Patterns for Privacy (P4P)

Principal applicant

dr. Jaap-Henk Hoepman
Digital Security
Mailbox 47
Institute for Computing and Information Sciences
Radboud University Nijmegen
P.O. Box 9010, 6500 GL Nijmegen, the Netherlands
Phone: +31 24 3652077
Fax: +31 24 3652298
Email: jhh@cs.ru.nl

Application history

This is a new application, for the 2014 NWO Cyber Security call.

2 Summaries[1]

2.1 Scientific summary

The World Economic Forum [20] has recognised that the economic value of personal data is threatened by a steady decline in trust by all stakeholders, and recommends to develop principles to encourage the trusted flow of personal data. The proposal for a new European data protection regulation [6] explicitly requires data protection by design and by default. This shows that privacy by design [4] is becoming a significant economic and regulatory factor. It is therefore crucial to support developers in satisfying these requirements with practical tools and guidelines.

This proposal aims to achieve just that.

During our study of privacy design strategies [d, e] we discovered that a comprehensive and readily applicable set of tools to support system designers to design for privacy does not exist. In particular, a systematic study of privacy design patterns is wanting. Only a small, incomplete and inconsistent patchwork of privacy design patterns exists [10, 11, 15, 14, g].

To bridge this gap, the project will

- develop a framework to express and study privacy design patterns,
- develop a comprehensive catalogue of such privacy design patterns, and
- develop tools to support system designers to apply privacy design patterns throughout the system development lifecycle.

TNO, our industrial project partner, is busy raising a consortium that will implement a national health data infrastructure. It will use our results in the development of such personal health information providers.

2.2 Lekenabstract

Privacy by design [4] is een ontwerp filosofie die als doel heeft IT systemen privacy vriendelijker te maken. Uitgangspunt van deze ontwerp filosofie is de constatering dat privacy (net als security) een kern eigenschap van een IT systeem is die in hoge mate bepaald wordt door het onderliggende systeemontwerp. Als gevolg hiervan kan privacy bescherming niet naderhand aan een al bestaand systeem worden toegevoegd. In plaats daarvan moet privacy vanaf het begin meegenomen worden. Het fundamentele principe van privacy by design is dus dat privacy eisen gedurende het hele ontwikkeltraject van een systeem moeten worden meegenomen. Dat wil zeggen: vanaf het moment dat over de eerste systeem concepten wordt nagedacht tot en met de werkelijke implementatie van het systeem.

Volgens het World Economic Forum (WEF) creëert de explosieve groei in de hoeveelheid en kwaliteit van persoonlijke gegevens die digitaal verwerkt worden significante mogelijkheden voor nieuwe vormen van economische en sociale vooruitgang. Zij onderkent echter ook dat vele high profile datalek incidenten en de perceptie van machteloosheid die mensen ervaren er voor hebben gezorgd dat alle stakeholders steeds minder vertrouwen in de IT systemen (en de informatie-samenleving in zijn geheel) hebben gekregen [20]. Het WEF beveelt daarom onder meer aan om breed gedragen principes te ontwikkelen die de betrouwbare verwerking van persoonlijke gegevens ondersteunen. Daarnaast bevat het voorstel voor een nieuwe Europese verordening voor data protectie [6] de expliciete eis dat privacy de default is, en stelt zij de toepassing van privacy by design verplicht.

Dit toont duidelijk aan dat privacy by design een significante economische en juridische factor is geworden. Het is daarom van groot belang dat ontwikkelaars aan deze eisen tegemoet kunnen komen en ze daarbij te ondersteunen met de juiste richtsnoeren en hulpmiddelen.

Het blijkt echter dat een alomvattende en makkelijke toepasbare verzameling hulpmiddelen die systeem ontwikkelaars zouden kunnen helpen privacy by design toe te passen niet bestaat. Meer in het bijzonder geldt dat een systematische studie naar zogenaamde privacy design patterns ontbreekt. Deze privacy design patterns kunnen juist systeem ontwerpers helpen privacy eisen al vroeg tijdens het ontwerpproces mee te nemen.

Om deze lacune op te vullen stelt dit project zich de volgende doelen.

[1] We follow the numbering of sections as used in the template provided in the call.

- Ontwikkel een framework om privacy design patterns uit te drukken en te bestuderen.
- Ontwikkel een uitgebreide catalogus van zulke privacy design patterns
- Ontwikkel hulpmiddelen die systeem ontwikkelaars helpen om deze privacy design patterns in de praktijk toe te passen.

TNO is de industriële partner in dit project. Zij zal de resultaten gebruiken in de ontwikkeling van een platform voor diensten die gebruikers van persoonlijke gezondheidsinformatie gaan voorzien.

2.3 Keywords

Privacy by design, privacy design patterns, privacy enhancing technologies.

3 Additional information

3.1 Classification

Computer Science.

3.2 NCSRA-II Research theme(s)

This proposal fits the following two NCSRA-II research themes.

- Identity, privacy and trust.
- Secure design and engineering.

3.3 Multidisciplinarity

This project is multidisciplinary to a limited extent: it will use approaches both from computer science and information science.

4 Proposal members

4.1 Members of the research team

The Digital Security group of the Radboud University Nijmegen is a leading research group into computer security in the Netherlands. It works on a broad range of topics in computer security and privacy, including applied cryptography, privacy enhancing technologies, security protocols, smartcards and RFID, and the security and correctness of software. Members of the group are also active in the broader societal issues surrounding security & privacy, such as privacy and e-voting, and interaction with disciplines outside computer science such as cryptography and law. They also regularly carry out commercial contract research to apply and inspire high quality academic research. The research group received an outstanding rating in the latest national research evalution exercise for computer science (2010).

The research will be embedded in the research already performed by the Privacy & Identity Lab[2], of which the Digital Security group of the RU Nijmegen is a member (and host). Other members are TNO and Tilburg Institute of Law and Technology. The Privacy & Identity Lab (PI.lab) is sponsored by SIDN[3]. The main applicant, dr. Jaap-Henk Hoepman, serves as scientific director of the PI.lab. He will supervise the PhD student. Prof. Bart Jacobs will serve as promotor. See table 1 for details.

4.2 Participating partners

In this project, TNO is the main participating partner. TomTom, NS (the Dutch railway company), KPN (the leading Dutch telecom operator) and HP Netherlands will join the advisory board.

Role	Contact	Company
participant	Gabriela Bodea Milena Kooij-Janic	TNO
advisory	Simon Hania	TomTom
advisory	Rachel Marbus	NS
advisory	Rence Damming	KPN
advisory	Gilles Ampt	HP

Table 2: Participating partners

TNO is the Netherlands Organisation for Applied Scientific Research. It has 3,900 employees. TNO's total consolidated revenue equalled €587 million in 2013. It is an independent research

[2] http://www.pilab.nl
[3] http://www.sidn.nl

Role	Name	Institute	FTE
PhD student (requested)	n.n.	RU Nijmegen	1.0
supervisor	dr. Jaap-Henk Hoepman	RU Nijmegen	0.1
promotor	prof.dr. Bart Jacobs	RU Nijmegen	p.m.
project member	drs. Christiaan Hillen	RU Nijmegen	p.m.

Table 1: Research team

organisation whose expertise and research make an important contribution to the competitiveness of companies and organisations, to the economy and to the quality of society as a whole. TNO's unique position is attributable to its versatility and capacity to integrate this knowledge.

The Security and Strategy & Policy groups of TNO jointly participate in this project. They advice government and middle to large corporations on all issues involving information security (including privacy) and policy. Recent projects these groups were involved in are a project on privacy by design [g], an impact assessment of RFID privacy policies for the European Commission, MECIS (on the societal and economical impact of intelligent sensor networks, e.g., on privacy), an "Alliantie Vitaal Bestuur" project on privacy friendly architectures for e-government for the Ministry of the Interior, and the currently running "Actieplan Privacy" project, investigating the possibilities for privacy-friendly innovation, and in which privacy-by-design is a core element. TNO is a member of ECP.NL[4]. Privacy is a spearhead of involvement for TNO for the coming years, as witnessed by its active involvement in the Privacy & Identity Lab.

5 Description of the proposed research

5.1 Motivation and objectives

The goal of privacy[5] by design is to take privacy requirements into account throughout the system development process, from the conception of a new IT system up to its realisation [4]. The underlying motivation for this approach is that by taking privacy serious from the start the final system will be more privacy friendly.

In the context of developing IT systems, privacy by design implies that privacy protection is a system requirement that must be treated like any other functional requirement. As a result, also privacy protection will have an impact on the design and implementation of the system. To support privacy by design, we therefore need guiding principles to support the inclusion of privacy requirements throughout the system development life cycle

But there is a considerable gap to be bridged here [9].

An important methodology during the design phase is the application of so called software design patterns. These design patterns refine the system architecture to achieve certain functional requirements within a given set of constraints. During software development the availability of practical methods to protect privacy is high during actual implementation, but low when starting the project. Numerous privacy enhancing technologies (PETs) exists that can be applied more or less 'of the shelf'. Before that implementation stage, privacy design patterns can be used in the system design phase. Significantly less design patterns exist compared to PETs, however. And at the start of the project, during the concept development and analysis phases, the developer stands basically empty handed. This project aims to close this gap, by developing a structured collection of privacy design patterns, and develop the corresponding tools to support engineers to apply them in practice.

Design patterns do not necessarily play a role in these early phases of the software development cycle. The main reason is that such design patterns are already quite detailed in nature, and more geared towards solving an implementation

[4] www.ecp.nl

[5] As is often done in the context of privacy-by-design we use the word privacy to denote the more restricted concept of data protection in this proposal.

problem. Privacy design strategies have recently been proposed to address the lack of tools at the concept development and analysis phases [d]. This project also aims to further develop these privacy design strategies.

We believe design patterns can also help bridge the gap between the outcome of a Privacy Impact Assessment (PIA), and the subsequent mitigation of the identified risk during system development. A privacy impact assessment is a "methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts" [21]. The UK was the first country in Europe to publish a PIA guidance in 2007, revising it in 2009 [18]. All PIA methodologies include a process step in which measures to avoid or mitigate a privacy risk need to be identified. But no concrete guidance is given on how to elect these measures, let alone how to ensure that these measures are effectively implemented during the actual development process.

The overarching objective of this project is to give IT designers concrete tools to support privacy-by-design. In this project we contribute to this by focusing on privacy design patterns, and considering the following three concrete (sub)objectives.

- Develop a framework to express and study privacy design patterns, including privacy design strategies. The framework should make it easy to use the outcome of a privacy impact assessment to select a set of appropriate privacy design patterns.
- Develop a comprehensive catalogue of such privacy design patterns, indexed and categorised according to the developed framework.
- Develop tools to support system designers to apply privacy design strategies and privacy design patterns during concept development and design phases of the development lifecycle. These tools should easily integrate into existing system development methodologies used in practice.

A secondary objective is to make the software development community aware of these privacy design patterns, strategies and tools, and to encourage their use in actual software development.

The research approach, related research and scientific relevance is outlined below. The valorisation and societal and economical relevance is discussed in section 6.

5.2 Research approach

Design patterns The concept of a *design pattern* is a useful vehicle for making design decisions about the organisation of a software system. A design pattern

> "provides a scheme for refining the subsystems or components of a software system, or the relationships between them. It describes a commonly recurring structure of communicating components that solves a general design problem within a particular context." [2]

Typically, the description [7] of a design pattern contains at least its name, purpose, context (in which situations does it apply), implementation (its structure, components and their relationships), and the consequences (its results, side effects and trade offs when applied). Many design patterns exist, at varying levels of abstraction.

However, for privacy, few privacy design patterns have been explicitly described to date. We are aware of the work of Hafiz [10, 11], Pearson [15, 14], van Rest *et al.* [g], and a recent initiative of the UC Berkeley School of Information[6]. Many more privacy design patterns potentially exist though, but so far have never been described as such. Sweeney's *k-anonymity* concept [17] is a classical example of an idea that implicitly defines a privacy design pattern. Also the concept of a *zero knowledge proof* [8] can be viewed as a design pattern. In fact many of the privacy enhancing technologies (described below) implicitly define a corresponding privacy design pattern. Another good example of a possible pattern is *attribute based credentials* [3, 1].

[6] http://privacypatterns.org/

One of the goals of this project is to make these implicit design patterns explicit, and describe them in a technology neutral way.

Design strategies More general principles that guide the system architecture without imposing a specific structural organisation or schema for the system exist. These are too high level to be described by a design pattern. These principles are expressed in terms of *design strategies*. They are somewhat related to architecture patterns[7] and defined as follows [d].

> A design strategy describes a fundamental approach to achieve a certain design goal. It has certain properties that allow it to be distinguished from other (fundamental) approaches that achieve the same goal.

Design strategies do not necessarily impose a specific structure on the system although they certainly limit the possible structural realisations of it. Therefore, they are also applicable during the concept development and analysis phase of the development cycle. Eight privacy design strategies have been defined to date: MINIMISE, HIDE, SEPARATE, AGGREGATE, INFORM, CONTROL, ENFORCE, and DEMONSTRATE. These privacy design strategies have been derived from existing privacy principles [13, 19], data protection laws [5], and current standardisation in the privacy-by-design area [12].

Privacy design strategies make explicit which high level decisions can be made to protect privacy, when the first concepts for a new information system are drafted. The strategies also provide a useful classification of privacy design patterns and the underlying privacy enhancing technologies.

This approach builds on the framework by Spiekermann and Cranor [16] that distinguishes four stages of privacy-friendliness (ranging from fully identified to completely anonymous). In their framework, the two highest stages are achieved through a privacy-by-architecture approach. The two lowest stages require a privacy-by-policy approach. They see these two approached as essentially mutually exclusive: "In contrast, if companies do not opt for a privacy-by-architecture approach, then a privacy-by-policy approach must be taken where notice and choice will be essential mechanisms for ensuring adequate privacy protection" [16]. In other words, a system that is engineered as privacy-by-architecture does not process privacy sensitive data and therefore does not need privacy-by-policy.

The privacy design strategies perspective is less binary: a system architecture will hardly ever guarantee full privacy, and a privacy policy alone does not give sufficient privacy guarantees either. The aim is to provide system designers concrete strategies to actually engineer privacy, from both perspectives. Some of these strategies cover the privacy-by-architecture approach. Others cover the privacy-by-policy approach. These strategies are not mutually exclusive, however. Any subset of the strategies can be applied in parallel when designing a system in a privacy friendly manner.

How the research objectives are addressed As explained earlier, many privacy enhancing technologies (PETs) implicitly define a privacy design patterns. We will study existing PETs to uncover these implicit patterns, and describe them explicitly. Furthermore, the study of privacy design strategies [d] has revealed that in several important areas of privacy protection, hardly no privacy design patterns exist. This is especially the case for ways to process data separately, and for ways to give users meaningful control over personal data stored about them. These steps will contribute to building a comprehensive catalogue of privacy design patterns.

The privacy design strategies themselves serve as a starting point to develop a privacy design pattern framework. The privacy design strategies define the high level goals a privacy design pattern should achieve, and also provide a first rough outline of the structure, consequences and concerns associated with typical design patterns that belong to that strategy. These

[7] See http://best-practice-software-engineering.ifs.tuwien.ac.at/patterns.html, and The Open Group Architecture Framework (TOGAF) http://pubs.opengroup.org/architecture/togaf8-doc/arch/chap28.html

goals, structure, consequences and concerns will be matched with the typical results one obtains when applying a privacy impact assessment (PIA). We will study several PIA methodologies and analyse their outcomes, focusing on how these results should be interpreted and used to decide on the application of certain privacy design strategies and privacy design patterns.

Existing software development methodologies, especially those that are used in practice (see below) will be investigated for their potential to support privacy by design. In particular we will study if and how privacy design patterns can be integrated into them, and what tooling needs to be developed in order to facilitate that integration. Prototype tools will then developed later on during the project, in parallel with the development of the design patterns themselves.

Progress of our research and our project results will be reported through academic papers in leading conferences and journals in the field.

In order to ensure that the project develops patterns and tools that are relevant for and applicable to privacy-by-design in industry, we plan to do the following.

First of all, we will establish an advisory board that will meet with the project team twice a year. We have already secured membership of the board of four senior executives directly responsible for privacy by design. They represent four very large Dutch companies (see section 4.2).

Secondly, we aim to interview important stakeholders, and especially software developers active in the development of privacy-sensitive software, at the start of the project. We also plan to organise a workshop, to bring together stakeholders and scientists active in the field of privacy-by-design. This workshop will be organised during the first year of the project.

In order to achieve the secondary objective of making the software development community aware of these privacy design patterns and strategies, and to encourage their use in actual software development, we plan to do the following.

First of all, we will set up a wiki that will make the privacy design patterns that we develop immediately available to the community. The wiki will allow feedback on the patterns described, and will also allow others to contribute proposals for privacy design patterns. The wiki will be structured based on the privacy design pattern frameworks, and allows visitors to access and search the patterns from different perspectives. Moreover, at the end of the project we will organise a second workshop to disseminate and discuss the project results.

See section 7.1 for a detailed description of the tasks and deliverables of this project.

5.3 Innovation of the proposed research

The three objectives described at the end of section 5.1 will, when achieved, result in the following innovations and new insights.

The development of a privacy design pattern framework (objective 1) will streamline the translation from identified risks in a privacy impact assessment into concrete actions that can be implemented at the design level (and beyond, see below). Currently this is typically a haphazard affair.

The development of a comprehensive catalogue of privacy design patterns (objective 2) significantly advances the current state of the art in the area of privacy by design (as argued in section 5.1). Moreover, this catalogue will provide new insights into the extent (and limits) of privacy by design from a technological perspective. It will provide a clearer demarcation of those privacy risks that can be mitigated by technological means, and those that need to be mitigated through other (legal, policy or organisational) means. Finally, the catalogue is necessary to support the privacy design pattern framework, as it provides the bridge between the privacy risks identified during the privacy impact assessment and the concrete measures that can be implemented during system development.

The development of tools for privacy by design during system development (objective 3) will allow for tighter integration of privacy by design in system development. When developed in conjunction with the privacy design pattern framework, it will allow the outcome of a privacy impact assessment to more directly and con-

cretely influence the actual system implementation, in a more straightforward, perhaps even semi-automatic, fashion. This is especially important as a privacy impact assessment is not just a one-shot tool but rather a process that should be executed periodically even after the system has been deployed [21]. Moreover, these tools will contribute to a more structured approach to privacy by design during system development, which in return result in system that more robustly protect our privacy.

Word count The total number of words in this section (excluding this paragraph) is 2300 (approximately).

6 Valorisation and relevance

6.1 Relevance

One of the main objectives of the National Cyber Security Strategy Agenda (NCSRA-II) is to "To improve the security and trustworthiness of the ICT infrastructure and ICT services". In the context of the NCSRA-II, security includes the privacy protection. This project contributes to this objective, as it develops concrete tools and methodologies for privacy by design. As argued earlier in this proposal, such tools and methodologies are essential if one wants to systematically design future ICT infrastructure and services in a privacy friendly way. There is a certain amount of urgency associated with the development of such tools and methodologies, as the European Commission is steadily progressing with a proposal for a new European data protection regulation [6]. This regulation, currently expected to become adopted in 2015, will make privacy by default and privacy by design a mandatory requirement for all future ICT infrastructure and services that process personal data.

As indicated in section 3.2 this proposal fits the following two NCSRA-II research themes: (1) Identity, privacy and trust, and (8) Secure design and engineering. With its focus on developing privacy design patterns, the project contributes to the core of the first NCSRA-II research theme, by developing new building blocks for privacy protection. Because the patterns are, by definition, generic in nature, they will applicable in most of the application domains listed in the NCSRA-II. As stated in the NCSRA-II in the description of the secure design and engineering theme: "Ideally, systems should be designed with security and privacy in mind from the start - ensuring Security by Design or Privacy by Design.". This project is all about privacy by design. It will develop the tools and methodologies (that are currently still lacking) to design and implement privacy friendly systems from the very start.

6.2 Valorisation

The World Economic Forum [20] has recognised that although the explosive growth in the quantity and quality of personal data has created a signifcant opportunity to generate new forms of economic and social value, high-profile data breaches and individual perceptions of powerlessness have resulted in a lack of trust among all stakeholders. It recommends, among others, to develop and agree on principles to encourage the trusted flow of personal data. The proposal for a new European data protection regulation [6] explicitly requires data protection by design and by default.

This shows that privacy by design is becoming a significant economic and regulatory factor. It is therefore crucial to support developers in satisfying these requirements with practical tools and guidelines.

Last year's revelations of the dragnet surveillance capabilities of the NSA and GCHQ have increased public awareness of the risk of unlimited collection of personal data. Even large commercial service providers that process huge amounts of personal data of their customers (like Google, Yahoo, and others) have been proven not be immune to infiltrations by these agencies. More recent developments also reveal an increased concern of individual citizens w.r.t. their online privacy. After the announcement in the beginning of this year that WhatsApp (a popular messaging services) would be acquired by Facebook, more secure and privacy friendly alternatives saw a sudden increase of users.

As explained in the introduction, very few concrete tools for privacy-by-design currently exist

to support system developers. Given the above developments, both at the policy level as well as the customer demand level, we expect an increasing demand for privacy friendly products and services. In fact KPN (one of the companies in the advisory board of this project) recently announced[8] it is committed to sell 500.000 copies of the BlackPhone[9] (a secure, Android based, smartphone developed by Silent Circle and Geeksphone) to its customers. Clearly they see a market. This would have been unthinkable only a year ago.

With an expected increase in demand for privacy friendly products, production needs to catch up. To do so in a sustainable manner, privacy by design must be incorporated in the system development processes [f]. We expect the results of our project to have a major impact in this area. First of all the catalogue of privacy design patterns will prove to be extremely useful for the faster and more reliable design of more privacy friendly systems. Secondly, a more streamlined translation of privacy risks (identified through a primacy impact assessment) into product design will decrease time to market. This time is further reduced by making this translation more automatic based on the tools we will develop during our project.

But apart from improvement of privacy in existing markets, there is a potential for an entirely new market of privacy friendly products and services. Privacy design strategies and privacy design patterns have been identified as important and promising building blocks to achieve privacy-friendly innovation [b].

The principles and tools developed in this project will also be validated during the development of so-called personal health information providers by TNO. In fact, TNO aims to raise a consortium that will implement such a health data infrastructure at the national level. The system will collect health and medical data, from several sources (including patient sensors). Privacy is of utmost concern, given the sensitive nature of the data being processed. The user (patient) plays a central role, and the intention of the consortium is put the user in control. The framework, tools and patterns to be developed within this project will be used to achieve this goal.

To increase the uptake of the results of our project, we ensure that we both receive valuable input from industry during the first phase of our project (using a stakeholder consultation workshop which will ensure our project plans are aligned with industry needs), and disseminate our results in the last stage of the project (using a second dissemination workshop). Throughout the project the advisory board will be kept informed of project progress and will be asked for their insights to increase practical relevance of the project.

As a final step in increasing the impact of our results, we will contribute to ongoing standardisation activities in this are, for example the ISO 29100 privacy framework [12] drafted by ISO JTC 1 /SC 27.

Word count The total number of words in this section (excluding this paragraph) is 1050 (approximately).

7 Project planning

7.1 Phasing

Based on the discussion of the research approach in section 5.2, we have divided the project in the following tasks.

- Perform a literature study on privacy by design, privacy design patterns and privacy impact assessments.
- Perform a literature study on system development methodologies and their associated tooling.
- Investigate (using interviews and questionnaires) the use of system development methodologies in industry, and the uptake (and integration) of privacy by design in system development practices.
- Organise a workshop on the current state of practice of privacy-by-design in industry.

[8] http://www.blackenterprise.com/technology/geeksphones-blackphone-makes-security-simple/

[9] https://www.blackphone.ch

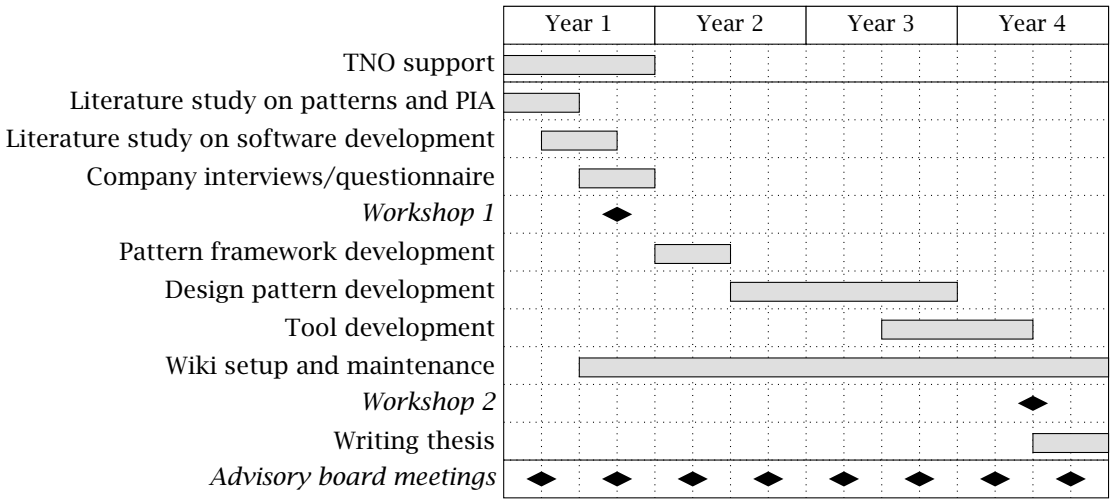

Figure 1: Project planning

- Develop a privacy design pattern framework to study and express privacy design patterns.
- Develop privacy design patterns and combine them, together with existing privacy design patterns, into a comprehensive catalogue.
- Develop new tools or extend existing tools for system development to integrate the use of privacy design patterns.
- Set up and maintain a wiki to collect privacy design patterns and tools for privacy by design.
- Organise a workshop for the dissemination of and discussion on the project results.
- Write a PhD thesis.

These tasks will deliver the following results.

- An overview of current privacy design patters and privacy impact assessment methodologies, and their relationships and dependencies.
- An overview of current system development methodologies, and if and how they are actually used by industry. This includes an analysis of current industry approaches towards privacy by design.
- A framework for privacy design patterns.
- A comprehensive catalogue of privacy design patterns, supported by a wiki.
- Several academic papers, to be published in academic conferences and journals, on the above topics.
- Prototype tools that allow the use of privacy design patterns in commercially used system development methodologies.
- A PhD thesis on privacy patterns for privacy by design.

The planning of the project in relation to these tasks and deliverables is represented as a Gantt chart in figure 7.1.

At the moment TNO has committed to be involved in the first year of the project, to study personal health information providers (as explained in section 6.2). This activity will help the foundational steps to be undertaken by the requested PhD student within the project, especially providing a more practical view on the subject matter. We expect TNO continue its involvement in the project after this, if only through its participation in the Privacy & Identity Lab (of

which this project will be a part). We have not formally sought commitment for this, as this was unnecessary according to the formal funding scheme rules.

7.2 Education and training

The requested PhD (and in fact the project as a whole) will be part of the Privacy & Identity Lab (PI.lab). As such the PhD student will participate in the quarterly PI.lab events, the seminars organised by the PI.lab partners, and collaborate with both the other PhD students of the PI.lab as well as the senior PI.lab staff. As the PI.lab is a multidisciplinary research organisation consisting of computer scientists, legal scholars, social scientist, and policy experts, the PhD student will be exposed to a very rich and diverse set of research disciplines, backgrounds and knowledge.

Part of the training program will involve attending a relevant summerschool, and visits to relevant conferences in the field. If possible, an exchange with a sister institute abroad during the second half of the project will be set up. Any deficiencies in the education of the selected candidate can easily be remedied by attending relevant courses taught by the Kerckhoffs Institute[10], which offers a master programme in computer security.

8 References

8.1 Literature (internal)

The following papers have been written by researchers from both TNO and the Radboud University Nijmegen involved in this proposal.

[a] Gergely Alpár and Jaap-Henk Hoepman. A secure channel for attribute-based credentials [short paper]. In *ACM Digital Identity Management Workshop (DIM)*, pages 13–18, Berlin, Germany, November 8 2013.

[b] Colette Cuijpers, Just Eijkman, Marc van Lieshout, Arnold Roosendaal, Bas van Schoonhoven, and Anne Fleur van Veenstra. Actieplan privacy. Een inventarisatie van best practices & best technologies. Technical report, Privacy & Identity Lab, July 2013.

[10] http://www.kerckhoffs-institute.org

[c] David Galindo and Jaap-Henk Hoepman. Non-interactive distributed encryption: A new primitive for revocable privacy. In *Workshop on Privacy in the Electronic Society (WPES)*, pages 81–92, Chicago, IL, USA, October 17 2011.

[d] Jaap-Henk Hoepman. Privacy design strategies, October 2012. eprint arXiv:1210.6621. A preliminary version was presented at the Amsterdam Privacy Conference (APC 2012) and the Privacy Law Scholars Conference (PLSC 2013).

[e] Bert-Jaap Koops, Jaap-Henk Hoepman, and Ronald Leenes. Open-source intelligence and privacy by design. *Computer Law & Security Review*, 29(6):676–688, December 2013.

[f] Marc van Lieshout, Linda Kool, Gabriela Bodea, James Schlechter, and Bas van Schoonhoven. Stimulerende en remmende factoren van privacy by design in Nederland. Technical Report R10006, TNO, May 2012.

[g] Jeroen van Rest, Daniel Boonstra, Maarten Everts, Martin van Rijn, and Ron van Paassen. Designing privacy-by-design. Presented at the Annual Privacy Forum 2012, Limmasol, Cyprus.

8.2 Literature (external)

[1] Stefan Brands. *Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy*. MIT Press, 1 edition, 2000. ISBN 0-262-02491-8.

[2] Frank Buschmann, Regine Meunier, Hans Rohnert, and Peter Sommerlad. *Pattern-Oriented Software Architecture, Volume 1: A System of Patterns*. John Wiley & Sons, 1996.

[3] Jan Camenisch and Anna Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In Birgit Pfitzmann, editor, *EUROCRYPT*, volume 2045 of *Lecture Notes in Computer Science*, pages 93–118. Springer, 2001.

[4] Ann Cavoukian. Privacy by design – the 7 foundational principles. Technical report, Information and Privacy Commissioner of Ontario, jan 2011. (revised version).

[5] 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. *OJ C L*, 281:0031 – 0050, November 23 1995.

[6] 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. *OJ C*, 102:24, April 5 2012.

[7] Erich Gamma, Richard Helm, Ralph Johnson, and John Vlissides. *Design Patterns: Elements of Reusable Object-Oriented Software*. Addison-Wesley, 1994.

[8] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM J. Comput.*, 18(1):186–208, 1989.

[9] Seda Gürses, Carmela Troncoso, and Claudia Diaz. Engineering privacy by design. In *Conference on Computers, Privacy & Data Protection (CPDP 2011)*, 2011.

[10] Munawar Hafiz. A collection of privacy design patterns. In *Proceedings of the 2006 conference on Pattern languages of programs*, PLoP '06, pages 7:1–7:13, New York, NY, USA, 2006. ACM.

[11] Munawar Hafiz. A pattern language for developing privacy enhancing technologies. *Softw. Pract. Exper.*, 2011. doi: 10.1002/spe.1131.

[12] ISO/IEC 29100. Information technology – Security techniques – Privacy framework. Technical report, ISO JTC 1/SC 27.

[13] Organisation of Economic Co-Operation and Development. OECD guidelines on the protection of privacy and transborder flows of personal data, 1980.

[14] Siani Pearson and Azzedine Benameur. Decision support for design for privacy: A system focused on privacy by policy. In *PrimeLife/IFIP Summer School 2010: Privacy and Identity Management for Life*, Helsingborg, Sweden, August 2010. (to appear).

[15] Siani Pearson and Yun Shen. Context-aware privacy design pattern selection. In Sokratis K. Katsikas, Javier Lopez, and Miguel Soriano, editors, *Trust, Privacy and Security in Digital Business (TrustBus), 7th International Conference*, LNCS 6264, pages 69–80, Bilbao, Spain, August 30–31 2010. Springer.

[16] Sarah Spiekermann and Lorrie Faith Cranor. Engineering privacy. *IEEE Trans. Software Eng.*, 35(1):67–82, 2009.

[17] Latanya Sweeney. k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(5):557–570, 2002.

[18] UK Information Commissioner's Office. PIA handbook v2, 2009.

[19] US Federal Trade Commission. Privacy online: Fair information practices in the electronic marketplace, a report to congress, 2000.

[20] World Economic Forum. Rethinking personal data: Strenghtening trust, May 2012.

[21] David Wright. The state of the art in privacy impact assessment. *Computer Law & Security Review*, 28(1):54–61, February 2012.

9 Requested Budget

The complete budget appears in table 3, and is described in more detail below.

Item	Amount	
personnel		
- 1 PhD student	€206.000	
additional		
- travel	€20.000	
total cost	€226.000	
cash co-funding		
- TNO		€21.000
Funding requested		€205.000
in kind co-funding		
- TNO (200 h.)	€23.200	
Project budget	€249.200	

Table 3: Project budget

9.1 Requested personnel budget

We request funding for one PhD student for four years, at the standard rate of €206.000 (including the €5.000 bench fee).

9.2 Requested additional budget

We request additional funding of €20.0000 for travel for conference visits to present project results and other dissemination activities.

9.3 Co-funding of the consortium partners

In-kind co-funding TNO will support the project by allocating 200 man hours at €116 hourly rate for a total of €23.200. This is more than the required 10 % of the total requested funding of €205.000.

Cash co-funding TNO will support the project with an in cash contribution of €21.000. This is more than the required 10 % of the total requested funding of €205.000. The cash co-funding will be used to cover part of the personnel expenses.

9.4 Total project budget overview

In the total project budget overview in table 3 we have subtracted the cash contribution from the costs to compute the requested funding.