Privacy Enhancing Technologies: Evolution and State of the Art

A Community Approach to PETs Maturity Assessment

DECEMBER 2016

www.enisa.europa.eu European Union Agency For Network and Information Security

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.

Contact

For queries in relation to this paper, please use opsec@enisa.europa.eu
For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

This document is the result of a long discussion process. We would like to thank everybody who discussed with us, most notably the community of the annual privacy forum.

Table of Contents

1. Introduction 4
2. Requirements, Advantages and Challenges of a PETs Maturity Repository 5
2.1 The need for PETs 5
2.2 Requirements for a PET Maturity Repository 6
2.3 User groups, benefits and advantages of the PET Maturity Repository 6
2.4 Challenges to adoption and real-world utilization of the PETs Maturity Repository 8
3. Towards building a community 11
3.1 Hosting and maintenance 11
3.2 Dissemination and promotion 12
3.3 Content generation and trust building 14
3.4 Continuous improvement 14
4. Current situation and short-term action items 16
4.1 Hosting and dissemination 16
4.2 Platform development continuation 16
4.3 Gathering users: support for early assessments 16
5. Conclusions and future work 18

1. Introduction

Since 2014, ENISA, with its partners, conducts a wide spectrum of studies related to privacy and data protection by design. A key aspect of this work was to engage a wide spectrum of communities. Academia (legal and technology experts), regulatory authorities (DPAs), policy makers (mainly European Commission), and industry contributed to these reports and projects.

While these studies' target audience are policy makers and developers, we presented these results to the global research community for validation. One of the main outcomes of these studies is a comprehensive methodology for Privacy Enhancing Technologies (PETs) maturity assessment. In this particular study, the authors have identified that development of ICT tools that support the PET assessment process (referred to as (*PETs) assessment tool*) by gathering information on indicators and guide experts and the assessor through the assessment process is essential for the creation of a functioning community of contributors. In April 2016, ENISA initiated a project focused on providing such tools. As its main result, in September 2016 a prototype of the online PETs maturity assessment tool was presented to the public. This online tool is a direct continuation of ENISA studies and is providing an IT service (in a form of web application) that facilitates the formation of an expert community, which can perform technology maturity assessments. The tool supports the publication of the assessment results in a structured and searchable fashion. However, to evaluate and update the maturity assessment methodology, a wide community of active users is needed. In the reminder of the document we will refer to the collection of finished assessments as *(PETs) maturity repository*, and the assessment tool, repository, and its users as *(PETs) maturity platform*.

This document provides recommendations on how to build and maintain an online community for PETs maturity assessments, which is assisted by ENISA's tool. The presented community development approach seeks to guide developers and to empower individuals and groups of people with the set of skills they need to actively participate in the PETs assessments process. It presents four key areas which should be taken into account while developing the community: hosting and maintenance, dissemination and promotion, content generation and trust building, and continuous improvement. Each of these is discussed briefly, followed by a short review on the current state of this initiative.

2. Requirements, Advantages and Challenges of a PETs Maturity Repository

2.1 The need for PETs

There has always been a need for privacy-enhancing technologies in certain application domains. Medical research cannot be performed responsibly without strong anonymity and pseudonymity guarantees, as it is the case with many military and high-security domains of application. With the 2016 European General Data Protection Regulation (GDPR)[1] this need has come into focus, not just for those special application domains, but for most European companies and organizations that process personal data. In article 25 of the GDPR, companies are required to follow the principle of "Privacy by Design", i.e. privacy properties need to be considered throughout the entire development cycle. Today an IT product is usually build using pre-existing building blocks and technology. For this, privacy-enhancing technologies play a major role in implementing such Privacy by Design approaches into real-world systems, thereby making them essential tools of the information systems of tomorrow.

Despite this rising demand for PETs, their documentation is often weak and scattered. To our knowledge, few data sources exist that give guidance on utilization of a given PET or that help to select the right PET for a given purpose nor does a publicly available and reasonably well-maintained repository of PETs exist. Some initiatives like the Privacy Patterns project[2], the ISO29100 catalogue of privacy patterns[3], or the List of PETs at Stanford's CyberWiki[4] attempted to collect and partially systemize PETs; however, those three collections themselves have almost no overlap, and differ both in focus and listing criteria for the PETs they cover. Neither of these initiatives attempts to deal with questions of implementation, applicability, quality, or even maturity of PETs.

There exists, however, a huge body of work in the field, i.e. research articles that propose, discuss, or break individual PETs, which are published in peer reviewed conference proceedings such as the Privacy-Enhancing Technologies Symposium[5] or the Annual Privacy Forum[6]. However, the scientific process these conferences usher is focused on knowledge discovery and originality. The contributions only relate to each other as far as needed to demonstrate novelty and progress. Information on how to apply a new technology is usually sketchy and neither well-structured nor concise enough for developers. For example, if one article features a new type of PET, there might exist an implementation of that PET or not; it might have been tested under real-world conditions or not; it might have been implemented as a ready-to-use product or as a wiggly prototype on a Ph.D. student's laptop. There might even exist several other articles that trivially break the assumed privacy-enhancements of a proposed PET. Neither of these issues can be trivially or timely determined from the sheer investigation of those research articles.

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
[2] https://www.privacypatterns.org/
[3] http://privacypatterns.wu.ac.at:8080/catalog/
[4] https://cyberlaw.stanford.edu/wiki/index.php/PET
[5] Privacy Enhancing Technologies Symposium, https://petsymposium.org
[6] Annual Privacy Forum, http://privacyforum.eu/

Given that these sources are among the best resource pools to be found on the topic of PETs in the public domain, it can be seen that there certainly is a high demand for a more complete, concise, and well-maintained source of information on the set of existing PETs and on their readiness for application or in other words a PETs maturity repository.

2.2 Requirements for a PET Maturity Repository

In order to implement and operate a reasonable, complete, concise, easy-to-use, properly-maintained and full-featured PETs maturity repository, there are several key requirements to be met. These requirements address the relevant stakeholders, such as

- the host organization of the PET maturity repository,
- the community of PET experts to maintain the repository, and
- the community of users that profit from the PET repository.

The PETs maturity repository needs to comply to several requirements for each group. Furthermore, stakeholders have expectations to each other. We will detail out toese in the following section.

2.3 User groups, benefits and advantages of the PET Maturity Repository

We believe, the demand for access to information on privacy-enhancing technologies is rising. This has impact on several types of stakeholders (see Figure 1) that would all profit from the existence of a well-maintained PETs maturity repository.

Figure 1 The stakeholders of a PET Maturity Repository.

Most obviously, *software developers* can directly profit from access to information on real-world usable PETs, probably accompanied with links to publicly available source code repositories, implementation details, documentation, and integration support for quickly being able to utilize high-quality PETs in their

products. Moreover, based on the readiness assessment accompanying each PET in the repository, developers can easily determine which PETs are of sufficient level for utilization, and which are still in a pre-utilization stage that would make implementation complex or impossible. Similarly, they learn about PETs that are outdated, broken, or otherwise not reasonable to be utilized in modern software products. Based on the quality assessment, developers can even compare and rank different PETs for the same application scenario, thereby profiting from the expertise of the board of experts that assessed the PET in consideration. If, for example, two PETs for the same application scenario, with equal readiness levels, differ with respect to their quality levels, the developer can safely decide for the one with higher quality level, providing stronger guarantees on privacy-enhancement for the resulting software product.

For *companies*, the PET Maturity Repository allows for a peek on new technologies that are not yet in the market, but soon will make their debut as a component within a software product. This enables them to adopt the new trends early, eventually becoming front-runners of privacy within their domain of application, or even creating new markets in that respect. The repository provides such companies with an easy way to assess which PETs are worth being considered for a pilot implementation, and which might need more research and/or real-world testing before becoming business-ready. The PET readiness assessment level of PILOT provides exactly the stage of readiness required in such a case, and by means of the repository, the list of PILOT-level PETs can easily be accessed and evaluated.

Data protection authorities and other *government bodies* with responsibility in the privacy area can rely on the PET Maturity Repository to quickly and with limited need for in-house expertise judge on the capabilities of a PET. This allows for better quality of supervision activities, e.g. in cases where companies make false claims about capabilities of qualities of a PET their product utilizes. In such cases, the corresponding PET entry in the PET Maturity Repository allows for a quick comparison, both whether the proclaimed quality characteristics are shared by the community experts, and whether implementation of such a PET is even feasible given the current stage of PET readiness. For instance, this might become relevant if companies claim to have implemented a certain PET, such as a Fully Homomorphic Encryption scheme. In such a case, the repository allows for a quick check on whether this is a realistic possibility or just an overbold marketing claim of the product maintainers. Moreover, companies might claim that a certain protection property cannot be implemented with the available technology to reduce costs. Today it is very hard to disprove this claim, not so with an extensive technology repository.

Research institutions can utilize the PET Maturity repository to quickly gather information on interesting state-of-the-art PETs in RESEARCH level, which might be worth being supported to start a real-world validation phase with. Based on the quality assessment, they can even sort out the least promising candidates, allowing for an optimization of the resources spent on the best candidate PETs.

Individual privacy Researchers can benefit from such a repository as well. Similar to the position of the IACR Cryptology ePrint Archive[7] in the realm of cryptology, a PET Maturity Repository would allow such researchers for publishing and promoting the latest PETs that they have been working on in a precisely targeted way. Probably, along with developing such PETs, these researchers would become experts or even assessors of their own PETs within the community of the PET Maturity Repository, which in turn would be beneficial for their scientific reputation.

Research funding agencies can profit from the repository in order to quickly assess which types of PET are becoming relevant (i.e. raise from IDEA readiness level to RESEARCH readiness level), and can utilize that information to shape their research funding strategies accordingly. Also, they can easily determine high-

[7] Cryptology ePrint Archive, https://eprint.iacr.org/

quality PETs in RESEARCH level that might be worth being supported for a real-world implementation, e.g. by funding a pilot study.

Finally, *society* as a whole can profit largely from the existence of such a repository, as it allows interested citizens to quickly and without a need for in-depth expertise judge on the marketing claims of companies with respect to privacy preservation of their products. A quick look at the readiness assessment of such a product might allow to determine that the PET utilized was broken already, or that it is far from real-world readiness, making such a marketing claim become bogus. Similarly, the quality assessment gives a direct indicator on whether a product is judged of good quality with respect to privacy-enhancement or not, based on the analysis of independent experts in the field.

2.4 Challenges to adoption and real-world utilization of the PETs Maturity Repository

In order to achieve the goals stated above, the PET Maturity repository has to get past some critical challenges to its real-world implementation. These range from finding an appropriate host organization to gathering a critical mass of community experts to testing and validating the ideal design and feature list of the platform tools.

Finding an appropriate host

Apart from the development and continuous improvement of the technical implementation of the platform, an even more critical issue is that of finding the ideal host organization. Given that the host organization has full control over the platform's internal and external behaviour, there is a high demand for trustworthiness of this host not to interfere with the operation of the platform. Especially when dealing with experts in the area of privacy, issues like this can easily become challenges that probably have a major effect on other aspects such as community gathering. If the community does not trust the host organization of the PET maturity platform to be neutral against the individual assessments performed on the platform, or if there is reason to doubt the fair and equal treatment of all parts of the expert community, this will most likely have severe impacts on the size and willingness of the community in total.

In this respect, a major part of the challenge is in finding the right organization type. If the platform is operated by a single private sector host company, this immediately raises concerns against its neutrality. Will it feature better assessment results for PETs utilized in its products? Will it dominate the expert community of the platform with its own employees? Will it keep staying neutral and operational towards the platform if it gets sued by a competitor company for results of a PETs assessment, e.g. if the assessment negatively impacts on that other company's products? Each of these issues raises concerns, tentatively excluding this option from being an ideal hosting scenario.

A purely government-instantiated organization, such as public bodies of the European Commission, also has some trust issues. First, none of the existing government organizations on the European level assumes to have a mandate or to operate a platform such a repository as of today. In fact, the bodies ENISA had contact with, were reluctant to assume responsibilities and were in doubt if such activities would be in their mandate. Hence, none of them would be allowed to host and operate the platform as of tomorrow; each choice would require new regulation being instantiated. Second, government organizations on member state level may face political criticism from other member states if they would host a pan-European platform like this on a nationally controlled organization, even if that organization would be an expert in the field of privacy, such as a data protection authority of one of the European Union's member states. Third, even if a government-instantiated body on the European Level, such as ENISA or the European General Data Protection Supervisor's office would be legitimized to host the platform, this choice would likely

still be considered questionable by at least some experts in the realm of privacy, since many privacy experts do not trust state organizations unconditionally. Thus, a purely government-operated platform may distract a critical part of the community from participating in – and thus supporting – the platform.

The ideal host appears to be a consortium of organizations that mutually control each other and thereby eliminate the individual issues of each type of organization. Such consortium-based collaboration is a common organizational structure e.g. in the realm of joint research projects in Europe, or with public-private partnership project consortia. Having such a consortium would probably eliminate most of the issues seen for individual host organizations, and thereby might be able to attract the most number of experts for the required community to maintain the PET Maturity repository. However, such a host is non-trivial to be found.

Community gathering

As outlined above, gathering and including a sufficient amount of experts in the realm of privacy-enhancing technologies is one of the key challenges to the success of the PETs maturity repository platform. A large base of experts in the field is required in order to meet the minimum criteria for performing an assessment on the platform. Currently, each assessment requires at least five domain experts for each PET assessment, thus the group of community experts has the largest demand for manpower within the whole platform. This demand can probably be addressed by recruiting experts from the research domain. As is already established with the scientific publication process, where each new research article needs to be reviewed by at least three domain experts before being published, the experts of the PET Maturity repository may work without gratuity. Their compensation for participating in an assessment as an expert consists in the scientific reputation gained from being considered as an expert. Hence, in order to motivate such experts to join the platform, it is necessary to allow these experts to gain such reputation from their work in a best-possible manner. This may range from listing the expert's names along with the assessment results to dedicated awards and designations of experts that contributed substantially to the platform, e.g. in number of assessments performed.

In order to foster this expert attribution, it is necessary to identify the ideal approach of attribution and reputation for community experts of the platform. Here, the platform contains several open research questions, such as on a rating system for assessments, which in turn is also a rating system of the experts involved in these assessments, or on a platform-maintained database of domain experts where potential assessors can pick and choose experts from. Several technical methods to support the reputation-building capabilities of the PET Maturity platform are possible, and it is essentially necessary to test and analyse the ideal approaches to be implemented in the final, real-world implementation platform. This, obviously, requires additional research efforts to be performed.

Apart from the expert involvement, another key stakeholder group is that of the assessors. Assessors are the ones keeping the platform alive, as each new assessment process is binding community members to the platform, e.g. as experts or as users of the assessment results. Hence, in terms of gathering a community, the assessors have a most significant role. Thus, the platform should be implemented to support the tasks of the assessors in a best possible manner. As with the expert gathering, again, this may include reputation-based motivations to become an assessor within the platform, but additional motivations may be relevant as well. In order to identify these potential motivations, it becomes necessary to identify the exact needs of the assessors within the PET Maturity platform. Are they in for the reputation of being an assessor? Are they actually developers of PET technologies themselves, trying to make their own PETs more public, or seeking inputs on the quality attributed to their PETs by community experts? Are they users of the assessment results themselves? For what purposes? Here, a lot of open questions exist that probably can only be answered by a large-scale survey among potential users and supporters of the platform. Such a

survey should seek to collect and rank the different motivations of potential assessors, and seek to optimize the technical workflow within the platform so that these motivations are well considered.

Beyond these two more active stakeholder groups, the largest set of people obviously consists in users of the assessment results. Here, as was discussed before, a large variety of different types of users with different potential motivations exists. However, it is not yet clear which of these user types are relevant for the platform, what exact needs those users actually have, and how the results of the individual assessments can ideally be presented to best-possibly fulfil the needs of these users. The current, generic approach of presenting the assessment outcomes, along with a sorting functionality, might help with the task of navigating the set of existing assessments, however, there might be more specific needs to filter the assessment list for the particular needs of the different user types. Some might only want to see current or most recent assessments, some might be interested in a specific application domain only, some might have an interest in the activities of specific assessors, experts, or organization members only, or may only want to see results of a certain quality or readiness level. Each of these restrictions have to be supported by the platform, based on the exact needs of the particular type of users.

Again, a survey among the interested user groups of the PET Maturity repository would be necessary to gather insights with respect to these issues. Then, the results of the survey must be analysed with respect to possibilities of technical support functionality that the platform could provide in order to meet the demands of the user groups. Subsequently, these functionalities need to be implemented and added to the platform services for evaluation. Finally, an evaluation needs to be performed with respect to the degree of acceptance of such new functionalities by the users. Thus, this process requires continuous monitoring of the platform functionalities, in order to gather the required information for this evaluation. It is therefore inevitable to operate the PET Maturity platform in a testbed environment that allows for monitoring and continuous development as long as the test and evaluation processes run. Unfortunately, to some extent, this counteracts the trust establishment into the host organization discussed above. Monitoring of user behaviour in the PET Maturity platform may be required for evaluation, but at the same time may confirm the concerns of privacy experts with respect to trustworthiness and privacy compliance of the host organization. Here, advanced privacy-enhanced techniques may become necessary to be applied to the platform itself, in order to transparently allow for both monitoring and privacy preservation of platform users at the same time. This requires additional research efforts, in order to evaluate the ideal solutions for such a scenario. It might be a good idea to focus on this – quite common – problem scenario and the PETs that resolve it as focus of the early test assessments of the PET Maturity platform. Then, the platform would already become of use by optimizing its own implementation with respect to privacy enhancement.

Generally speaking, there are several options and functionalities that could be implemented to ease the use of the PET Maturity platform according to the different needs of its users. However, in order to identify and implement the most promising ones, it is inevitable to run a preliminary version of the platform in a test and evaluation environment, along with research efforts, such as the user survey, that shape the way for the evolution of the platform.

3. Towards building a community

With the aim to build a PETs maturity assessment community in mind, we can derive from the requirements for the platform, some immediate action items can be derived. In this section, we recapitulate these requirements, indicating their current state, and the next steps needed. While in our community members have different roles, see

Figure 2, initially the foremost challenge is to find a long-term host for the platform.

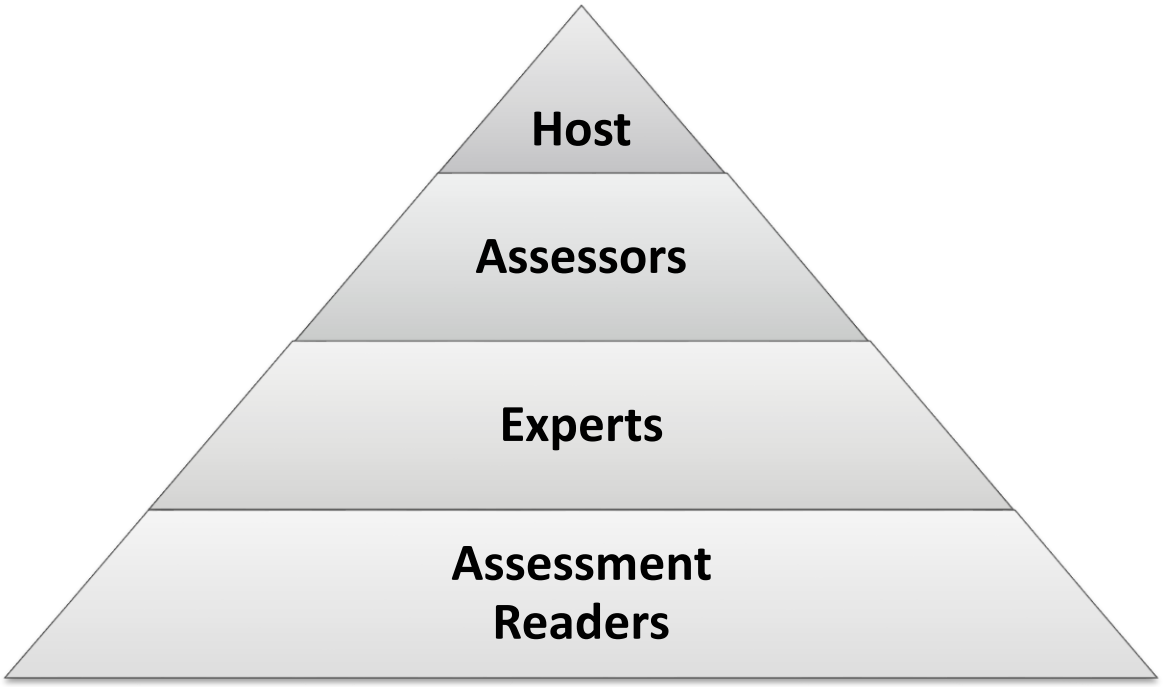

Figure 2 Roles in a Maturity Assessment Community.

Host. The organisation which is responsible for hosting and maintenance of the PET maturity assessment tool and its content (conducted PET maturity assessments, online community of users etc.).
Contributor (as assessor or expert). Individual professionals with an expertise in the data privacy domain, actively involved in content generation as an assessor or a member of the board of experts for a specific PET maturity assessment(s).[8]
Reader. An organisation, an individual professionals or enthusiast who is passively consuming collected content (conducted PET maturity assessments) or is a random users encountering the tool on the Internet.

3.1 Hosting and maintenance

A community needs a home; an online community needs an online platform. For this reason, a key element of success is to find a long-term partner who will host, maintain, promote and possibly further develop the PET Maturity Assessment Platform according to the feedback gathered from the involved community. The purpose for the online PETs maturity assessment tool, which should be globally recognisable,

[8] Note, individuals might be mandated by organizations or act otherwise with an agenda; transparency is key here.

and trusted, is to host and maintain an up-to-date repository of Privacy Enhancing Technologies (PETs) maturity assessments. In order to keep the repository up to date and consistent, the conduction of assessments, according to the methodology[9] developed by ENISA, is fully integrated in the platform. One of the biggest challenges is therefore to find such a partner who will invest own resources to support the PETs maturity assessment concept and will further continue the project.

A key element of success while building the online PETs maturity assessment community is to find a long term partner who will host, maintain, promote and possibly further develop the tool according to community feedback.

While building the tool, creators have performed an initial analysis of potential candidates for tool hosting and maintenance. The intention was to classify organizations worldwide that are related to data protection, such as authorities, public and private organisations, or developers of ICT products and standardization bodies, in order to select best candidates for becoming the host of this platform. Over 120 different organisations (in terms of size, profitability, geographical distribution and capacitates) were identified and prioritised for first contact.

In 2017, ENISA and its partners will take the following actions to engage potential long-term hosts (already identified or to be identified) for the PETs maturity assessment repository.

Prepare an online survey for gathering initial feedback regarding the scope of candidate involvement for host, assessors, experts, and supporters,
prepare dissemination materials presenting the basic PET Maturity Assessment Platform concept and next steps for adaptation to market,
prepare letters of support from ENISA and its managing bodies and search for political support,
prepare a strategy for sharing the software (including e.g. IPRs, source code access, licence and other agreements),
send a direct messages with the above mentioned materials to the candidates, or engage candidate representatives during individual meetings or at key venues such as data privacy-related conferences.

The PET maturity assessment tool host should

- be an international (EU or global), business independent, recognisable and trusted organisation (or umbrella organisation of such organisations),
- be actively involved in data privacy and ICT security issues,
- have resources (IT infrastructure, experts, time) to deploy and maintain the tool.

Finding a host should be considered as a top priority task for building the PET maturity assessment online community as it affects other activities e.g. dissemination, marketing and continuous development.

3.2 Dissemination and promotion

Dissemination is the process of making the PETs maturity assessment tool available to all stakeholders and to the wider audience, e.g., data privacy organisations and individual experts). Dissemination is essential for the success of the tool and its sustainability in the long term. Essentially the purpose of dissemination and promotion during first steps of building the community is **to raise awareness about the existence of**

[9] https://www.enisa.europa.eu/publications/pets last visited December 2016

the PET maturity assessment online tool and encourage potential users to try the tool. For this reason, the tool host and ENISA should promote the solution and maximise its visibility within data privacy domain. Dissemination process is also crucial for finding potential candidates for the tool host as mentioned above. Stakeholders, relevant institutions, organisations, and individuals who are the target of dissemination and promotion activities can be classified according to the level of commitment.

To build a community and sustain the PET maturity assessment tool, dissemination and promotion activates should be subordinated to the following sequence: find a host, maximise contributors to generate more content (PET maturity assessments), attract viewers and convert them into active contributors.

The following dissemination channels should be considered for building the community.

- publications, and talks at data privacy and security conferences and workshops,
- collaborative events, e.g. organizing own conferences and workshops,
- PET maturity assessment tool host's and ENISA's official websites,
- PET maturity assessment tool host's and ENISA's social media channels,
- dedicated, new social media channels (to be created PETs maturity assessment platform's Twitter, Facebook profiles),
- forums and other data privacy expert's online spaces,
- direct communication (e.g. newsletters)

First dissemination activities have already been conducted. The PET maturity assessment tool was presented during APF2016 (Annual Privacy Forum 2016), 7-8 September 2016 in am Main, Germany.

Dissemination requires a clear strategy explaining how the visibility of the tool will be maximized. ENISA together with the future host needs to create a set of promotional materials (flyers, posters, online banners etc.) should be produced. An important part of such materials is a tool visual identity. The developers of the tool have drafted such visual identity (colour scheme, logo etc.); however, it reviewed to incorporate the visual identity into the organisation brand of the future host and ENISA. The brand loyalty is critical for efficient dissemination therefore its activities should be preceded by decisions regarding visual identity (at least on a general level of tool naming, basic trademarks). Moreover, for the online tool, a brand recognition is also based on domain name. ENISA or the tool host should decide about the domain where the tool will be always available on the Internet. The domain name is transferable, regardless the actual tool hosting server address and location, therefore it should be fixed as soon as possible for dissemination and promotion purposes.

Setting the domain name for the PET maturity assessment online tool is important for the efficient dissemination and promotion.

Possible performance indicators for dissemination and promotion:

- total number of homepage visits,
- total number of new sessions (unique users),
- total number of registered accounts,
- average time of using the tool by registered users,
- bounce rate (percentage of users leaving before further exploring the tool),
- total number of social media feeds/re-feeds, followers,
- total (and per user) number of started/ finished assessments.

3.3 Content generation and trust building

The PETs maturity assessment tool provides an online mechanism to perform the collaborative process of maturity assessments according ENISA's methodology (including support for the community aspects and archiving of results). However, beyond this the tool is not providing added value to its users. This has to come from its content, PET maturity assessments. For this reason, the content should be considered as a critical resource in community building process. The more valuable content is available, the more users will be attracted to try the tool, join the community and finally to provide new content. This cycle is typical for all online platform-like solutions and is also applicable for PET maturity assessment tool.

The content (PET maturity assessments) should be considered as a critical resource in community building process. The more valuable content is available, the more users will be attracted to try the tool, join the community and finally to provide new content.

However, the **content quantity** (number of PET assessments stored in the repository) is not enough to ensure tool sustainability and community growth. The following other content characteristics should also be considered.

Quality. In particular, within data privacy domain, available content (PET assessments) should be verified and of a high quality, vendor independent and unbiased to build appropriate level of trust.
Diversity. To not limit the interest of possible viewers and contributors, available content should be diversified in terms of PET types (APIs, SDKs, SaaS, plugins, software libraries, hardware devices etc.), versions, purpose etc.
Validity. Available content should reflect the current state-of-the-art and up-to-date PETs. As new technologies for data security and privacy are constantly evolving, obsolete and not valid PETs assessments should be clearly indicated and if possible new assessments for such PETs should be conducted.
Transparency. Moreover, the process of content creation needs to be transparent. This includes the identity of the assessor and experts as well as their relation to the target of assessment.
Verifiability. The proposed assessment process was designed with the aim to objectivise subjective views on the technology readiness and quality of a target of assessment by collecting and providing evidence. This evidence needs to be made available.

While it is mainly the tool host responsibility to stimulating content quantity, quality, diversity and validity by involving skilled experts it the tool maintenance process and encouraging for community growth, it is transparency and verifiability that is key to build confidence and trust in the community.

Performance indicators for content generation and trust building include

- total number of completed/ongoing PET maturity assessments,
- average size of a board of experts,
- total number of unique assessors,
- total number of assessments per category (e.g. type),
- average assessments update time (time between assessments),
- average assessment duration.

3.4 Continuous improvement

It is important for both ENISA and the host to include a continuous improvement process for the PET maturity assessment tool. It includes methods of getting feedback from users and upgrading the tool regard-

ing **concepts** (e.g. methodology for the PET maturity assessment), **software** (e.g. user experience, interactions, look and feel, performance, data entities) and **content** (e.g. conducted assessments, community of users). As a result, the tool development roadmap should be updated and appropriate actions should be executed according to given priorities (e.g. reported software bugs fixing). The development of the tool should be continued in order verify implemented within the tool hypothesis and to adjust it to the real needs of users and according to their suggestions (add new, remove outdated and update existing features). Building trust for online tools like PET maturity assessments repository is a long term process which efforts can by completely undone without taking into account users feedback.

Once the tool is established and recognisable within the data privacy domain and first early adopters are acquired, there is a need to sustain users' engagement. The continuous improvement is crucial for this process. Critical errors should be fixed as soon as possible, while other request (minor software bugs fixes or new features) should be prioritised and implemented accordingly.

Performance indicators for the continuous improvement include

- total number of issues reported/fixed,
- total number of new features requests/implemented,
- total number of critical errors reported/fixed.

4. Current situation and short-term action items

4.1 Hosting and dissemination

In an ongoing effort to continue development and foster community gathering until a valid long-term host is found, an intermediate solution currently in negotiation is to have the current state of the PET Maturity Assessment Platform being hosted and continued by the consortium of a European research project. Concretely, the EU project TRUESSEC is currently negotiating a Memorandum of Understanding with ENISA to elaborate the exact technical, legal, and organizational requirements for hosting the platform within their project duration, which is 2 years as of Jan 2017. Due to the backing of this research project, which is a Coordination and Support Action (CSA) within the EU's H2020 research agenda, the tasks of hosting and dissemination of the PET Maturity Assessment Platform is likely taken over by this very research project's consortium. This clearly sets an excellent basis for the action items of hosting, dissemination, and continuation.

However, TRUESSEC's project duration is set to two years. This sets a tight timeframe to find a long-term host. Moreover, it is not yet clear how the necessary resources for hosting and maintenance (such as server operation, mail account maintenance, user support, and dissemination material production costs) can be provided beyond 2017. Here, additional funding is required.

4.2 Platform development continuation

The current state of the platform's software implementation provides the necessary functionalities for performing early PET maturity assessments. However, during the development of the platform, the implementers identified several points that should be addressed for getting a more robust, more reliable, more usable, and thus more successful platform implementation.

Here, it is necessary to continue development of core functionalities of the platform's software implementation, as well as gathering and implementing extended functionalities as suggested by early adopters and user feedback. This is a critical component especially in the early phase of operation of the platform, as a lack of usability/utility may distract early users from continuous participation in utilizing the platform.

Thus, besides core hosting, the continuous development and improvement of the platform itself needs to be performed, and needs to be given the required resources.

4.3 Gathering users: support for early assessments

The most essential ingredient of a successful PET maturity assessment platform consists in its users, that is its assessors, its experts, its assessment readers. During the two ENISA projects that developed both methodology and implementation of the platform, a lot of individuals have taken actions to promote and disseminate the platform in early announcements. However, it is not likely that this will lead to a huge amount of volunteers ready to become assessors themselves within the platform, especially with a lack of public awareness, if there are no clear incentives to participate. This hurdle can only be overcome by performing and publishing some excellent early assessment results. As each newly completed assessment process results in yet another item of interest – the assessment report – on the platform, it can help in attracting more users to the platform, initially as assessment readers, but subsequently as experts or even assessors themselves.

However, it is necessary to have at least some good assessment results for some highly prominent examples of PETs being shown on the platform at an early stage, in order to get to the critical mass of a self-supporting user community. These early assessments can only be performed if there are other incentives than reputation being involved. Here, early promotion activities like sponsored assessments or assessment quality competition awards may help with stimulating a community of early adopters. Again, such promotion efforts require some resources in order to be performed, which need to be contributed externally.

5. Conclusions and future work

Building an online community of users is particularly hard because members are often anonymous and relations between them are virtual. For the PET maturity assessments repository tool it is even harder due to the fact that it is primarily designed for a specific group of users involved in data privacy issues. For this reason, it is important to address several issues immediately:

First, it is inevitable to find a trustworthy host that will invest own resources to support the PETs maturity assessment concept and will stimulate growth of the community to continue the project.

Second, dissemination and promotion activities for attracting users and gathering a community is required, including early assessments to be shown as examples of utility.

Third, continuation and improvement of the platform implementation needs to be performed.

Finally, once a significantly large community exists, continuous feedback integration into the development of the platform needs to be addressed.

Once these issues have been resolved, the resulting platform for assessment of maturity and technology readiness of Privacy-Enhancing Technologies has the capability to play a major role in the adoption and implementation of the European General Data Protection Regulation in all parts of Europe and beyond.

ENISA

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

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

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