Standards and privacy engineering – ISO, OASIS, PRIPARE and Other Important Developments

Antonio Kung, CTO

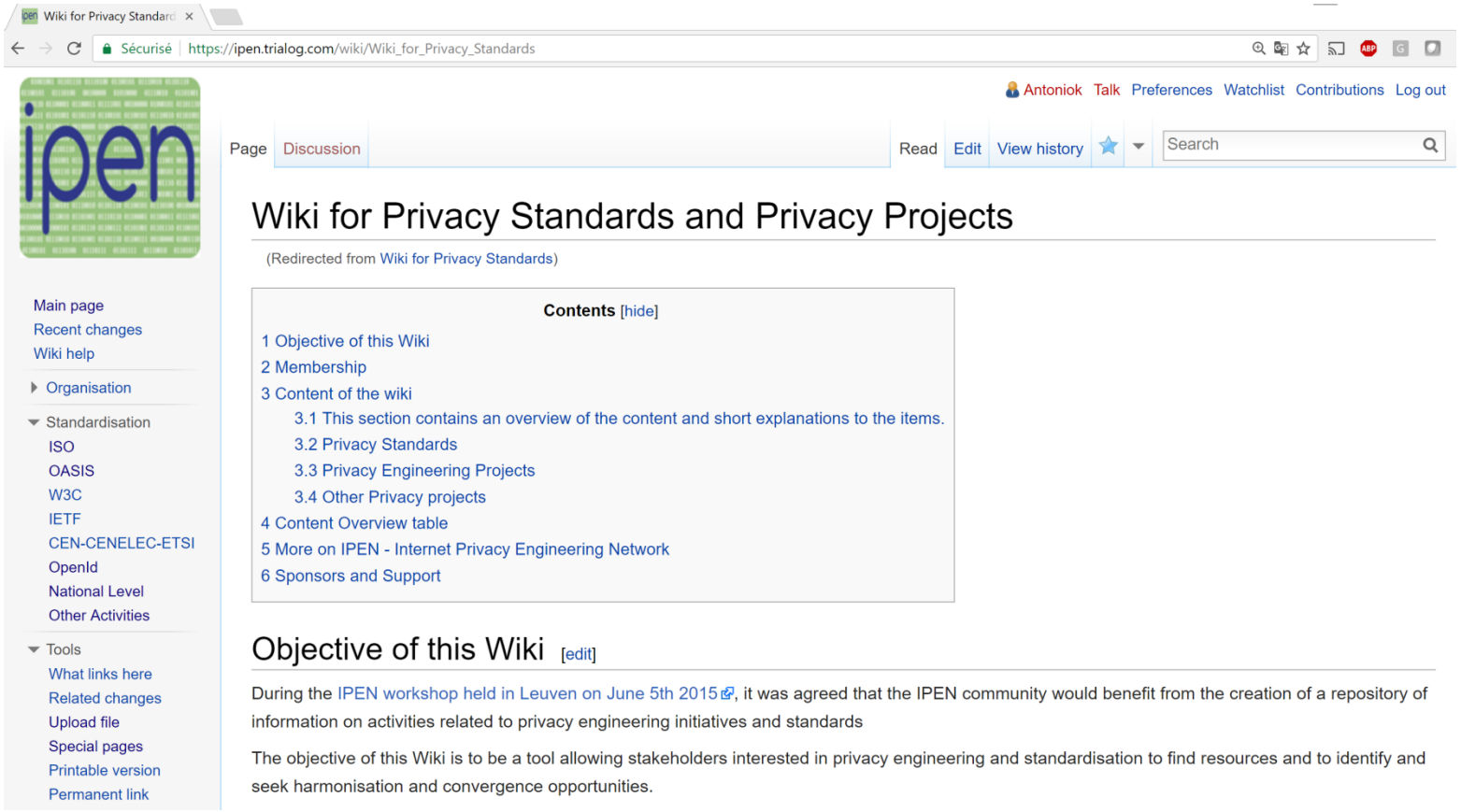
25 rue du Général Foy, 75008 Paris

www.trialog.com

Introduction Speaker

- Engineering background
- Involved in standardisation
  - Privacy engineering (ISO 27550)
  - Big data – Security and privacy fabric (ISO 20547-4)
  - Privacy in smart cities (Study period)
  - Privacy guidelines in the IoT (Study period)
  - OASIS
- Others
  - European Innovation Platform – Smart Cities and Communities
    - Citizen approach to data: privacy-by-design
  - Coordinator PRIPARE
    - pripareproject.eu
    - Methodological Tools to Implement Privacy and Foster Compliance with the GDPR

IPEN member (ipen.trialog.com)



Trialog

- Trialog focuses on innovation since 1987
- Security (since 2000)
  - Connected vehicles
- Privacy (depuis 2007)
  - Intelligent transport system (Sevecom, Preciosa)
  - Pripare
  - Create-IoT

Member

OASIS
Advancing open standards for the information society

PRIPARE

Liaison

ISO

CREATE-IoT

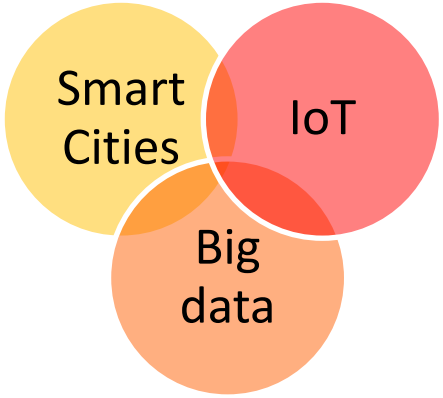
Outline

- Privacy from a policy maker viewpoint
- Overview of standards
- Security and privacy for the IoT
- 27550 Privacy engineering

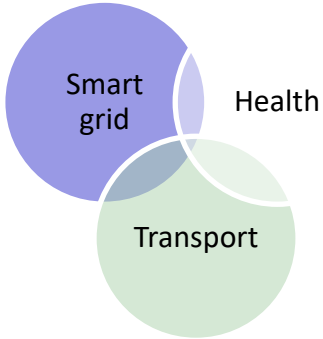
Privacy from a Policy Maker Viewpoint

Example of smart cities

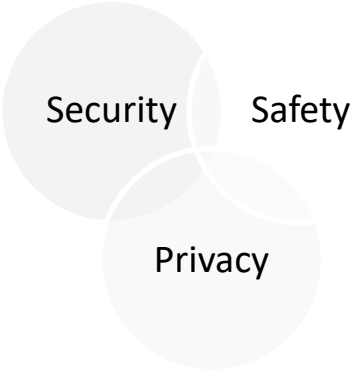
Deals with Complex Ecosystems



Ecosystems



Domains



Concerns

Must take into account

- General Data Protection Regulation (GDPR)
- May 25th 2018

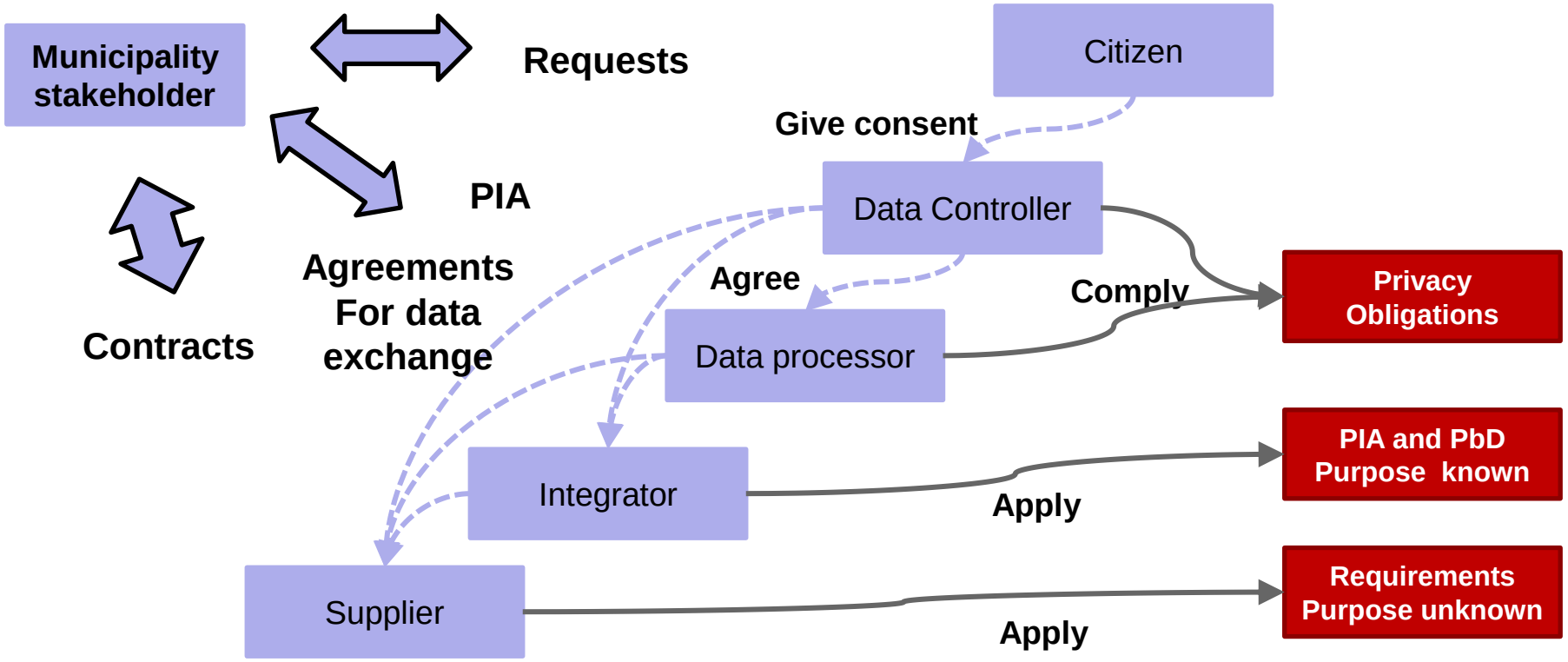
- Data controllers
- Data processors
- Data Protection Officers
  - All public authorities
  - Companies processing a large number of data subjects e.g. 5000
- Sanctions for breaches
  - up to 20,000,000 EUR
  - up to 4% of the annual worldwide turnover

Must understand these terms

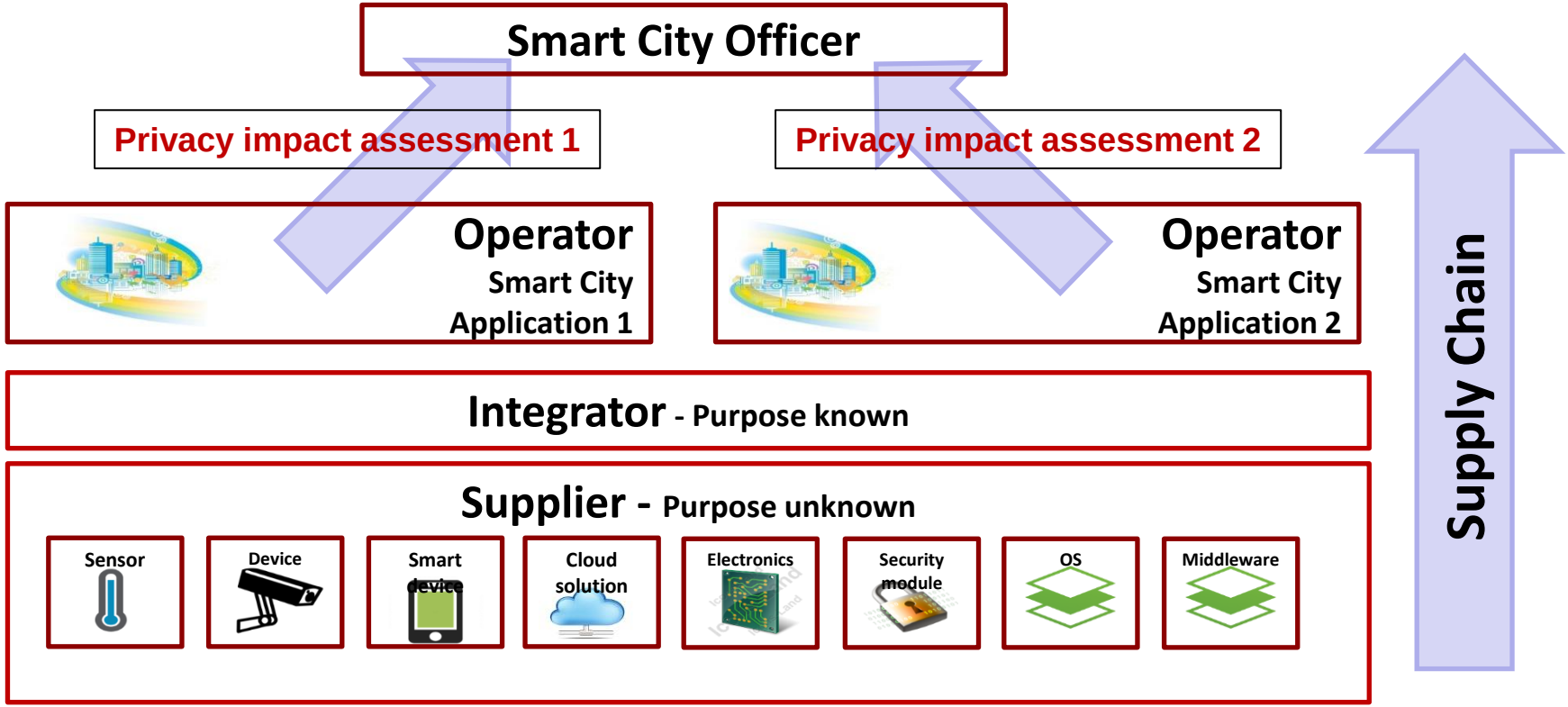
- Privacy-by-design: PbD
  - Institutionalisation of privacy management
  - Integration of privacy concern in the engineering of systems
- Privacy-by-default
  - Highest level of protection by default
- Privacy Impact assessment: PIA
  - Process that evaluates impact on privacy

- Note that the GDPR uses the term “data protection” instead of “privacy”

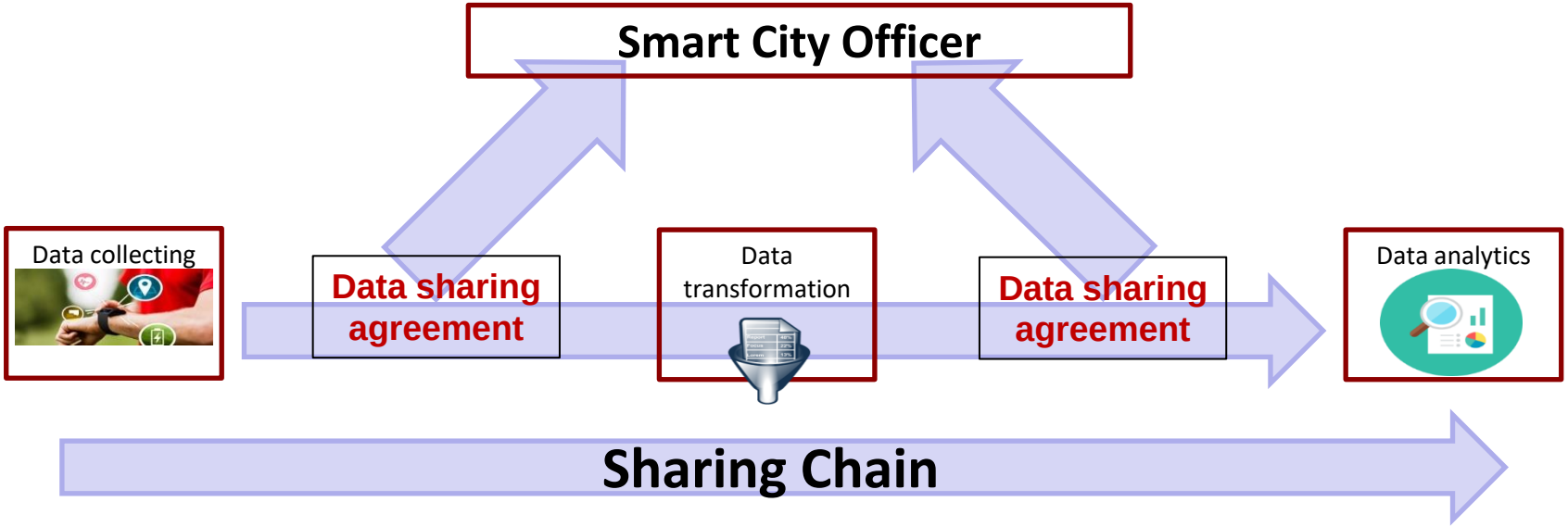
Must Manage Privacy in Complex Ecosystem



IoT Vision: Supply Chain



Big Data Vision : Sharing Chain



Several Types of Concerns

Stakeholder		Legal Compliance Concern	Management Concern	System Lifecycle Concern
Demand side	Policy maker 	**Compliance Check / Follow standards** **Transparency**		
	**Operator** Data Controller 	Regulation **GPDR**	Privacy Impact Assessment **PIA**	Privacy-by-Design **PbD**
	Operator Data processor 		Sharing Agreement	
Supply side	**Supplier** 	**Operators Requirements**		

Guidelines for GDPR Compliance

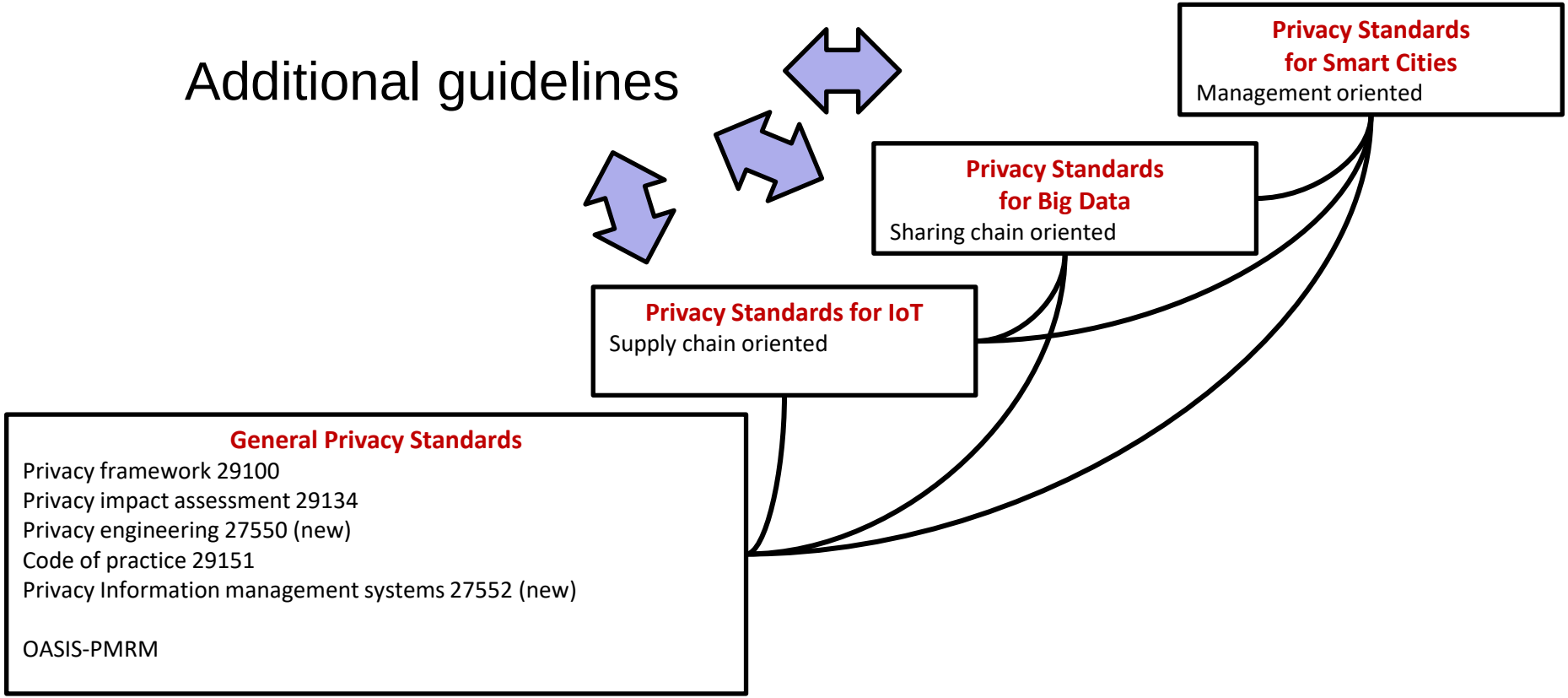
- Sharing cities project
  - H2020 (http://www.sharingcities.eu)
  - London, Milan, Lisbon, Bordeaux, Burgas, Warsaw
- Program on GDPR compliance
  - March 2017 – Workshop on use cases
  - June 2017 – Workshop on PIAs
  - Further – Applying a management plan for GDPR compliance

Proposed content

- Privacy management plan
  - Governance scheme
  - Roles and duties
    - Data controllers
    - Data processors
    - Suppliers
  - Resources and staff
- Management
  - Repository of PIAs and data sharing agreements
  - Interaction with citizens
    - Transparency (dashboard)
    - Complaints
  - Breach management
  - Continuous improvement
- Templates
  - PIA template
  - Data sharing agreement template
  - Privacy notice template
  - Supplier privacy support description template

Overview of Standards

Possible Landscape (Author Vision)



ISO/IEC Standards

- 29100 Privacy framework
- 29134 Privacy impact assessment
- 29151 Code of practice for PII protection

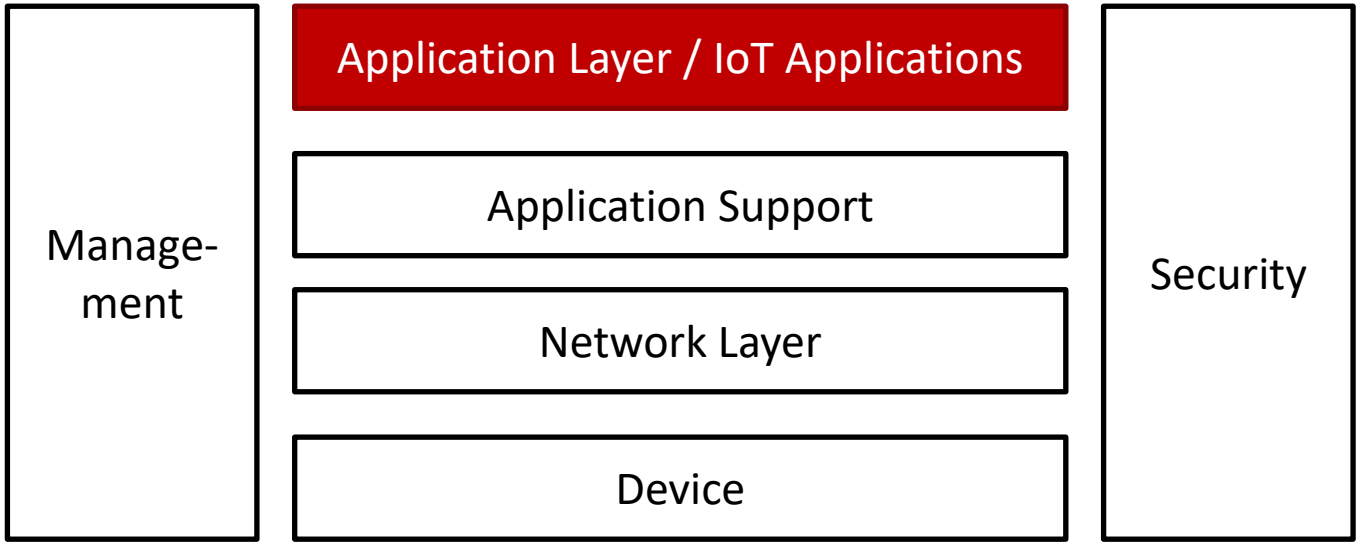
- 27550 Privacy Engineering
- 27551 Requirements for attribute-based unlinkable entity authentication
- 27552 Privacy management – requirements

- 20547-4 Big data reference architecture: Security and privacy fabric
- ISO Study period
  - Privacy in smart cities
  - Privacy guidelines in the IoT

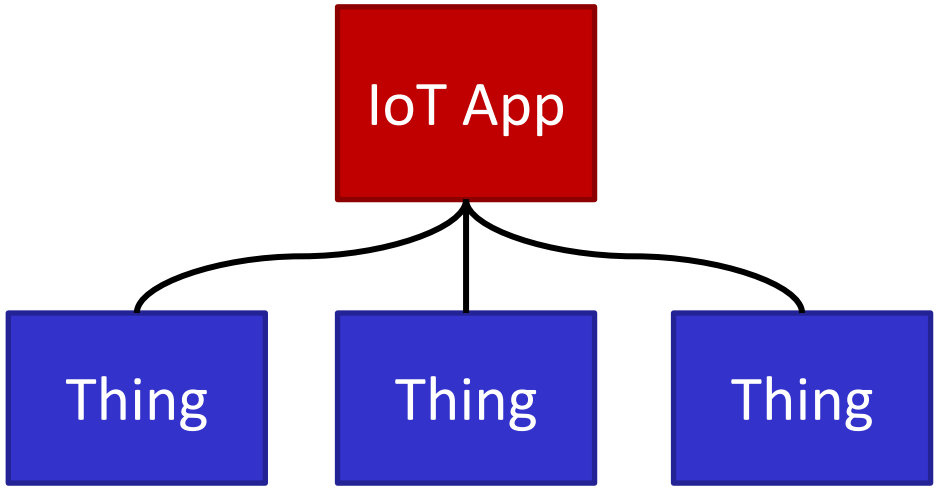
Security and privacy for the IoT

Study period

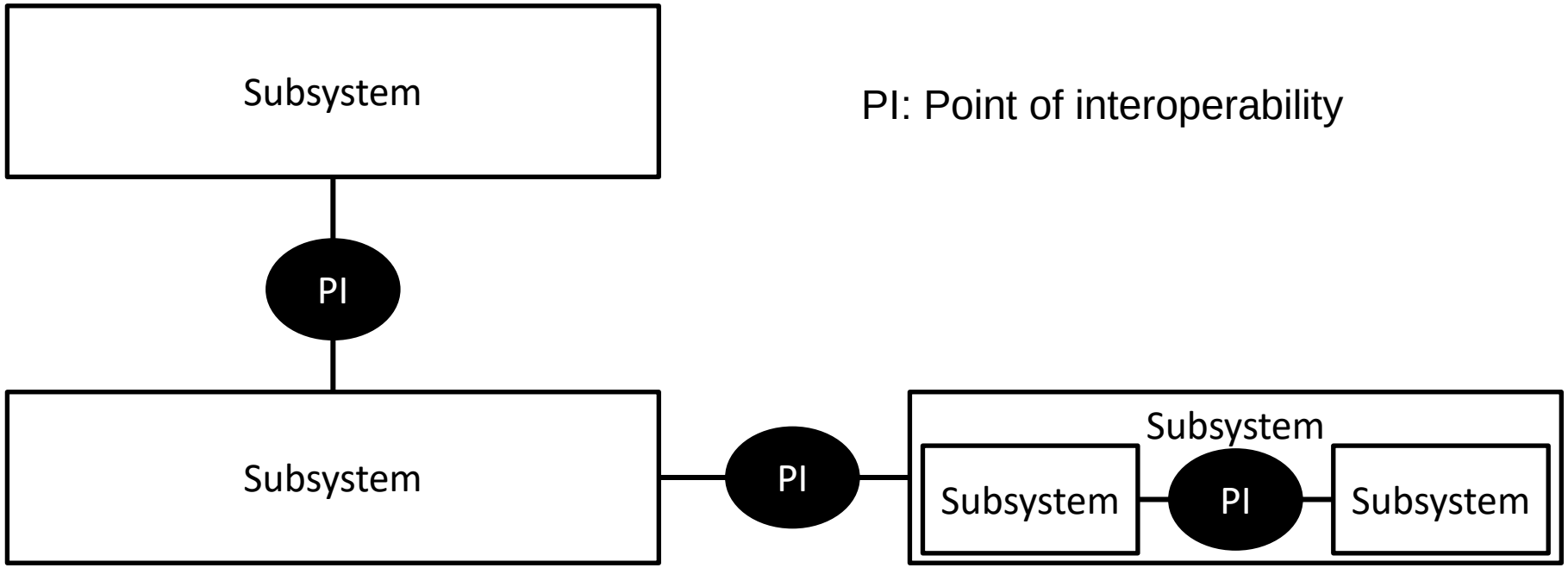
IoT Architectural Viewpoint



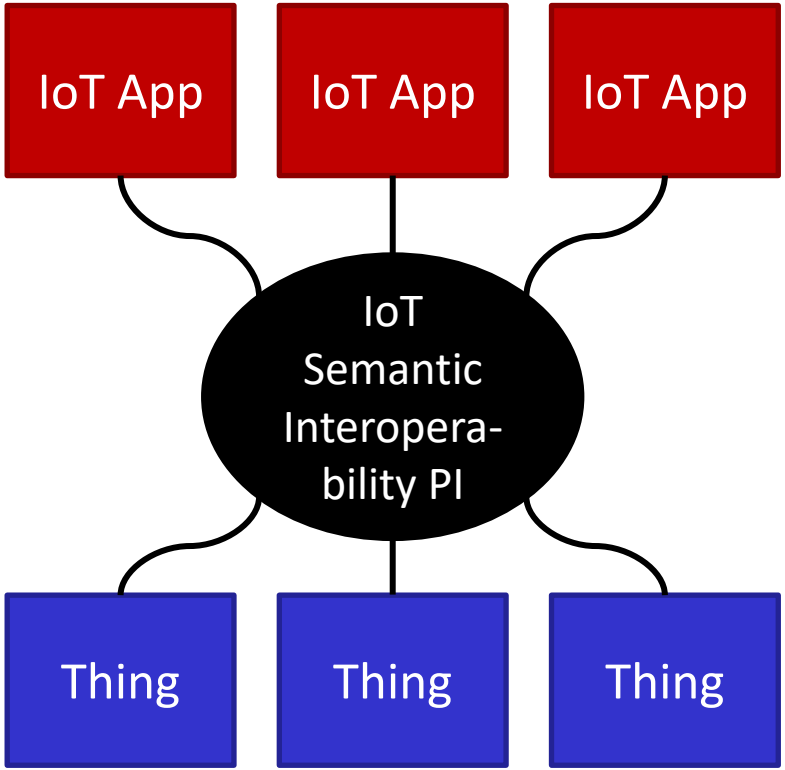
IoT Abstract Viewpoint



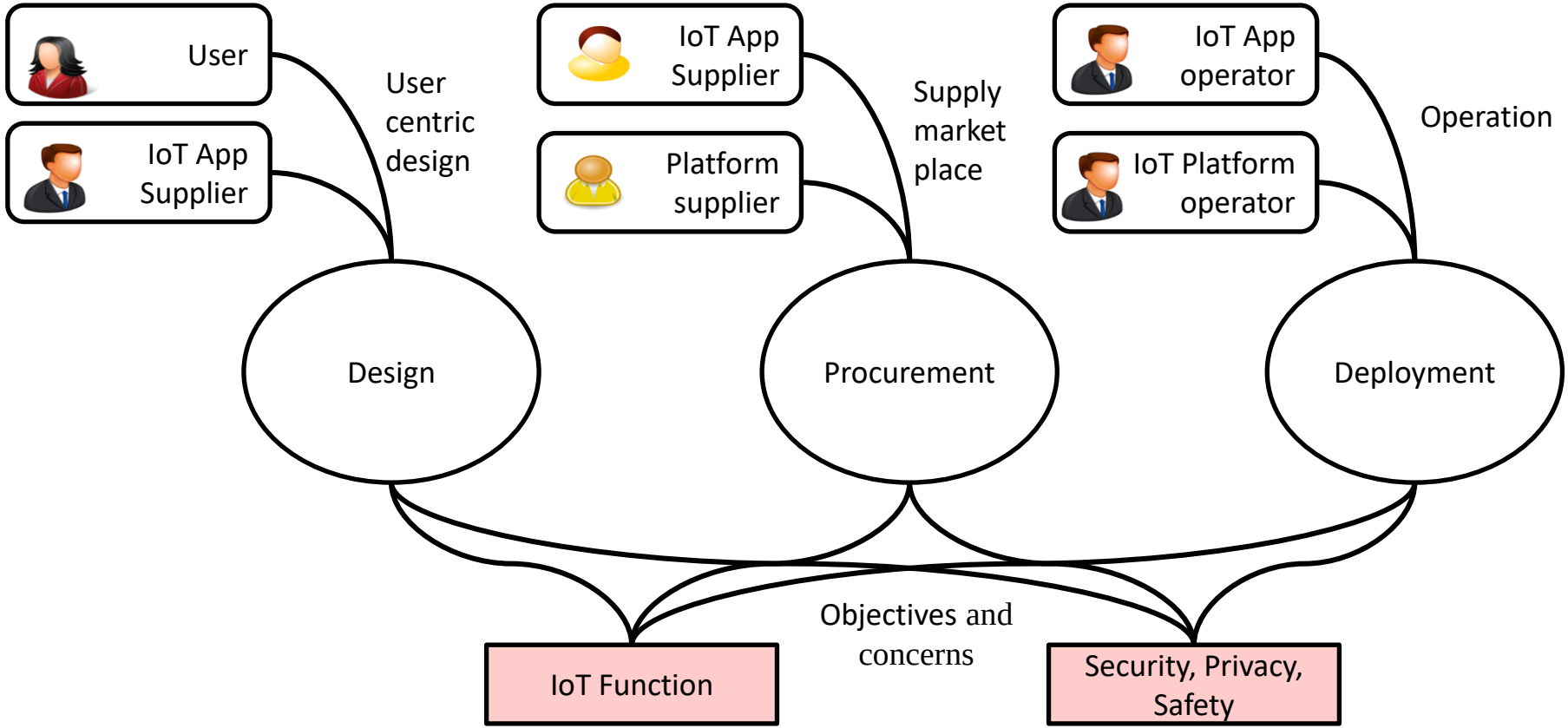
Interoperability Viewpoint



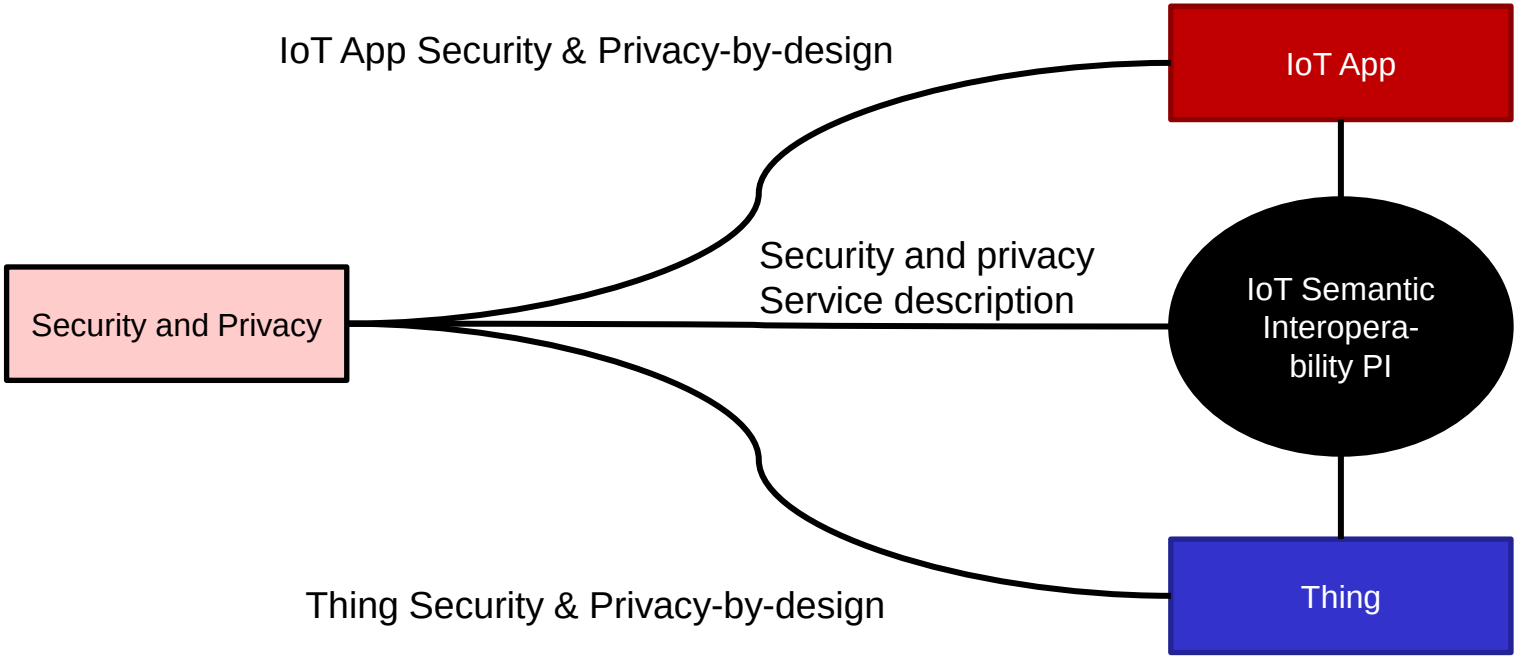
IoT Semantic Interoperability Viewpoint



IoT Systems Stakeholders

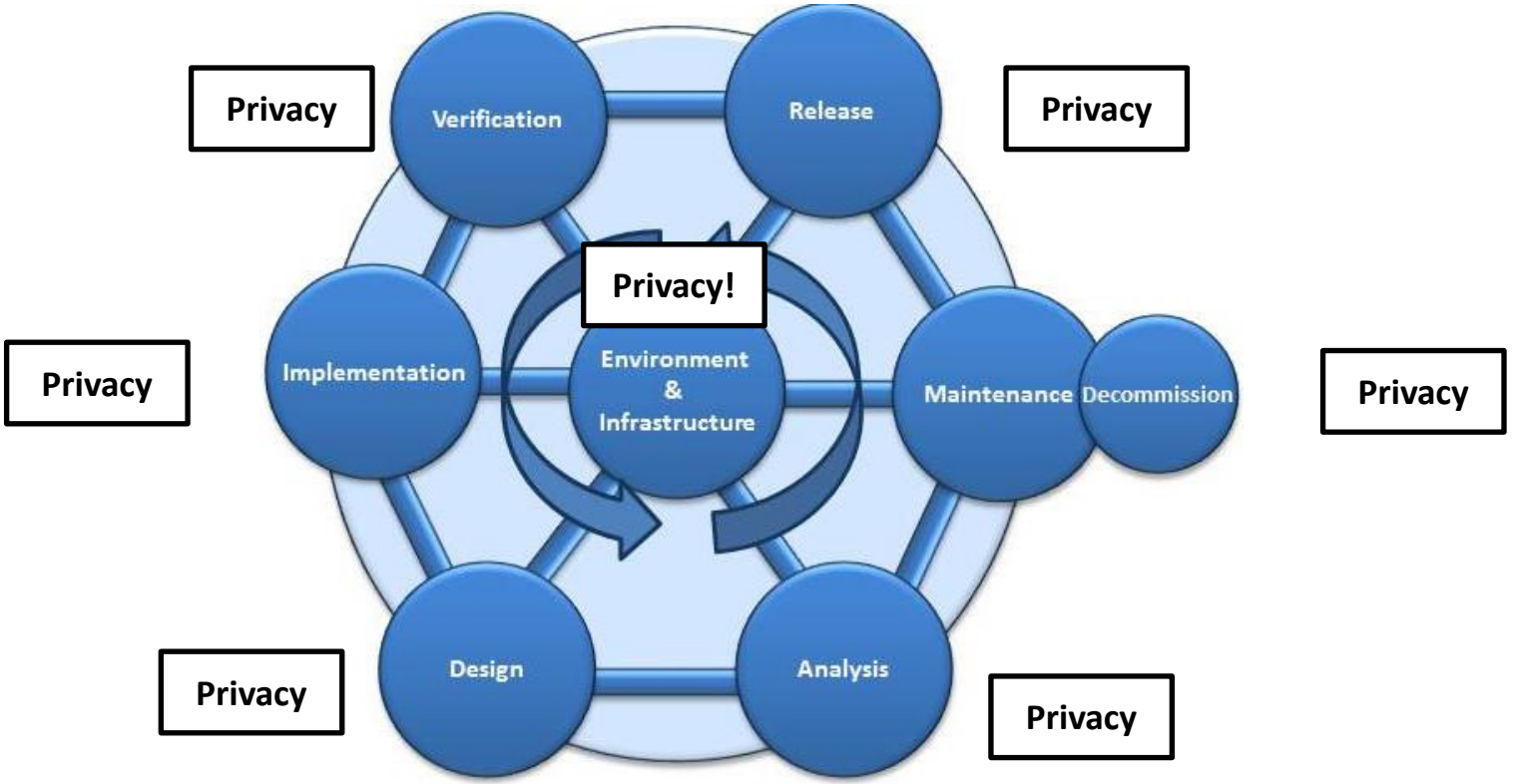


IoT Security and privacy from an Interoperability Viewpoint



27550 Privacy Engineering

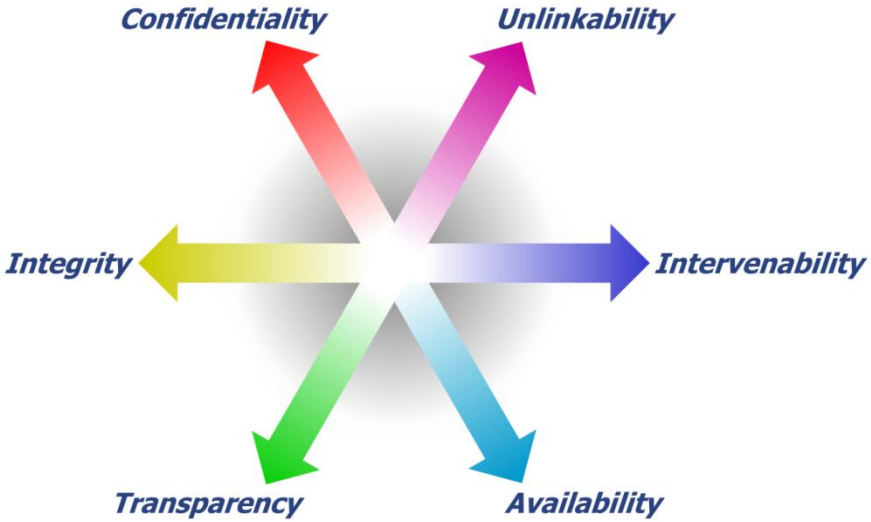
Privacy Engineering: Integrating privacy concerns



Beyond CIA

- Confidentiality
- Integrity
- Availability

- Unlinkability
- Intervenability
- Transparency

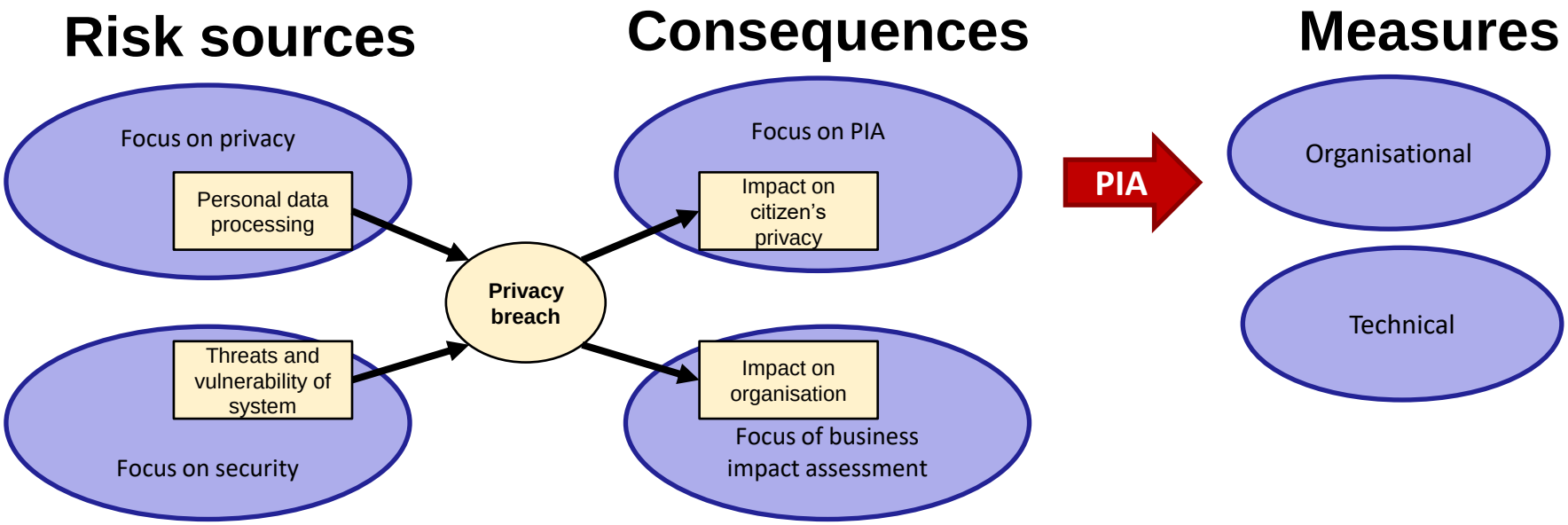


From ULD: ieee-security.org/TC/SPW2015/IWPE/2.pdf

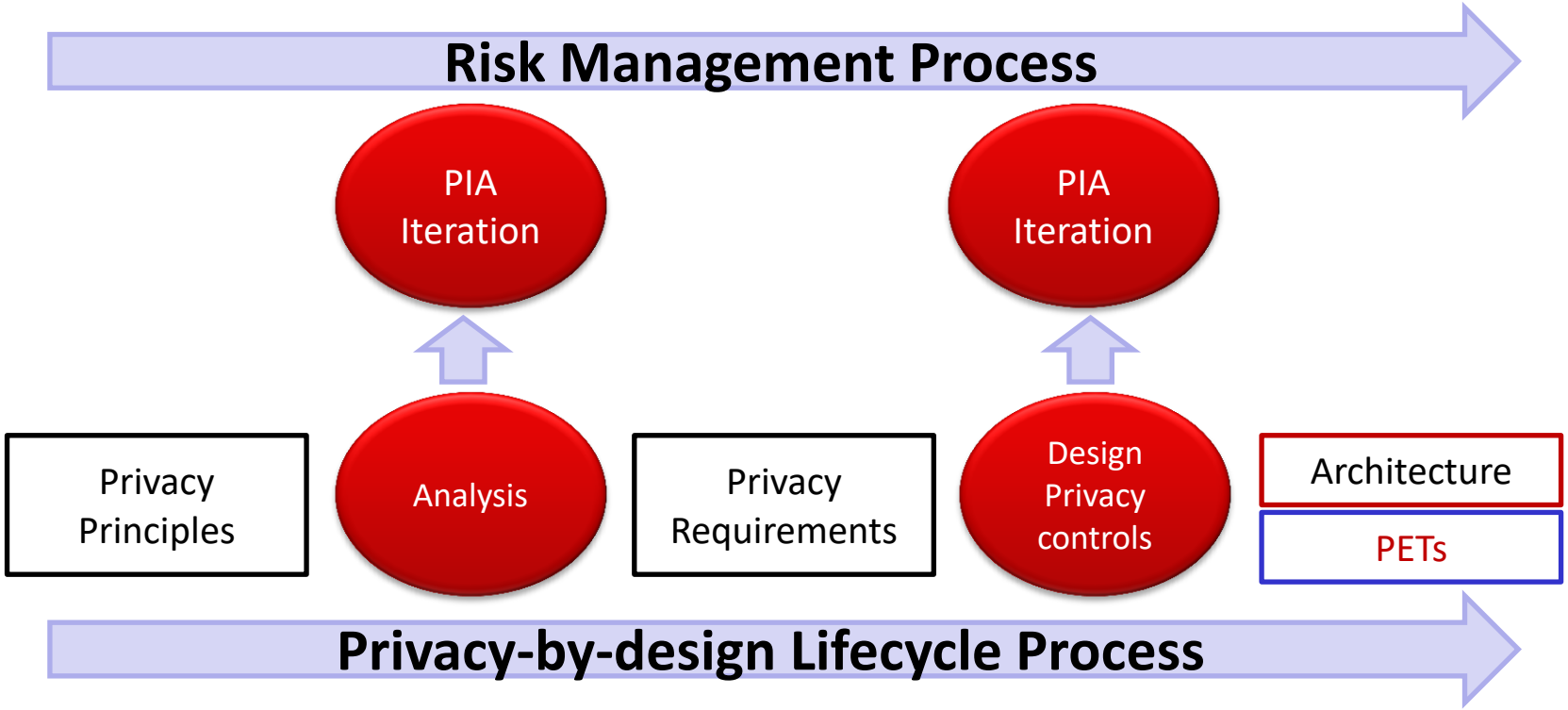
ISO 15288 System Life Cycle Processes

- Agreement
  - Acquisition
  - Supply
- Organisational project-enabling
  - Life cycle model management
  - Infrastructure management
  - Portfolio management
  - Human resource management
  - Quality management
  - Knowledge management
- Technical management
  - Project planning
  - Project assessment and control
  - Decision management
  - Risk management
  - Configuration management
  - Information management
  - Measurement
  - Quality assurance
- Technical
  - Business or mission analysis
  - Stakeholder needs and requirements definition
  - System requirements definition
  - Architecture definition
  - Design definition
  - System analysis
  - Implementation
  - Integration
  - Verification
  - Transition
  - Validation
  - Operation
  - Maintenance
  - Disposal

Privacy Impact Assessment



Privacy-by-design



From Principles to Services: OASIS-PMRM

Service		Purpose
Core policy services	Agreement	Manage and negotiate permissions and rules
	Usage	Control PII use
Privacy assurance services	Validation	Ensures PII quality
	Credential certification	Ensure appropriate management of credentials
	Enforcement	Monitor proper operation, respond to exception conditions and report on demand evidence of compliance where required for accountability
	Security	Safeguard privacy information and operations
Presentation and lifecycle services	Interaction	Information presentation and communication
	Access	View and propose changes to stored PII

From security properties to security threats: STRIDE

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

From privacy properties to privacy threats: LINDDUN

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 actvities	**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

https://distrinet.cs.kuleuven.be/software/linddun/catalog.php

ISO 27550 Privacy Engineering (2nd Working Draft)

- Privacy engineering
  - Security and privacy
  - System engineering
  - Risk management
- Privacy engineering processes
  - Negotiation
    - Acquisition
    - Supply
  - Organisation
    - Competence management
    - Knowledge management
  - Technical management
    - Risk management
  - Cycle
    - Stakeholders' privacy expectation
    - Privacy principle operationalisation
    - Privacy engineering architecture
    - Privacy engineering design
- Annex A Specific guidelines
  - Supporting Domains
  - Supporting agile programming
  - Supporting small organisations
- Annex B Objectives to identify capabilities
  - Privacy engineering objectives
  - Privacy protections goals
- Annex C Cheat sheets
- Annex D Risk models
  - NIST, CNIL
- Annex E Methodologies
  - PMRM
  - LINDDUN
  - PRIPARE

Conclusion

- ISO/IEC 27550 Privacy engineering
  - Provides a system life cycle process vision
  - Integrates current body of knowledge
  - Will evolve
- Standards and guidelines
  - Still in the making
  - There is now a core of common standards
  - Could be complemented by specific privacy guidelines
    - Management oriented for smart cities
    - Supply chain oriented for IoT
    - Sharing chain oriented for big data

www.trialog.com

Questions?