PRIPARE

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

PRIPARE: un projet Européen visant à définir une pratique intégrée de protection de la vie privée par construction

PRIPARE: towards an integrated privacy-by-design practice

27 Mai 2015

Antonio Kung. Trialog. www.trialog.com

PRIPARE (prip areproject.eu)

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

Support Action Mission:

- Define and Support practice of privacy-by-design
- Provide educational material to foster risk management culture

Integrates disconnected practices

Ontario IPC PbD principles

PIA

Privacy Impact Assessments

Privacy Management Reference Model (PMRM)

Microsoft Security Development Lifecycle

Risk management

PEARs

Privacy Enhancing Architectures

ISO Standards (29100, 29101, 24760, 29134, 29151)

Outline

- Privacy-by-design?
  - An example of what can be achieved
  - One important phase: Risk analysis
  - One important phase: Design
  - Integrating Risk analysis and Design?
- Privacy-by-design in Practice
- On-going standardisation

PRIPARE

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

Privacy-by-design?

Privacy-by-Design (PbD)?

- A possible definition
  - Institutionalisation of the concepts of privacy and security in organisations and integration of these concepts in the design of systems
  - See blog (http://www.securityengineeringforum.org/blog/show/id/27)

PRIPARE

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

Example

Electronic Tolling Systems (ETS)

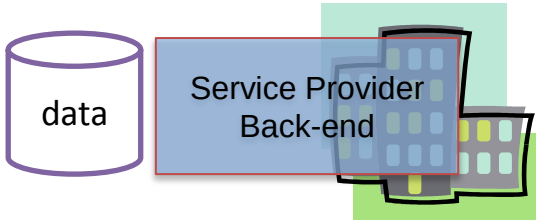
PrETP: Privacy-Preserving Electronic Toll Pricing J.Balasch. et al. 19th USENIX Security Symposium 2010

Description

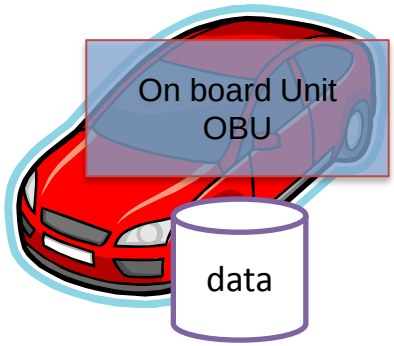
- User pays for using roads, depending on context
  - Type of road
  - Time/date
  - Traffic
  - Type of vehicle, …
- Public authority manages infrastructure using policies
  - Congestion
  - Energy
  - Big event (sports game…)

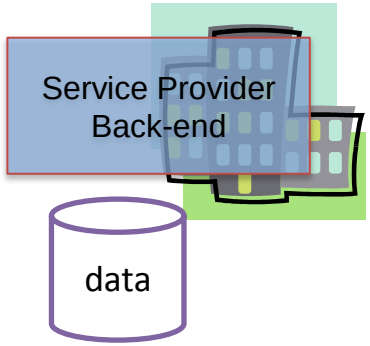
Approaches

- **Model A**: personal data and fees handled by SP backend



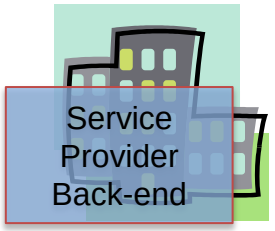
- **Model B**: fees handled by SP backend, personal data handled by OBU



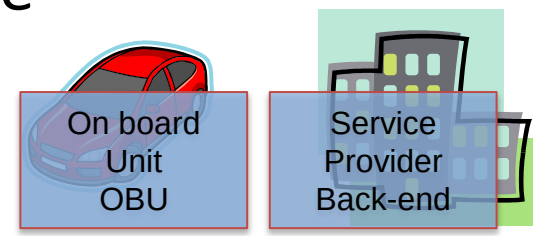


Comparison

- **Model A**: Data kept at SP level (millions of users)



- **Model B**: Data kept in vehicles (one user). Proofs sent to SP (zero-knowledge technology)



- Model B preserves privacy
- But different architectures…,
- Bur different interoperability requirements…

PRIPARE

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

One Important PbD Phase

Risk Management

Risk management

- Identification, assessment, and prioritization of risks
- A generic process
  - identify, characterize threats
  - assess the vulnerability of critical assets to specific threats
  - determine the risk (i.e. the expected likelihood and consequences of specific types of attacks on specific assets)
  - identify ways to reduce those risks
  - prioritize risk reduction measures based on a strategy

Security Risks: STRIDE cheat sheet

Property	Description	Threat
Authentication (authentification)	The identity of users is established (or you're willing to accept anonymous users).	**S**poofing (usurpation)
Integrity (intégrité)	Data and system resources are only changed in appropriate ways by appropriate people.	**T**ampering (altération)
Nonrepudiation (non répudiation)	Users can't perform an action and later deny performing it.	**R**epudiation (répudiation)
Confidentiality (confidentialité)	Data is only available to the people intended to access it.	**I**nformation disclosure (divulgation de l'information)
Availability (disponibilité)	Systems are ready when needed and perform acceptably.	**D**enial Of Service (déni de service)
Authorization (authorisation)	Users are explicitly allowed or denied access to resources.	**E**levation of privilege (élevation de privilège)

Privacy Risks: LINDDUN cheat sheet

Type	Property	Description	Threat
Hard privacy	Unlinkability	Hiding the link between two or more actions, identities, and pieces of information.	**L**inkability (possiblité de créer un lien)
	Anonymity	Hiding the link between an identity and an action or a piece of information	**I**dentifiability (possibilité d'identifier)
	Plausible deniability	Ability to deny having performed an action that other parties can neither confirm nor contradict	**N**on-repudiation (non répudiation)
	Undetectability and unobservability	Hiding the user's actvities	**D**etectability (possilbité de détecter)
Security	Confidentiality	Hiding the data content or controlled release of data content	**D**isclosure of information (divulgation d'information)
Soft Privacy	Content awareness	User's consciousness regarding his own data	**U**nawareness (méconnaissance)
	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 (non conformité)

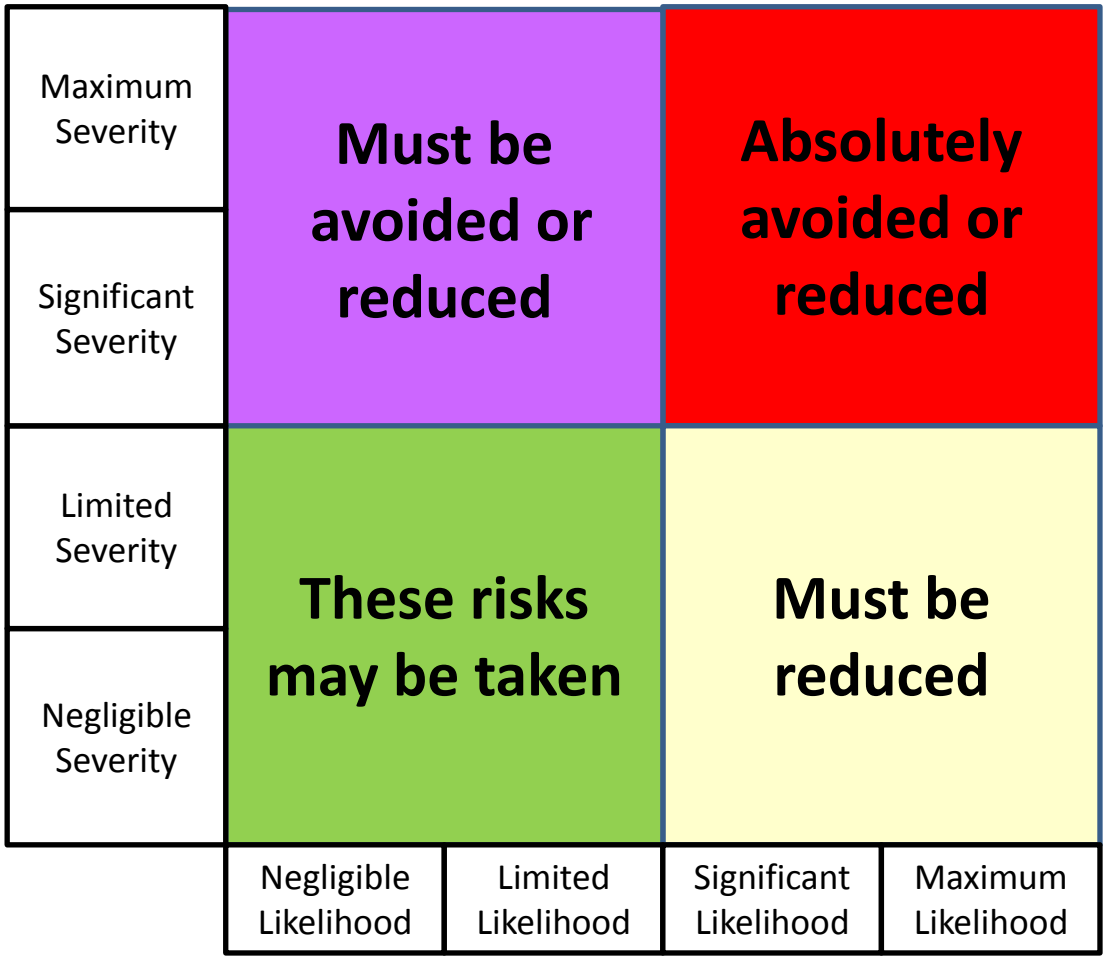
CNIL Privacy Risk Analysis

- French DPA

- Feared Events
- Threats

From CNIL methodology document

Risk = f(Severity, Likelihood)



PRIPARE

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

One Important PbD Phase

Design

OASIS PMRM (Privacy Management Reference Model): Services

	Service	Purpose
From OASIS PMRM	Agreement	Management of permissions and rules
	Usage	Controlling personal data usage
	Validation	Checking personal data
	Certification	Checking stakeholders credentials
	Enforcement	Monitor operations and react to exceptions
	Security	Safeguard privacy information and operations
	Interaction	Information presentation and communication
	Access	Data subject access to their personal data
From PRIPARE	Accountability	Log and audit management

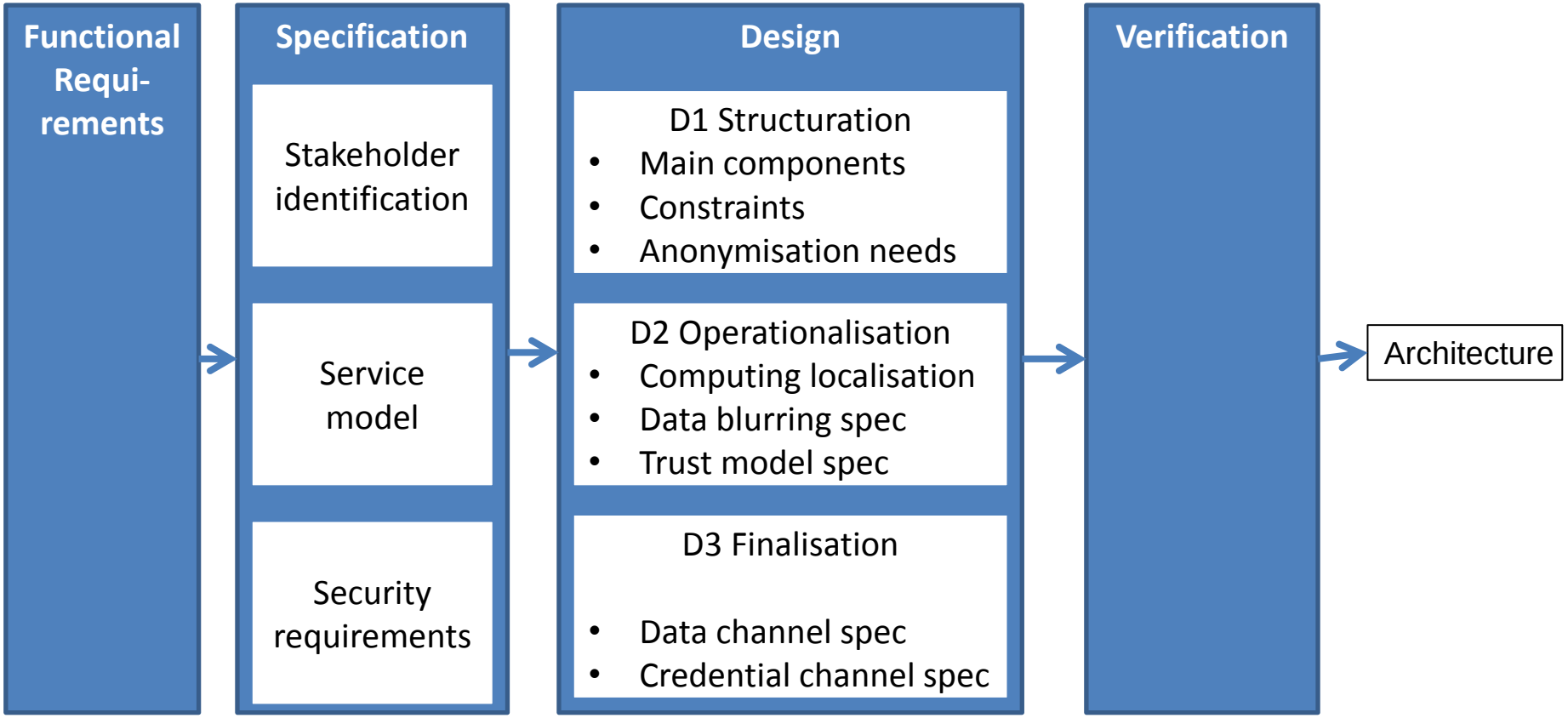
Kung: PEARs

Antonio Kung. PEARs: Privacy Enhancing ARchitectures. Annual Privacy Forum. Lecture Notes in Computer Science Volume 8450, 2014

Strategy		Tactics Examples
1 Minimization	Collection of personal information should be kept to a strict minimum	• Anonymize credentials (e.g. Direct anonymous attestation) • Limit processing perimeter (e.g. client processing, P2P processing)
2 Enforcement (application)	Provide maximum protection of personal data during operation	• Enforce data protection policies (collection, access and usage, collection, retention) • Protect processing (e.g. storage, communication, execution, resources)
3 Transparency and accountability (redevabilité)	Maximum transparency provided to stakeholders on the way privacy preservation is ensured	• Log data transaction • Log modifications (policies, crypto, protection) • Protect log data
4 Modifiability	Cope with evolution needs	• Change Policy • Change Crypto Strength and method • Change Protection Strength

Thibaud Antignac PhD Thesis

- Formal methods for Privacy-by-design. February 25th, 2015
  - Include a process proposal focusing on minimisation
  - Includes a formal verification framework proposal



Hoepman: Design Strategies

Jaap-Henk Hoepman. Privacy design strategies . In ICT Systems Security and Privacy Protection - 29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco

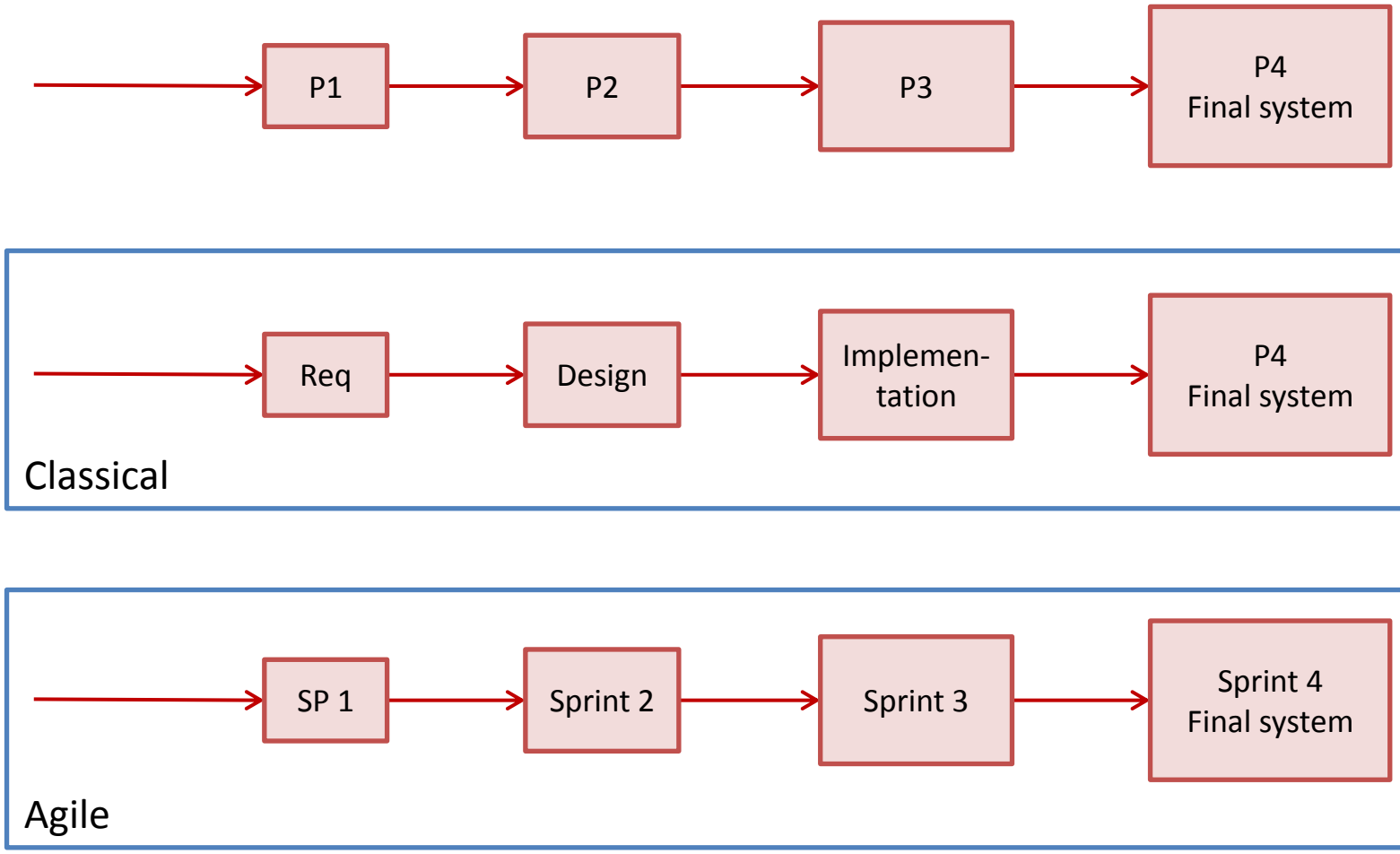
Strategy		Patterns Examples
1 Minimization	Amount of processed personal data restricted to the minimal amount possible	• select before you collect • anonymisation / pseudonyms
2 Hide	Personal data, and their interrelationships, hidden from plain view	• Storage and transit encryption of data • mix networks • hide traffic patterns • attribute based credentials • anonymisation / pseudonyms
3 Separate	Personal data processed in a distributed fashion, in separate compartments whenever possible	• Not known
4 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
5 Inform	Transparency	• platform for privacy preferrences • Data breach notification
6 Control	Data subjects provided agency over the processing of their personal data	• User centric identity management • End-to-end encryption support control
7 Enforce	Privacy policy compatible with legal requirements to be enforced	• Access control • Sticky policies and privacy rights management
8 Demonstrate	Demonstrate compliance with privacy policy and any applicable legal requirements	• privacy management systems • use of logging and auditing

PRIPARE

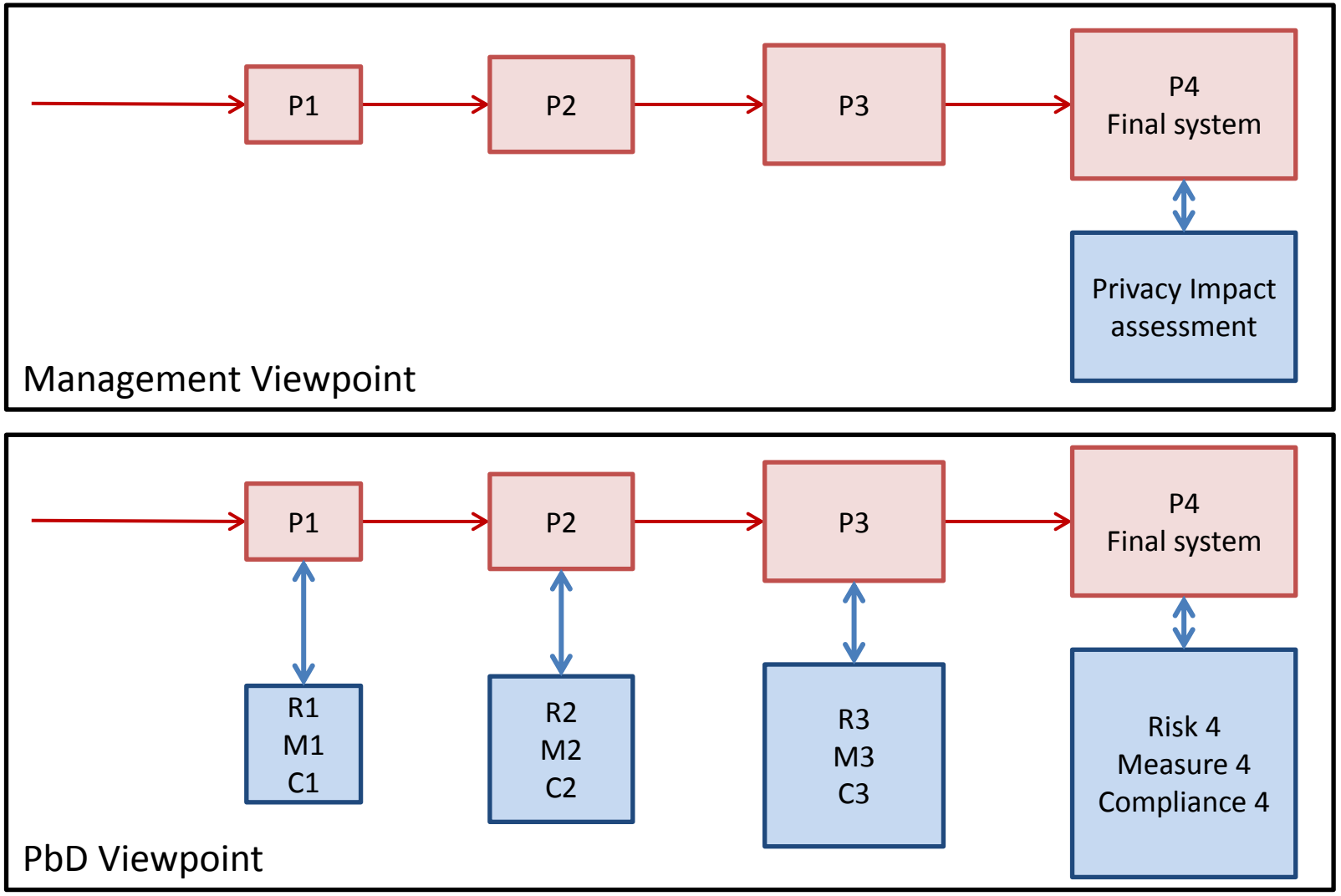
PReparing **I**ndustry to **P**rivacy-by-design by supporting its **A**pplication in **RE**search

Integrating Risk analysis and Design?

A Process Vision



Integration of Risk and Design in Process



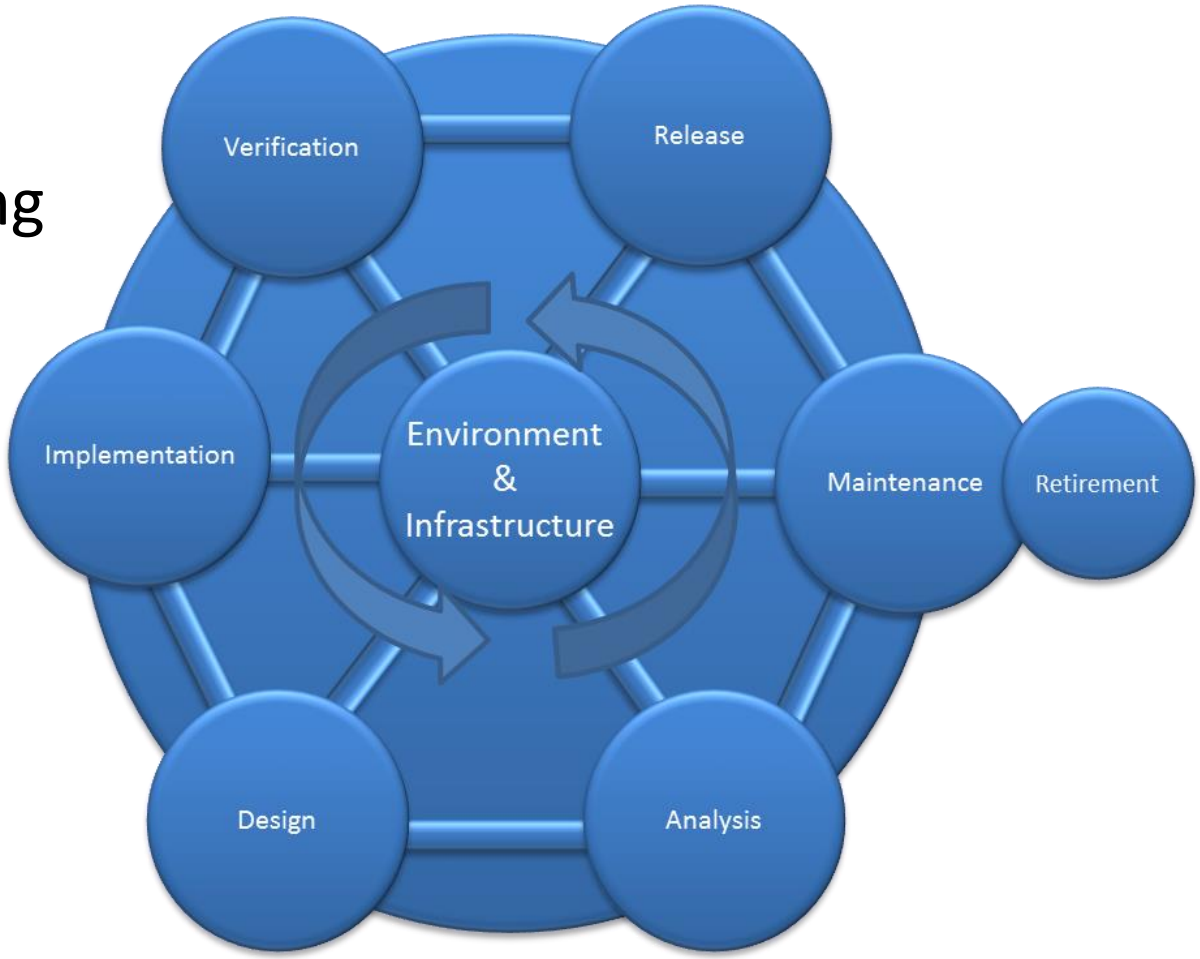
PRIPARE

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

Privacy-by-design in Practice?

PRIPARE PbD Methodology

- Covers entire life cycle
- Focuses on two privacy engineering activities
  - Privacy risk analysis
  - Design for privacy preservation
- Focuses on one privacy management activity
  - Compliance management



Practicing PbD

- Depends on type of system
  - Risk scale
  - Complexity scale
- Depends on type of development
  - Research (we must integrate PbD even at research level)
  - Innovation
  - Industry
- Depends on type of integration
- Depends on stakeholder viewpoint

Type of System

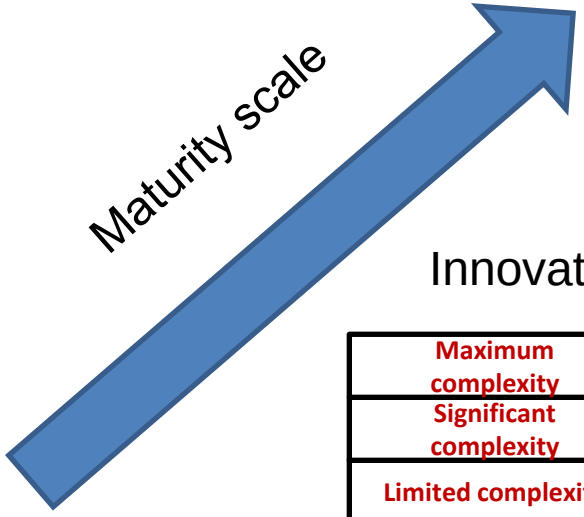
Figures are just examples

Maximum complexity	x2	x6	x11	x17
Significant complexity	x2	x5	x9	x13
Limited complexity	x1	x3	x6	x10
Simple	x1	x2	x4	x7
	Negligible risk	Limited risk	Significant Risk	Maximum Risk

Complexity scale

Risk scale

Type of Development



Deployment

Maximum complexity	x6	x18	x33	x51
Significant complexity	x6	x15	x27	x39
Limited complexity	x3	x9	x18	x30
Simple	x3	x6	x12	x21
	Negligible	Limited risk	Significant Risk	Maximum Risk

Innovation

Maximum complexity	x4	x12	x22	x34
Significant complexity	x4	x10	x18	x26
Limited complexity	x2	x6	x12	x20
Simple	x2	x4	x8	x14
	Negligible	Limited risk	Significant Risk	Maximum Risk

Research

Maximum complexity	x2	x6	x11	x17
Significant complexity	x2	x5	x9	x13
Limited complexity	x1	x3	x6	x10
Simple	x1	x2	x4	x7
	Negligible risk	Limited risk	Significant Risk	Maximum Risk

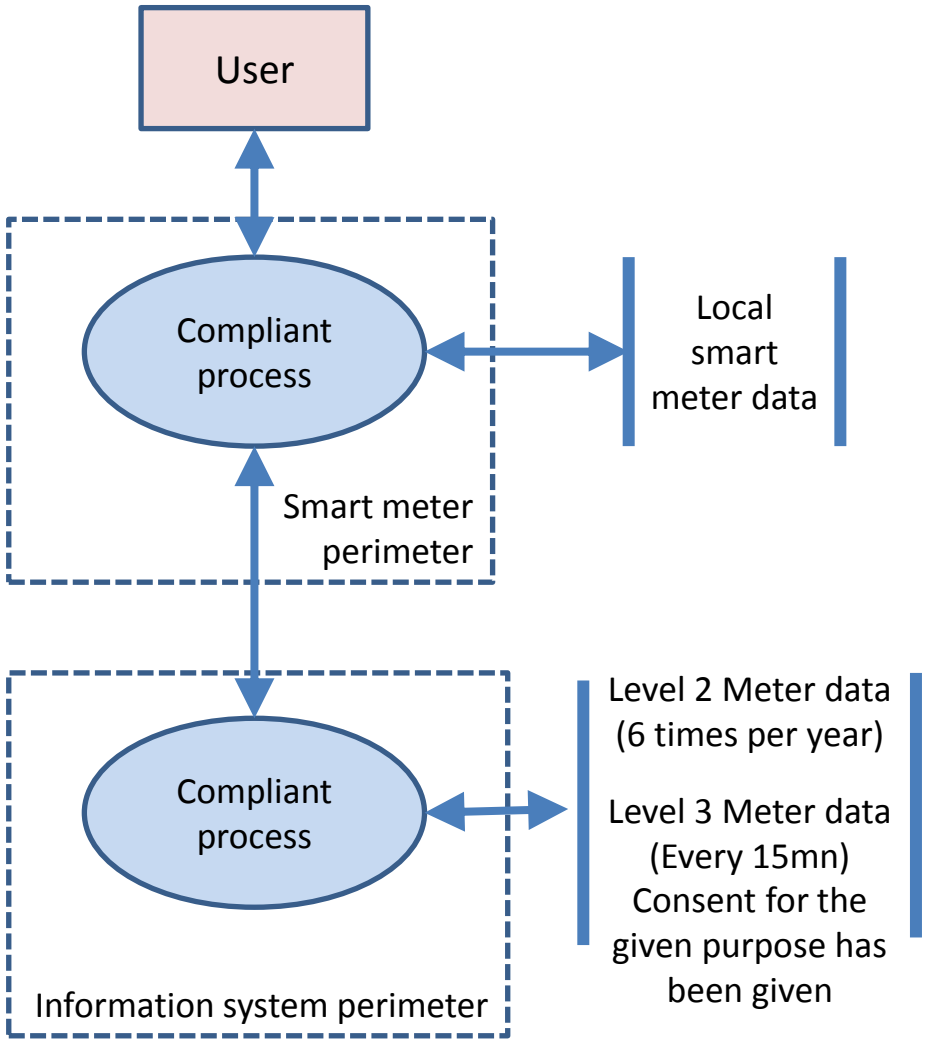
Integration / Stakeholder Viewpoint

- Integration
  - Platform vs Application
  - System vs subsystem
- The stakeholder viewpoint
  - Citizen / Corporate
  - Manager / Designer / Lawyer / Ethicist

Smart Grid Example

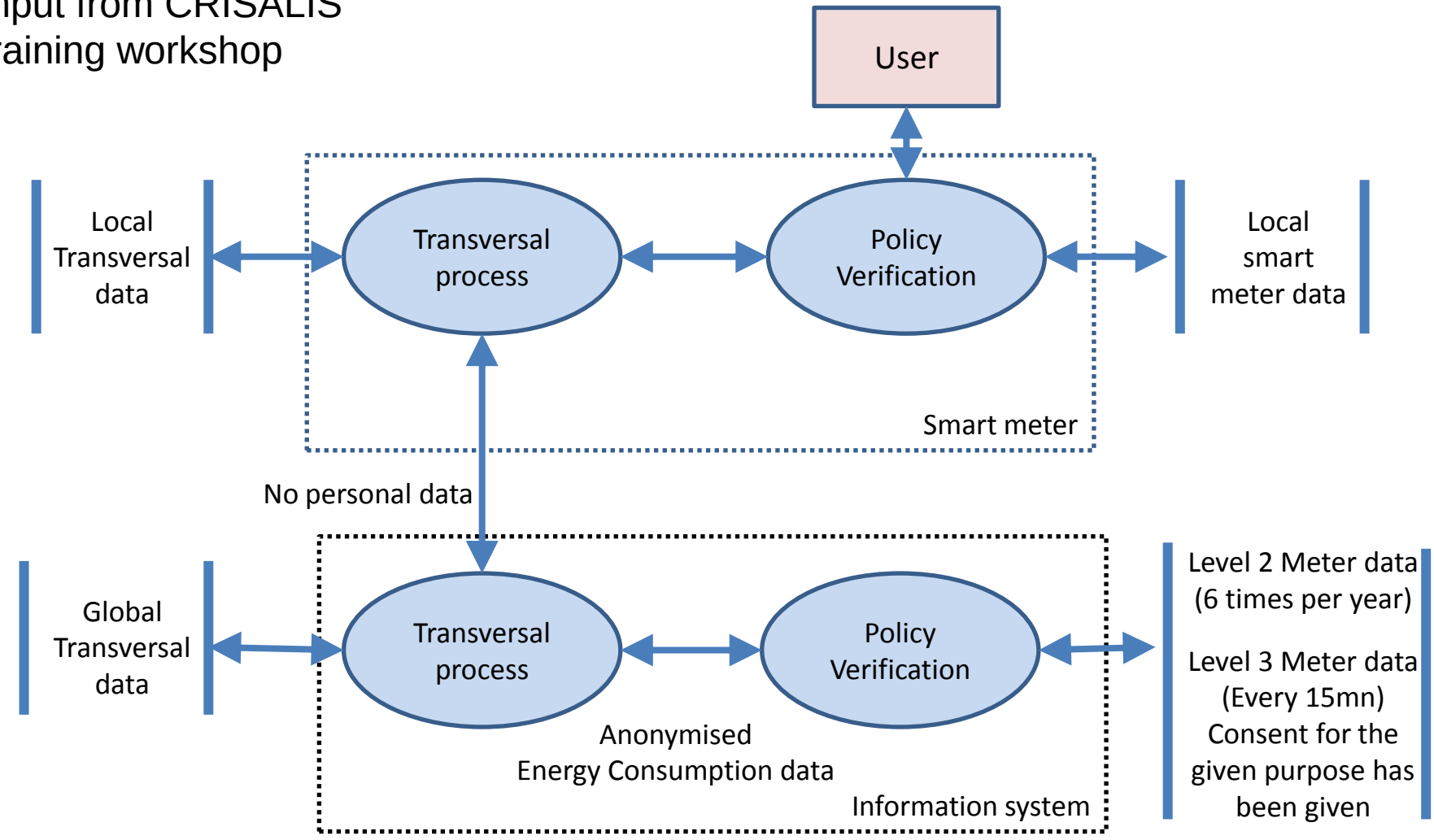
Input from
CRISALIS
FP7 Project
training workshop

Based on
Netherlands
Regulation



Transversal System PbD in Smart Grid

Input from CRISALIS training workshop



Impact on PbD Practice

- In the case of a nominal case that is well understood (e.g. smart meter)
- PbD process for additional transversal features must follow an incremental PbD process where the constraints and properties resulting from the nominal case must be preserved

PRIPARE

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

Existing initiatives/standards

Platforms and Standards

- Platforms
  - NIST Privacy engineering workshops
  - IPEN: Internet Privacy Engineering Network
    - Workshop Leuven. June 5th 2015.
- Standards
  - OASIS
    - PMRM Privacy Management Reference Model
    - PbD-SE Privacy-by-design for software engineers
  - ISO/IEC SC27/WG5
    - 29100 Privacy framework
    - 29134 Privacy impact assessment
    - 29151 Code of practice for personally identifiable information
    - …
  - JWG8 CEN/CENELEC: PbD for security products

PRIPARE

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

Thanks

Antonio Kung. Trialog. Antonio.kung@trialog.com
www.trialog.com