

On the security, privacy and usability of online seals

An overview

Version December 2013





About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Hannes Tschofenig, NSN, Finland

Melanie Volkamer, CASED/TU Darmstadt, Germany

Nicola Jentzsch, DIW Berlin, Germany

Simone Fischer Hübner, Karlstad University, Sweden

Stefan Schiffner, ENISA

Rodica Tirtea, ENISA

Contact

For contacting the authors please use sta@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of-the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

© European Union Agency for Network and Information Security (ENISA), 2013

Reproduction is authorised provided the source is acknowledged.

Executive summary

This report analyses the conditions under which **online security and privacy seals (OSPS)** can be deployed to support users to make an informed trust decision about Web services and their providers with respect to the provided security and privacy. This report is motivated by the numerous policy documents, that mention marks, seals, logos, icons, (collectively referred as OSPS) as a mean enabling users to judge on the trustworthiness of services offered on the Web.

The field of OSPSs has also developed in maturity. Therefore, we aim at analysing the current situation and identified key challenges for online signals in practise. Based on these challenges, this report identifies possible solutions and corresponding recommendations and next steps that ENISA and other stakeholders should follow for enabling users in judging on the trustworthiness of services offered on the Web.

The key challenges and corresponding recommendations of this report are:

- **Lack of awareness.** Many users are not aware of the existence of OSPSs at all. Furthermore, they are not aware on which signals they can and should base their decision on as there are many including a few which are not trustworthy. **Partners from the Safer Internet Programme, working groups on awareness raising from different institutions should provide educational material to spread knowledge of the existence and meaning of OSPS.**
- **Lack of standards.** As a result of different design requirements and business models a broad range of seals is available today. This variety makes it difficult for users to decide whether one seal provides stronger protection than another. **Standardisation of OSPS will be important to make them easily recognisable and correctly understood.** Standardisation bodies **should also define standards for trustworthy OSPSs. This will also improve user experience as they do not need to remember as many OSPS providers as they need today.**
- **Lack of validity checks.** Most of those who are aware do not check the validity of the online signals; even worse some signals are merely images on the web page and as such very hard to check. Hence, forgeries are possible and easy. **Service providers need to provide users with OSPSs that can be automatically checked (for example, in the form of cryptographic certificates). Web browser developers need to implement these automatic checks.** However, pure market forces are not very likely to lead to this ideal situation. **Thus, policy makers (at EU level and national level) should investigate the enforcement of corresponding standardized mechanisms for Web browsers. Furthermore, they should investigate strategies in case promises made regarding seals are not met.**
- **Lack of usability.** Given the intrinsic complexity of Web services it is very likely that the result of an evaluation by an OSPS issuer is not just 'pass' or 'fail' but multi-dimensional. As there is neither space nor are users generally willing to read long explanations, **researchers and web designers need to develop corresponding icons communicating the results. These icons could be based on research on privacy icons.** Note, designers need to take care of cultural and legal differences.
- **Lack of presence.** The effectiveness of trust signals needs to be improved, and this is likely to occur when a more mature market with well-known players (online service providers) is achieved; and also when users attain a more precise understanding of their meaning of a trust seal in a web page. **Regulatory bodies at EU and national level should set incentives for service providers to obtain online security and privacy seals.**



Table of Contents

Executive summary	iii
1 Introduction	1
2 The policy context	3
2.1 Strategic policy documents related to ICT and cyberspace	3
2.2 Protection of personal data in the EU	3
2.3 Communication on e-commerce and other online services	5
2.4 Community code relating to medical products	6
3 Security and privacy requirements and evaluation	7
3.1 Challenges	7
3.2 Solutions	8
4 Communication Issues	10
4.1 Challenges	10
4.2 Solutions	11
5 Verification of online security and privacy seals	14
5.1 Challenges	14
5.2 Solutions	14
6 Economic aspects	15
7 Summary and recommendations	18

1 Introduction

In online environments, end users are interacting with a variety of Web services on a daily basis. Many Web services already exist and more and more are provided every day. Users have to make decisions about the level of trust they place in these services. This trust decision does not only include the trust that a certain service level is provided, but has also a range of privacy and security implications.

For many users and for various reasons (including their lack of knowledge, access, and time), it is difficult (if not impossible) to make a well-grounded trust decision. Hence, policy makers propose in several policy documents (see Section 2) the establishment of **online security and privacy seals (OSPS)**. The idea of online security and privacy seals is the following:

During an **evaluation** it is checked if a Web service of a provider fulfils **security and privacy requirements** that are defined for the respective OSPS. After a positive evaluation the OSPS is issued (usually) by a third party who was contracted to conduct the evaluation. Afterwards, this approval needs to be **communicated to the user** (e.g. in terms of self-claimed text and/or pictograms on the Web page, or as electronic certificate). In order to avoid fraud it must be possible to **verify** whether the provided information is authentic. These three steps form a **chain of trust** (Figure 1) that needs to be formed from the OSPS **issuer** to the awareness of the **user**. Thus, this approach is very similar to well-known and established approaches from real world such as TÜV¹, GS² and CE³.

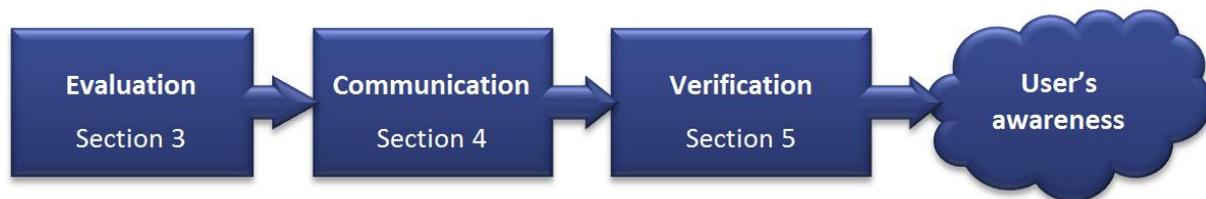


Figure 1 Trust Chain for Online Security and Privacy Seals

In this report, we aim to analyse this idea, identify **challenges** which should be addressed for a successful establishment of OSPS. The document provides **solutions** or directions for future research to tackle each of the identified challenges. In the case that there is not yet an appropriate solution available, we provide (research) directions to develop a solution and point to mitigation strategies.

Furthermore, the report reflects economic aspects of OSPSs. From a market perspective, their primary goal is to induce competitive pressure and steer the market towards more secure and privacy preserving Web services. They enable Web services to differentiate themselves from competitors by obtaining such OSPSs and by building up a good reputation in the market place.

Correspondingly, we first (Section 2) provide an overview of policy documents mentioning and/or recommending the establishment of OSPSs. Afterwards (Section 3), we analyse the first aspect of OSPS namely the **evaluation** by defining adequate security and privacy **requirements** as well as corresponding **evaluation methods**. In Section 4 we address **communication challenges** and corresponding **solutions**. Moreover, in Section 5 we address **verification challenges** and the

¹ Technischer Überwachungs-Verein, English: Technical Inspection Association, associa

² German seal for products; its certification process is regulated in "Produktsicherheitsgesetz"

³ http://ec.europa.eu/enterprise/policies/single-market-goods/cemarking/index_en.htm



appropriate **solutions**. We analyse **economic aspects** of OSPSs (Section 6) and conclude the paper with a list of recommendations (Section 7). Finally, we include two annexes, which provide in-depth insights on security and privacy assessment challenges, and research directions in privacy icons as tool for human computer interaction.

2 The policy context

Recently published policy documents refer to OSPs that would improve the interactions of users in online environments. In this section we set the current context by examples; it is not intended to list all the policy documents that mention signals.

2.1 Strategic policy documents related to ICT and cyberspace

Digital Agenda for Europe

The *Digital Agenda for Europe*⁴, one of the European Commission (EC) initiatives of the Europe 2020 Strategy, identifies policies and actions to maximize the benefits of Information and Communication Technologies (ICT). Actions are proposed as part of the modernization of the European personal data protection regulatory framework in order “to make it more coherent and legally certain”. For example, action #4 is specifically dedicated to the “review of the European data protection regulatory framework with a view to enhancing individuals’ confidence and strengthening their rights” and creating “EU online trustmarks⁵ for retail websites”. Such an action is proposed to improve the competition, to enhance consumer protection and to allow for comparability of prices and products across the EU.

The Cybersecurity strategy of the European Union

As a step to implement the Digital Agenda, the European Commission together with the High Representative of the Union for Foreign Affairs and Security Policy, have published⁶ a cybersecurity strategy for the European Union in February 2013. The cybersecurity strategy⁷ – “An Open, Safe and Secure Cyberspace” – provides a list of priorities and actions aimed at enhancing cyber resilience of information systems, reducing cybercrime and strengthening EU international cyber-security policy and cyber defence, while promoting values of freedom and democracy and ensuring the safe growth of the digital economy.

As a part of this strategy, ENISA together with all relevant stakeholders is invited to contribute in developing technical and good practice guidelines for Network and Information Security (NIS) that take into account data protection. With relevance to this paper, the strategy proposes to increase cooperation and transparency about security in ICT products and the improvement of “*the information available to the public by developing security labels or kite marks helping the consumer navigate the market.*” to promote a single market for cybersecurity products.

2.2 Protection of personal data in the EU

Transparency of personal data processing for the data subjects is an important legal privacy principle. Here, data processing is considered transparent for data subjects if they are in control of their data and gave informed consent to the processing.⁸ Information that needs to be given to data subjects for a valid consent covers typically the elements of information listed in Article 10 of the Data

⁴ European Commission, A Digital Agenda for Europe, COM(2010)245, 19.05.2010, available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245R%2801%29:EN:NOT> (last accessed on 30.10.2012).

⁵ Key words are underlined by editor in the cited paragraphs (here and in following subsections) to highlight the message.

⁶ EU Cybersecurity plan to protect open internet and online freedom and opportunity, Reference: IP/13/94, 07/02/2013 available at: http://europa.eu/rapid/press-release_IP-13-94_en.htm?locale=en

⁷ Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - JOIN(2013) 1 final, 7/2/2013, available at: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667

⁸ Art. 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent, 01197/11/EN, WP187, adopted 13th June 2011.

Protection Directive 95/46/EC⁹; includes at the very least the identity of the data controller, and the data processing purposes. Moreover, further information needs to be given in so far as such further information is necessary to guarantee fair data processing; this can include the recipients or categories of recipients of the data, whether replies to questions are obligatory or voluntary, and information about the individual's rights.

Recently, the Art.29 Working Party discussed in their Opinion 5/2012 on Cloud Computing¹⁰ a lack of transparency with regard to the cloud services' processing operations. Privacy threats may arise from the controller not knowing or not informing the data subjects about the chain with multiple processors and subcontractors, different geographic locations, transfer to third countries outside the EEA or disclosure requests by law enforcement. The later aspects are important even if data is processed at a services side located in the EEA; data transfers to the US may take place and become subject for requests by US law enforcement services.

Moreover, data subjects are often not well informed about the applicable consumer laws and rights, especially if cloud brokers or mediators are involved in cross-border e-commerce transactions.¹¹

Privacy notices in the form of long legal statements are, however, usually neither read nor easily understood by end users. In Section 5.2, we will discuss work on how such information to be provided in privacy policies can be complemented by policy icons for illustrating policy elements in an easily noticeable and comprehensible manner.

The Communication on personal data protection

As a key objective of the comprehensive approach on data protection in the general frame of the strengthening of the rights of the individuals, the Commission communication on a comprehensive approach on personal data protection in the European Union¹², supports the enhancement of the control of the citizens over their personal data. In this context, *"[...] the Commission will explore the possible creation of EU certification schemes (e.g. 'privacy seals') for 'privacy-compliant' processes, technologies, products and services."*

The proposed Regulation on data protection

In January 2012 the European Commission proposed regulation on data protection that will replace the existing Data Protection Directive.¹³ The proposal for the new regulation contains specific provisions relevant to certification, data protection seals, and marks. In Article 39, of the proposed regulation is stated *"[...] the Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors"* and further that *"the Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks"*.

⁹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L No. 281, 23.11.1995.

¹⁰ Art. 29 Data Protection Working Party, Opinion 5/2012 on Cloud Computing, 01037/12/EN, WP 196, adopted July 1st 2012.

¹¹ This was one of the elicited challenges of an HCI focus group meeting organized by the EU FP7 project A4Cloud with participants from Konsument Europa, which took place in February 2013 at Karlstad University (see A4Cloud Deliverable D:C-7.1 on General HCI Principles and Guidelines – forthcoming).

¹² European Commission, A comprehensive approach on personal data protection in the European Union, Communication COM(2010) 609, 04 November, 2010, p. 9, available at: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf (last accessed on 04.10.2011).

¹³ European Commission, Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 25 January 2012, available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (last accessed on 20.02.2012)

The European Parliament (EP) provided amendments¹⁴ in January 2013; and some of the amendments mention standardized icon-based representations. The amendment 51 for preamble (77) adds the need for *reliable and verifiable* possibilities to assess the seals and marks used: “*In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms, data protection seals and marks should be encouraged, allowing data subjects to quickly, reliably and verifiably assess the level of data protection of relevant products and services.*” Although paragraph 3 of article 39, which referred to delegated acts of the EC for laying down technical standards for certification mechanisms and data protection seals and marks, was removed, new paragraphs were introduced, namely:

- paragraph 1a stating “*The data protection certification mechanisms shall set down the formal procedure for the issue and withdrawal of a data protection seal or mark and ensure the financial and factual independence and proficiency in data protection of the issuing organisation. The criteria for certification, the individual results of a successful certification and an intelligible meaningful summary justification shall be made readily accessible to the public.*”
- paragraph 1b says “*The data protection certification mechanisms shall in particular ensure compliance with the principles set out in Article 5, 23 and 30, the obligations of the controller and the processor, and the data subject’s rights.*” In the Justification is mentioned that “[a]ny certification mechanisms must set out the formal procedure for the issuance and withdrawal of the seal and must be independent” and “[a]ny certification mechanisms must ensure compliance with data protection principles and data subject rights”.

The need for icon-based information about privacy policies is stated in the EP report in Amendment 118, referring to Article 13: “*Information for data subjects shall be provided in a format offering data subjects the information needed to understand their position and make decisions in an appropriate way. Therefore the controller shall provide and communicate its data protection policies through an easily understandable icon-based mode of description for the different types of data processing, their conditions and consequences.*” In the following Amendment is further stated that icon-based mode of description should cover “[...] *the nature of the processing, duration of storage, transfer or erasure of data by establishing icons or other instruments in order to provide information in a standardised way.*” Note: at the moment of writing, the draft regulation on data protection is still highly volatile and hence the above remarks might not reflect the situation at reading time correctly, cf MEMO/13/923 22/10/2013¹⁵ of the European Commission.

2.3 Communication on e-commerce and other online services

The Communication¹⁶ “*A coherent framework for building trust in the Digital Single Market for e-commerce and online services*” published in January 2012, list among its 5 priorities the improvement of “*operator information and consumer protection*”. Action 9 of the communication includes “*contributing to the creation of trustmarks*” according to the recent directive on Directive

¹⁴ European Parliament report on the Data Protection Regulation:

http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf

European Parliament report on the Data Protection Directive:

http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/923/923072/923072en.pdf

EC memo “Commission welcomes European Parliament rapporteurs’ support for strong EU data protection rules”, 8th on January 2013, available at: http://ec.europa.eu/commission_2010-2014/reading/pdf/m13_4_en.pdf

¹⁵ http://europa.eu/rapid/press-release_MEMO-13-923_en.htm

¹⁶ European Commission, COM (2011)942, 11.1.2012 “A coherent framework for building trust in the Digital Single Market for e-commerce and online services” context described at: http://ec.europa.eu/internal_market/e-commerce/communication_2012_en.htm (last visited October 2012), available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0942:FIN:EN:PDF> (last visited October 2012).

2011/62/EU of 8 June 2011, amending Directive 2001/83/EC on the Community code relating to medicinal products for human use.

2.4 Community code relating to medical products

The Community code relating to medical products for human use¹⁷ has been amended (Directive 2011/62/EU of 8 June 2011) and the new consolidated version specifies the common grounds for “*common logo [...] clearly displayed on every page of the website that relates to the offer for sale at a distance to the public of medicinal products.*” A harmonized, common logo across the EU requires, as stated in the article 85c of the Directive, implementation acts to address “*the technical, electronic and cryptographic requirements for verification of the authenticity of the common logo*” and “*the design of the common logo*”.

¹⁷ The consolidated version was published in 2011, after the publication of Directive 2011/62/EU of 8 June 2011 amending Directive 2001/83/EC on the Community code relating to medicinal products for human use, as regards the prevention of the entry into the legal supply chain of falsified medicinal products. OJ L 174 of 1.7.2011 available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2001L0083:20110721:EN:PDF> (last visited October 2012).

3 Security and privacy requirements and evaluation

Users' trust in a service is roughly defined as the users perceived likelihood that their requirements to the service are fulfilled. This includes requirements w.r.t. security, privacy, data protection, and quality of service. In this report, we focus on privacy and security requirements. Due to the non-functional nature of these requirements, users cannot assess directly if the requirement is fulfilled or not. However, the evaluation whether a service provides adequate security and privacy, can be done by a third party (the OSPS issuer).

There are many factors to consider when evaluating the trustworthiness (i.e. privacy and security) of Web services such as scope, granularity, validity period, etc. (see Annex A for detailed description of all these factors). Currently, different OSPS issuers have different scopes and focuses. Some narrowly focus on privacy compliance whereas others also consider technical security and privacy aspects. Evaluation methods range from self-disclosure to in-depth penetration tests and on-site audits, see Annex A: . Consequently, different issuers consider different sets of requirements and different evaluation methods which they are supposed to describe in the seal description e.g. on their Web page.

In this section we describe the problems and challenges with the current requirement definitions and evaluation approaches.

3.1 Challenges

With the existence of OSPS we can observe a **shift** from users making trust decisions about Web services **to making trust decision about OSPS issuers (Challenge 1)**. However, issuer regulation is almost non-existent, making the situation even worse since everyone can become an OSPS issuer.

Note that trust in OSPS has two aspects. One is, trust that the OSPS issuers **properly check** what they claim to check. In addition, trust that the OSPS issuers **select adequate security and privacy requirements** and fitting evaluation methods. But, it is not clear what adequate means and for whom it is adequate. Currently, there is a wide range of OSPS issuers, which use different evaluation methods. From this starting point, it is hard if not impossible to agree on a common list of adequate security and privacy requirements and corresponding evaluation methods. Thus, users have themselves to actually check and **judge the expressiveness of the undertaken evaluation**, i.e., whether the addressed requirements and applied evaluation methods are adequate for them (**Challenge 2**). However, the lay users lack sufficient expertise in the field to enable them to make an informed decision. As such, users cannot judge on the meaning and value of OSPS. For example, when asking participants about the meaning of an OSPS, misconceptions have been identified¹⁸ as some users believed that OSPSs indicate that a web page is free of viruses or that it has been verified by the company that provides the payment method. This situation can lead to misinterpretations by users: e.g., it might be that only the data protection policy as such has been evaluated while users believe that its implementation has been evaluated too. Thus users assign a higher trust level to the corresponding Web service than appropriated.

Note even for experts, it is a cumbersome and error prone task to decide if the undertaken evaluation is adequate. In addition, experts are expensive. This forces service providers to trade off evaluation quality and the cost for the evaluation (see also Section 6 for a discussion of the economic aspects).

¹⁸ I. Kirlappos, A. Sasse, N. Harvey; Why trust seals don't work: A study of user perception and behaviour, University College London, Department of Computer Science

Another challenge is that it is difficult if at all possible for the user to **check whether (exactly) the same service** is in place than the one that has been evaluated (**Challenge 3**).

3.2 Solutions

In this section we present solutions and ideas to address the challenges presented above.

Solution 1. There exist different models to address the challenge that users need to judge on the trustworthiness of certificate issuers in other security contexts: e.g. (1) The Common Criteria model distinguishes between the certificate issuer and the evaluation body which are independent institutions. The evaluation body is accredited by the certificate issuer. Furthermore, the evaluation body conducts the evaluation according to the Common Criteria rules and the certificate issuer observes the process and finally issues the certificate. Thus, users do not need to know and judge on the trust of all the different evaluation bodies but only on the few certificate issuers (usually only one institution per country) (2) Hierarchical public key infrastructures such as the SMIME certification model, distinguishes between root CAs and 'standard' CAs. Again the root CAs accredits the standard CAs to issue certificates. However, root CAs are not involved in the process of issuing certificates. Similarly to the previous model, users only need to know and judge on the trust of all the standard CA but only the few root CAs. Correspondingly, one of these two models is recommended for OSPs in order to address Challenge 1. As such, standards for OSPs issuer accreditation are required.

Solution 2. The problem that different issuers use different requirements and different evaluation methods. In addition, it is up to the user to decide which are adequate and which not - this should be addressed by corresponding standards. These standards should define for which type of Web service (including which type of data requested from the user) which security and privacy requirements need to be ensured, how the OSPs issuers have to conduct the evaluation and how often it needs to be repeated. Due to the economic influence (see Section 6), future research is necessary to figure out whether one set of requirements and evaluation methods for each Web service type is adequate and as such either a Web service ensures them or not or whether different levels are distinguished (similar to the different evaluation assurance levels in the Common Criteria context). Note, the first case is easier to communicate to the user than the later one (see Section 4 for communication aspects).

Challenge 3 is not entirely solvable. OSPs need to be bound to the originally certified service. As long as a service is non-customized software only, e.g., an app, the OPSP can be bound to the service using a cryptographic hash. However online services are often highly customized and contain non-electronic parts. Here traditional policy enforcement can help, that is, OSPS requires regularly re-evaluation. Moreover, this re-evaluation should happen randomly to avoid that the service provider can prepare to deliver better service just for the time of the evaluation. Moreover, issuers need to take measures that allow service users to file complaints, if there is a suspicion of fraud. Furthermore, a non-technical solution could be the implementation of liability rules by the regulators.

Additional remarks

In the context of this year's work, ENISA in parallel to this activity also conducted a study of the experiences from using certification schemes in case of Information Security Management Systems.



The results of this work are reported in the ENISA survey¹⁹ on certification practice in EU Member States. Although the authors understand that it is not sound to assume that the experiences from the deployment and use of security certification schemes can also be applicable in the case of privacy seals, we believe that it is of worth to note that in the context of the privacy debate, seals are considered as means to increase the trust of users towards an offered online services. However, the experience from the use of security seals indicates that the biggest benefit coming from their deployment and use is not that much on increasing the level of security that users feel but rather in improving the level of preparedness of an organisation that deploys them.

¹⁹ Security certification practice in the EU. Information Security Management Systems - A case study, ENISA study, 2013, available at: <http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/security-certification-practice-in-the-eu-information-security-management-systems-a-case-study>

4 Communication Issues

The result of the OSPS issuers' evaluation about a service needs to be communicated to the user. Obviously, it is important that users are aware of OSPS in general but also that the evaluation results are communicated in a way that users perceive them and take them into account when judging on the trustworthiness of the offered Web service. Only if this is the case, can the user make an informed decision about the trustworthiness of an offered Web service. Currently, OSPS issuers usually provide only one OSPS and the evaluation result is either pass or fail. In case of pass the result is communicated by integrating a corresponding pictogram on the service provider's web page. The position of the pictogram on the web page is decided by the Web service.

4.1 Challenges

In the empirical study on OSPSs conducted in Germany²⁰ only 40% out of 112 respondents knew the concept of OSPSs in the web. Similar results were reproduced for the entire European population by The European Consumer Centres' Network.²¹ Without **knowing this concept** it is obviously not possible to consider OSPSs when judging the trustworthiness of Web services (**Challenge 1**).

Nowadays, OSPS are not the only security and privacy indicator users consider. Others are e.g. the green bar in terms of an extended validation certificate or results from external services such as Web of Trust. Several researchers showed that average users do not consider or only rarely consider any of these security and privacy indicators when assessing the trustworthiness of a service: Turner et al.²², for instance, showed that the service provider's reputation, previous experiences with the service and third party recommendations play a role for ordinary users to feel secure when using a web service. Egelman et al.²³ showed that so-called trust signals for end users on a web page are:

- look and feel of a web page (including design, writing, and grammar, no pop ups and no/less advertisement),
- the fact that the web page and the company are known (also phishing Amazon pages look trustworthy as Amazon is well known and the page looks the same),
- the data requested (users seem to be scared if too much information is requested).

Researchers also evaluated the relevance of OSPSs for users' trust decisions while interacting with a Web service: An empirical study on OSPSs conducted in 2011 in Germany²⁰ showed that OSPSs are not the main signal for users to judge a Web service as trustworthy. On the question how to decide whether or not to trust a Web service only 21% of the users selected "displaying an OSPS" as criterion of their decision. Similar results were found by an empirical study conducted in the UK²⁴: several web pages were presented to the 62 participants to assess their trust decisions; some displayed OSPSs while others did not. It turned out that 38% of the participants did not notice any

²⁰ M. Volkamer, F. Karayumak, M. Kauer, D. Halim and R. Bruder; Security versus Trust Signals in 2011 in Germany

²¹ Trust marks report 2013, "Can I trust the trust mark?", ECC-Network, 2003, available at (last visited December 2013):

<http://www.konsumenteuropa.se/PageFiles/159275/Trust%20Mark%20Report%202013.pdf>

²² Turner, C. W., M. Zavod & W. Yurcik, "Factors that Affect the Perception of Security and Privacy of E-commerce Web Sites". Proceedings of the Fourth International Conference on Electronic Commerce Research, Dallas TX, November 2001.

²³ Egelman, Serge, Cranor, L. F., & Hong, J. (2008). You've been warned: an empirical study of the effectiveness of web browser phishing warnings. Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems, CHI '08 (pp. 1065–1074). New York, NY, USA: ACM. doi:10.1145/1357054.1357219

Wu, Min, Miller, R. C., & Garfinkel, S. L. (2006). Do security toolbars actually prevent phishing attacks? CHI '06 (pp. 601–610). New York, NY, USA: ACM. doi:10.1145/1124772.1124863

The Influence of trustworthiness of website layout on security perception of websites: Michaela Kauer, Florian Kiesel, Felix Ueberschaer, Melanie Volkamer, Ralph Bruder; In: Current Issues in IT Security 2012, vol. I, no. 18, p. 215-220, Duncker & Humblot, 2012. ISBN 978-3-86113-115-1. ISSN 1862-7625.

²⁴ I. Kirilappos, A. Sasse, N. Harvey; Why trust seals don't work: A study of user perception and behaviour, University College London, Department of Computer Science

of the displayed OSPS, while only 20% of them noticed all. Again, users gave value to other aspects mainly related to professionalism. Thus, another challenge for communicating OSPSs is the general **mismatch between trust signals and any security and privacy indicator** (including OSPSs) (**Challenge 2**).

This mismatch is caused by the way these indicators, including OSPSs, are communicated to the users; namely either as passive or active interventions. Nowadays, passive interventions dominate. Passive interventions are either part of the content of the Web page, as pictograms or provided by services like Norton Safe Web. Furthermore, browsers are able to integrate them, e.g., chrome's signal lights (green, orange, red) extension LinkExtend²⁵. Studies show that these passive interventions are rarely noticed or taken into account by users when evaluating the trustworthiness of a Web service. This is mainly caused by the users' focus on the required service and not on security. This is in particular true for OSPSs as they are displayed at different places by different Web services. Here, the actual position of such information on the screen turned out to make a difference, e.g., displaying it on the top of the screen and the force to look up can increase the concentration of the user.

Alternatively, active security interventions can be used, e.g. if no OSPS is provided then a warning is displayed. This warning requires the user to take actions before continuing. However, nowadays active security interventions do not support users' decision on the trustworthiness of a Web service either. There are many reasons for this, like too many false positives, i.e., warnings that are displayed although the risk is very low, causing the habit of always ignoring warnings. Thus, another challenge of OSPSs is how to communicate them in a way that they are **perceived by the user** (**Challenge 3**).

Furthermore, privacy and security requirements are in fact multi-dimensional and continuous. Hence, the result of the evaluation is neither trustworthy 'yes/no' nor a single scalar 'x% trustworthy'. It is clear that these multi-dimensional and continuous results of the evaluation need to be communicated appropriately to the user (**Challenge 4**).

Finally, currently, it is easy for users to get confused by the meaning and need for OSPS because nowadays there exists a small, but market dominating number of highly trusted services that do not carry any OSPS, such as amazon and eBay (**Challenge 5**).

However, this situation puts a high burden on upcoming services. From a user perspective, this is undesirable since monopolized markets tend to result in higher prices. But even from the market leaders point of view the situation is problematic: a fraudulent service provider, that knows on which signals users base their trust, can easily imitate the look and feel of a trusted service and by this profit from their reputation. This finally will harm the reputation of the initially trusted service. The challenge is, how OSPS can reach a high enough coverage over all services in such a way that an uncertified service looks at least suspicious, if not untrusted at all.

4.2 Solutions

In this section we present solutions and ideas to address the challenges presented above.

Solution 1. First of all, a basic training and raising awareness of these processes is needed. This can also be in terms of advertisements on different media. User recognition can be improved if OSPSs are awarded by companies which the users know and are reputed in terms of security.

²⁵ <https://addons.mozilla.org/de/firefox/addon/linkextend-safety-kidsafe-site/>

Solution 2. It is also important to motivate users to consider OSPs and inform themselves about consequences if they do not. This is challenging as well, as statistics show that although Internet users express high levels of concern about cyber security they frequently become victims of cyber-attacks²⁶. Therefore it is important to consider users' Mental Models on Internet Security. Note, this is also necessary when communicating the results.

Solution 3. Standardisation is needed where OSPs are displayed. In order to ensure that these symbols are displayed at the same position for any webpage, they should be loaded into the browser pane.²⁷ Thus, it is necessary, to convince browser developers to enable this and in particular display all OSPs in the same way in order to make it easier for users to recognize them. Studies need to be conducted on how to display them to make sure that users notice them. E.g., as attention increases by movements the OSPs in the browser pane could 'blink' once before being displayed constantly.

Solution 4. The different aspects of the evaluation result need to be communicated in an understandable way. As there is limited space and users are generally not willing to read long explanations, it is recommended to develop corresponding icons communicating the results. When developing such icons, further challenges have to be met: The icons can only be effective if they are both *individualized* (including demographics²⁸ and personality as well as mental model²⁹ about threats, risks and who is the target of attacks) and *contextualized*³⁰ (e.g. electronic banking versus information searching) and taking the identified trust signals (see Challenge 2). Note, designers of such icons need to take care of cultural and legal differences in case of European wide OSPs.

As a starting point for the development of icons representing the possible results of the OSP issuer's evaluation one can consider the research on policy icons that graphically represent elements of privacy policies of services. They aim to make policies easily understandable for the end user. An overview of the conducted research and research results is provided in Annex B0. .

Solution 5. For Challenge 5 (i.e. big players do not go for an OSPs and thereby confuse users regarding the need of OSPs) enforcement can be a solution. In this area, a number of different options exist to provide incentives for the analysed party to increase transparency for the service offering, and to improve their software and service in terms of security and privacy. Similar conditions can be found in business contracts that require such an assessment. For example, the Payment Card Industry Data Security Standard (PCI DSS)³¹, which applies to organizations that accept, process, store and transmit credit and debit card data, requires that merchants and service providers implement a comprehensive security program. Violating PCI DSS may lead to fines from the card brands, and even worse civil liabilities³².

Another option is self-regulation. Self-regulation implies web service providers to be aware and deal diligently with security and privacy related issues without the mandatory existence of government regulation or enforcement mechanisms. This self-regulation in security and privacy can come into existence due to several reasons: to increase user confidence, to differentiate from competitors, as a

²⁶ Special Eurobarometer 390 / Wave EB77.2 EU citizens' experience and perceptions of cyber security issues

http://ec.europa.eu/public_opinion/archives/eb_special_399_380_en.htm

²⁷ Compare to the lock symbol of ssl.

²⁸ Fogg, B., Marshall, J., Laraki, O., Osipovich, A., Varma, C., Fang, N., Paul, J., et al. (2001). What makes Web sites credible?: a report on a large quantitative study. Proceedings of the SIGCHI conference on Human factors in computing systems (pp. 61–68).

²⁹ Fogg, B. J. (2003). Prominence-interpretation theory: explaining how people assess credibility online. CHI EA '03 (pp. 722–723). New York, NY, USA: ACM. doi:10.1145/765891.765951

³⁰ Towards the Systematic Development of Contextualized Security Interventions: Steffen Bartsch and Melanie Volkamer; In: Designing Interactive Secure Systems (DISS), BCS HCI 2012, 2012.

³¹ Although PCI DSS was created by credit card companies it has been adopted (via reference or in parts) in actual law in some regions. For example, Nevada mandates compliance with PCI DSS since 2010, as described in <http://bit.ly/M31FAZ>.

³² The DatalossDB is a project aiming to document data breaches world-wide, see <http://datalossdb.org/>.



way of increasing corporate social responsibility, etc. However, self-regulation means privacy and security standards are enhanced on a voluntary basis. This may not be the preferred approach of users, which probably would rather have an independent third party supervising that their privacy and security is protected, and therefore attesting that the online service meets some certain minimum standards. Furthermore, pure self-regulation is not an option in territories where there is personal data protection legislation, as some sort of mechanism must exist in order to enforce regulation compliance, and to protect citizens when their rights are not respected.

A mixed approach is also possible, with self-assessment being conducted regularly in order to produce a constant improvement cycle, while third party assessment being done periodically to review policies and procedures against standards and to independently evaluate the level of security and privacy protection in place.

5 Verification of online security and privacy seals

OSPS issuers have (and publically provide) a list of issued seals, including the information when the seal was issued and for how long. They also provide information about how they evaluated the Web services and according to which requirements. As there are many issuers, it is not practical for the user to check on all their web pages whether the visited Web service is listed on any or not. Therefore, the Web services integrate a corresponding pictogram on their web pages. As these pictograms usually contain the logo of the issuing company it is easy to recognize who the OSPS issuer is. In order to check the details and the seals authenticity, a link is integrated in a way that when clicking on an authentic pictogram one is forwarded to the issuer's web page and in particular the web page provides information about the corresponding Web service. As faked pictograms may also forward the user to a page that looks like the OSPS issuer's web page, the user also needs to check whether the visited page is authentic.

5.1 Challenges

In a UK study³³ the researchers observed that many users **did not check the validity of OSPSs** or whether they were merely an image. This shows that forgeries are possible – just by displaying a corresponding seal icon on the web page. However, distrust was mentioned by some participants as seals are perceived as easily spoofed or faked. These participants are not aware that they could check the seals. This is not too surprising as a couple of Web services still do not properly integrate their legitimate OSPS. Here, the pictogram is only presented as an image by the web page, but not actually linked to the OSPS issuer (**Challenge 1**).

Those users who know that they need to check the validity of displayed OSPS's pictograms are also not very likely to check its legitimacy, as well as to check the evaluated requirements and used evaluation methods because of the **effort and time** to do so and the fact that also for them the first goal is not security but e.g. to buy something on the internet (**Challenge 2**).

However, even if the information is displayed in an understandable way, it might still be the case that the user is unable to compare this with his own preferences (**Challenge 3**).

5.2 Solutions

Solution 1 and 2. First two challenges can be addressed by integrating automatic checks in the Web browser. In case a Web service gets an OSPS, it includes some corresponding information in its web pages. This information is transferred to the browser. The browser checks its validity and the value/quality of the evaluation automatically. In case the Web service owns a valid OSPS the corresponding information is displayed (ideally as icon in the browser chrome). Note, it is assumed that the Web browser is trustworthy.

Solution 3. Besides checks on the authenticity the browser needs to compare the user's privacy preferences automatically. This is only possible if the OSPS comes with a machine readable component. Researchers have proposed (semi) structured formats for legal documents to make them (a) easier to understand for ordinary users and (b) to make them automatically checkable. A comparative study was presented in 2009 by McDonald et.al.³⁴

33 I. Kirlappos, A. Sasse, N. Harvey; Why trust seals don't work: A study of user perception and behaviour, University College London, Department of Computer Science

34 McDonald, Aleecia M., et al. "A comparative study of online privacy policies and formats." Privacy enhancing technologies. Springer Berlin Heidelberg, 2009

6 Economic aspects

The concept of OSPS faces economic challenges. OSPSs are intended to improve the user’s decision by providing additional information in terms of compliance with security and privacy standards. Hence OSPSs are intended to reduce information asymmetries between Web services providers and users.

In many cases, OSPS serve as justification for increasing the price charged to the users. For example, users who are sensitive to security and privacy standards are willing to pay more for using an evaluated Web service. However, the economics of OSPSs shows that such hopes could be disappointed, because OSPSs introduce new asymmetries and are not always playing a role in a user’s purchase decision, cf. Section 4.

There are a number of advantages of OSPSs, but there are also disadvantages. There is the potential to increase the Web service providers’ incentives to improve on standards. However, this will only be the case if the characteristic in question (technical security or privacy) weighs heavy in a user’s decision. In this case, it has no reputation-improving impact that is reflected in greater sales. If obtaining an OSPS does not translate into measurable effects in sales, firms will not have an economic incentive to invest in this signal.

Supply side: Web Service Provider	Demand side: Users
<p>Advantages:</p> <ul style="list-style-type: none"> ▪ Possibility of credible signalling ▪ Increase of reputation and trust ▪ Incentive to improve product/service quality regarding data protection ▪ Differentiation in competition & decrease in competition ▪ External evaluation mechanism that can reveal weaknesses in processes in firms (quality assurance) ▪ Internal risk control optimization 	<p>Advantages:</p> <ul style="list-style-type: none"> ▪ Credible quality sign, higher protection of users ▪ Additional variable in the purchase decision ▪ Increase in comparability ▪ Increase in choice (if firms differentiate) ▪ Decrease in information costs ▪ Generation of data protection awareness and risk awareness, priming on security issue
<p>Disadvantages:</p> <ul style="list-style-type: none"> ▪ Increase in investment expenditures to obtain a seal or trust mark ▪ Minimum standards can act as market barriers, if there are low-end providers that do not fulfill the standards ▪ Possible justification for price rises ▪ Sunk investment in seals, if they play no role in a user’s decision 	<p>Disadvantages:</p> <ul style="list-style-type: none"> ▪ Additional variable can further complicate decisions/comparisons ▪ Seals must not increase transparency if certification mechanisms are not transparent ▪ Low-quality demand might not be satisfied if there are minimum standards

Table 1 Advantages and Disadvantages of OSPS³⁵

By this, additional information asymmetries are introduced as users do not know whether they can trust a particular OSPS or not. If firms can obtain an OSPS too easily, many will do so, which devalues the OSPS as a signal of quality. Users then may opt to ignore the OSPS. If standards are set fairly high by the OSPS issuer, not many firms obtain the OSPS and it will not develop into a profitable business for the issuer. Competition between the latter might reduce the standards for OSPS granting procedures as the issuers try to obtain market share in the market for OSPSs. This is especially the case, if evaluated firms can be bound contractually through renewal clauses and therefore can be

³⁵ Source: Jentzsch, N. (2012) Was können Datenschutz-Gütesiegel leisten? Wirtschaftsdienst, June 2012, Vol. 92, Issue 6, pp. 413-419, with author’s modifications.

locked-in by the issuer. Thus where firms compete in the market for OSPSs, it may exacerbate the situation it is supposed to improve.

Regulators may prevent the latter by setting minimum standards for OSPS-issuing as well as for the experts that evaluate firms in terms of skill sets requested. Moreover, the latter as well as the payment structure regarding the OSPSs should be transparent and open to the public for scrutiny. As discussed in the part on policy context in this report, the latest version of the Data Protection Directive only requires that the institution granting the seal or mark must ensure there are formal procedures of granting and revoking the OSPS. Moreover, the draft regulation demands that the granting institution also ensures independence. It states that certification criteria, results, and summary justifications must be made readily available to the public.³⁶

It is intended to ensure that interested users are able to judge the granting-process themselves as well as potential conflicts of interest. For example, if an OSPS-issuer is paid by the evaluated firm, there might be a conflict of interest resulting in a positive evaluation. This ought to be made public as well.

At this point in time, little is known about how users include OSPSs in their decision-making process in general. There are a few empirical and experiment works (in the area of privacy), but they are based on a rather low number of subjects. Other works are often not conducted under 'clinical conditions' (i.e. laboratory), which do not allow for cause-effect analyses. Therefore, there are a number of open questions. For example, we do not know whether an OSPS increases the willingness to pay for a product or service. We also do not know whether it increases the inclination to purchase, although the firm also has a privacy policy. In addition, little is known about the ratio of accepted and rejected firms at the granting institution.

While OSPSs have the potential to improve the variety of products/services in the market, they will only do so if users appreciate them. Moreover, whereas they bear the potential for justification of price increases, companies will only invest in such OSPSs if they see that there is a critical mass of users in the market willing to pay for price-mark-ups. Regulators can improve the environment for such OSPSs by setting minimum standards for the quality of such certificates, as well as standards for the accreditation of experts. It is clear that potential conflicts of interest between the OSPS-seeking as well as granting institution ought to be avoided. In the worst case, OSPSs lead to increased prices, confused users who ignore them and non-transparent OSPS-granting procedures. The first step, therefore, would be to find out whether OSPSs are relevant in user decisions.

Theoretically, OSPSs have the potential of lowering information asymmetries, but at the same time they have the potential to introduce new ones. They can act as an OSPS of differentiation, but again in order to become such they must be meaningful and important as a mechanism to support a user's decision.

It is questionable whether it will be possible to establish a unified international standard of a privacy OSPS. The reason is that there are a number of different regulatory regimes, at the EU level, the national regimes, regional standards, and industry standards.

Differentiated demand is the reason why in the past a variety of OSPSs were created. While the variety can be confusing, a user can often only compare whether a firm has an OSPS or not, not whether one OSPS provides stronger protection than another.

A regulator should keep track of the conflicts of interest that may arise between certifying institutions and certified firms. Otherwise, phenomena arise like in the financial services industry

³⁶ Article 39 of the proposed Data Protection Regulation, available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

between rating-demanding firms and rating agencies, where the latter are dependent on generating profits from the former.

It is recommended to perform first tests on the effect of OSPs on user decisions in the laboratory and in field experiments in order to understand their impact regarding the purchase of goods and services. In this area, evidence-based policy is definitely a good thing, before setting up expensive and large-scale certification schemes. The research could also inform decision makers about the best design for such OSPs. Again, the design and its interaction with user decisions should be analysed first.

If OSPs do not play a role in user decisions in the market, the hope to find market-discipline effects through privacy/security certification will not be realised. An evidence-based approach could prevent the misrouting of investments into efforts that will in the medium term not lead to a greater protection of users in terms of technical security and data protection.

7 Summary and recommendations

The ultimate goal of **online security and privacy seals (OSPS)** is to make service offerings more secure and privacy friendly. In this report, we analysed under which conditions **OSPSs** can support users to make an informed decision on the trustworthiness of a service and its provider. We sketched the **chain of trust**, namely **evaluation of the Web service provider, communication of the result of the evaluation and verification of the authenticity of a communicated OSPS**, which needs to be established from the seal **issuer** to the **user's awareness**. We started with a short **review** of current regulations that mention such seals as a means to establish trust. Furthermore, we analysed the three stages of the trust chain and detailed out challenges and sketched solutions and recommendations.

The main identified challenges on the user side are that they:

- do not know the general concepts of OSPS,
- do not understand what the signals stand for (e.g., data protection, security, service/product quality) including what has been evaluated (scope) and how (which methods were in place) as well as when and how often are services re-evaluated (and the meaning of a possibly years old assessment),
- are not aware of the need of checking the authenticity of OSPS and how do this,
- do not check, although they know, as it is too much effort and it takes too much time to do so.

In addition, it is challenging to identify proper standards both for the evaluation and the accreditation of OSPS issuers. This is because they should be appropriate to base decisions on them, but they cannot be too expensive as then only big players can afford them. As such, different levels of assessment seem to be appropriate; however then it is even more challenging to communicate the multi-dimensional results to the end users in an understandable way, for example using icons and other graphical representations, to convey differences to end users.

We proposed and discussed solutions and derive the following recommendations:

- EU or international **standards for evaluation** are required to address all the above challenges. Due to different types of services and due to different budget limitations for such an evaluation, different levels or categories are required and should be considered by such a standard.
- Browser developers need to **implement** these standards for **automatic checks**.
- Additional information also needs to be **adequately represented** by the online security and privacy seal. In order to facilitate the comparison of certificates, the EC could issue work on traffic light systems that enable vertical comparisons relating to the strength of protection granted by a product or service.
- Policy makers should investigate **enforcement strategies** in case promises made with seals are not met. This is particularly important for those cases when regulatory enforcement is chosen as a preferred approach.
- Further **research** is needed to better understand user behaviour regarding **passive and active security interventions**. New strategies and new interventions need to be provided that are more effective than the current ones. This should be individualized and contextualized.



- Further work is needed for improving the **awareness** of the users on OSPS but also on security signals in general; as well as the level of understanding on how they are functioning and on how seals can be checked / validated. ENISA should continue this activity by attempting to increase the awareness of these issues.

Annex A: Relevant Factors for the Evaluation

Evaluation (assessments or analysis) is the basis for any OSPS. It is important to know the different relevant factors of an evaluation and how they influence each other. The different factors and corresponding sub aspects are shown in Figure 2 and they are described in the subsequent paragraphs.



Figure 2: High level decision aspects.

A.1 Scope

With the analysis of software and services, the scope of the analysis plays an important role in the amount of effort it takes and the type of procedures involved. The possibilities are broad ranging from the analysis of single protocol properties to skills of personnel working in a company.

For an automated analysis, the choices are limited to a more restricted scope but may lead to a real-time result. Still, there are a number of popular examples of automated analysis techniques. A known example is the HTTPS lock icon, which results from a successful SSL/TLS handshake that offers channel security and authentication of the Web server. Another example of an automated analysis is the EFF “Terms of Service” tracker³⁷ that keeps track of changes in privacy notices of big Internet websites and publishes the changes for the end users.

The analysis of complete service offerings, such as privacy notices, human resource skills, and process maturity, often requires human involvement. Consequently, it is more time consuming. For example, the “Terms of Service; Didn’t Read” project³⁸ aims to summarize privacy notices of popular online services based on the observations that most end users do not read the terms of service since they are typically hard to read, difficult to find, and fairly long. The Payment Card Industry Data Security Standard (PCI DSS), as another example, also requires significant personnel resources even in case of self-assessments³⁹, which is applicable for merchants with a low number of annual credit card transactions.

Furthermore, it may not be possible to carry out some analysis without special privileges, such as access to source code or company-internal documentation. Thus, the scope of the analysis is linked to the type of analysis conducted (e.g., who the analysis party is).

A.2 Baseline for analysis

Since the security and privacy requirements vary between jurisdiction and also between sector (e.g., healthcare industry, financial industry, etc.), the following question could be raised: What baseline reference is suitable when analysing products and services: Should the product or service be assessed against generic privacy principles, for example, the OECD privacy principles or the Madrid resolution, or rather against specific data protection and/or security regulation? Choosing generic principles can be advantageous because it gives the service providers more freedom to demonstrate compliance with sound principles. Due to the global nature of the Internet and the desire of many companies to reach a maximum number of users this offers benefits regardless of the specific location of a given end user. However, the benefit of using a specific security and privacy regulation is that compliance is achieved with the assessment, which, for many service providers that are bound to comply with a certain regulation, can be a driving force to conduct the assessments. More narrow focused regulation and assessment programs are often more detailed in terms of what a specific service provider needs to fulfil. For example, PCI-DSS assessment is done based on detailed instructions on how to secure the network infrastructure categorized into six control objectives⁴⁰.

A.3 Type of analysis

Automated analysis (e.g. the use of automatic vulnerability analysis tools) can detect actual security deficiencies in web pages that could be exploited by malicious users to either gain access or destroy private information. On the other hand, manual assessment (e.g. reviewing the privacy and security policies) can be more effective in assessing the general management procedures of the web page when dealing with data from their users. Neither approach is perfect: the use of both of them simultaneously should offer the best results in terms of protection of private information.

³⁷ TOSBack – The terms-of-service tracker: <http://tosback.org>

³⁸ Terms of Service; Didn’t Read – <http://tosdr.org>

³⁹ PCI DSS Self-Assessment Questionnaire – https://www.pcisecuritystandards.org/documents/pci_dss_saq_instr_guide_v2.0.pdf

⁴⁰ The six control objectives, namely “build and maintain a secure network”, “protect cardholder data” “maintain a vulnerability management program”, “implement strong access control measures”, “implement strong access control measures”, “regularly monitor and test networks”, “maintain an information security policy”, are briefly summarized at http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard. A more detailed description can be found in the PCI DSS standard itself: https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

A good privacy policy and security management practices would lead to a more securely designed environment. However, undetected vulnerabilities often do exist. Vice versa, a securely designed and operated web page may not mean much in terms of privacy if the policy of the company is faulty (e.g. the web page provides personal data given by users to external parties without their explicit consent).

However, the more complete and profound the analysis is the more associated cost it will have. This may not be feasible to implement for some web pages that belong to minor entities in terms of size or resources. A balanced approach should be taken, bringing into consideration both the sensitivity of the data and the technological environment.

A.4 Cost coverage

Many, although not all assessments, incur costs to the participating parties. In particular, if the assessment requires humans to perform the assessment then costs can be potentially quite high. The cost of the assessment will also be determined by the depth of the analysis, as well as, the extend of the service offering, and the frequency of the assessment. The costs, however, are not necessarily paid by the party that is audited. Magazines often publish product comparisons and perform a variety of assessments without being paid by the company whose products are analysed. An example of such a magazine is Stiftung Warentest⁴¹, but many other magazines, blogs, and daily newspapers provide similar product reviews. Sometimes the costs are covered as part of research grants and, as those funding source drain away these services tend to slow down in their level of activity or cease to exist.

Not all organizations releasing software libraries on the Internet have the financial means to pay for a security and privacy assessment. This includes many of the open source activities and individual developers contributing their code to the public. Many of the core Internet infrastructure services are available as open source software, such as OpenSSL⁴², GnuTLS⁴³, BIND⁴⁴, Apache⁴⁵, OpenIkeV2⁴⁶, FreeRADIUS⁴⁷. Of course, security and privacy aspects are being addressed in those development events, but in the same style as the rest as the software development, i.e., based on contributions by other developers rather than via compliance to certification programs.

A more detailed discussion of the economic aspects can be found in Section 6.

A.5 Validity period

Software and services frequently change; this often includes changes of the security and privacy properties. This change is not only due to technological changes but also due to changes in the organizational structure and the goals businesses try to achieve. Updates to services and products may be required due to the collecting and processing of additional or different customer data, may respond to changes in the regulator environment (e.g., due to new data protection regulation), and maybe reflect new business models.

All of this implies that privacy assessments should be conducted on a periodical basis in order for their results to be valid. Nonetheless, the periodicity may not necessarily be fixed, but could be

⁴¹ Stiftung Warentest offers a wide range of product comparisons, many of which are unrelated to privacy or security. However, some tests are specifically focused on online services and their privacy properties. See, for example, <http://www.test.de/thema/datenschutz/>.

⁴² OpenSSL Library: <http://www.openssl.org/>

⁴³ GnuTLS Library: <http://www.gnutls.org/>

⁴⁴ Bind Domain Name Server: <http://www.isc.org/downloads/bind/>

⁴⁵ Apache: <http://www.apache.org/>

⁴⁶ OpenIkeV2: <http://openikev2.sourceforge.net/>

⁴⁷ FreeRADIUS: <http://freeradius.org/>

adjustable. What a suitable timeframe for a re-assessment should be and who decides about such the triggers that demand such a re-evaluation is difficult to state in general.

Annex B: Privacy icons

Privacy Icons have been studied a lot both in the privacy policy and the privacy preference context. An overview of this research is provided in this section.

Privacy policy icons

Privacy policy icons have been researched and developed for visualising policy elements in privacy policies stated for websites with the objective of making the content of legal policy statements easier to access and comprehend. Privacy policies containing lengthy legal phrases are usually, if they are read at all, not comprehensible to most end users^{48, 49}. One of the 10 Usability Heuristics for User Interface Design defined by Jakob Nielsen is the “match between system and the real world”⁵⁰. A user interface which uses real-world metaphors, e.g. in form of suitable icons, is easier to learn and understand. This section first discusses policy icons that graphically present elements of privacy policies of services sides for making policies more transparent and easily understandable. Finally, an example for icons expressing the user’s privacy preferences is given.

Policy icons should be based on semiotic studies and preferably be standardised and usable across cultures. However, the policy aspects for which icons can be helpful vary across legal regimes. Moreover, icons in form of symbols that are well understood in one cultural domain are not necessarily understood by other cultures.

Creative Commons-like policy icons were proposed by Rundle⁵¹, which, however, were mainly targeted at the US American legal privacy regime and not matching with European privacy principles. For instance, her icon set included icons for indicating that a services side takes reasonable steps to keep a user’s data secure and grants users the right to access their data. However, according to the EU Data Protection Directive 95/46/EC, services sides have a legal obligation to take reasonable measures to secure personal data (Art. 17) and to grant data subjects access to their data (Art. 10) – hence in Europe, these rights and obligations are anyhow mandatory privacy rules and thus do not need to be displayed prominently by icons.

Further Creative Common-like privacy icons have been initiated by Aza Raskin and further developed by a Mozilla-led working group with further contributors from Stanford and Disconnect.me⁵², which should as standardised and legal declarations backed up by clear legal definitions be able to replace complex legal documents. However, the Mozilla privacy icon project has not reported any further results since 2011. Both Mary Rundle’s icon set and the set of the Mozilla icons (displayed in Figure 3) target the US privacy regulations, hence they are not suitable to display the core policy information that is required by Art. 10 EU Data Protection Directive 95/46/EC. Furthermore, policy statements such as that a website “might keep your data indefinitely” do not comply with the data minimisation principle that can be derived from the EU Directive. Nonetheless, it is notable that it includes special icons informing end user about how easily web sites are cooperating with requests by law enforcement. As already pointed out by the Art. 29 Working Party on their Opinion on Cloud

⁴⁸ Jensen, C. and Potts, J., Privacy policies as decision-making tools: An Evaluation of online privacy notices, in CHI 2004, 6, 471-478, 2004

⁴⁹ Protor, R., Ali, A., Vu, K.-P. L., Information requested by Web Sites and User’s comprehension of Privacy Policies, Poster Proceedings of the Symposium of Usable Privacy and Security (SOUPS 2006), July 14-16, 2006, Pittsburgh, PA

⁵⁰ Nielsen, J. 10 Usability Heuristics for User Interface Design. January 2005. <http://www.nngroup.com/articles/ten-usability-heuristics/>

⁵¹ Mary Rundle, “International Data Protection and Digital Identity Management Tools”, presentation at IGF 2006, Privacy Workshop I, Athens, 2006, available online: <http://identityproject.lse.ac.uk/mary.pdf>

⁵² https://wiki.mozilla.org/Privacy_Icons

Computing (cf. section 2.2) and as it also became apparent after the revelation of the PRISM program; this is an important aspect that is often not transparent to end users.



Figure 3: Beta version of proposed privacy icons developed by a Mozilla- led working group (see: <https://icons.disconnect.me/icons>)

Within the scope of the PrimeLife EU project, a set of policy icons addressing the legal transparency requirements of the Data Protection Directive 95/46/EC has been developed by the Independent Center for Privacy Protection in Kiel/Germany, which can be used illustrate core privacy policy statements, namely statements about what types of data are collected/processed, for what purposes, and what are the processing steps⁵³.

An intercultural comparison test of the PrimeLife policy icons was conducted at Karlstad University in the form of a paper mock-up test with 17 Swedish and 17 Chinese students, which gave insights into which icons seem to be well understandable and which require improvements⁵⁴. Icons, which were by most of the Swedish and Chinese students associated with the correct policy element and thus were understood well by both test user groups, were the following ones displaying types of data (personal data, medical data, payment data), the purpose “shipping” and the processing steps (storage, retention).

⁵³ Holtz, L., Nocun, K., Hansen, M. Displaying privacy information with icons. In Fischer-Hübner, S. et al.: Proceedings of the PrimeLife/IFIP Summer School 2010, Helsingborg, 2-6 August 2010, Springer 2011

⁵⁴ Fischer-Hübner, S., Zwingelberg, H. UI Prototypes: Policy Administration and Presentation – Version 2. PrimeLife, Deliverable D4.3.2, June 2010. www.primelife.eu

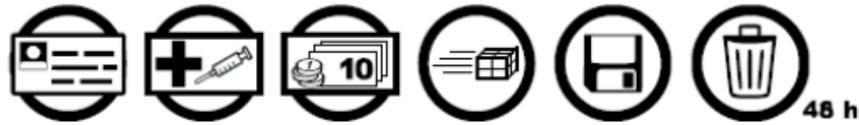


Figure 4 Example of understood PrimeLife policy icons by test participants with different cultural backgrounds

However, the tests also showed that the test persons with different cultural backgrounds had different understandings of some of the icons. While Swedish test persons had for instance no problems in understanding the “post horn” as an icon for the purpose “shipping”, this icon was not understood by Chinese test persons. These tests demonstrated well that finding privacy icons that are well understood by different cultures is a special challenge.

The policy generator tool by Iubenda⁵⁵ also uses icons for types of data that are collected, purposes of use, and parties involved & contacts of the data controller along with some basic explanatory text in short privacy notices that it is generating in addition to a link to a full text policy statement (following the Art. 29 Working Party’s Recommendation of multi-layered privacy notices⁵⁶). The selection of icons is expressive enough to comply with legal transparency requirements of Art.10 EU Data protection Directive.

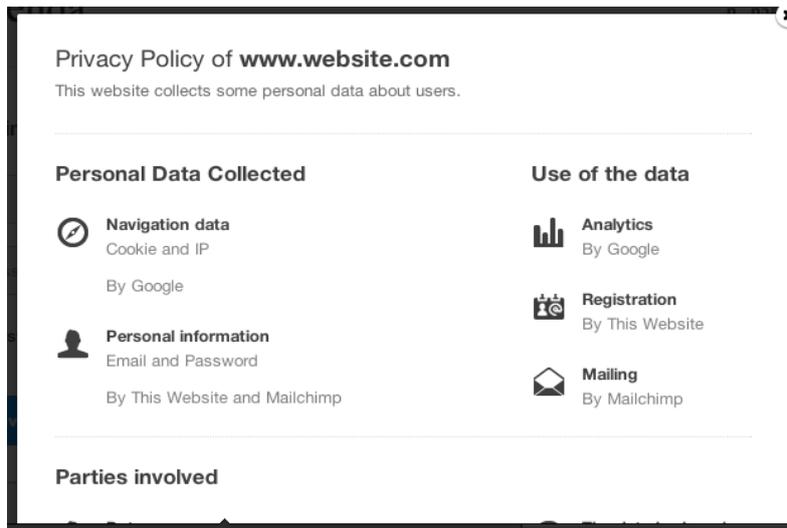


Figure 5: Short privacy notice including icons created by the Iubenda privacy generator.

Further proposals for icons complementing short privacy notices were suggested by the CommonTerms project⁵⁷ and the U.S. Department of Commerce’s NTIA (National Telecommunication & Information Administration) for mobile app short privacy notices⁵⁸. The short privacy notices of these two approaches are however not presenting all information that Art.10 of the EU Data Protection Directive requires.

On October 21, 2013, the LIBE Committee of the European Parliament approved a compromise text of the proposed [EU General Data Protection Regulation](#)⁵⁹. It includes the new Article 13a requiring that data controllers use standardised information policies for informing data subject on how

⁵⁵ <https://www.iubenda.com/en>

⁵⁶ Art.29 Working Party: Opinion on More Harmonised Information Provisions 1198704/EN WP 100. (2004)

⁵⁷ <http://commonterms.net>

⁵⁸ http://www.ntia.doc.gov/files/ntia/publications/ntia_ui_comps_update_7.23.pdf

⁵⁹ European Commission (2013). Proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7 0025/2012 – 2012/0011(COD)). Compromise amendments on Articles 1-29. Passed 21 October 2013.

personal data is being collected, retained, and shared with third parties and how encryption is used. In an annex, graphical policy icons are provided to be used by standardised policies in yes/no icon based tables along with textual descriptions for informing data subjects about the policy particulars pursuant to the new Article 13a. This icon- based table structure of standardised policies was initially suggested and developed by the vice president of the European parliament Alexander Alvaro⁶⁰, as depicted in the example in **Error! Reference source not found. Error! Reference source not found.**

ICON	ESSENTIAL INFORMATION	FULFILLED
	No personal data is collected beyond the minimum necessary for each specific purpose of the processing	
	No personal data is retained beyond the minimum necessary for each specific purpose of the processing	
	No personal data is processed for purposes other than the purpose it was provided for	
	No personal data is disseminated to private third parties for purposes other than the purpose it was provided for	
	No personal data is sold	
	No personal data is retained in unencrypted form	

Figure 6 Example of icon-based standardised information policy as suggested by Alexander Alvaro and as required by the compromise text of the proposed EU Data Protection Regulation

While the approach of having standardised policy icons can facilitate an easier recognition and comparison of policy aspects, the icons of the compromise amendments do not seem to be very intuitive and not easily and unmistakably recognizable by their symbolic depictions (e.g., the first icon in Figure 4 could rather be (mis-)understood as symbolising that persons can be uniquely identified). Therefore, such icons should preferably undergo further HCI improvements and usability tests.

Privacy preference icons

Further icons sets for e-mail have been developed within the Privicons project and submitted as an Internet Draft to the IETF⁶¹ by researchers from Stanford and the PrimeLife EU project. Privicons are attached to emails and can express how a sender would like his email to be treated by the recipient (“washing tags for email privacy”)⁶². They are thus expressing aspects of the user’s privacy preferences in contrast to the privacy policy icons mentioned above, which are visualising aspects of a services side’s privacy policy. A Chrome extension for Privicon gmail icons has been developed⁶³.

⁶⁰ Alvaro, A (2013). LIFECYCLE DATA PROTECTION MANAGEMENT – Ein Beitrag zur Anpassung der europäischen Datenschutzgesetzgebung an die Erfordernisse des 21. Jahrhunderts, 30. January 2013. <http://www.alexander-alvaro.de/inhalte/lifecycle-data-protection-management-ein-beitrag-zur-anpassung-der-europaischen-datenschutzgesetzgebung-an-die-erfordernisse-des-21-jahrhunderts/>

⁶¹ König, U. and Schallaböck, J., Privacy Preferences for E-Mail Messages, Internet Draft, June 2012, draft-koenig-privicons-04, <http://tools.ietf.org/html/draft-koenig-privicons-04>

⁶² <http://privicons.org/>

⁶³ <https://chrome.google.com/webstore/detail/privicons-for-gmail/nijcfdbcfngcechlklbgmjlknkheled#detail/privicons-for-gmail/nijcfdbcfngcechlklbgmjlknkheled>

The Privicon initiative is thus concept-wise similar to the **Do Not Track (DNT)** approach⁶⁴, which uses an http header field to express the user's preference not to be tracked by web applications.

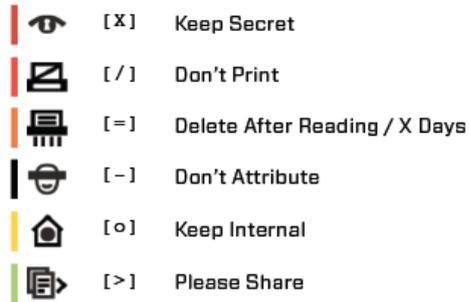


Figure 7 e-mail preference icons.

⁶⁴ W3C, Tracking Preference Expression (DNT), W3C Working Draft 30 April 2013, <http://www.w3.org/TR/tracking-dnt/>

**ENISA**

European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vasilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias, Marousi 151 24, Athens, Greece



PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu