion forums, WP specific folders, a project Wiki and calendar. Figure 5 shows the TRUESSEC file structure on the platform.

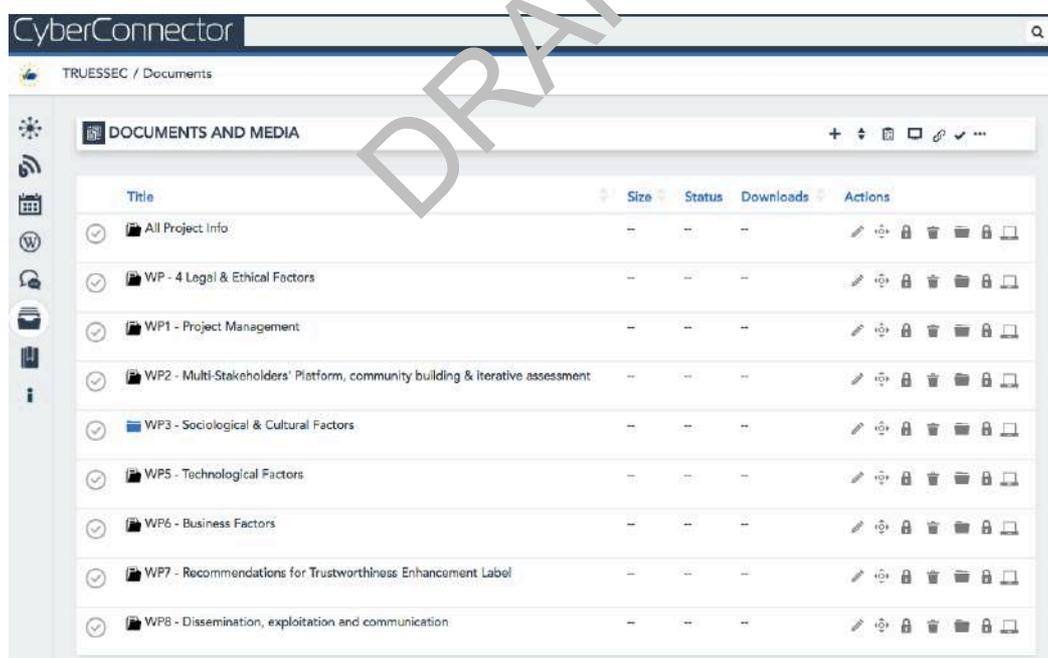


Figure 5. Internal communication file structure.

4.2.3.1. Internal Project Meetings

The project coordinator (DIGICAT) has chaired regular project meetings, and the project has had four full face-to-face management meetings which are detailed below:

- Digital Catapult Centre, London, UK – 24th January 2017

Dissemination level: PUBLIC

- Universidad Politécnica de Madrid, Spain – 4th & 5th July 2017
- University of Graz, Austria – 27th June 2018
- University of Lille, France – 11th December 2018

From M8, when SUPPA work started to yield findings, the project coordinator has also facilitated regular interdisciplinary meetings that seek to encourage interactions across the disciplines and to draw together common strands across them. These activities have been augmented by online interactions on CyberConnector and complemented by more ad hoc interactions between those working in various disciplines.

Individual work package leaders have organised meetings as necessary.

4.3. Common promotional material

4.3.1. Brochure

Figure 6 shows the brochure created to support all partners in the promotion of TRUESSEC.eu. This brochure contains information on the project objectives, information about the project consortium and our key aims. The brochure is available in PDF format, which partners can distribute physically or digitally.

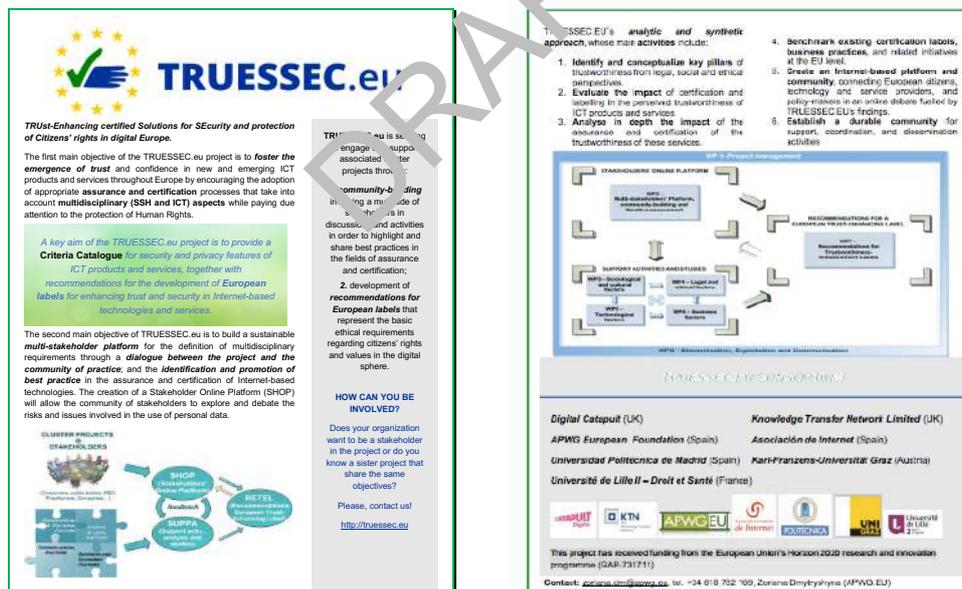
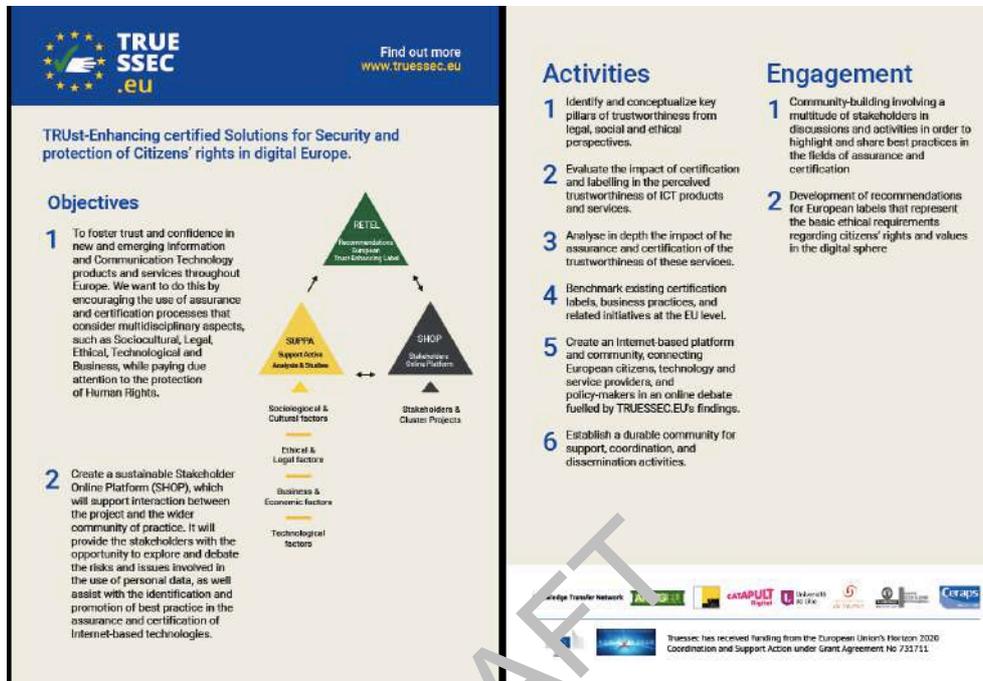


Figure 6. TRUESSEC.eu Brochure.

A new brochure was produced in the second year of the project and is shown in Figure 7.



TRUESSEC.eu Find out more www.truessec.eu

TRUSt-Enhancing certified Solutions for Security and protection of Citizens' rights in digital Europe.

Objectives

- To foster trust and confidence in new and emerging information and Communication Technology products and services throughout Europe. We want to do this by encouraging the use of assurance and certification processes that consider multidisciplinary aspects, such as Sociocultural, Legal, Ethical, Technological and Business, while paying due attention to the protection of Human Rights.
- Create a sustainable Stakeholder Online Platform (SHOP), which will support interaction between the project and the wider community of practice. It will provide the stakeholders with the opportunity to explore and debate the risks and issues involved in the use of personal data, as well as assist with the identification and promotion of best practice in the assurance and certification of Internet-based technologies.

Diagram: A central triangle with RETEL (Recommendation Europe Trust Enhancing Label) at the top, SERPA (Support Active Analysis & Studies) at the bottom left, and SHOP (Stakeholder Online Platform) at the bottom right. Below SERPA are factors: Sociological & Cultural, Ethical & Legal, Business & Economic, and Technological. Below SHOP is Stakeholders & Citizen Projects. Arrows connect the three main components.

Activities

- Identify and conceptualize key pillars of trustworthiness from legal, social and ethical perspectives.
- Evaluate the impact of certification and labelling in the perceived trustworthiness of ICT products and services.
- Analyse in depth the impact of the assurance and certification of the trustworthiness of these services.
- Benchmark existing certification labels, business practices, and related initiatives at the EU level.
- Create an Internet-based platform and community, consisting European citizens, technology and service providers, and policy-makers in an online debate fuelled by TRUESSEC.EU's findings.
- Establish a durable community for support, coordination, and dissemination activities.

Engagement

- Community-building involving a multitude of stakeholders in discussions and activities in order to highlight and share best practices in the fields of assurance and certification
- Development of recommendations for European labels that represent the basic ethical requirements regarding citizens' rights and values in the digital sphere

Logos: eEurope Transfer Network, CATAPULT Digital, University of Luxembourg, University of Applied Sciences, University of Vienna, CorapiS

TRUESSEC has received funding from the European Union's Horizon 2020 Coordination and Support Action under Grant Agreement No 731711

Figure 7. TRUESSEC.eu Brochure.

5. Events

As per the Grant Agreement, APWG, as WP8 leader, has worked with consortium partners to determine appropriate events and working groups, and to identify prospects to contribute to publications, where the dissemination impact will be good. This has been documented in to some extent in deliverable “D8.1 1st year dissemination plan and activities progress report”, but the opportunities have been extended since that deliverable was published; for example, the consortium has contributed a chapter to the Cybersecurity section of a book published by River Publishers, which captures the ECoSP 2018 workshop held in Hamburg.

The consortium as a whole has been committed to communicating and disseminating project developments at events that present opportunities to share and promote the campaigns associated with the project, which are detailed in section [3.3](#).

DRAFT

6. Communication activities and progress summary

The project has made substantial progress with regards to communication activity. At M12 the project had established a visual identity through a unique project logo and brand, identified key stakeholders and had a unified set of messages and campaigns to support the project objectives. The project also has live communication channels across web, social, email and face-to-face to further support promotion.

Moving forward, the consortium aims to take forward its work and recommendations through communication between the consortium partners and with their networks, and through sharing of information to allow for active engagement with key stakeholders using the SHOP, which we see as an ongoing asset, and through other established communications channels as described in this document.

DRAFT

7. Annexes

7.1. Annex 1

Example Presentation Template



TRUESSEC.eu

TRUSt-Enhancing certified Solutions for SEcurity and protection of Citizens' rights in digital Europe

DRAFT

Location
Date **/**/**

Title

Sub title

Content

- Bullet 1

Thank you



7.2. Annex 2

Standard letter head created to support the requirement for any official written communication.



TRUESSEC.EU 731711

For the attention of:

[Redacted]

Reference: Invitation and agreement to join the High-Level-Advisory Board of the TRUESSEC.eu Project

Dear [Redacted],

Thank you for your invitation to join the High-Level Advisory Board of TRUESSEC.EU, the H2020 project on TRUST-Enhancing certified Solutions for SEcurity and protection of Citizens' rights in digital Europe. I understand the main objective of the project is to foster trust and confidence in new and emerging ICT products and services throughout Europe. The aim is to encourage the adoption of appropriate assurance and certification processes. The project is 24 months in duration, and is scheduled to finish in January 2019.

This letter is to confirm that I, [Redacted] in my current position as [Redacted], am willing to contribute to the project as a member of a High-level Advisory Board.

Against this background I am ready to support this project in the following activities, subject to specific mutual agreement between the project coordinator of TRUESSEC.EU and me:

- enhancing the visibility of TRUESSEC.EU towards my network
- providing a political point of view on the questions the project is dealing with;
- liaising the project with other stakeholders (including from the policy making level) and activities
- acting as key-note speaker at events of TRUESSEC.EU
- reviewing and commenting on the draft project documents.

Expenses related to participation in the High-level Advisory Board will be compensated by the TRUESSEC.EU-project upon prior agreement and up to a limit determined appropriate.

Sincerely,

[Redacted signature block]

[Redacted]