PRIPARE

PReparing **I**ndustry to **P**rivacy-by-design by supporting its **A**pplication in **RE**search

PRIPARE's New Vision on Engineering Privacy and Security by Design

CYBER SECURITY & PRIVACY FORUM 2014

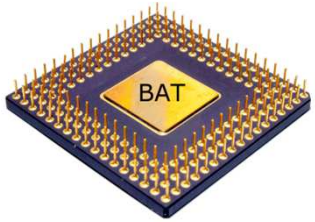
Nicolás Notario (nicolas.notario@atos.net)

Atos

What is PSbD?

An approach that takes privacy and security into account during the whole engineering process

A series of privacy and security principles



Helps to design and choose Best Available Technologies and Techniques

Ensuring that engineered systems are secure and privacy-respectful

State of the art

Ontario IPC PbD principles

Full Functionality – Positive-Sum, not Zero-Sum

Privacy Impact Assessments

More than a compliance check

Privacy Management Reference Model

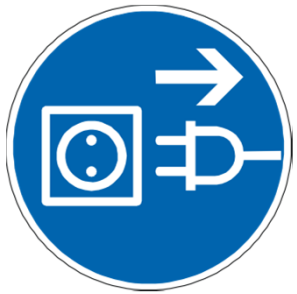
Understanding and analysing privacy policies and their management requirements; selecting technical services which must be implemented to support privacy controls

Risk Management

remove, minimise, transfer or accept identified risks

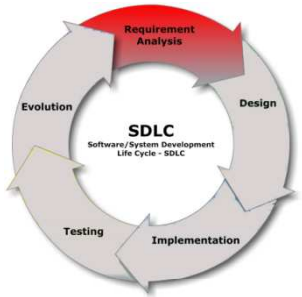
Privacy Enhancing ARchitectures

The problem



Current practices are disengaged with engineering practices

Unexperienced designers have no guidelines to produce privacy-supporting designs



Current approaches mainly focus on analysis & design phase

The architectural dimension is not well addressed

PRIPARE's approach: PSbD methodology

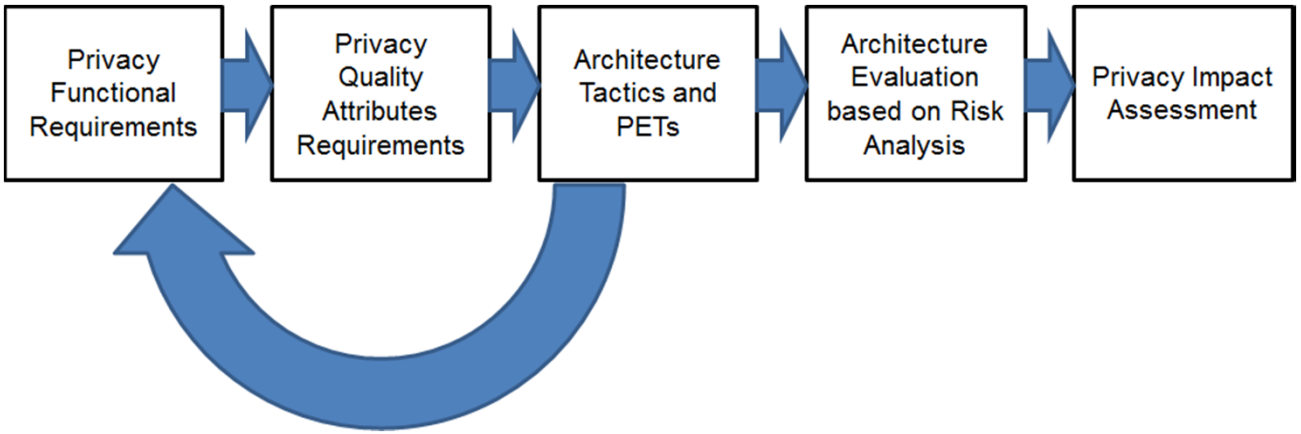
- Designed to cover the whole system lifecycle
- Short, easy-to-understand and easy-to-use
- Flexible so it can adapt depending on the nature of the project and the information collected
- Integrated with risk assessment standards
- Useful for different types of stakeholders
- Engaged with system engineering practices (complements existing methodologies)

PRIPARE - Analysis

- Complement PMRM with PIA and (Privacy) Risk management approaches for the analysis stage.
- The output of this stage would be a boundary object that holds all extracted information that can then be selected according to each stakeholder's interests (privacy officers, system designers, developers…)
  - Application description
  - Information flows
  - Stakeholders
  - Domains
  - Touch points
  - …

PRIPARE - Design & Implementation

- Apply PEARs approach



- Use privacy patterns to aid in the effective design of secure systems that support privacy
- Use architecture tactics to tailor patterns during the design & implementation phases
- Perform Static Analysis of the system

PRIPARE – Verification, Release & maintenance

- Apply a Privacy and Security Test Plan during the verification stage (privacy & security verification)
- Perform Dynamic Analysis
  - Heartbleed example
- Final Privacy and Security reviews
- Privacy & Security Incidents Response Plan
- Publish PIA Report (& foreseen updates)
- Execute the Incident Response Plan
- Verification of privacy and security policies enforcement

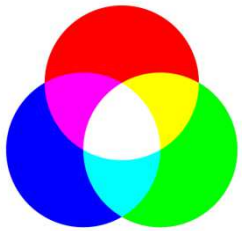
Approaches/desirable features comparison

	PIA	Risk Management (CNIL)	PMRM	PEAR	PRIPARE
Ensures system's legal compliance	★★★	★★	★★	★	★★★
Provides system's architectural aspects	★	★	★	★★★	★★★
Useful for multiple stakeholders	★★	★	★★★	★	★★★
Useful for system engineers	★	★	★★	★★★	★★★
Identifies privacy risks	★★★	★★★	★★★	★	★★★
Supports multiple domains (organisational or legal)	★★	★	★★★	★	★★★
Supports privacy patterns	★	★	★★	★★★	★★★
Provides accountability for privacy decisions	★★★	★★★	★★★	★★	★★★

Degree of support:
★ Low ★★ Medium ★★★ High

PRIPARE – Open challenges

What privacy or security metrics can assist during the design process in order to ensure that taken decisions are correctly assessed?



How can PRIPARE complement the wide variety of system engineering methodologies?. I.e. Scrum lacks a design phase or formal requirements analysis

Is there a way to truly and easily verify (statically and dynamically) that security and privacy non-functional requirements are being covered?

PRIPARE

PReparing **I**ndustry to **P**rivacy-by-design by supporting its **A**pplication in **RE**search

Thank you for your attention

Questions?

Website: www.pripareproject.eu

Nicolás Notario: nicolas.notario@atos.net

Project Co-ordinator
Antonio Kung (Trialog)

Technical Co-ordinator
Christophe Jouvray (Trialog)