European Commission | Horizon 2020 European Union funding for Research & Innovation

TRUESSEC.eu

Deliverable D7.3. Perceived levels of security & privacy

WP7

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:	D7.3
Status:	

Title of Document:	D7.3. Perceived levels of security & privacy
Dissemination Level:	Public

Author(s):	Jon Kingsbury (KTN), Iwona Wilk (KTN), Richard Foggie (KTN)
Reviewed by:	

Created on:	08/10/2018
Last update:	19/11/2018

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:	
Periodic report:	
Date of submission of the periodic report:	
Version:	2.6
Project website address:	http://truessec.eu/
The report is elaborated on the basis of the:	

CHANGE HISTORY

Date	Change	Author
08/10/2018	Draft with outline	Jon Kingsbury, Iwona Wilk (KTN)
25/010/2018	Background debates	Jon Kingsbury, Iwona Wilk (KTN)
02/11/2018	Section 3	Jon Kingsbury, Iwona Wilk, Richard Foggie (KTN)
09/11/2018	Conclusions	Jon Kingsbury, Iwona Wilk, Richard Foggie (KTN)
13/12/2018	First draft	Jon Kingsbury, Iwona Wilk, Richard Foggie (KTN)
	Quality review	Jose Maria del Alamo (UPM)
	Addressing reviewer's comments, final version.	Jon Kingsbury, Iwona Wilk, Richard Foggie (KTN)

Disclaimer: This publication reflects only the views of the author/s, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Table of Contents

1. Introduction

1.1. *TRUESSEC.eu Work Package (WP) 7 context and motivation*

This document is the third deliverable from *TRUESSEC.EU WP7 Recommendations for Trustworthiness Enhancement Label*. The main goal of WP7 is to define recommendations for trust-enhancing labels with the aim to promote the integration of tools that assess and certify the level of compliance of ICT products and services with regard security and privacy, so as to encourage their use of and ultimately enhance the perception of their trustworthiness. To achieve this objective, the WP7 in its first deliverable (D7.1) has carried out a study of 24 European and international labelling schemes identifying the incentives and barriers to their adoption. Then, the second deliverable (D7.2) focused on providing a transdisciplinary Criteria Catalogue for Trustworthy ICT products and services. This deliverable, (D7.3) was performed in parallel with the fourth deliverable (D7.4) and defines the relevant levels of conformance with regard to security and privacy. The fourth deliverable (D7.4) focuses on develop methodological guidelines for assessment, certification, and labelling for trustworthy ICT products and services.

1.2. *Relationship to other TRUESSEC.eu deliverables*

This deliverable focuses on summarizing the debate and feedback to the TRUESSEC project via the SHOP platform; feedback from other, "sister" EU-funded research projects in our certification and labelling cohort; and from the number of debates on certification, labelling and trust that have been conducted as part of TRUESSEC's WP2. It also takes analysis from and combines the results of D7.1 (the evaluation of existing labels) and D7.2 (TRUESSEC's recommendations for a Criteria Catalogue for assurance and certification). TRUESSEC has also had considerable interaction with its Advisory Board, including a special advisory workshop held in London in February 2018, where input from the Board members has proved to be invaluable in shaping our thinking. This report, in summary format, analyses the perceived levels of security & trust for online services from within industry, citizens and other stakeholders to offer a conclusion that includes a list of considerations for future TRUESSEC deliverables. The purpose of this deliverable is to help inform the final recommendations that TRUESSEC makes to the European Commission in deliverables D7.4 and D7.5. In particular, it attempts to define some applicable levels of granularity for cybersecurity, based upon the feedback provided.

2. Background

2.1. *Core areas of Trustworthiness*

TRUESSEC.eu, taking account, on the one hand, the European values and fundamental rights and, on the other hand, the findings of legal, ethical, sociological, business and technological support studies, has agreed upon six Core Areas of trustworthiness, namely transparency, privacy, anti-discrimination, autonomy, respect, and protection.

- **Transparency.** - The ICT product or service is provided in line with information duties regarding personal data processing and the product/service itself.
- **Privacy.** - The ICT product or service allows the user to control access to and use of their personal information and it respects the protection of personal data.
- **Anti-discrimination.** - The ICT product or service does not include any discriminative practices and biases.
- **Autonomy.** - The ICT product or service gives users the opportunity to make decisions and respects those decisions. The ICT product or service also respects other parties'/persons' rights and freedoms.
- **Respect.** - ICT products or services are to be provided in accordance with the legitimate expectations related to them.
- **Protection.** - ICT products and services are provided in accordance with safety and cybersecurity standards.

On the basis of these Core Areas, the first draft of twelve criteria have been identified, which can be used to evaluate and compare the trustworthiness of ICT products and services: information, user-friendly consent, enhanced control mechanisms, privacy commitment, unlinkability, transparent processing of personal data, anti-discrimination, cybersecurity, product safety, law enforcement declaration, appropriate dispute resolution, and protection of minors[1].

2.2. *The TRUESSEC Debates*

To date, four TRUESSEC-specific debates have been held on the matter of labelling for certification and trust for online services. These are described below:

- **Business factors** debate, held at the Digital Catapult, London in September 2017.
- **Legal & Technology factors** – Annual Privacy Forum, Barcelona, in June 2018
- **Ethical Factors** – "In ICT We Trust conference", Graz in June 2018
- **Labelling & Certification** debate – European Cyber security Forum (CYBERSEC), Krakow, October 2018

In addition, TRUESSEC partners have participated in a variety of other European and international debates presenting the issues and work undertaken as part of the TRUESSEC project. Most of these

[1] More details can be found in D7.2

supplementary interactions are summarized on the SHOP platform and the full range of these is listed within WP 8.

3. Summary of feedback/insights

Broadly speaking, the insights presented to TRUESSEC around the scope and nature of certification and labelling are consistent with the conclusions provided by the deliverables D7.1 and 7.2. These are outlined in summary below.

3.1. *The "Tricky" Issue of Trust:*

The issue of "trusted service", its various definitions, and the application of technology, user experience and adherence to the increasing amount of Internet regulation and business best practices in order to enhance the notion of "Trust" in the perception of citizens, has been a constant subject area in the inter-disciplinary research process of the TRUESSEC project. At the MyData Conference in Helsinki during August 2018, TRUESSEC's central research objective – the Criteria Catalogue for enhanced trust – was presented. Feedback from this presentation was consistent with much of the debate from our various stakeholders. To summarise this, and the other relevant input around the topic of **Trust** we have received, includes:

- Trust (which includes the belief that the object of trust is trustworthy) is a process of continuous validation, not a one-time result of technical efforts. Context matters. Humans calibrate their trust depending on the interaction context.

- Feedback from both our Advisory Board and from several of the "sister" projects that presented at the "In ICT we Trust" conference in June 2018 highlight the importance of transparency in fostering trusted solutions. This often arose as a focus on the usability and ease of peer communication adopted by user-recommendation systems (for instance eBay, AirBnB, TripAdvisor), but from a technical point of view, transparency in how services are developed, patched and collect and process personal data secure are key areas which are likely to enhance user trust.

- Building trust is an exercise in communication (as is reflected in the TRUESSEC.eu criteria catalogue). The problem is how to communicate what has been done to foster security.

- There has been considerable debate about the role of the state in either helping or hampering the development of citizen trust in Internet services. On the one hand, EU regulation is seen as a progressive move to protect citizens. On the other, trust in giving personal information to state-owned organisations remains low.

- While much of TRUESSEC's work has focused on the privacy, cybersecurity and legal protections offered by the EU, the ethical issues of trust are clearly of growing concern to EU citizens. For instance, there is a growing perception around the ethics of online content – characterised by the increased media debate around "Fake News". Meanwhile, an enhanced use of Artificial Intelligence (AI) has given rise to emerging concern around the ethical decision-making process of machines and the potential for increased discrimination. These issues were covered in depth by the debates and conference organised by TRUESSEC in Graz. They have resulted in the TRUESSEC project being determined to focus on a solution which “goes beyond the current law”, in order to explore the potential for labelling which describes ethical approaches to concepts such as “justice”. TRUESSEC.eu locates the "core areas" of trust in ICT in: privacy, transparency, autonomy, anti-bias, respect and protection.

- A high-level criteria catalogue for trustworthiness – has been well received when presented to crowds at the various cybersecurity and privacy conferences attended by TRUESSEC partners, but criticized on the grounds that fundamental values are rather abstract and hence difficult to discern and evaluate for ordinary people. The final recommendation to arise from the catalogue should take account of integrating its principles in a “testable” and easy to understand format. This issue is consistent with the conclusions arrived at in the final section of D7.2.

- TRUESSEC’s recommendations will include the presentation of a draft online “transparency” survey, which will attempt to distil the criteria catalogue into a manageable set of Yes/No questions, with links to the relevant certification documents. This approach, which takes note of the type of industrial best practice outlined in D6.3 (namely, Transparency reporting), is consistent with the fact that no one single certification process exists which can cover the very wide range of applications for an EU label.

3.2. *Legal compliance and “Going beyond the current law”:*

- There has been significant debate with stakeholders about the concept of extending trust for online products and services beyond the current levels of legislation. This has been characterized within the TRUESSEC project as “going beyond the current law” to explore such areas as ethical considerations (for instance to avoid some areas of discrimination not covered by legal statute). This has generally been well received by audiences, both at TRUESSEC debates and at the various conferences where TRUESSEC has been presented.

- Throughout the project, those we have consulted with have highlighted the specific benefits of an EU regulatory regime, working with industry, which can take the lead globally to ensure that Europe remains at the forefront of both thought and industrial leadership. The conclusion is that such an approach offers the citizens of Europe the best protection of some of the less favourable aspects of the Internet while ultimately maximizing the potential for an effective digital single market across the continent.

- However, stakeholders have, at times, questioned the practicality of this aspiration, especially since many smaller organisations are currently grappling with new legislation, such as GDPR and the NIS Directive[2]. Therefore, the final recommendations must strive to meet the aspiration without swamping them with considerations that are onerous to them.

3.3. *Cybersecurity and levels of granularity:*

- As stated above, the cybersecurity community remains somewhat ambivalent about the use of labels to certify products and security. However, B2B certification, in the form of penetration testing, operational business practices (for instance adoption of ISO 27001 and others) is a standard requirement in many areas for business-to-business supply chain credibility.

- However, citizens/consumers tend to have a greater awareness of (and hence more comfort with) consumer services for scanning and fixing cybersecurity issues (for instance, Sophos home security systems). The D6.1, 6.2 and 6.3 deliverables highlighted the usage of endpoint security software that would be useful both for businesses moving to a “bring your own device to work” model of operation as well as citizens. In this case, certification is much less relevant than the security precautions protecting individual devices. Labelling which is compatible with these forms of security would go far in helping citizens to understand that they have a greater level of protection and hence would enhance trust.

- Deliverables D6.1 onwards also discuss the best practice of two-factor authentication as a valuable way of ensuring users are aware that they are, to some greater extent, being protected.

- At the Business Factors debate in London in September 2017, one of TRUESSEC’s Advisory Board members led a group discussion which highlighted that one important area of transparency for online products and services was to separate out security patch updates from feature updates. Information along these lines might be included as a relevant survey question in the draft recommendations.

- Some organisations, such as ARM Holdings plc, were particularly keen to demarcate particular elements of cybersecurity. For instance, there has been significant debate concerning the elements of personal information security versus cybersecurity focused on citizen safety. Since there already exists regulation around the safety of products within the EU (the CE mark), it has been suggested that this label be further extended into cyber-physical devices and services beyond their current applications (medical devices). The blurring between cybersecurity, safety, personal information security and ethical considerations was as apparent with the cybersecurity community we have consulted with as it has been with the other stakeholders.

[2] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

- Some aspects of cybersecurity should not be referred to in a transparency report, although they might well be subject to certain elements of certification, such as "red or white hat" penetration testing[3]. The obvious reason for this is that organisations are unlikely to benefit from being completely transparent about their methods of protection. This feedback was especially vociferous from the financial services and critical national infrastructure organisations that TRUESSEC has engaged with.

3.4. *The use of Labels:*

- There are no extant labels that integrate all four of the major areas of the TRUESSEC project (cybersecurity, data protection, consumer protection, ethics).

- Despite an increase in focus by European-wide, national and global organisations on certification processes[4] (an increasing number of which are specific either to individual sectors, levels of perceived risk, technologies and handling of data), labelling initiatives struggle to generate the engagement necessary to be acknowledged by the public.[5] It is naïve to rely solely on labelling to enhance perceived levels of trust.

- Labels, even the ones that are generated by user-feedback and thereby focus primarily on consumer usefulness and quality of service (for instance, Trustpilot), do not provide sufficient clarity on "hidden" trust issues, such as cybersecurity. For instance, in addition to the general lack of knowledge regarding cybersecurity measures undertaken by organisations, there is often also the misperception in the minds of citizens between self-assurance and 3rd party certification around security aspects of labelling.

- Most of the feedback (especially from the cybersecurity community) has been somewhat wary of labelling as a solution because of an acknowledgement that security is a dynamic, ongoing issue for service providers (dynamic, for instance, in the form of software patches or new classes of potential attacks). Effective cybersecurity is based upon continued best practices, rather than a "snapshot" in time, which produces a single label. Nevertheless, that feedback notwithstanding, certification retains a high level of attention and usage within specialized business supply chains.

- In key areas of security, cloud computing, GDPR and organizational assurance within companies, much progress has been made to understand and propagate certification, both at a national and European "framework" level. There is consequently significant work still to do within Europe to highlight this good work in order to boost levels of citizen trust for services that are complying with enhanced regulation.

[3] More details around testing, including "White and Black Box" testing are described in D7.4

[4] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework

[5] D7.1 section IV - Conclusions

- As ENISA has stated: “it has become clear that there is no one-size-fits-all approach to certification and labelling.”[6] Its feedback to TRUESSEC echoed the findings from its 2017 report “ICT security certification in EU”, which showed that a majority of respondents favoured a common label across the EU: “Such a label would indicate that the products have been certified within a certification scheme in accordance with EU rules and provide visual notice that product’s features comply with specific requirements.”[7] It should be noted that the idea of a common, EU-wide label, which confirms global standards of certification, goes beyond ENISA’s current strategic focus of a cybersecurity “framework”.

- Labelling for Internet of Things (IoT) devices is an **urgent area of concern**. This issue plays to the EU-wide focus on “Secure by Design” and matches policymakers’ worries about poor security practices in Internet-connected consumer devices, where established CE labelling does not currently cover cybersecurity risks to safety or privacy[8].

- There is a need to tread a careful path between the trustworthiness of a label and the relative ease and affordability of which it can be adopted, especially by business.

- Governance issues abound. Since there is no one organisation that offers a label across all four areas of concern, there is also no one organization that currently certifies for all of these areas. This is an issue that is further explored in D7.4 (methodological recommendations) and will be revisited in D7.5 (implementation roadmap), when it is proposed that a relevant organization (potentially ENISA) should have gubernatorial oversight over the issuing of an EU trust label

[6] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwinpY7396HeAhVLIlAKHWN0Am0QFjABegQICBAC&url=https%3A%2F%2Fwww.enisa.europa.eu%2Fpublications%2Fcertification_survey%2Fat_download%2FfullReport&usg=AOvVaw2jiEQjdrWJMjs_9mqzwIQM

[7] Reference as above, page 12

[8] The arguable single exception here is healthcare, which tends to be regulated and certified according to CE guidelines.

4. Conclusions

In providing a high-level summary of the various stakeholder interactions, above, our subsequent deliverables will have some useful insights around the interdisciplinary approach we have adopted. There has been significant interest in the TRUESSEC approach from stakeholders, especially to re-think some of the issues around trust and security from a wide range of perspectives – often bringing different skillsets and insights together where the actors involved would otherwise not connect. The key challenge for the final recommendations will be the need to balance the admirable goal of ethical principles outlined in the Criteria Catalogue with the practical issues around certification and labelling – such as awareness; the certification process; and the oversight of testing and standards as the Internet evolves. These issues are discussed in the deliverable D7.4 and in the implementation roadmap to be outlined in D7.5.

5. Footnotes and References

[1] D7.2

[2] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

[3] More details around testing, including “White and Black Box” testing are described in D7.4

[4] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework

[5] D7.1 section IV - Conclusions

[6] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwinpY7396HeAhVLIlAKHWN0Am0QFjABegQICBAC&url=https%3A%2F%2Fwww.enisa.europa.eu%2Fpublications%2Fcertification_survey%2Fat_download%2FfullReport&usg=AOvVaw2jiEQjdrWJMjs_9mqzwIQM

[7] Reference as above, page 12

[8] The arguable single exception here is healthcare, which tends to be regulated and certified according to CE guidelines.

Dissemination level: <public >

This document was produced under the TRUESSEC.EU project (EC H2020 CONTRACT: 731711).