Report on the Workshop on Assessing the Maturity of Privacy Enhancing Technologies

Marit Hansen, Jaap-Henk Hoepman, Meiko Jensen, Stefan Schiffner

Report on the Workshop on Assessing the Maturity of Privacy Enhancing Technologies

Marit Hansen[1], Jaap-Henk Hoepman[2], Meiko Jensen[1], and Stefan Schiffner[3]

[1] Unabhängiges Landeszentrum für Datenschutz, Kiel, Germany
marit.hansen@privacyresearch.eu and meiko.jensen@rub.de
[2] Radboud University, Nijmegen, The Netherlands
jhh@cs.ru.nl
[3] European Union Agency for Network and Information Security (ENISA)
Stefan.Schiffner@enisa.europa.eu

Abstract. Privacy enhancing technologies (PETs) are regarded as an important building block for implementing privacy guarantees. However, the maturity of different PETs varies and is not easy to determine. In this paper, we present an assessment framework that allows to compare the maturity of PETs. This framework combines two rating scales: one for technology readiness and one for privacy enhancement quality. The assessment methodology has been tested in two experiments, one of them being conducted at the 2015 IFIP Summer School on Privacy and Identity Management with junior and senior researchers. We describe the first experiment and how we gathered feedback on our assessment methodology in an interactive workshop. The results were used to refine and improve the assessment framework.

Keywords: Privacy, Data Protection, Privacy Enhancing Technologies, PETs, PET Readiness, PET Maturity, Maturity Assessment, Technology Readiness

1 Introduction

Privacy enhancing technologies (PETs) have been demanded by various stakeholders as an important building block for maintaining and improving privacy guarantees in an increasingly computerised world: John Borking and Charles Raab regard PETs as "a promising aid to achieve basic privacy norms in lawful data processing" [4]. Ann Cavoukian points out that PETs "embody fundamental privacy principles by minimising personal data use, maximising data security, and empowering individuals" and stresses that "PETs can be engineered directly into the design of information technologies, architectures and systems" [5].

In 2007 the European Commission stated in a Memo: "The Commission expects that wider use of PETs would improve the protection of privacy as well as help fulfil the data protection rules. The use of PETs would be complementary to the existing legal framework and enforcement mechanisms." [8]. However, today's adoption of PETs in practice is low. In the information security realm

catalogues of tools, algorithms, and methods exist that support data controllers and developers in choosing the appropriate measures to protect their assets. For privacy and data protection, this work has not been done, yet. A first step can be seen in a report on Privacy and Data Protection by Design published by the European Union Agency for Network and Information Security (ENISA) [7], which gives an overview on today's landscape concerning privacy engineering. While the report identifies different maturity levels of PETs, it does not provide criteria on how to assess the individual maturity. All the same, the European General Data Protection Regulation [3] will demand data protection by design (Art. 23 General Data Protection Regulation) which will encompass the usage of PETs.

For this purpose, data controllers and data processors as well as supervisory authorities will have to decide which PETs are considered state-of-the-art and have to be taken into account when designing, implementing, or operating an information system. Also, standardisation bodies, funding organisations, or policy makers may be interested in knowing about the maturity of a PET. This was the starting point for our work on developing a methodology that can provide comparable information on the maturity of different PETs.

We decided not to limit our view on technology readiness levels as introduced by NASA for arbitrary technologies [12], because we are convinced that a mere assessment of technology readiness may result in a misleading outcome for privacy technologies if the quality for privacy protection is neglected. Therefore, we aim at assessing individual results for technology readiness and privacy enhancement quality as a second dimension that are combined into an overall PET maturity score.

In a workshop at the IFIP Summer School on Privacy and Identity Management 2015 we presented our interim results and conducted a preliminary evaluation of our methodology with the audience to receive early feedback. This paper describes our approach, the interaction with the audience, and lessons learnt. A final version of the overall results has been published as an ENISA report [10].

The remainder of the text is organised as follows: After we have briefly introduced related work such as technology readiness levels in Section 2, we present our framework developed for assessing PET maturity, cf. Section 3. The following Section 4 describes the evaluation performed during the IFIP Summer School and its results. Finally, Section 5 summarises our findings.

2 Related Work

The National Aeronautics and Space Administration (NASA) uses the Technology Readiness Levels (TRL) scale, that ranges from 1 to 9 [12]. For the NASA TRL scale guidance reports and TRL Calculators are provided to help gathering the necessary information. The European Commission uses nine Technology Readiness Levels in its funding programme Horizon 2020 [9] that are comparable to the NASA TRL scale:

- TRL 1: basic principles observed
- TRL 2: technology concept formulated
- TRL 3: experimental proof of concept
- TRL 4: technology validated in lab
- TRL 5: technology validated in relevant environment (industrially relevant environment in the case of key enabling technologies)
- TRL 6: technology demonstrated in relevant environment (industrially relevant environment in the case of key enabling technologies)
- TRL 7: system prototype demonstration in operational environment
- TRL 8: system complete and qualified
- TRL 9: actual system proven in operational environment (competitive manufacturing in the case of key enabling technologies; or in space)

Many aspects of the TRL approach have been critically discussed over the last decades, in particular by pointing out limitations and needs for a multidimensional approach [13]. Improvements of the process have been proposed for the TRL assessment process [15]. In particular it has been pointed out that assessing 'readiness' without regarding 'quality' is of limited value, e.g. [16]. For PET assessment it is questionable whether readiness scores are meaningful without knowledge about the privacy enhancement quality: a wide adoption of a PET with a high readiness score, but unsatisfying protection may prevent the development and deployment of better solutions.

Many privacy researchers are working on determining selective privacy properties of information and communications technologies which shows the current need for expert knowledge in the assessment process. For an overview on relevant criteria we took into account standards related to security properties and quality assessment methodologies, such as ISO/IEC 27004 [1], NIST Special Publication 800-55 [6], Control Objectives for Information and Related Technology (COBIT) [11], and the recently released ISO/IEC standard 25010 on Systems and Software Quality Requirements and Evaluation (SQuaRE) [2].

3 The Assessment Framework

In this section, we present a four-step assessment process and define the scale for readiness as well as the scale for quality. We also point out how the assessment should take place and how the individual results are combined to express the maturity of a PET.

3.1 The assessment process

The assessment process consists of four steps (see Figure 1) that are performed by the person responsible for the assessment: the *assessor*.

First, the assessor properly defines the *Target of Assessment* (ToA), i.e. the PET in focus. Without clarity on the PET to be assessed, its scope, its boundaries, and its interfaces a meaningful assessment is not possible. Different versions

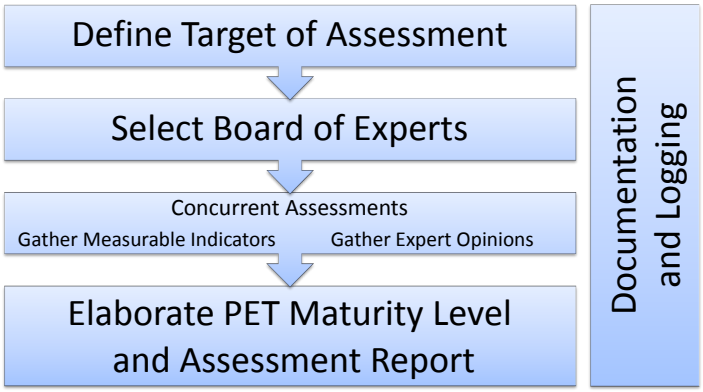


Fig. 1. Overview of the PET Maturity Assessment Process

of a PET usually have to be assessed separately, e.g. if the running code still lacks some privacy functionality that is conceptualised for a future version.

Second, the assessor creates a board of experts whose opinions will be used as input in the assessment process. The experts should be familiar with the domain of application the PET is assessed and/or with privacy engineering. We believe that at least five experts should be involved if possible. Different expert boards likely will have differing results. While reproducibility of the assessment cannot be guaranteed (and exact reproducibility is highly unlikely), the process should be transparent for maximum comprehensibility.

Third, the assessor gathers measurable indicators as well as asks for the expert opinions by means of dedicated forms, consisting of both a scale-based assessment and a detailed opinion comment part.

Fourth, the assessor combines the separate results—a *Readiness Score* and a *Quality Assessment*—into the final *PET Maturity Level*. Further, the assessor compiles the Assessment Report from the collected input as well as the documentation and logging processes.

The involvement of the experts and the combination of their opinions and measurable indicators both for readiness and quality evaluation is illustrated in Figure 2.

The following subsections describe the scales for readiness and quality as well as criteria for their assessment.

3.2 A scale for readiness

The intuitive understanding of readiness denotes whether a PET can be considered state-of-the-art, i.e., it can be deployed in practice at a large scale, or whether effort, i.e. time and money, is needed to achieve this goal. On this basis we define the following levels, see also [10].

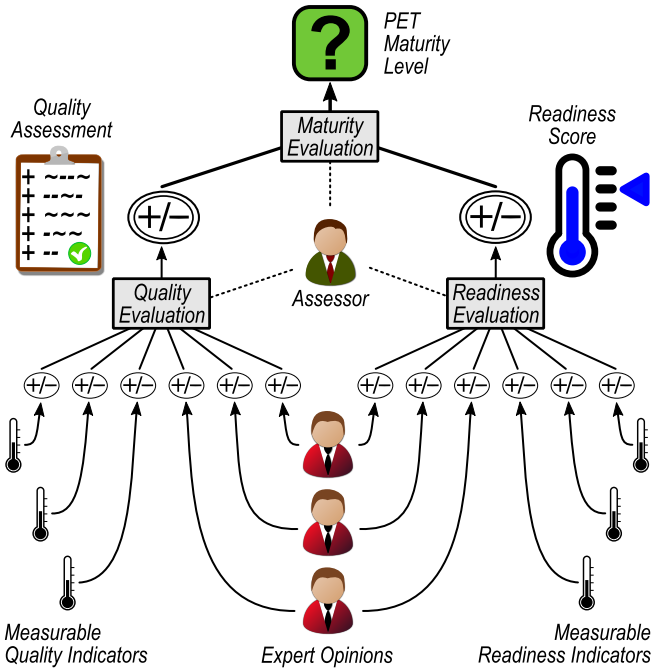


Fig. 2. PET Maturity Assessment Methodology

`idea:` Lowest level of readiness. The PET has been proposed as an idea in an informal fashion, e.g. written as a blog post, discussed at a conference, described in a white paper or technical report.

`research:` The PET is a serious object of rigorous scientific study. At least one, preferably more, academic papers have been published in the scientific literature, discussing the PET in detail and at least arguing its correctness and security and privacy properties.

`proof-of-concept:` The PET has been implemented, and can be tested for certain properties, such as computational complexity, protection properties, etc. "Running code" is available. No actual application of the PET in practice, involving real users, exists. Not all features are implemented.

`pilot:` The PET is or has recently been used in practice in at least a small scale pilot application with real users. The scope of application and the user base may have been restricted, e.g. to power users, students, etc.

`product:` The highest readiness level. The PET has been incorporated in one or more generally available products that have been or are being used in practice by a significant number of users. The user group is not a priori restricted by the developers.

`outdated:` The PET is not used anymore, e.g., because the need for the PET has faded, because it is depending on another technology that is not maintained anymore, or because there are better PETs that have superseded that PET.

Note that over its lifetime a PET may have different readiness levels, depending on its evolution. Also, there are transition phases where mixed levels could be appropriate, e.g. a readiness level of `pilot/product` for a PET that is currently being beta-tested as a (commercial) general purpose product after having been used in some pilots.

Threshold indicators can help determining the readiness level:

`idea`→`research`**:** This threshold indicator is met if there exists at least one scientific publication that focuses on the ToA.

`research`→`proof-of-concept`**:** This threshold indicator is met if there exists at least one working implementation (e.g. laboratory prototype, open source project, proof of existing code, or similar, that compiles and executes, and implements the ToA).

`proof-of-concept`→`pilot`**:** This threshold indicator is met if there exists at least one real-world utilisation of the ToA, with non-laboratory users, performed in a real-world application context.

`pilot`→`product`**:** This threshold indicator is met if there exists at least one product available in a business market, or in a context in which the utilisation of the ToA happens in a real-world business context with transfer of value.

`product`→`outdated`**:** This threshold indicator is met if 1) the only technology that allows for utilising the ToA gets obsolete or ceases to exist, or 2) a devastating quality problem of the ToA was revealed, which cannot be fixed.

3.3 A scale for quality

The following characteristics for PET quality have been developed from the ISO/IEC system and software quality models standard ISO 25010 [2] with several adjustments. For more information see [10].

Protection: Protection should be understood as the degree of protection offered (in terms of for example unlinkability, transparency, and/or intervenability) to prevent privacy infringements while allowing access and normal functionality for authorised agents. Also depends on the type of threats and attacks against which the PET offers protection.

Trust assumptions: Trust assumptions are characterised by the technical components and/or human or institutional agents that need to be trusted, and the nature and extent of trust that must assumed in order to use the PET. The more components or agents need to be trusted, the lower the score. For example, whether the system assumes an honest but curious adversary, whether the system is based on a non-standard cryptographic assumption, whether it relies on a trusted third party, or whether a trusted hardware component is used. Standard assumptions, for instance that the software and hardware need to be trusted, are out of scope. Note that trust assumptions can also be legal, i.e. a juridical process is a critical part of the protection offered, or organisational, i.e. the protection offered depends on procedural safeguards.

Side effects: Side effects are the extent to which the PET introduces undesirable side effects. These effects include increased organisational overhead due to key management, increased use of bandwidth (without performance impact) due to cover traffic, etc. Assessing side effects depends on the composability, i.e. how easy it is to compose the PET with other components without negatively influencing these components, and on the number and severity of these side effects themselves.

Reliability: Reliability is the degree to which a system or component performs specified functions under specified conditions for a specified period of time. It is measured in terms of fault tolerance and recoverability, as well as in terms of the number of vulnerabilities discovered.

Performance efficiency: Performance efficiency is the performance relative to the amount of resources used under stated conditions. It is measured in terms of resource use, i.e., storage, computational power, and bandwidth and speed, i.e., latency and throughput.

Operability: Operability is the degree to which the product has attributes that enable it to be understood, and easily integrated into a larger system by a system developer. It is measured in terms of appropriateness, recognisability, learnability, technical accessibility, and compliance.

Maintainability: Maintainability is the degree of effectiveness and efficiency with which the product can be modified or adapted to underlying changes in the overall system architecture. It is measured in terms of modularity, reusability, analysability, changeability, modification stability, and testability. Open source software typically scores high on this characteristic. Also, systems that have an active developer community, or that have official support, score high.

Transferability: Transferability is the degree to which a system or component can be effectively and efficiently transferred from one hardware, software or other operational or usage environment to another. It is measured in terms of portability and adaptability.

Scope: The scope refers to the number of different application domains the PET is applied in or is applicable to.

The quality characteristics cannot be automatically assessed in a meaningful way. Instead, expert knowledge is necessary. However, several soft indicators can support the experts:

Protection 1) documented protection levels and properties.

Trust assumptions 1) documented trust assumptions. 2) described adversarial model. 3) legal measures. 4) organisational measures.

Side effects 1) documentation on known side effects.

Reliability 1) availability of stress test reports. 2) the number of unsuccessful or successful penetration tests. 3) number of vulnerabilities discovered.

Performance efficiency 1) benchmarks or performance figures for storage, computational power, bandwidth, latency and throughput.

Operability See maintainability.

Maintainability 1) whether the system is modular in design. 2) whether test suits exist. 3) whether the ToA is open source. 4) availability, extent and detail of documentation. 5) whether an active developer community exists.

Transferability 1) list of different software and/or hardware platforms the ToA has been ported to. 2) evidence regarding the amount of work needed to port the ToA. 3) whether the ToA uses general purpose programming languages and build environments, and standard libraries. 4) availability and detail of instructions to port the ToA to other platforms.

Scope 1) list of application domains the ToA is known to be applicable to. 2) number of different products serving different markets that use the ToA.

For the quality assessment the experts assign for each of these nine characteristics a score in the following five-value range:

−− (very poor)	− (poor)	0 (satisfactory)	+ (good)	++ (very good)

The experts are asked to assign an overarching total quality score on the same scale. The standard calculation would be to combine the nine individual scores with different weights:

- The characteristics *protection* and *trust assumptions* have a factor 3 weight.
- The characteristics *side effects*, *reliability* and *performance efficiency* are calculated with factor 2.
- For the remaining characteristics, i.e. *operability*, *maintainability*, *transferability*, and *scope* factor 1 is used.

By this way of calculation, the importance of *protection* and *trust assumptions* for PET quality is clearly emphasised.

3.4 Combining readiness and quality to express maturity

For combining the information on readiness and quality on the maturity of a PET, we propose to communicate the overall scale in the following way, putting the quality score into superscript:

$$\texttt{readiness}^{\text{quality}}$$

For instance, a PET maturity level of $\texttt{pilot}^{+}$ denotes readiness level `pilot` and quality +. Figure 3 contains all possible combinations.

4 Evaluation

During the work on PET maturity, we discussed our interim results with several people from the privacy engineering domain. In addition, we conducted two evaluations: one evaluation strictly following the four-step process with roles of the assessor and experts under rather controlled conditions that took part in autumn 2015, and previously another less formal experiment for gathering early feedback. This second evaluation experiment was conducted during the 2015 IFIP Summer School with the participants who were willing to contribute. Both evaluations are described in [10] where it is also pointed out that further work has to be invested for assessing a wide range of PETs.

Fig. 3. Overview of Possible PET Maturity Level Values

4.1 2015 IFIP Summer School experiment

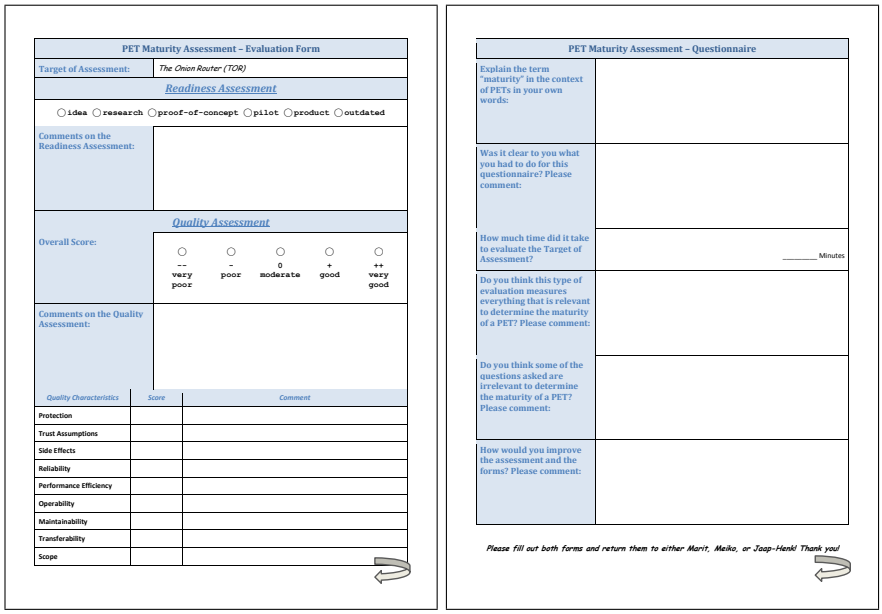
In August 2015, the IFIP Summer School on Privacy and Identity Management took place in Edinburgh. All attendees were invited to participate in the evaluation. The audience consisted of both experienced scientists on privacy engineering or privacy requirements and Ph.D. students from the disciplines of law, computer science, or social sciences. A workshop on "Assessing PET Maturity" was held on Wednesday, 19th of August, 2015. Prior to this workshop, all participants were asked to fill out a questionnaire for assessing a specific PET. Note that no precautions were taken to avoid double submissions or to prevent exchange of opinions between participants. The different readiness scales and privacy enhancement quality characteristics (see Section 3.2 and Section 3.3) were explained to the participants in two pages of introductory text as part of the questionnaire.

As Target of Assessment the tool for anonymising Internet communication *TOR – The Onion Router* was chosen because most of the Summer School attendees had probably at least heard about that PET or had gathered some practical experience. For simplicity reasons, we did not give more information on the Target of Assessment than "The Onion Router (TOR)" (see Figure 4).

The questionnaire was filled in by 14 attendees. Most of them took less than 20 minutes for filling in the questionnaire, only one person needed significantly more time. During the workshop with several more people who had not filled in the questionnaire, the results of the evaluation were presented and discussed.

4.2 Evaluation results

Looking at the definitions in the readiness scale, most participants thought that for TOR the readiness level of `product` would be appropriate (see Figure 5). Two participants were in favour of `pilot`, one person considered TOR as `outdated`. In the discussion at the workshop most people agreed on the readiness level



PET Maturity Assessment – Evaluation Form

Target of Assessment: The Onion Router (TOR)

Readiness Assessment

○ idea ○ research ○ proof-of-concept ○ pilot ○ product ○ outdated

Comments on the Readiness Assessment:

Quality Assessment

Overall Score:

○ -- very poor	○ - poor	○ 0 moderate	○ + good	○ ++ very good

Comments on the Quality Assessment:

Quality Characteristics	Score	Comment
Protection		
Trust Assumptions		
Side Effects		
Reliability		
Performance Efficiency		
Operability		
Maintainability		
Transferability		
Scope		

PET Maturity Assessment – Questionnaire

Explain the term "maturity" in the context of PETs in your own words:	
Was it clear to you what you had to do for this questionnaire? Please comment:	
How much time did it take to evaluate the Target of Assessment?	_____ Minutes
Do you think this type of evaluation measures everything that is relevant to determine the maturity of a PET? Please comment:	
Do you think some of the questions asked are irrelevant to determine the maturity of a PET? Please comment:	
How would you improve the assessment and the forms? Please comment:	

Please fill out both forms and return them to either Marit, Meiko, or Jaap-Henk! Thank you!

Fig. 4. Questionnaire for evaluating TOR

`product`. In the debate it was scrutinised whether a valid business model is necessary for the assessment `product` and how the attacks by the National Security Agency, as reported in the files from Edward Snowden's NSA revelations (e.g. for TOR [14]), would influence the evaluation.

In the quality assessment, the differences were bigger (see Figure 6): One participant attested poor quality (−), the others regarded TOR's quality as good (+). One participant did not vote at all. In such a situation, the detailed comments would have to be discussed among the experts, as it is known in reviewers' discussions on the quality of an academic paper. Also, it makes sense to document the reasoning so that it becomes clear which sources have been used by the experts, how reliable they may be, and whether their judgement focuses on specific usage contexts.

It is also interesting to look in more detail into the differing assessment results for each quality characteristic (see Figure 7). Obviously the participants had different views on several aspects regarding TOR. The characteristic *protection* was not regarded as poor or very poor by any participant. In the discussion it turned out that in particular the characteristic *side effects* were understood differently by the participants. Variations in assessments for *operability*, *maintainability*, and *transferability* can be explained by different practical experience with the tool.

Despite all differences in the detailed assessment, almost all participants agreed both on readiness and quality, resulting into a PET maturity level of $\texttt{product}^{+}$.

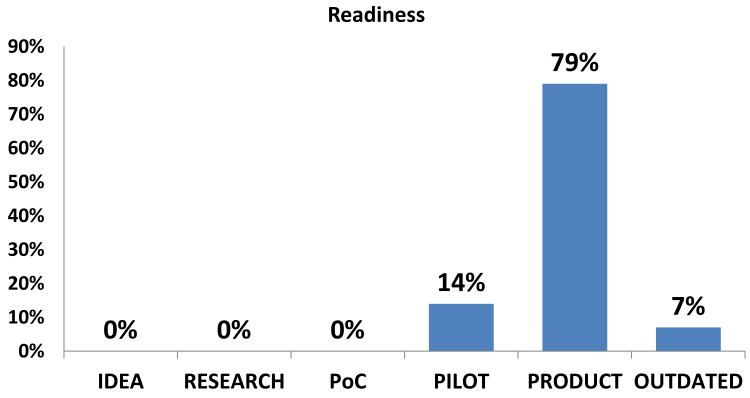


Fig. 5. Readiness Assessment of TOR

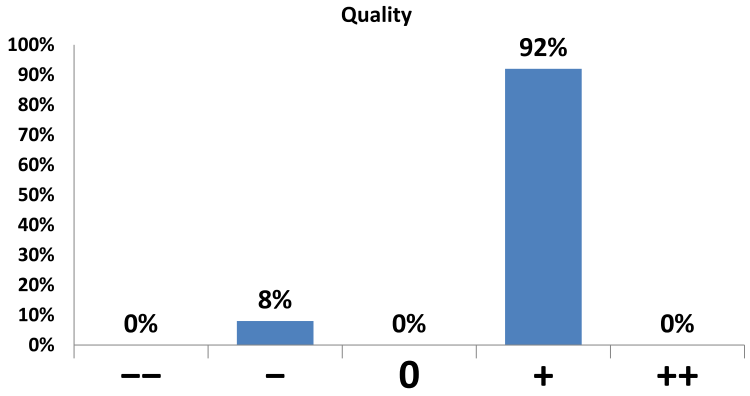


Fig. 6. Quality Assessment of TOR

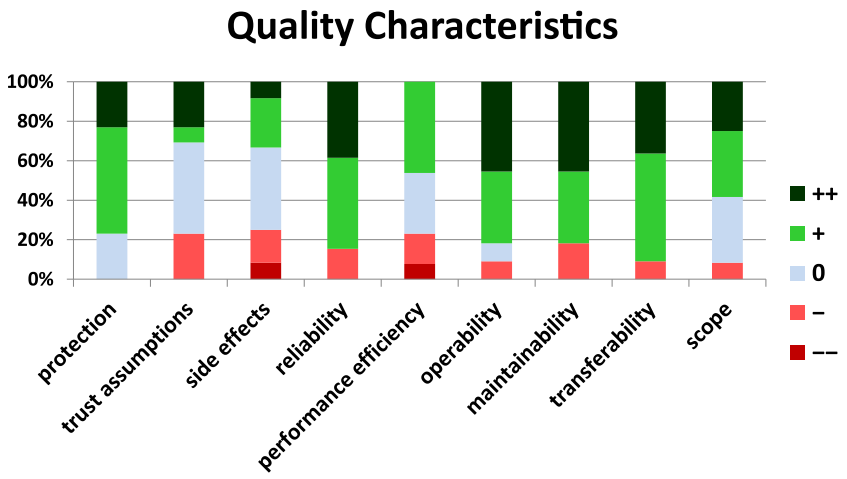


Fig. 7. Quality Characteristics Assessment of TOR

The experiment's results were used to prepare a controlled small-scale study for another PET maturity assessment where the roles of the assessor and experts were clearly assigned, the experts were chosen on the basis of their knowledge, it was enough time for an evaluation, the experts met in a phone call to discuss their individual results, and the procedure was well documented (see [10]). This following evaluation of our PET maturity assessment methodology focused on the adequacy, ease of use, effectiveness, and effort required to evaluate a PET.

Both experiments showed that the methodology is easy to use for experts, but probably not for non-experts. Also the lack of practical experience can be a problem when being asked to score characteristics related to operation of a PET. The separation between readiness and quality scores was acknowledged by the participants in the experiments. It was also evident that a fully automatic assessment on the basis of easily collectable and measurable indicators would not yield reliable results. Therefore the combination with an assessment by human experts was regarded as a necessity for a meaningful outcome.

Since the experts' opinions play an important role, the exact results may not be reproducible with other groups of experts. The tasks of the assessor, especially the choice of experts, the definition of the Target of Assessment, and the consolidation of the individual results, have to be exercised with due diligence.

The methodology should be further investigated with a larger number of PET assessments and an evaluation of the documented assessment processes. We believe that the consistent application to a set of different PETs will elicit the usefulness of the methodology.

5 Conclusions

The assessment of privacy enhancing technologies will become increasingly important as soon as the European General Data Protection Regulation has come into force. However, this is not an easy endeavor. In particular the direct application of the Technology Readiness Level scale could lead to misunderstanding if the privacy enhancement quality is ignored in the assessment.

We have proposed a framework for assessing both PET readiness and PET quality properties that can be combined into a PET maturity score. For this, we use input measurable indicators as well as human experts who are involved in the assessment process in a way comparable to scientific reviewers. In preparation of a controlled experiment that strictly followed the proposed process (see [10]) we used the opportunity of the interdisciplinary IFIP Summer School on Privacy and Identity Management to test the developed questionnaires and gather feedback from the participants.

We hope that the developed methodology will be used for assessing the maturity for PETs with varying complexity. Our vision is an easily accessible repository with PETs and their assessment results where readiness and quality can be discussed, where input for further improvements can be collected, and where researchers and developers can contribute to advance the state-of-the-art. This could boost the deployment of PETs by system developers and designers, the

demands from data controllers and data processors, and the integration in the checking and consulting activities of the supervisory authorities competent for privacy and data protection.

Acknowledgments. Part of this work was supported by the European Commission, FP7 ICT programme, under contract no. 318424 (FutureID project). S. Schiffner is currently employed by ENISA; the views presented in this paper are those of the authors and do not necessarily reflect those of ENISA. The work documented in this paper is part of ENISA's ongoing efforts to foster the uptake of privacy-enhancing technologies in Europe.

References

1. ISO/IEC 27004: Information technology – Security techniques – Information security management – Measurement (2009)
2. ISO/IEC 25010: Systems and software engineering – Systems and software quality requirements and evaluation (SQuaRE) – System and software quality models (2011)
3. European Parliament legislative resolution of 12 March 2014 on the 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)0011 - C7-0025/2012 - 2012/0011(COD)) (2014) (2014), http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0212
4. Borking, J.J., Raab, C.D.: Laws, PETs and other Technologies for Privacy Protection. Journal of Information, Law & Technology (JILT) 1(1) (2001), http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_1/borking
5. Cavoukian, A.: Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards, chap. Privacy by Design: Origins, Meanings, and Prospects for Assuring Privacy and Trust in the Information Era, pp. 170–208. IGI Global (2012)
6. Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., Robinson, W.: Performance Measurement Guide for Information Security. NIST Special Publication 800-55 Revision 1 (2008), http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf
7. Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.H., Le Métayer, D., Tirtea, R., Schiffner, S.: Privacy and Data Protection by Design – from policy to engineering. Tech. rep., ENISA (2014), http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design/at_download/fullReport
8. European Commission: Privacy Enhancing Technologies (PETs) – the existing legal framework. MEMO/07/159 (May 2007), http://europa.eu/rapid/press-release_MEMO-07-159_en.htm
9. European Commission: Horizon 2020 – Work Programme 2014-2015, Annex G. Technology readiness levels (TRL). European Commission Decision C (2014)4995 of 22 July 2014. Tech. rep. (2014), http://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf

10. Hansen, M., Hoepman, J.H., Jensen, M., Schiffner, S.: Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies: Methodology, Pilot Assessment, and Continuity Plan. Tech. rep., ENISA (2015), https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/pets
11. ISACA: COBIT 5 for Information Security (2012), http://www.isaca.org
12. Mankins, J.C.: Technology Readiness Assessments: A Retrospective. Acta Astronautica 65, 1216–1223 (2009)
13. Nolte, W.L.: Did I Ever Tell You About the Whale?, Or Measuring Technology Maturity. Charlotte, North Carolina: Information Age Publishing (2008)
14. NSA: Tor Stinks – presentation slides as part of Edward Snowden's NSA revelations (June 2012), https://cryptome.org/2013/10/nsa-tor-stinks.pdf
15. Olechowski, A.L., Eppinger, S.D., Joglekar, N.: Technology Readiness Levels at 40: A Study of State-of-the-Art Use, Challenges, and Opportunities. MIT Sloan Research Paper No. 5127-15. Tech. rep., MIT (2015), http://dx.doi.org/10.2139/ssrn.2588524
16. Smith, J.D.: An Alternative to Technology Readiness Levels for Non-Developmental Item (NDI) Software. In: Proceedings of the 38th Annual Hawaii International Conference on System Sciences – HICSS '05 (2005)