PReparing Industry to Privacy-by-design by supporting its Application in REsearch

Contribution to Study Period on Privacy Engineering Framework

Project:	PRIPARE
Project Number:	ICT-6106
Title:	Contribution to Study Period on Privacy Engineering Framework
Version:	v1.0
Date:	06/08/2015
Confidentiality:	Public
Author/s:	Antonio Kung, Christophe Jouvray (Trialog), Nicolas Notario, Alberto Crespo (Atos), Samuel Martin, José del Álamo (UPM), Carmela Troncoso (Gradiant).

Part of the Seventh Framework Programme Funded by the EC - DG CNECT

Table of Contents

SUMMARY 4
LIST OF FIGURES 5
ABBREVIATIONS AND DEFINITIONS 5
1 INTRODUCTION 6
2 PRIVACY FRAMEWORK VERSUS PRIVACY ENGINEERING FRAMEWORK 7
2.1 ABOUT FRAMEWORKS 7
2.2 POSITIONING PRIVACY ENGINEERING IN ORGANISATIONS 7
2.3 WHY A PRIVACY ENGINEERING FRAMEWORK? 10
2.3.1 Need for Convergence of Terms 10
2.3.2 Need for Guidance 10
2.3.3 Paving the way to Future Privacy Engineering Standards 11
3 RECENT CONTRIBUTIONS TO A PRIVACY ENGINEERING FRAMEWORK 12
3.1 MITRE CALL FOR A PRIVACY ENGINEERING FRAMEWORK 12
3.2 NIST CONTRIBUTION ON PRIVACY ENGINEERING OBJECTIVES 12
3.3 ULD CONTRIBUTION ON PROTECTION GOALS FOR PRIVACY ENGINEERING 12
3.4 OASIS CONTRIBUTION ON OPERATIONALISATION 13
3.5 LINDDUN CONTRIBUTION ON PRIVACY THREAT ANALYSIS 13
3.6 HOEPMAN CONTRIBUTION ON DESIGN STRATEGIES 13
3.7 PRIPARE CONTRIBUTION ON A PRIVACY ENGINEERING METHODOLOGY 14
3.7.1 Goal-oriented Elicitation of Privacy Operational Requirements 15
3.7.2 Architecture Change Resulting from the Design of Privacy Controls 17
3.7.3 Lifecycle Oriented Methodology 18
3.7.4 Integration into Existing Methodologies 19
3.7.5 Recommendation on Privacy Controls Verification 19
4 STRAWMAN PRIVACY ENGINEERING FRAMEWORK (SPEF) 20
4.1 BASIC CONCEPTS FOR PRIVACY ENGINEERING 20
4.1.1 Privacy engineering and Privacy-by-Design 20
4.1.2 Privacy engineering objectives 21
4.1.3 From Privacy Principles to Privacy Operational Requirements 21
4.1.4 From Privacy Operational Requirements to Privacy Controls 23
4.1.5 Life Cycle Approach 25
4.2 PRIVACY ENGINEERING PRINCIPLES 27
4.3 LIST OF TERMS 28

4.4 ADDITIONAL TERMS 29
5 CONCLUSION 30
ANNEX 1 TAKING INTO ACCOUNT EXISTING REFERENCES 31
ANNEX 2 TAKING INTO ACCOUNT EXISTING METHODOLOGIES 34
A2.1 SOFTWARE AND SYSTEM ENGINEERING METHODOLOGIES 34
A2.1.1 Waterfall 34
A2.1.2 Iterative or incremental 34
A2.1.3 Prototype 35
A2.1.3 Agile 36
A2.2 PROJECT MANAGEMENT METHODOLOGIES 36
A2.2.1 PMBOK 36
A2.2.2 PRINCE2 37
ANNEX 3 REFERENCES 39

Summary

This contribution is made by the PRIPARE project further to the first call of contributions made by ISO/IEC JTC 1/SC 27 Working Group 5 on the study period on privacy engineering framework.

The contribution

- *provides a rationale for a privacy engineering framework*. It analyses the meaning of framework, contrasts privacy management and privacy engineering, and explains why a framework is needed
- *summarises a wealth of recent contributions*: Mitre call for a privacy engineering framework, NIST contribution on privacy engineering objectives, ULD contribution on protection goals for privacy engineering, OASIS-PMRM contribution on operationalisation, LINDDUN contribution privacy threat analysis, Hoepman's contribution on design strategies, and PRIPARE contribution on goal-oriented requirements engineering, privacy enhancing architectures, lifecycle oriented methodology and integration into existing methodologies
- *provides a Strawman privacy engineering framework (SPEF)*. The SPEF covering basic concepts for privacy engineering, privacy engineering principles and definitions of terms. The SPEF integrates most of current contributions features, including those of PRIPARE.
- *explains how the contribution takes into account existing references* such as ISO/IEC 29100, 29101, 29134, 29151, 27034, ISO/IEC 42001, 15288, 12207, CNIL methodology for privacy risk management, NIST Report on Privacy Engineering, OASIS-PMRM and OASIS-PbD-SE, EDPS Internet Privacy Engineering Network, MITRE Privacy Engineering Framework, Centre for Information Policy Leadership research on Privacy Risk Management
- *explains how a privacy engineering methodology based on the proper framework can support a spectrum of development methodologies.* Examples of how PRIPARE engineering methodology is integrated are provided.

The contribution concludes that

- a convergence of understanding is possible,
- a framework is needed in order to federate all existing contributions and pave the way for future standards,
- the submission of a NWIP on a privacy engineering framework further to consolidation of PRIPARE and other contributions within the study period.

List of Figures

Figure 1: Essential Privacy Elements in Organisations 8
Figure 2: Management Viewpoint of Process Concerns 9
Figure 3: Engineering Viewpoint of Process Concerns 10
Figure 4: Privacy Engineering in WG5 Roadmap 11
Figure 5: Privacy Engineering Framework in WG5 Roadmap 11
Figure 6: PRIPARE Goal-oriented and Risk-based Requirement Elicitation 16
Figure 7: Architecture Decisions Associated with PETs 17
Figure 8: PRIPARE methodology phases 18
Figure 9: SPEF Goal-oriented and Risk-based Requirement Elicitation 22
Figure 10: SPEF supporting PEARs and PETs 24
Figure 11: SPEF Organisation Normative Framework 26
Figure 12: Waterfall methodology phases 34
Figure 13: Iterative methodology phases 35
Figure 14: Prototype methodology phases [30] 35
Figure 15: Scrum methodology phases 36
Figure 16: PMBOK process and knowledge matrix 37
Figure 17: PRINCE2 seven processes 38

Abbreviations and Definitions

Abbreviation	Definition
CNIL	Commission Nationale de l'Informatique et des Libertés
DPIA	Data Protection Impact Assessment
EDPS	European Data Protection Supervisor
EU	European Union
ISO	International Standards Organization
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
PbD	Privacy by Design
PbD-SE	Privacy by Design Documentation for Software Engineers
PEAR	Privacy Enhancing ARchitecture
PET	Privacy Enhancing Technology
PIA	Privacy Impact Assessment
PII	Personal Identifiable Information
PMRM	Privacy Management Reference Model
PRIPARE	PReparing Industry to Privacy-by-design by supporting its Application in REsearch
SPEF	Strawman Privacy Engineering Framework

1 Introduction

PRIPARE (pripareproject.eu) is a support action funded by the European Commission. It includes the following partners:

- Trialog (France)
- Atos (Spain)
- Trilateral Research and Consulting (UK)
- Inria (France)
- The American University in Paris (France)
- Gradiant (Spain)
- Universidad Politécnica de Madrid (Spain)
- University of Ulm (Germany)
- Fraunhofer SIT (Germany)
- Waterford Institute of Technology (Ireland)
- Katholieke Universiteit Leuven (Belgium)

One of the missions of PRIPARE is to specify a privacy and security-by-design software and systems engineering methodology, using the combined expertise of the research community and taking into account multiple viewpoints (advocacy, legal, engineering, business).

In October 2014, a liaison was established with ISO/IEC JTC1/SC27/WG5. In May 2014, PRIPARE experts proposed the creation of the SP on privacy engineering framework. This was accepted by WG5 and a call for contributions by August 2015 was made.

This document is the contribution of PRIPARE. It is co-authored by Antonio Kung, Christophe Jouvray (Trialog), Nicolas Notario, Alberto Crespo (Atos), Samuel Martin, José del Álamo (UPM), Carmela Troncoso (Gradiant), but the contribution of all other partners is acknowledged. The document is structured as follows:

- Section 2 explains the positioning of a privacy engineering framework and the motivation for the specification of such framework.
- Section 3 summarises the various existing contributions related to privacy engineering.
- Section 4 provides the specification of a strawman privacy engineering framework.
- Section 5 concludes on the potential of a NWIP on privacy engineering framework.
- Annex 1 shows how this contributions takes into account the references listed in this study period terms of reference.
- Annex 2 shows how this contribution takes into account existing software and system methodologies.

2 Privacy Framework versus Privacy Engineering Framework

2.1 About Frameworks

The term framework is defined as follows:

- a system of rules, ideas, or beliefs that is used to plan or decide something: e.g. a legal framework for resolving disputes (Cambridge online dictionary)
- a set of assumptions, concepts, values, and practices that constitutes a way of viewing reality (www.thefreedictionary.com)
- A basic structure underlying a system, concept, or text: e.g. the theoretical framework of political sociology (www.oxforddictionaries.com)

ISO 29100 [1] defines a privacy framework. As stated in the standard, it provides *a privacy framework which*

- *specifies a common privacy terminology;*
- *defines the actors and their roles in processing personally identifiable information (PII);*
- *describes privacy safeguarding considerations; and*
- *provides references to known privacy principles for information technology.*

[ISO29100] is applicable to natural persons and organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services. Paraphrasing the free dictionary definition, ISO29100 therefore provides therefore a set of assumptions, concepts, values and practices for privacy in organisations dealing with personal data[1].

The Study period objective is to assess whether *a privacy engineering framework* is needed *which*

- *specifies a common privacy **engineering** terminology;*
- *defines the actors and their roles in **the engineering of systems** processing personally identifiable information (PII);*
- *describes considerations on **engineering** privacy safeguards; and*
- *provides references to known privacy **engineering** principles for information technology.*

Paraphrasing the free dictionary definition, ISO29100 therefore provides therefore *a set of assumptions, concepts, values and practices for **privacy** in organisations dealing with personal data* while a standard on a privacy engineering framework would provide *a set of assumptions, concepts, values and practices for **privacy engineering** in organisations dealing with personal data.*

2.2 Positioning Privacy Engineering in Organisations

Figure 1 illustrates what we believe are essential elements of privacy in organisations. The left part shows important organisation objectives:

- integrating the concept of privacy in organisations,

[1] 29100 actually refers to PII: personally identifiable information instead of personal data.

- integrating the concept of privacy in the engineering of systems.

The centre part shows two important viewpoints:

- the management viewpoint, which focuses on elements (processes, practices, concepts) which are important to managers in their activities,
- the engineering viewpoint, which focuses on elements (engineering requirements, design, implantation, verification, maintenance) which are important to engineers in their activities.

The right part shows important process concerns to both managers and engineers: risk assessment, system development, and system compliance:

- risk assessment focuses on quantifying privacy risks in systems dealing with personal data and mitigating them by reducing their likelihood or their consequences,
- system development focuses on specifying and implementing technical solutions for privacy control in systems dealing with personal data. System development can involve decisions to integrate sub-systems supplied by third parties,
- system compliance focuses on ensuring that an organisation is doing what is expected and that systems developed within the organisations are doing what is expected. System compliance involves challenging processes such as privacy protection assurance, evaluation and verification. System compliance allow external stakeholders (e.g. consumers, policy makers, procurers) to assess whether they can trust the organisation and/or the systems.

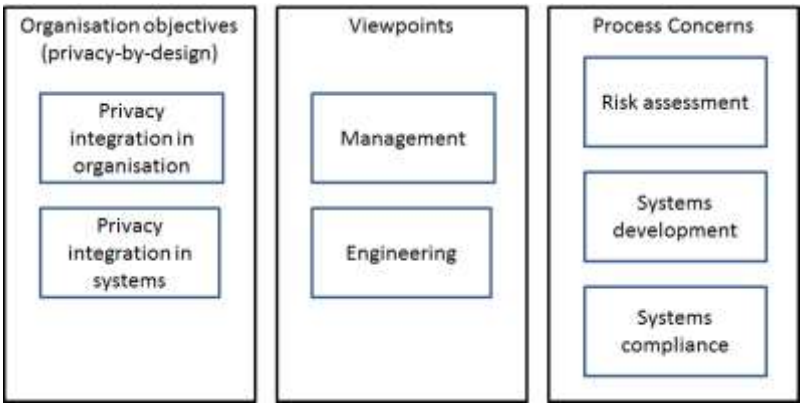

Figure 1: Essential Privacy Elements in Organisations

Figure 2 shows examples of how privacy can be supported from a management viewpoint throught the use of standards or guidelines:

- ISO 29134 [2] is a reference that can be used by managers to ensure that privacy risk management is carried out. CNIL privacy impact assessment [3] or the smart grid task force data protection impact assessment templates are other examples [4],
- OASIS-PMRM [3] is a reference that can be used by managers to ensure that privacy analysis (i.e. identify appropriate operational privacy management functionality and supporting mechanisms) is carried out,
- ISO 29151 [6] is a reference that can be used by managers to ensure that a well-known list of privacy controls is used.

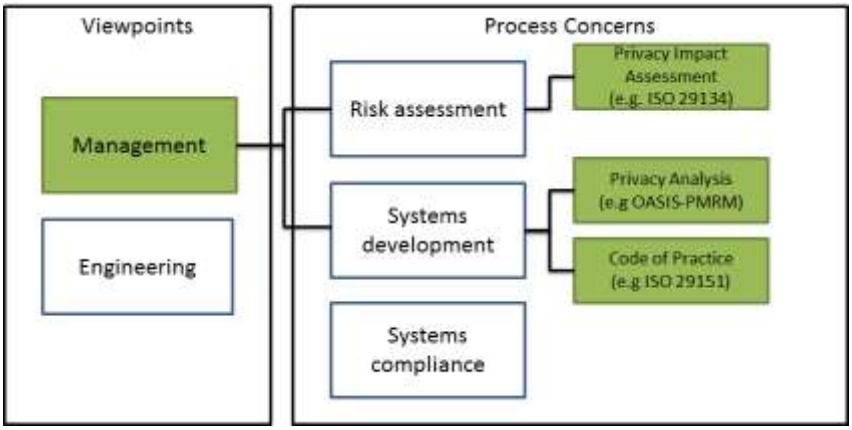

Figure 2: Management Viewpoint of Process Concerns

Figure 3 shows examples of how privacy could be supported from an engineering viewpoint (most references are research proposal – they might need maturation before adoption):

- LINDDUN [7] is a methodology that can be used by engineers to identify threats and design mitigation solutions. It provides a list of threat categories to consider (Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, Non-compliance). LINDDUN explains to engineers how to specify a system using data flow diagrams, and to identify and mitigate threats using elements of the diagrams.
- PEARS [8] explains how to specify an architecture which improves privacy using architecture concepts such as quality attributes, architecture tactics. It is based on Carnegie-Mellon work on software architecture [9]. It provides a list of architecture strategies (Minimisation, Enforcement, Transparency, Modifiability). PEARS explains to engineers how to specify and evaluate an architecture using quality attributes, architecture strategies and tactics.
- Hoepman [10] explains design strategies by identifying data oriented strategies (minimize, hide, separate, aggregate) and process oriented strategies (inform, control, enforce, demonstrate). Hoepman describes to engineers how to design a system using a number strategies and how to implement reusable solution (called privacy patterns).
- Agile development methodology [11] is a design methodology which focuses on flexible and evolutionary development. It explains to engineers how to develop prototypes that can iteratively evolve into improved versions[2].

[2] Note that the integration of privacy engineering into Agile methodologies is a challenge because of the lack of a design phase

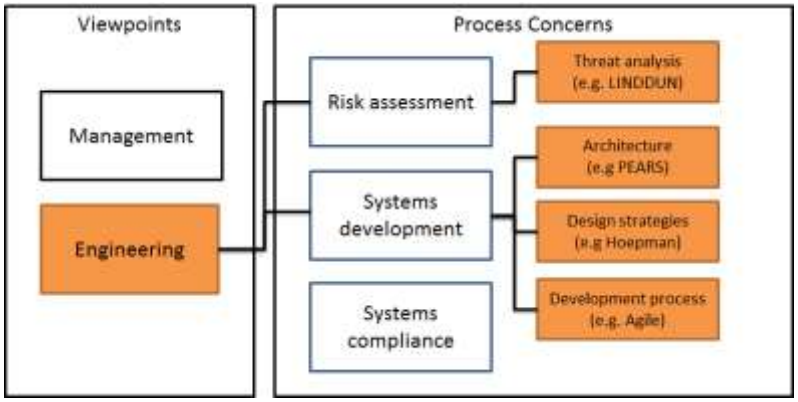

Figure 3: Engineering Viewpoint of Process Concerns

Examples in Figure 2 and Figure 3 are illustrative. They are not meant to be definitive categorisation. Standards such as ISO 29134, OASIS-PMRM, ISO 29151 are also useful from an engineering viewpoint. For instance OASIS-PRMM explains to engineers how to apply an iterative process to identify privacy functions and associated requirements.

The difference between a management viewpoint and an engineering viewpoint is the following

- Management focuses on what system is developed and on checking that it is developed properly
- Engineering focuses on how a system is developed and on testing it properly.

2.3 Why a Privacy Engineering Framework?

2.3.1 Need for Convergence of Terms

A number of concepts and principles for privacy engineering have been debated in the last years, for instance

- privacy-by-design principles (privacy-by-policy, privacy-by-architecture [12], minimization [13], enforcement, transparency [14]),
- privacy protection objectives (predictability, manageability, disassociability [16]) or privacy engineering objectives (unlinkability, transparency, intervenability [15])

We believe that **a selection and a convergence of terms** is needed. Further, the relation between those terms and other concepts need to be explained (e.g. Ann Cavoukian's privacy principles [18] versus ISO 29100 privacy principles [1]). This could be the objective of a privacy engineering framework.

2.3.2 Need for Guidance

Most references today (standards, guidelines) are management oriented and risk oriented or have a legal perspective. From an engineering viewpoint this is not sufficient. **Engineers need guidance that is methodology-oriented, and goal-oriented.** They need to get guidance on approaches that take privacy into account during the whole lifecycle process. Beyond risks that they must mitigate, engineers must also have a clear set of functional objectives concerning the system they develop (i.e. they need a goal oriented design approach).

2.3.3 Paving the way to Future Privacy Engineering Standards

The advent of a privacy engineering practice will depend on the availability of a number of standards. We believe that while it may bel too early to define these standards, we can now focus on the conditions that will facilitate the development of such standards through the definition of a privacy engineering framework.

Figure 4 shows the positioning of privacy engineering in the WG5 roadmap [19]. In this figure, there is a placeholder called privacy engineering which links to the ISO privacy framework [1].

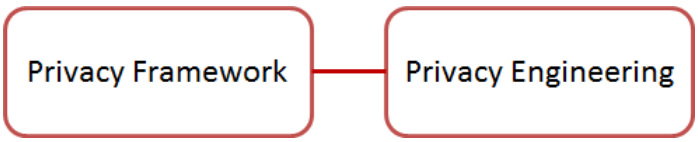

Figure 4: Privacy Engineering in WG5 Roadmap

The study period will work on the conditions that will enable roadmap scenarios such as those depicted by figure 3 and figure 4.

Figure 5 shows the replacement of the *privacy engineering* box by a *privacy engineering framework* box focuses on this placeholder. This can allow in the future the expansion towards other standards, e.g. a privacy engineering methodology, or a privacy risk analysis.

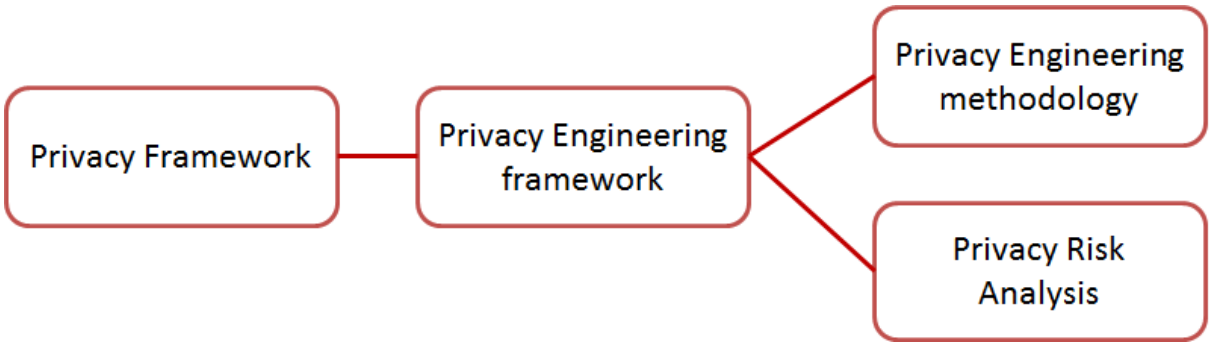

Figure 5: Privacy Engineering Framework in WG5 Roadmap

3 Recent Contributions to a Privacy Engineering Framework

3.1 Mitre Call for a Privacy Engineering Framework

Mitre published in July 2014 a technical paper on the need for the privacy engineering framework [20]. It highlighted the need to address privacy from both an organisational viewpoint (well covered) and an engineering viewpoint (not well covered).

An organisation viewpoint integrates elements such as a privacy program management, a compliance-focused risk assessment approach, a strategy and planning, and policies.

An engineering viewpoint integrates elements such as privacy testing, privacy-sensitive design decisions, privacy requirements and control selection, and system focused risk assessment. These elements are not well taken into account.

3.2 NIST Contribution on Privacy Engineering Objectives

NIST published in May 2015 a technical paper on a risk management framework [16]. It focuses on two pillars: the definition of privacy engineering objectives (i.e. predictability, manageability, disassociability) to address the gap between high-level privacy principles and implementation and the definition of a privacy risk model to allow for an organisational risk management approach.

3.3 ULD Contribution on Protection Goals for Privacy Engineering

ULD[3] presented in May 2015 a paper on privacy protection goals for privacy engineering [15]. it extends security protection goals (i.e. confidentiality, integrity, availability) with privacy protection goals (i.e. unlinkability, transparency, and intervenability). As showed in the table below, it further defines three axes (which can be considered degrees of freedom): confidentiality – availability, integrity – intervenability, and unlinkability – transparency.

Confidentiality	**<-> Availability**
No access to data	<-> Full access to data
No access to services	<-> Full access to services
Authorised entities only	<-> Everybody

Integrity	**<-> Intervenability**
No changes to data	<-> All types of changes
No access to process	<-> Full process flexibility
Defined by processor	<-> Defined by individual

Unlinkability	**<-> Transparency**
No linkable data	<-> Full linkability of data
No disclosure of process	<-> Full disclosure of process
Need-to-know	<-> Want-to-know

[3] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (www.datenschutzzentrum.de). Data protection authority in the federal state of Schleswig-Holstein, Germany

3.4 OASIS Contribution on Operationalisation

OASIS-PMRM is the result of a 10-year plus undertaking [3]. It defines

- a conceptual model for privacy management, including definition of terms,
- a methodology to carry out a privacy analysis. The methodology is iterative and use case based. It leads to the definition of operation functional services necessary to support privacy controls,
- a set of operational services (agreement, usage, validation, certification, enforcement, security, interaction, access).

OASIS-PMRM defines one important concept: ***touch points***. Touch points are "intersection of data flows with privacy domains or systems within privacy domains. Here is one example provided by OASIS-PMRM related to EV (electric vehicle) charging.

> *When a customer plugs into the charging station, the EV On-Board System embeds communication functionality to send EV ID and EV Charge Requirements to the Customer Communication Portal. This functionality corresponds to a touch point.*

3.5 LINDDUN Contribution on Privacy Threat Analysis

LINDDUN [7] suggests a framework for threat analysis based on a list of threat categories, listed in the below table. It provides a method to describe systems (through data flow diagrams) and to identify threats (through graphical threat trees associated with elements of the diagrams).

Type	Property	Description	Threat
Hard privacy	Unlinkability	Hiding the link between two or more actions, identities, and pieces of information.	**L**inkability
	Anonymity	Hiding the link between an identity and an action or a piece of information	**I**dentifiability
	Plausible deniability	Ability to deny having performed an action that other parties can neither confirm nor contradict	**N**on-repudiation
	Undetectability and unobservability	Hiding the user's activities	**D**etectability
Security	Confidentiality	Hiding the data content or controlled release of data content	**D**isclosure of information
Soft Privacy	Content awareness	User's consciousness regarding his own data	**U**nawareness
	Policy and consent compliance	Data controller to inform the data subject about the system's privacy policy, or allow the data subject to specify consents in compliance with legislation	**N**on compliance

3.6 Hoepman Contribution on Design Strategies

Hoepman [10] focuses on design strategies. He defines two important engineering concepts: design strategies, and privacy patterns, i.e. high level engineering representations of PETs [32][33][34]. Design strategies allow for the selection of privacy patterns., which are implemented as PETs. Four data oriented strategies as well as four process oriented strategies are identified, and examples of patterns are provided, as showed in the below table.

Strategy		Examples of Patterns
Minimize	Amount of processed personal data restricted to the minimal amount possible	Select before you collect Anonymisation / Pseudonyms
Hide	Personal data, and their interrelationships, hidden from plain view	Storage and transit encryption of data Mix networks Hide traffic patterns Attribute based credentials Anonymisation / Pseudonyms
Separate	Personal data processed in a distributed fashion, in separate compartments whenever possible	Peer-to-peer arrangement Isolation and virtualisation
Aggregate	Personal data processed at highest level of aggregation and with least possible detail in which it is (still) useful	Aggregation over time (used in smart metering) Dynamic location granularity (used in location based services) k-anonymity Differential privacy
Inform	Transparency	Platform for privacy preferences Data breach notification
Control	Data subjects provided agency over the processing of their personal data	User centric identity management End-to-end encryption support control
Enforce	Privacy policy compatible with legal requirements to be enforced	Access control Sticky policies and privacy rights management
Demonstrate	Demonstrate compliance with privacy policy and any applicable legal requirements	Privacy management systems Use of logging and auditing

3.7 PRIPARE Contribution on a Privacy Engineering Methodology

PRIPARE[4] objective is to define an approach which takes privacy into account during the whole software and systems engineering process (lifecycle). In this undertaking we have identified the following challenges:

- There are no privacy practices or approaches addressing privacy through the whole system engineering lifecycle. In particular there is a big disconnect among existing best practices for privacy impact assessments[5] and research work on engineering reusability practices such as privacy patterns[6].

[4] FP7 project. See pripareprojet.eu
[5] such as ISO 29134 [2], the CNIL PIA [3], the EC Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems smart grid template [4]
[6] Such as [32][33][34], or repository attempts such as https://privacypatterns.eu, or http://privacypatterns.org/

- System engineers are not aware of privacy or ethical requirements nor of privacy-by-design principles. In particular privacy requirements are abstract and usually are formulated in legal or ethical terms, unrelated to specific technologies or methods[7].

The resulting PRIPARE methodology [21] is a set of processes, pointing to specific practices and methodologies, divided into classical system engineering phases (analysis, design, implementation, verification, release, maintenance and decommission). It also includes an environmental & infrastructure phase which acknowledges the privacy and security tasks that are horizontal to the organization and its projects and systems. The PRIPARE methodology also reuses OASIS-PMRM.

In this section we focus on PRIPARE main contributions to a privacy engineering framework:

- Concepts that combine privacy risk analysis with a goal-oriented elicitation of operational privacy requirement
- Concepts that integrate changes on architecture derived from the inclusion of privacy controls
- Concepts that cover the entire development lifecycle
- Concept that integrate the various existing development methodologies
- Recommendations on privacy controls verification

3.7.1 Goal-oriented Elicitation of Privacy Operational Requirements

PRIPARE [22] has defined an approach that combines a goal-oriented and a risk-based approach to discover and identify operational privacy requirements, as showed in Figure 6. Goal-orientation is the most straightforward approach [23] to engineer systems: engineers understand and build systems in terms of the goals they are intended to meet. This framework is defined as follows (in bold the important concepts):

> *The requirement analysis phase takes place in conjunction with risk management analysis.*
>
> *Risk management focuses on identifying the assets to protect in the system under development and the **threats** that might compromise the accomplishment of the **privacy principles** on these assets. Then a **treatment** is proposed to address the risk associated with the threat. This treatment may range from doing nothing (accept the risk) to including requirements that may avoid or reduce the **risk**.*
>
> *Requirement analysis is goal oriented: each **principle** is considered as a high level goal that the system must fulfil[8]. Each goal or **principle** is then refined into a set of lower-level **guidelines** required to meet the goal. Then a **success criterion** is proposed to address a guideline.*

[7] For instance Privacy by design principles formulated by Ann Cavoukian [18] [18] or in ISO29100 [1] are not operational;

[8] For example, data protection authorities' goals in Europe are related to the data protection principles stated in the EU GDPR, such as that of 'accountability' (i.e., ensuring and demonstrating compliance with data protection principles in practice)

*The set of **treatments** and **success criteria** are jointly referred as **operational requirements**.*

*The design phase has the objective to identify the **privacy controls** that are designed to meet the **operational requirements**. They are realised by measures designed to meet the **success criteria** and by countermeasures designed to meet the **treatments**.*

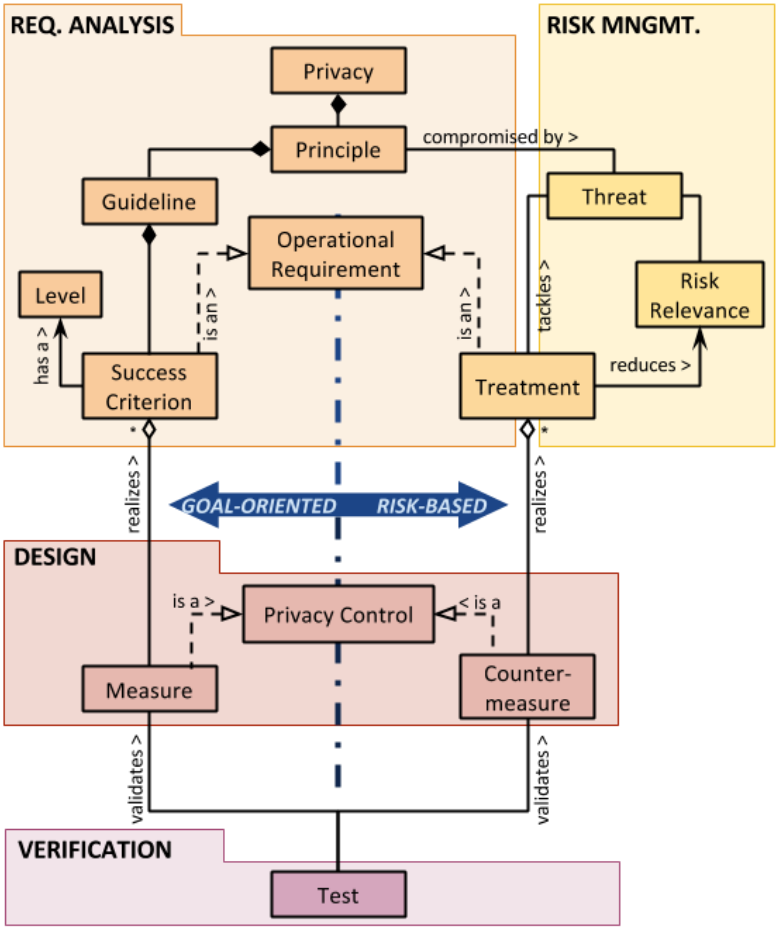

Figure 6: PRIPARE Goal-oriented and Risk-based Requirement Elicitation

There is a correspondence between the concepts of threats-treatments and of guidelines-criteria:

- A threat corresponds to a guideline
- A treatment corresponds to a criterium. Treatments and success criteria are both operational requirements
- A measure corresponds to a countermeasure. Both correspond to privacy controls.

However it is not expected to have a one-to-one mapping between threats and guidelines (or between treatments and criteria). It is rather expected that different operational requirements will be elicited by applying both the goal-oriented and risk based approaches.

The below tables show two examples.

Concept	Example on data minimization and proportionality
Principle	Data minimization and proportionality
Risk viewpoint: Threat	Accidental Data Leak
Risk viewpoint: relevance	Significant (Negligible, limited, significant, maximum)

Goal viewpoint: Guideline	Avoid or minimise the use of personal data along its whole lifecycle
Goal viewpoint: relevance	Relevant (Less Relevant, Relevant, Relevant and Essential)
Operational requirement (Treatment or Criteria)	Keep data from different services or different parties separated, and avoid combining them When some personal data is no longer needed for the specified purpose, delete or anonymise all the back-up data corresponding to that personal data
Privacy control	Architecture change to keep personal data in smart phone Anonymisation and attribute based credentials
Test	Conformance testing of architecture (personal data kept in smart phone) Conformance testing of anonymisation

Concept	**Example on transparency**
Principle	Transparency
Risk viewpoint: Threat	A data leak occurred. Organisation does not know which operation caused the leak
Risk viewpoint: relevance	Maximum (Negligible, limited, significant, maximum)
Goal viewpoint: Guideline	Provide a public privacy notice to the data subject
Goal viewpoint: relevance	Relevant and essential (Less Relevant, Relevant, Relevant and Essential)
Operational requirement (Treatment or Criteria)	Describe how the organisation processes personal data Describe the internal uses of personal data
Privacy control	Secure log of access and operations
Test	Battery of penetration tests

3.7.2 Architecture Change Resulting from the Design of Privacy Controls

The PRIPARE methodology [22] integrates the recognition that privacy operational requirements may lead to architecture changes (e.g. deciding that data is kept locally in a smart phone rather that globally on the cloud). The resulting architecture process which starts from operational requirements and produces architecture related decisions called PEARS (Privacy Enhancing Architectures) [8].

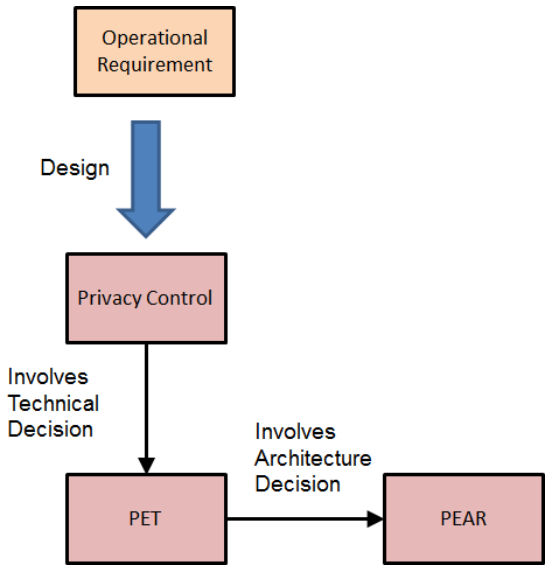

Figure 7: Architecture Decisions Associated with PETs

Figure 7 shows the relationship between operational requirements, PEARs, PETs and privacy controls. PETs are specified as the result of a privacy control design process, and can involve architecture change decisions called PEARs.

3.7.3 Lifecycle Oriented Methodology

As showed in Figure 8, PRIPARE privacy engineering is structured in seven different phases that match common and classic system engineering phases:

- **Analysis**: operational requirements elicitation
- **Design**: specification of privacy controls
- **Implementation**: transform the design into a built system
- **Verification**: ensure that the system meets privacy operational requirements
- **Release**: delivery to customer. Elaboration of an action plan to respond to the discovery of privacy breaches.
- **Maintenance**: reacting to privacy incidents.
- **Decommission**: Correctly dismantling the systems according to current legislation and policies.

An additional phase is integrated independent of the engineering process itself.

- **Environment & Infrastructure**: Putting in place an appropriate organizational structure, as well as in in-house awareness program[9]

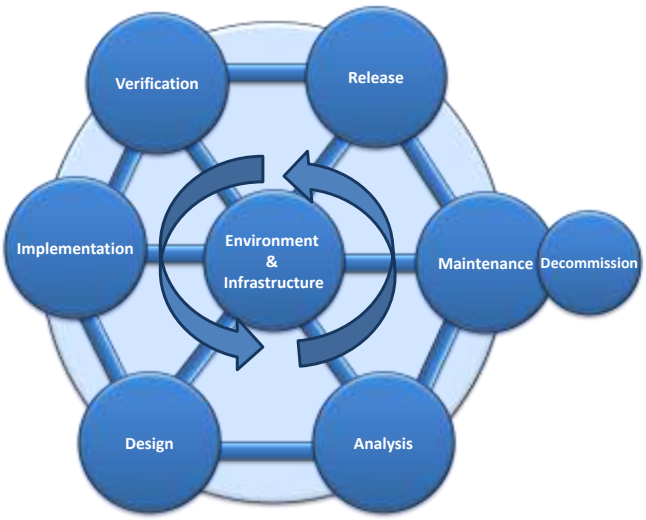

Figure 8: PRIPARE methodology phases

[9] This could be addressed by an approach similar to the organisational normative framework defined in ISO 27034 from application security.

3.7.4 Integration into Existing Methodologies

In order to ensure integration feasibility of PRIPARE methodology, each PRIPARE phase is structured into a set of processes:

Phase	Processes
Environment&Infrastructure	Organisational privacy architecture Promote privacy awareness
Analysis	Preliminary, functional description and high-level privacy analysis, privacy requirements operationalisation, legal compliance
Design	Privacy Control Design, PEAR Architecture impact evaluation, Privacy Enhancing Detailed Design
Implementation	Privacy implementation
Verification	Privacy Control Verification, Accountability, Static analysis, Dynamic Analysis
Release	Create Incident Response Plan, Create system decommissioning plan, Final Privacy review, Publish PIA report
Maintenance	Execute incident response plan, Privacy verifications
Decommissioning	Execute decommissioning plan

The smaller granularity allows for easier mapping into existing development methodologies (waterfall, iterative or incremental, prototyping, agile) and project management methodologies (PMBOK, PRINCE2).

3.7.5 Recommendation on Privacy Controls Verification

In parallel to work focusing on a privacy engineering methodology, the PRIPARE project has also prepared a report and recommendations and a research agenda [23]. We would like to highlight one important recommendation:

The evaluation and verification of the effectiveness of privacy controls is an overlooked topic. This stems from the belief that, similarly to other technologies, security/privacy mechanisms are plug and play: you include them and they work, while they offer very different protection in different scenarios (or even no protection) if they are not correctly implemented.

Significant research is needed in this area, for instance in the area of privacy quantification [24][25][26].

PRIPARE believes that privacy engineering must contain a placeholder for privacy control verification.

4 Strawman Privacy Engineering Framework (SPEF)

The following section provides a Strawman privacy engineering framework. Rather than focusing on providing a definitive content, it focuses on identifying important elements of a privacy engineering framework and explaining the rationale. This section reuses some of the previous figures and tables.

4.1 Basic Concepts for Privacy Engineering

4.1.1 Privacy engineering and Privacy-by-Design

The term privacy engineering is defined as follows

Privacy Engineering	A systematic, risk-driven process that operationalizes the Privacy-by-Design philosophical framework within IT systems. Privacy concerns are subsequently integrated into systems as part of the systems engineering process.

The term privacy-by-design is defined as follows

Privacy-by-design	Institutionalisation of the concepts of privacy and security in organisations and integration of these concepts in the engineering of systems.

Comment:

- The privacy engineering definition is inspired from MITRE [20]. Other definitions for privacy engineering could be used
  - Discipline of engineering systems integrating privacy as a non-functional requirement (inspired from Ann Cavoukian[10])
  - Collection of methods to support the engineering of systems that mitigate risks to individuals arising from the processing of their personal information within information systems (inspired from NIST [16])
- The privacy-by-design definition is taken from a blog entry contributed by PRIPARE[11]. The entry also refers to Ann Cavoukian's definition and proposes three other definitions
  - Approach to protecting privacy by embedding it into the design specifications of technologies, business practices, and physical infrastructures (Ann Cavoukian)
  - Approach to System Engineering which takes into account privacy and measures to protect ICT assets during the whole engineering process
  - Embedding privacy and security in the technology and system development from the early stages of conceptualisation and design and institutionalizing privacy and security considerations in organisations

[10] http://www.privacybydesign.ca/content/uploads/2014/01/pbd-priv-engineering.pdf
[11] http://www.securityengineeringforum.org/blog/show/id/27

- Applying a set of principles from the design phase of ICT systems in order to mitigate security and privacy concerns guiding designers and implementers decisions throughout the development of the systems

4.1.2 Privacy engineering objectives

Privacy engineering objectives express properties that need to be fulfilled by engineers designing privacy controls in a system.

Unlinkability	Ensures that privacy-relevant data cannot be linked across privacy domains or used for a different purpose than originally intended.
Transparency	Ensures that all privacy-relevant data processing including the legal, technical and organizational setting can be understood and reconstructed.
Intervenability	Ensures that data subjects, operators and supervisory authorities can intervene in all privacy-relevant data processing.

Comment:

- This section is taken from ULD[12] [15]. NIST [16] also provides 3 objectives (predictability, manageability, disassociability).
- High level engineering objectives are needed. They are similar to the confidentiality, integrity, availability objectives for security protection

4.1.3 From Privacy Principles to Privacy Operational Requirements

Privacy principles as defined in ISO29100 need to be applied in the requirement analysis of as system to identify privacy operational requirements. The engineering requirement analysis must take place in conjunction with a risk analysis activity.

4.1.3.1 Combining Goal oriented Analysis and Risk-based Analysis

The engineering requirement analysis phase takes place in conjunction with risk management analysis.

Risk management focuses on identifying the assets to protect in the system under development and the **threats** that might compromise the accomplishment of the **privacy principles** on these assets. Then a **treatment** is proposed to address the risk associated with the threat. This treatment may range from doing nothing (accept the risk) to including requirements that may avoid or reduce the **risk**.

Requirement analysis is goal oriented: each **principle** is considered as a high level concern that the system must fulfil. Each **principle** is then refined into a set of lower-level **guidelines** or

[12] The text is taken from https://www.datenschutzzentrum.de/guetesiegel/Privacy_Protection_Goals_in_privacy_and_data_protection_evaluations_V05_20120713.pdf

specific goals required to meet the concern. Then resulting engineering requirements of **criteria** are proposed to address the specific goals.

The set of **treatments** and **criteria** are jointly referred as **operational requirements**.

The design phase has the objective to identify the **privacy controls** that are designed to meet the **operational requirements**. They are realised by measures designed to meet the **success criteria** and by countermeasures designed to meet the **treatments**.

The resulting model is illustrated in Figure 9.

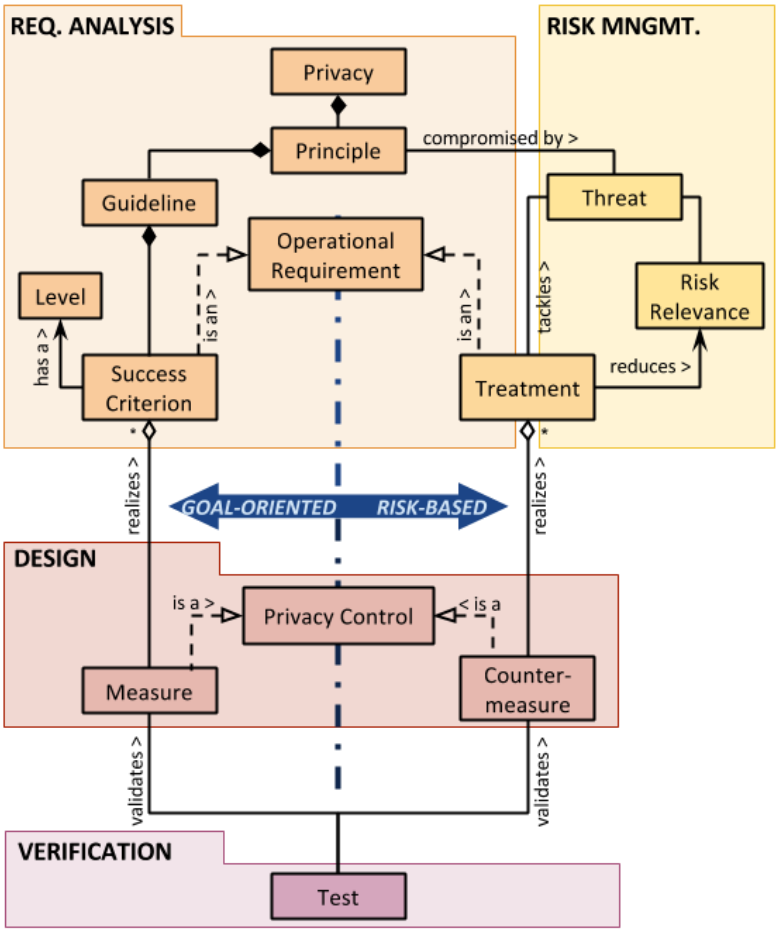

Figure 9: SPEF Goal-oriented and Risk-based Requirement Elicitation

Comment:

- This section is taken from PRIPARE [22].
- Engineers need to use goal oriented methods (positive thinking vs negative thinking). They also need use a method that clearly links to risk management and threat analysis

4.1.3.2 Operationalisation approach

An operationalisation approach is needed to identify the operational requirements. A number of steps are needed

- Step 1: Definition of scope of use case (inventory of services, applications, privacy principles, list of threats)

- Step 2: Detailed use case analysis (stakeholders, data flows and touch points)
- Step 3: Identify operational requirements (by carrying out a threat analysis and a goal oriented analysis)
- Step 4: Associate privacy functional services

Comments

- The steps described here are taken from OASIS-PMRM [5].
- Engineers need to be provided a methodology for operationalisation (i.e. identification of operational requirements)

4.1.3.3 Organisation Library

In order to help operationalisation the following knowledge is of interest within an organisation.

List of principles and associated catalog of guidelines and criteria	The following principles are identified: *consent and choice, purpose legitimacy and specification, collection limitation, data minimization, use, retention and disclosure limitation, accuracy and quality, openness, transparency and notice, individual participation and access, accountability, information security, privacy compliance* Organisations should maintain a catalog of guidelines and success criteria.
Categories of threats and associated catalog	The following categories of threats are identified: *Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, Non-compliance*. Organisations should maintain a catalog of threats and treatements.
Categories of privacy functional services and associated catalog	The following services are identified: *agreement, usage, validation, certification, enforcement, security, interaction, access*. Organisations should maintain a catalog of services.

Comments

- Catalog of threats is based on LINDDUN [7], list of principles is based on ISO 29100 [1], categories of services is based on OASIS-PMRM [5]
- Organisations must ensure that engineers reuse best practice and associated technology. A repository of associated knowledge (catalog) is needed

4.1.4 From Privacy Operational Requirements to Privacy Controls

Once operational requirements have been elicited, a design phase must be carried out that lead to the specification of privacy controls.

4.1.4.1 Model integrating Architecture Decisions

The design analysis phase involves decisions that can lead to architecture decisions or **PEAR**s (privacy enhancing architectures). For instance the design of a privacy control can involve decisions concerning data location which in turn may modify the system architecture.

Architecture decisions address mainly non-functional privacy requirements while Services address functional privacy requirements. The resulting model is showed in Figure 10.

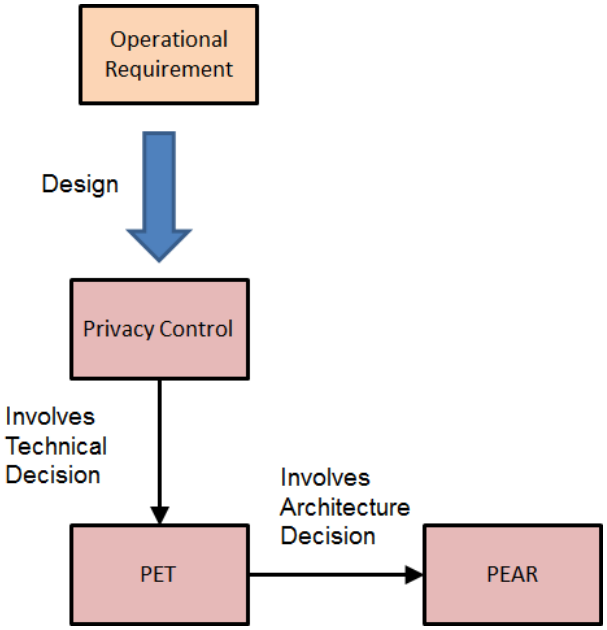

Figure 10: SPEF supporting PEARs and PETs

Comments

- Based on PEARS [8]
- Architecture decisions may have a greater impact in preserving privacy. They will be actually required in any future solution based on privacy enhancing technologies, e.g., attribute based credentials, multi-party computation, etc.
- Examples of privacy preserving solutions involving architecture decisions are PriPAYD [36] or PrETP [37].

4.1.4.2 Operationalisation

An operationalisation approach is needed to identify the privacy control. A number of steps are needed

- Step 1: Identification of privacy control (PETS) using privacy design strategies
- Step 2: if needed identification of architecture decisions (PEARs)
- Step 3: if needed evaluate architecture
- Step 4: Identification of privacy patterns
- Step 5: Evaluation of privacy control effectiveness (e.g. privacy quantification)
- Step 6: Evaluation of compliance

The concept of privacy pattern is key. A privacy pattern can focus on architecture aspects as well as functional behaviour aspects.

Comments

- Step 1 is based on Hoepman [10]. Step 2 and 3 are based on PEARS [8]. Step 4 is based on Hoepman [10]. Step 5 is based on PRIPARE recommendations [23]. Step 6 takes into account privacy impact assessment (i.e. it can be based on ISO 29134 [2])
- Engineers need to be provided a methodology for operationalisation (i.e. identification of privacy control and when appropriate identification of architecture decisions)

4.1.4.3 Organisation Library

In order to help operationalisation the following knowledge is of interest within an organisation.

List of design strategies and associated catalog of patterns and controls	The following categories of design strategies are identified: *Minimize, Hide, Separate, Aggregate, Inform, Control, Enforce* Organisations should maintain a catalog of privacy controls (for instance ISO 29151) and privacy patterns.

Comments

- Design strategies and privacy patterns are based on Hoepman [10]. Privacy patterns repositories initiatives have started (see https://privacypatterns.eu, or http://privacypatterns.org/).
- Organisations must ensure that engineers reuse best practice and associated technology. A repository of associated knowledge is needed.

4.1.5 Life Cycle Approach

Organisation carrying out privacy engineering must take into account all phases of the lifecycle. In order to allow for easier integration of privacy engineering activities into existing methodologies (waterfall, agile, prototyping), it is advised to structure a privacy engineering methodology into phases and processes that can then be easily integrated in an organisation development methodology.

4.1.5.1 Phases and Processes

The table below describes the main phases of a privacy engineering methodology, the associated system life cycle processes and possible activities.

Privacy Engineering Phase	**System Life Cycle Processes (ISO 15288)**	**Privacy Engineering Activities**
Environment & Infrastructure	Infrastructure management process Project privacy portfolio management process	Organisational privacy architecture Promote privacy awareness
Analysis	Stakeholder privacy requirements definition process Privacy requirements analysis process	Preliminary, functional description and high-level privacy analysis, privacy requirements operationalisation, legal compliance
Design	Privacy architectural design process	Privacy Control Design, PEAR Architecture impact evaluation, Privacy Enhancing Detailed Design
Implementation	Privacy implementation process	Privacy implementation
Verification	Privacy Verification process	Privacy Control Verification, Accountability, Static analysis, Dynamic Analysis
Release	Transition process	Create Incident Response Plan, Create system decommissioning plan, Final Privacy review, Publish PIA report
Maintenance	Maintenance process	Execute incident response plan, Privacy verifications
Decommissioning	Disposal process	Execute decommissioning plan

Comment:

- This section is inspired from PRIPARE [21], [22] taking into account ISO 15288

4.1.5.2 Environment & Infrastructure

The environment & infrastructure phase follows ISO 27034 [35] adapted to application privacy[13].

The concept of organisation normative framework is defined as a framework where all application privacy best practices recognized by the organization are stored, or from which they will be refined or derived. It comprises essential components, processes that utilize these components, and processes for managing the ONF itself. Figure 11 shows a high-level view of the ONF contents.

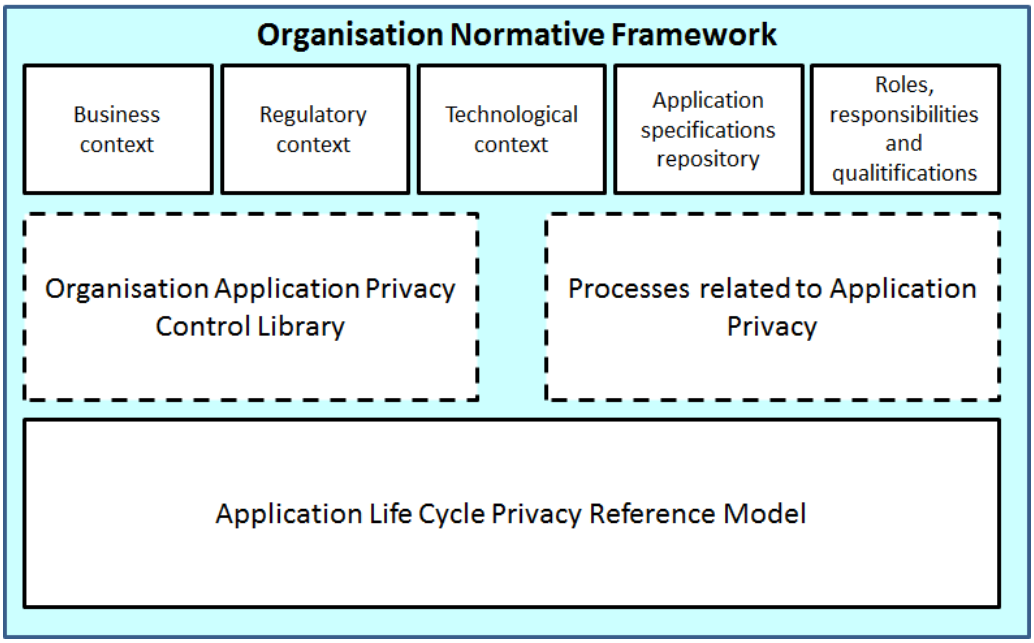

Figure 11: SPEF Organisation Normative Framework

For the purposes of correctly addressing application security concerns, an organization should have a formal ONF containing the following components:

- business context;
- regulatory context;
- technological context;
- application specifications repository;
- roles, responsibilities and qualifications;
- organization Application Control Library (i.e. privacy controls);
- processes related to application privacy;
- Application Privacy Life Cycle Reference Model

[13] A privacy engineering framework standard could be based on ISO27034, extended to application privacy

Comment:

- This section is taken from ISO 27034 [35] and PRIPARE [21].
- While ISO 27034 provides guidance on how to handle application security, a privacy engineering framework should also provide guidance on how to handle application privacy.

4.2 Privacy Engineering Principles

A number of privacy engineering principles are defined. These principles are added to the ISO 29100 privacy principles to further *guide the design, development, and implementation of privacy policies and privacy controls* from an engineering viewpoint.

Integration of risk management	Privacy engineering activities must be carried out jointly with the risk management activities needed to ensure proper handling of privacy. ISO 29134 and associated practices can be used as reference. The rationale for this principle is that while an engineering viewpoint must be taken, engineers must include a risk management perspective.
Integration of compliance	Privacy engineering activities must be carried out jointly with the compliance checking (e.g. technical oblications, legal obligations). The rationale for this principle is that while an engineering viewpoint must be taken, engineers must include a compliance perspective. This can involve impact assessment documents, assurance and conformance activities.
Unlinkability objective	Unlinkability is a privacy engineering objective. It ensures that privacy-relevant data cannot be linked across privacy domains or used for a different purpose than originally intended. The rationale for this principle is that unlinkability is a specific property for privacy.
Transparency Objective	Transparency is a privacy engineering objective. It ensures that all privacy-relevant data processing including the legal, technical and organizational setting can be understood and reconstructed. The rationale for this principle is that transparency is a specific property for privacy management.
Intervenability Objective	Intervenability is a privacy engineering objective. It ensures that data subjects, operators and supervisory authorities can intervene in all privacy-relevant data processing. The rationale for this principle is that intervenablity is a specific property for privacy management.
Integration of coal-orientation in	The identification of requirements in privacy engineering must include is goal orientation approach where engineers describe requirements in

requirement engineering	terms of the goals that must be met by systems. The rationale for this principle is that goal orientation is needed for engineering. It will complement requirements elicited through risk analysis.
Data oriented Design strategies	Privacy engineering includes data oriented design strategies. These strategies can help address the unlinkability objective. They often lead to architectural decisions (privacy enhancing architectures). The rationale for this principle is that data oriented design strategies will help meet unlinkability properties.
Process oriented Design strategies	Privacy engineering includes process oriented design strategies. These strategies can help address the transparency and intervenability objectives. The rationale for this principle is that process oriented design will help meet transparency and intervenability properties.
Lifecycle Support	Privacy engineering extends to the entire lifecycle. The rationale for this principle is that privacy management extends over the entire lifecycle. Consequently privacy engineering must extend over the entire lifecycle.
Privacy engineering knowledge capitalisation	Privacy engineering relies on knowledge capitalisation. Privacy controls can be stored and reuse (e.g. through privacy patterns). Processes can also be stored in organisation libraries. Organisation normative frameworks (as described in ISO 27034) can be used to this end. The rationale for this principle is that privacy-by-design must be institutionalised within organisations.

4.3 List of Terms

In red the new terms.

Privacy Engineering		A systematic, risk-driven process that operationalizes the Privacy-by-Design philosophical framework within IT systems. Privacy concerns are subsequently integrated into systems as part of the systems engineering process.
Privacy-by-design		Institutionalisation of the concepts of privacy and security in organisations and integration of these concepts in the design of systems
Privacy Engineering objectives		Properties that need to be fulfilled by engineers designing privacy controls in a system.
	Unlinkability	Ensures that privacy-relevant data cannot be linked across privacy domains or used for a different purpose than originally intended.
	Transparency	Ensures that all privacy-relevant data processing including the legal, technical and organizational setting can be understood and reconstructed.

	Intervenability	Ensures that data subjects, operators and supervisory authorities can intervene in all privacy-relevant data processing.
Privacy principle (ISO 29100)		Principles that guide the engineer in the engineering of systems
Privacy Operational Requirements		Engineering requirements addressing privacy principles
	Treatment against risks	Engineering requirements resulting from treatments of identified threats.
	Guidelines to meet goals	Engineering requirements resulting from identified privacy engineering objectives
Privacy control (ISO 29100)		Measures that treat privacy risks by reducing their likelihood or their consequences
	Privacy enhancing technology (ISO 29100)	Privacy control, consisting of information and communication technology (ICT) measures, products, or services that protect privacy by eliminating or reducing personally identifiable information (PII) or by preventing unnecessary and/or undesired processing of PII, all without losing the functionality of the ICT system
	Privacy enhancing architectures	Architecture decisions associated with privacy controls.
	Architecture (ISO 42010)	Fundamental concepts or properties of a system in its environment embodied in its elements, relationships, and in the principles of its design and evolution
	Architecting (ISO 42010)	Process of conceiving, defining, expressing, documenting, communicating, certifying proper implementation of, maintaining and improving an architecture throughout a system's life cycle (i.e., "designing")
Privacy control implementation		
	Privacy pattern	General reusable solution to a class of problems in privacy.
Life cycle process (ISO 12207)		
	Privacy engineering phases	Set of ISO 12207 processes logically grouped from a privacy engineering viewpoint
	Privacy engineering processes	ISO 12207 processes specialised to privacy engineering
	Privacy engineering activities	ISO 12027 activities dedicated to privacy engineering

4.4 Additional Terms

These terms depends on solutions and approaches used in the framework.

- OASIS-PMRM for operationalisation of privacy principles (e.g. touch points)
- CMU software architecture approach (e.g. architecture tactics, quality attributes)
- Hoepman design strategies (e.g. minimize, hide, separate, aggregate, inform, control, enforce, demonstrate)
- LINDDUN threat analysis (e.g. linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, Non-compliance)
- Selected development methodology

5 Conclusion

The wealth of contributions made recently on privacy engineering shows that

- a complete and convergence of understanding is possible
- a framework is needed in order to federate all those contributions

PRIPARE recommendations for the study period are

- to validate PRIPARE viewpoint during the study period
- to prepare for the submission of a NWIP on a privacy engineering framework

Annex 1 Taking into Account Existing References

The following table provides a high-level analysis on how the Strawman Privacy Engineering Framework can be related to the existing references

ISO 29100 – Privacy framework	*The privacy engineering framework should extend 29100 with an engineering viewpoint*
ISO 29101 – Privacy Architecture framework	29101 provides an architecture framework for ICT systems that process PII. It provide a component viewpoint consisting of three layers, a privacy setting layer, an identifer and access management layer, a PII layer. *The privacy engineering framework can use 29100 as a reference for an architecture framework.*
ISO 29134 – Privacy Impact Assessment guidelines	29134 describes a process to assess the potential impacts of a system in order to treat privacy risk. *29134 can be used in the risk management part of a privacy engineering framework.*
ISO 29151 – Code of practice for personally identifiable information	29151 offers guidance on a broad range of information security and PII protection controls. *29151 can be used in the design part of a privacy engineering framework.*
ISO 27034 – Application security	27034 is a set of standard focusing on application security. *All the standards are references that can be used to cope with security associated with data protection.* 27034-1 defines in particular an organization normative framework: a framework where all application security best practices recognized by the organization are stored, or from which they will be refined or derived. It comprises essential components, processes that utilize these components, and processes for managing the ONF itself. *The privacy engineering framework can also extend this organization normative framework to integrate privacy best practices, as showed in Figure 11.*
ISO 42010 – Systems and software engineering - Architecture	Standard for architecture descriptions of systems and software. 29100 uses ISO 42010. *Any item in a privacy engineering framework referring to an architecture description should use ISO42010.*
ISO 15288 - System Life Cycle	Systems Engineering standard covering processes and life cycle stages. *Any item in a privacy engineering framework referring to a system*

Processes	*process and life cycle stages should use ISO 15288.*
ISO 12207 - Software Life Cycle Processes	Standard for software life cycle processes. *Any item in a privacy engineering framework referring to a software life cycle process should use ISO 122087.*
CNIL privacy risk management	The CNIL risk management [27] is provides practical guidelines for privacy impact assessments. *These guidelines can be used for risk management in Figure 9 and integrated in the organisation normative framework in Figure 11.*
NIST report	The NIST report defines protection objectives. *These protection objectives could be the one defined in the Privacy Engineering framework.* The NIST report defines a risk management approach. *These guidelines can be used for risk management in Figure 9 and integrated in the organisation normative framework in Figure 11.*
OASIS-PMRM	Standard describing a methodology for privacy analysis to identify appropriate operational privacy management functionality and supporting mechanisms. *A number of concepts in OASIS-PMRM could be integrated in the privacy engineering framework (e.g. touch points).* *OASIS-PMRM can be used for privacy analysis and integrated in the organisation normative framework in Figure 11.*
OASIS-PbD-SE	Committee working on providing privacy governance and documentation standards for software engineers. Uses UML as a starting point *Standards developed by OASIS-PbD-SE can be integrated in the organisation normative framework in Figure 11.*
EDPS IPEN	Community led by EDPS[14]. A workshop took place in June 2015 with two livestreamed sessions on standardization[15], which led to two actions: • Creation of a wiki on privacy standards[16] • Task force (Antonio Kung, Achim Klabunde, Alexander Hanff) to draft a statement on the need for a privacy engineering framework *Action in progress – This document will be shared within the task force*
MITRE privacy engineering	Technical paper [20] highlighting the need to take an engineering viewpoint to integrate elements such as a privacy testing, privacy-

[14] https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/IPEN
[15] https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/IPEN/IPEN_Workshop_2015
[16] See http://ipen.trialog.com/. Contact Antonio.kung@trialog.com for an account

framework	sensitive design decisions, privacy requirements and control selection, and system focused risk assessment. *The privacy engineering framework should contain these elements. The Strawman privacy engineering framework contains them.*
Centre for Information Policy Leadership research on Privacy Risk Management	Think tank that has published documents on privacy risk managements[17] *These documents can influence the risk management part of privacy and be taken into account in practices that are integrated in an organization normative framework as in Figure 11.*

[17] https://www.hunton.com/files/Uploads/Documents/Centre/Role_of_Risk_Management_in_Data_Protection.pdf and https://www.informationpolicycentre.com/files/Uploads/Documents/Centre/A_Risk-based_Approach_to_Privacy_Improving_Effectiveness_in_Practice.pdf

Annex 2 Taking into Account Existing methodologies

This section is taken from a forthcoming version of [21]. It shows how the PRIPARE methodology can be integrated into existing methodologies. The approach is to structure PRIPARE privacy engineering methodology into a set of processes that can be integrated these methodologies.

A2.1 Software and system engineering methodologies

A2.1.1 Waterfall

The concept of the waterfall model was first formally described in Royces's 1970 article [29] but did not use the term waterfall.

Royce defined a common set of steps to all computer development process:

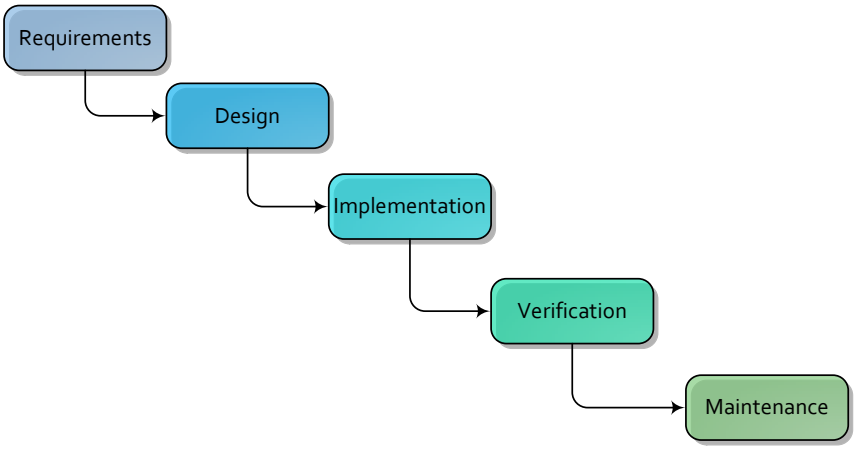

Figure 12: Waterfall methodology phases

PRIPARE's methodology will have to provide a linear alternative with sequential steps so it can match this methodology. Steps should be grouped into equivalent stages in the PSbD methodology for a seamlessly methodology integration.

A2.1.2 Iterative or incremental

Given the limitations of the waterfall model some modifications were made to make a more usable and realistic model.

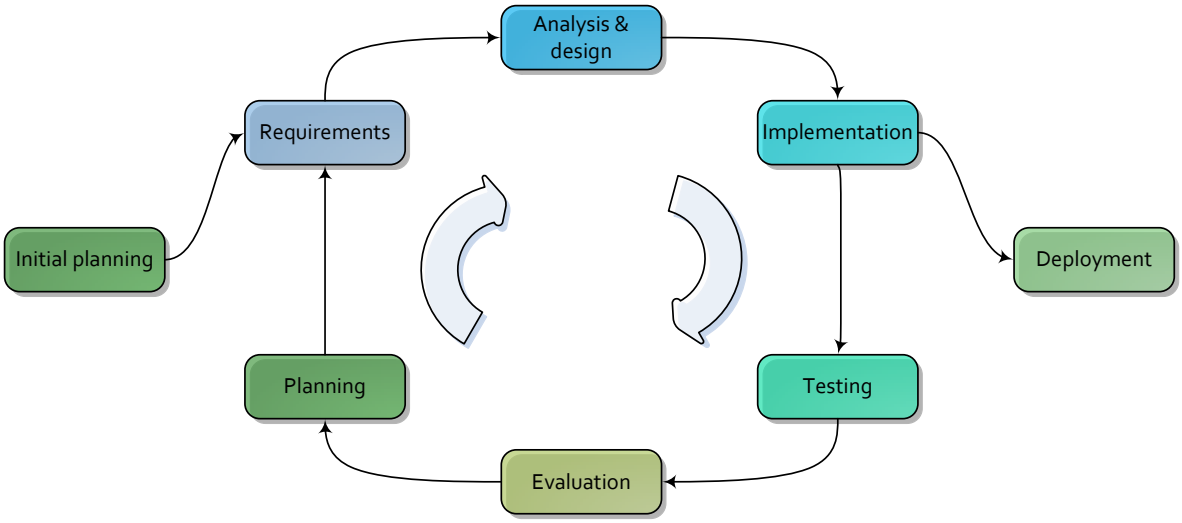

Figure 13: Iterative methodology phases

The iterative model has some benefits that the waterfall model lacks:

- Intermediate delivery steps, enabling the measure of the alignment with the project goals;
- Supports refactoring, enabling better designs;
- Uses developer and user's feedback;

A2.1.3 Prototype

The original purpose of this model is to evaluate non-final proposals for the design of the system by trying then out rather than interpreting its descriptions. It is also useful to present prototypes to end users so they can test them and input their feedback before the production is developed.

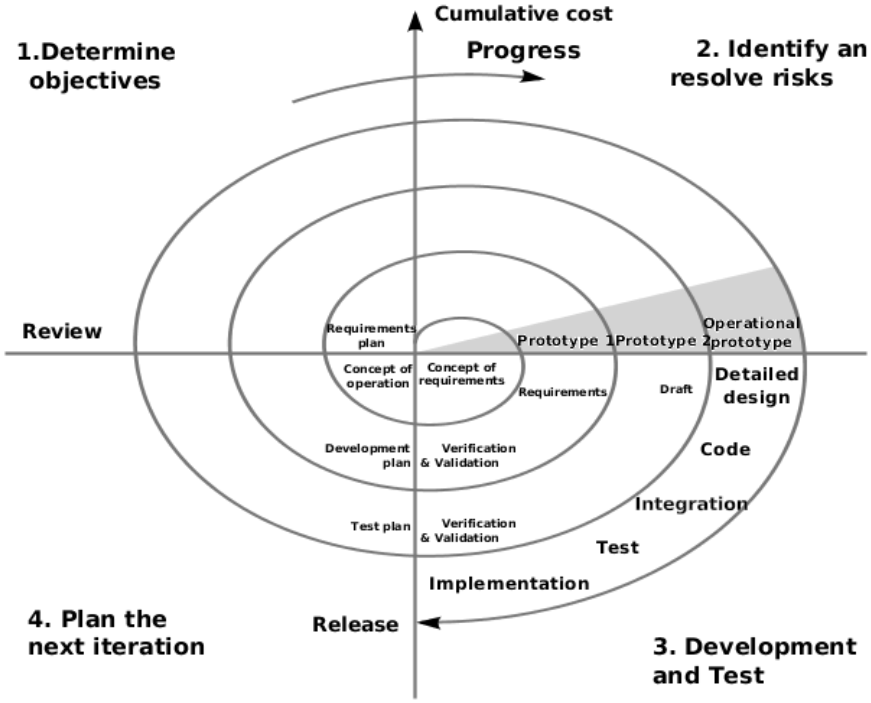

Figure 14: Prototype methodology phases [30]

The prototype model has some benefits that the waterfall and iterative models lack:

- Reduced time and costs; by providing end users with prototypes, the quality of elicited requirements will improve and minimise changes during implementation where the costs grow exponentially;
- Improved user involvement; engaging the customer or the end users during the prototyping phases allows them to provide more complete specifications that help to build a satisfactory product;

A2.1.3 Agile

In 2001 a group of software developers gathered to discuss lightweight development methods in reaction against other software development methods that were more heavy-weighted, harder to follow and flawed with several handicaps (e.g. inability to handle changes, higher cost and burden of documentation). As a result of the discussion they published the Manifesto for Agile Software Development that includes twelve principles [11]. This agile manifesto for software development can and has been adapted to a more generic approach that can be used as a project management methodology. Many methodologies follow the agile manifesto (e.g scrum, Kanban and extreme programming).

Even if it is the case that Scrum is only one of multiple agile methodologies, it is the most extended.

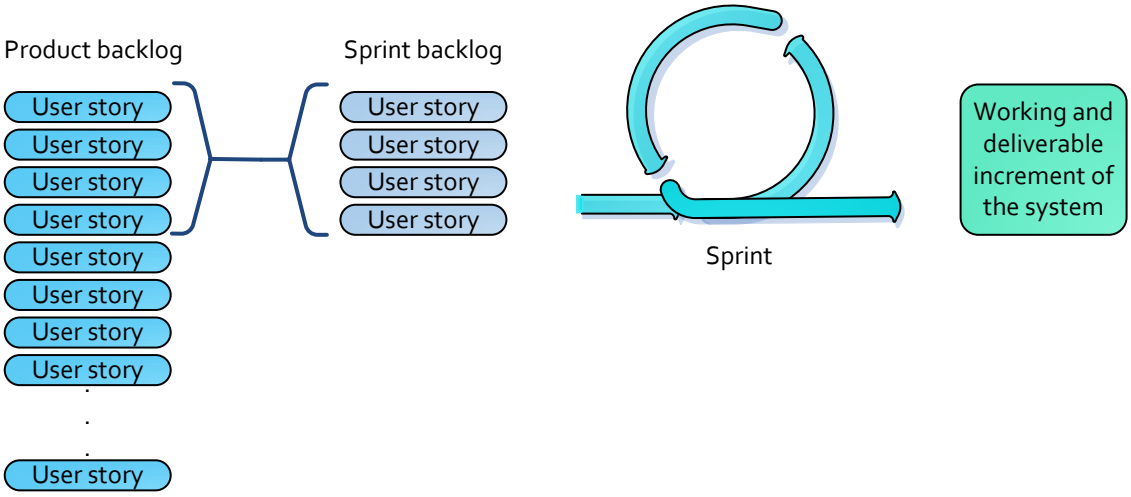

Figure 15: Scrum methodology phases

A2.2 Project management methodologies

Project management methodologies can be used to complement development methodologies.

A2.2.1 PMBOK

The PMI (Project Management Institute) developed the PMBOK® guide in an attempt to document a standard terminology and a compendium of guidelines and good practices for project management.

PMBOK® defines a set of processes in terms of inputs, tools and techniques and outputs. The process list is organized into five groups and ten different knowledge areas that should be followed during the project lifecycle.

Knowledge areas	Process groups				
	Initiating	Planning	Executing	Monitoring & Controlling	Closing
Integration					
Scope					
Time					
Cost					
Quality					
Human resource					
Communication					
Risk					
Procurement					
Stakeholders					

Figure 16: PMBOK process and knowledge matrix

A2.2.2 PRINCE2

PRINCE2 is a project management methodology developed by the Office of Government Commerce (OGC). It is widely used in the UK but has also been adopted more globally (mostly in Australia or Europe [31]). Despite the fact that PRINCE2 was initially developed for ITC project development; its last version is compatible with any project typology.

PRINCE2 is a process driven methodology that is based on:

- Seven principles: continued business justification, learn from experience, defined roles and responsibilities, manage by stages, manage by exception, focus on products and tailored to suit the project environment;
- Seven themes: business case, organization, quality, plans, risk, change and progress;
- Seven processes: Starting up a project, initiating a project, directing a project, controlling a stage, managing stage boundaries, managing product delivery and closing a project;

Each process provides the specific activities that have to be performed and the inputs and outputs that should be used or provided. Principles and themes should be followed during all the project management processes.

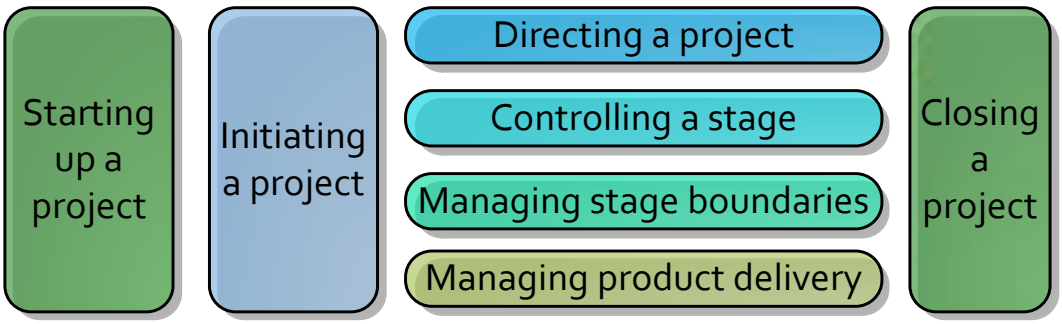

Figure 17: PRINCE2 seven processes

Annex 3 References

[1] International Organization for Standardization (ISO), Information technology – Security techniques – Privacy framework, ISO/IEC 29100:2011, First edition, Geneva, 15 Dec 2011.

[2] International Organization for Standardization (ISO), Privacy impact assessment -- Methodology, ISO/IEC WD 29134, Under development.

[3] CNIL Privacy Impact Assessment. http://www.cnil.fr/english/news-and-events/news/article/privacy-impact-assessments-the-cnil-publishes-its-pia-manual/

[4] EC Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems https://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

[5] Organization for the Advancement of Structured Information Standards (OASIS) *Privacy Management Reference Model and Methodology (PMRM),* Version 1.0. July 2013. http://docs.oasis-open.org/pmrm/PMRM/v1.0/PMRM-v1.0.pdf

[6] International Organization for Standardization (ISO), Code of Practice of Personally identifiable information protection, ISO/IEC WD 29151, Under development.

[7] LINDDUN privacy threat analysis methodology, https://distrinet.cs.kuleuven.be/software/linddun/

[8] Antonio Kung. “PEARs: Privacy Enhancing Architectures”. Annual Privacy Forum, May 21-22, 2014, Athens, Greece. Proceedings APF14 "Privacy Technologies and Policy". Lecture Notes in Computer Science Volume 8450, 2014, pp 18-29

[9] Software Architecture in Practice (3rd Edition), Len Bass, Paul Clementz, Rick Kazman. Addison-Wesley, 2012

[10] Japp Henk Hoepman. “Privacy design strategies”. ICT Systems Security and Privacy Protection - 29th IFIP TC 11 Int.Conf, SEC 2014, Marrakech, Morocco

[11] Beck, K., Mike Beedle, Arie van Bennekum, Alistair Cockburn, Ward Cunningham, Martin Fowler, James Grenning, Jim Highsmith, Andrew Hunt, Ron Jeffries, Jon Kern, Brian Marick, Robert C. Martin, Steve Mellor, Ken Schwaber, Jeff Sutherland and Dave Thomas, “Manifesto for Agile Software Development". Agile Alliance. http://agilemanifesto.org/

[12] S.Spiekermann, L.Cranor. “Privacy Engineering”. IEEE Transactions on Software Engineering, Vol. 35, Nr. 1, January/February 2009, pp. 67-82.

[13] S. F. Gürses, C. Troncoso, and C. Diaz. “Engineering Privacy-by-Design”. Computers, Privacy & Data Protection, 2011

[14] A.Kung, J.Freytag, F.Kargl. “Privacy-by-design in ITS applications”. 2nd IEEE International Workshop on Data Security and Privacy in wireless Networks, June 20, 2011, Lucca, Italy

[15] Marit Hansen, Meiko Jensen, Martin Rost: “Protection Goals for Engineering Privacy”; in 2015 International Workshop on Privacy Engineering (IWPE). http://ieee-security.org/TC/SPW2015/IWPE/2.pdf

[16] NISTIR 8062 (Draft). “Privacy Risk Management for Federal Information Systems”. May 2015. http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf

[17] European Data Protection Supervisor (EDPS), “European Data Protection Supervisor Glossary”. https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/Glossary.

[18] Ann Cavoukian, “7 Foundational Principles of Privacy by Design”, Information & Privacy Commissioner, Ontario, Canada. http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/

[19] ISO/IEC JTC1/SC27/WG5 N14652 WG5 Roadmap

[20] MITRE Privacy engineering framework. July 2014. http://www.mitre.org/publications/technical-papers/privacy-engineering-framework

[21] PRIPARE methodology. Draft version. http://pripareproject.eu/wp-content/uploads/2013/11/PRIPARE_Deliverable_D1.2_draft.pdf. Final version forthcoming (Oct 2015).

[22] Nicolás Notario, Alberto Crespo, Yod Samuel Martín García, José M. Del Álamo, Daniel Le Métayer, Thibaud Antignac, Antonio Kung, Inga Kroener and David Wright. “PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology”; in 2015 International Workshop on Privacy Engineering (IWPE). http://ieee-security.org/TC/SPW2015/IWPE/1.pdf

[23] Carmela Troncoso. PRIPARE Forthcoming report on Recommendations and Research Agenda. Deliverable D5.3. September 2015.

[24] Gervais, Arthur, Reza Shokri, Adish Singla, Srdjan Capkun, and Vincent Lenders. "Quantifying Web-Search Privacy." In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, pp. 966-977. ACM, 2014.

[25] Shokri, Reza, George Theodorakopoulos, Jean-Yves Le Boudec, and Jean-Pierre Hubaux. "Quantifying location privacy." In Security and Privacy (SP), 2011 IEEE Symposium on, pp. 247-262. IEEE, 2011.

[26] Humbert, Mathias, Erman Ayday, Jean-Pierre Hubaux, and Amalio Telenti. "Addressing the concerns of the lacks family: quantification of kin genomic privacy." In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, pp. 1141-1152. ACM, 2013.

[27] Goal-Oriented Requirements Engineering: A Guided Tour, A. van Lamsweerde, 5th International Symposium on Requirements Engineering, IEEE Computer Society Press, 2001

[28] Commission nationale de l'informatique et des libertés (CNIL), Methodology for privacy risk management - Methodology: http://www.cnil.fr/fileadmin/documents/en/CNIL-PIA-1-Methodology-EN.pdf. Tools (templates and knowledge bases): http://www.cnil.fr/fileadmin/documents/en/CNIL-PIA-2-Tools-EN.pdf. Good practices: http://www.cnil.fr/fileadmin/documents/en/CNIL-PIA-3-GoodPractices.pdf

[29] Royce, W., “Managing the Development of Large Software Systems”, *Proceedings of IEEE WESCON 26,* August 1970. http://www.cs.umd.edu/class/spring2003/cmsc838p/Process/waterfall.pdf

[30] Boehm, B, "Spiral Development: Experience, Principles and Refinements”, *Special report CMU/SEI-2000-SR-008*, July 2008. http://www.sei.cmu.edu/reports/00sr008.pdf

[31] Price Waterhouse and Coopers (PWC), “Insights and Trends: Current Portfolio, Programme, and Project Management Practice. The third global survey on the current state of project management”, 2012. http://www.pwc.com/us/en/public-sector/publications/global-pm-report-2012.jhtml

[32] M.Hafiz. A Collection of Privacy Design Patterns. Proceedings of the Pattern Language of Programs Conference, 2006.

[33] S. Romanosky, A. Acquistit, J. Hong, L. Cranor, B. Friedman, “Privacy Patterns for Online Interac3ons”, Proceedings of the Pattern Languages of Programs Conference, 2006

[34] N. Doty. “Privacy Design Patterns and And Patterns”, Trustbusters Workshop at the Symposium on Usable Privacy and Security. July 2013.

[35] ISO/IEC 27034:2011 Information technology — Security techniques — Application security

[36] C.Troncoso, G.Danezis, E.Kosta, J.Balasch, and B.Preneel. PriPAYD: Privacy-Friendly Pay-As-You-Drive Insurance. IEEE Transactions on Dependable and Secure Computing. 8(5), pp. 742-755, 2011.

[37] J.Balasch, A.Rial, C.Troncoso, C.Geuens, B.Preneel and I.Verbauwhede. PrETP: Privacy-Preserving Electronic Toll Pricing (extended version). 19th USENIX Security Symposium