PDP4E

Methods and Tools for GDPR Compliance through

Privacy and Data Protection 4 Engineering

Management of Privacy in Cooperative ITS

Antonio Kung

Trialog, 25 rue du Général Foy 75008 Paris

antonio.kung@trialog.com

Outline

❑Speaker

❑Policy maker viewpoint on privacy

❑ISO 27550 privacy engineering

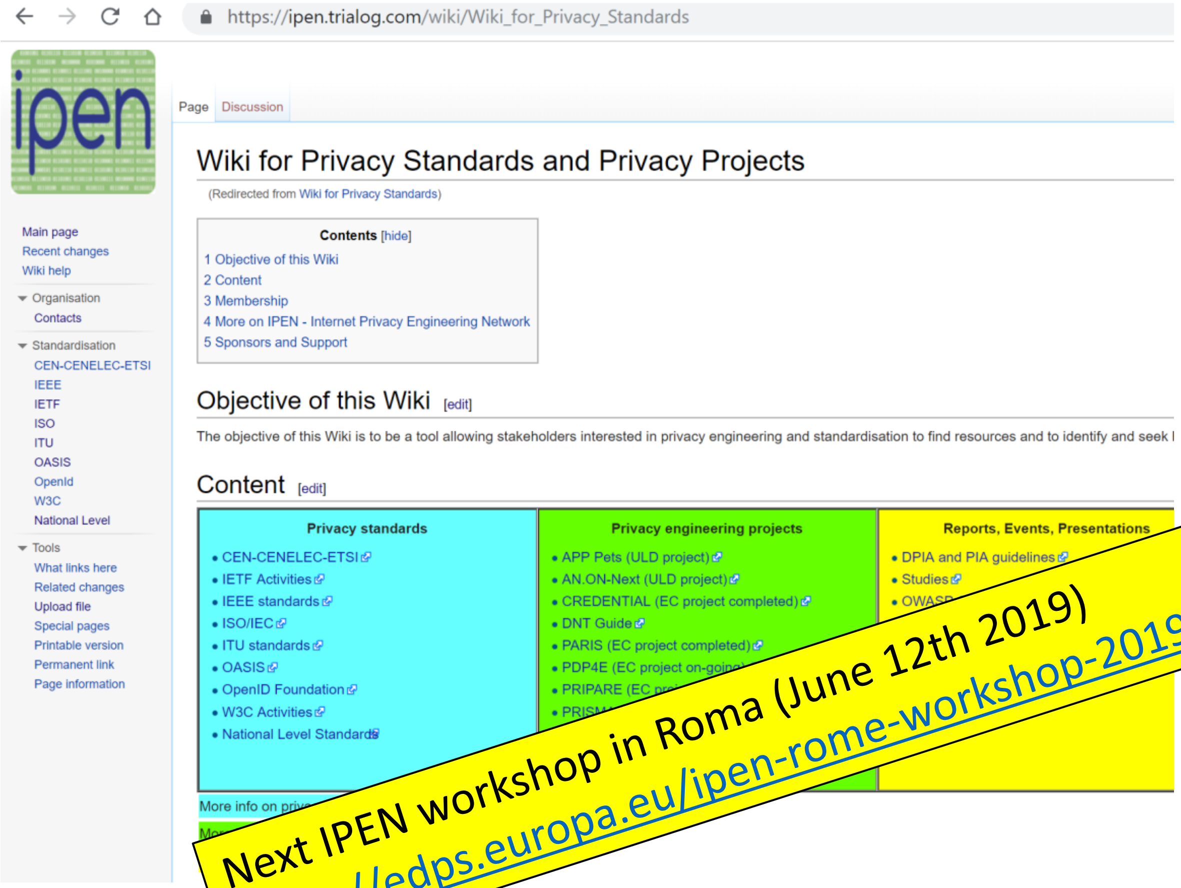
❑Privacy management in C-ITS

❑Recommandations

Speaker

- Engineering background
- Work related to C-ITS
  - FP6 SEVECOM (2006-2008)
    - EDPS opinion on eCall
    - Specification of pseudonym mechanism
  - FP7 PRECIOSA (2008-2010)
    - Privacy-by-design for ITS
  - FP7 Preserve (2011-2015)
    - Field operational test
  - SystemX ISE (2014-2017) and SystemX SCA (2018-2020)
    - Cybersecurity and misbehaviour detection
  - Consulting PFA
    - DPIA CAM message system
    - ISO 21434 Automotive cybersecurity engineeing
- Work related to privacy
  - FP7 PRIPARE (2013-2015)
    - Methodology
    - Liaison with ISO/IEC JTC1/SC27/WG5
    - Member of OASIS
  - H2020 PDP4E (2018-2020) - MDE
    - **C-ITS use case**
    - Smart grid big data use case
- Active participation in privacy standards
  - ISO 31000 – Privacy by design
  - ISO/IEC 20547-4 – Big data
  - ISO/IEC 27030 - IoT
  - ISO/IEC 27550 – Engineering
  - ISO/IEC 27556 – Preference management
  - ISO/IEC 27570 – Smart cities
- ISO study on impact of AI on privacy
  - Participation possible through the PRIPARE liaison
    - Antonio.kung@trialog.com

IPEN Member (ipen.trialog.com)



https://ipen.trialog.com/wiki/Wiki_for_Privacy_Standards

Main page
Recent changes
Wiki help

Organisation
- Contacts

Standardisation
- CEN-CENELEC-ETSI
- IEEE
- IETF
- ISO
- ITU
- OASIS
- OpenId
- W3C
- National Level

Tools
- What links here
- Related changes
- Upload file
- Special pages
- Printable version
- Permanent link
- Page information

Wiki for Privacy Standards and Privacy Projects

(Redirected from Wiki for Privacy Standards)

Contents [hide]

1 Objective of this Wiki
2 Content
3 Membership
4 More on IPEN - Internet Privacy Engineering Network
5 Sponsors and Support

Objective of this Wiki [edit]

The objective of this Wiki is to be a tool allowing stakeholders interested in privacy engineering and standardisation to find resources and to identify and seek l

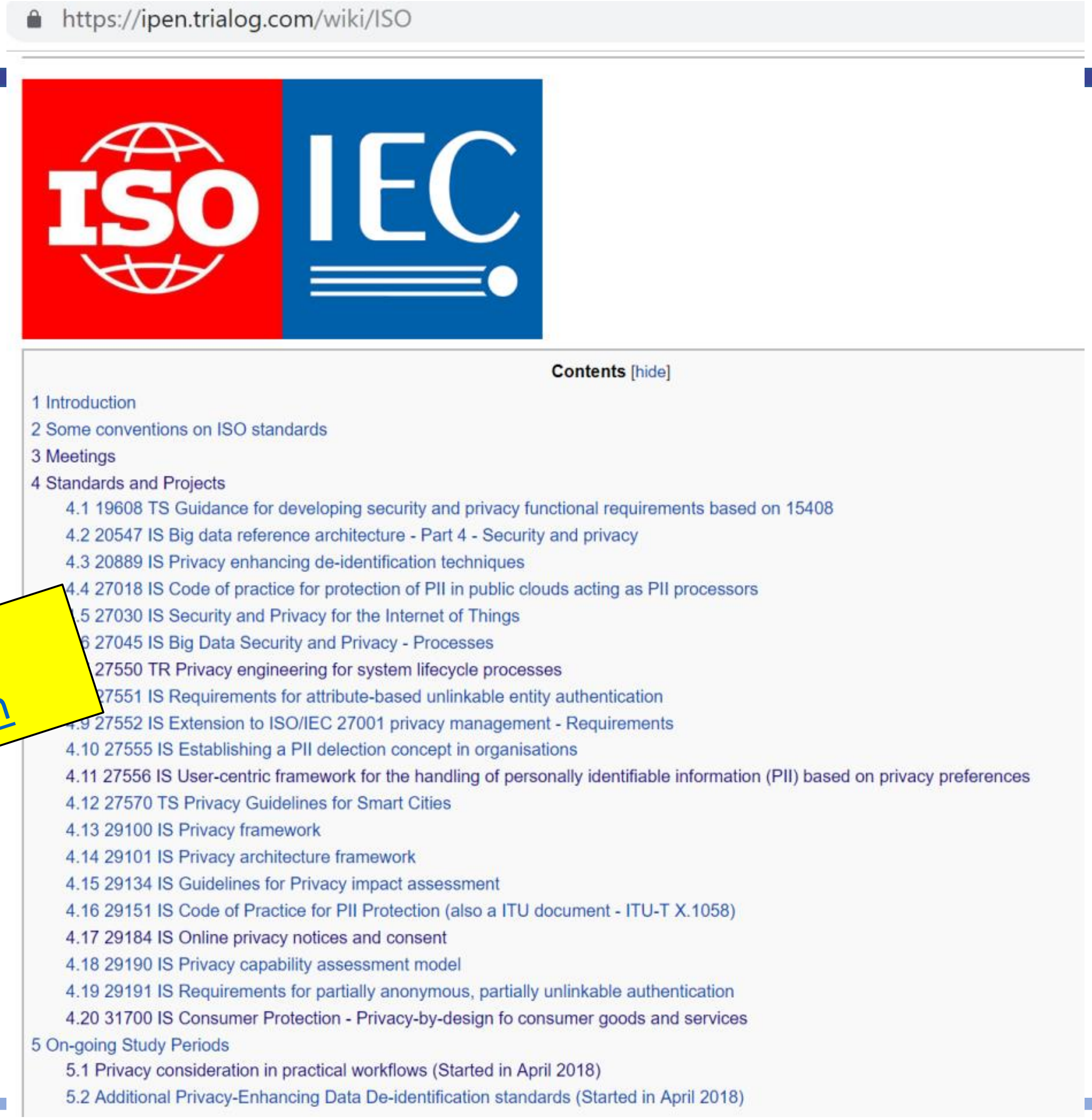
Content [edit]

Privacy standards	Privacy engineering projects	Reports, Events, Presentations
• CEN-CENELEC-ETSI	• APP Pets (ULD project)	• DPIA and PIA guidelines
• IETF Activities	• AN.ON-Next (ULD project)	• Studies
• IEEE standards	• CREDENTIAL (EC project completed)	• OWAS
• ISO/IEC	• DNT Guide	
• ITU standards	• PARIS (EC project completed)	
• OASIS	• PDP4E (EC project on-going	
• OpenID Foundation	• PRIPARE (EC pro	
• W3C Activities	• PRISM	
• National Level Standards		

More info on priv

Mor

Next IPEN workshop in Roma (June 12th 2019)
https://edps.europa.eu/ipen-rome-workshop-2019_en



https://ipen.trialog.com/wiki/ISO

Contents [hide]

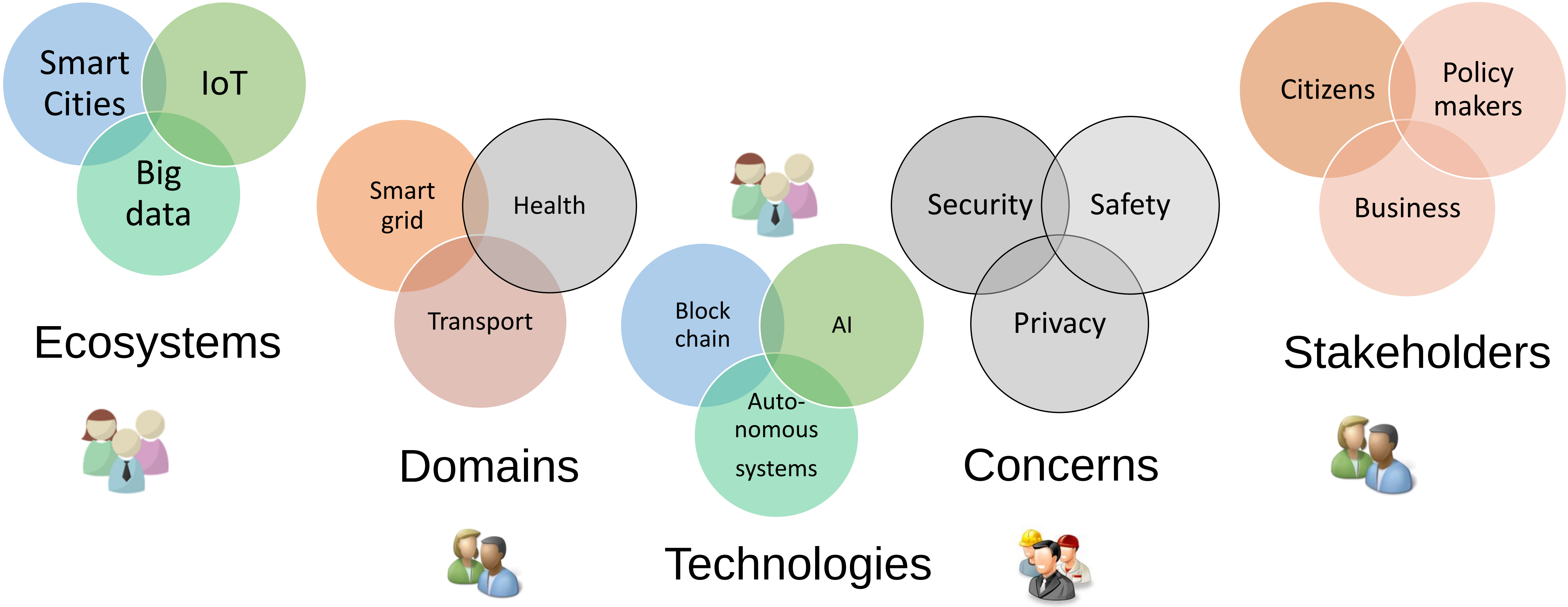
1 Introduction
2 Some conventions on ISO standards
3 Meetings
4 Standards and Projects
- 4.1 19608 TS Guidance for developing security and privacy functional requirements based on 15408
- 4.2 20547 IS Big data reference architecture - Part 4 - Security and privacy
- 4.3 20889 IS Privacy enhancing de-identification techniques
- 4.4 27018 IS Code of practice for protection of PII in public clouds acting as PII processors
- .5 27030 IS Security and Privacy for the Internet of Things
- 6 27045 IS Big Data Security and Privacy - Processes
- 27550 TR Privacy engineering for system lifecycle processes
- 27551 IS Requirements for attribute-based unlinkable entity authentication
- .9 27552 IS Extension to ISO/IEC 27001 privacy management - Requirements
- 4.10 27555 IS Establishing a PII delection concept in organisations
- 4.11 27556 IS User-centric framework for the handling of personally identifiable information (PII) based on privacy preferences
- 4.12 27570 TS Privacy Guidelines for Smart Cities
- 4.13 29100 IS Privacy framework
- 4.14 29101 IS Privacy architecture framework
- 4.15 29134 IS Guidelines for Privacy impact assessment
- 4.16 29151 IS Code of Practice for PII Protection (also a ITU document - ITU-T X.1058)
- 4.17 29184 IS Online privacy notices and consent
- 4.18 29190 IS Privacy capability assessment model
- 4.19 29191 IS Requirements for partially anonymous, partially unlinkable authentication
- 4.20 31700 IS Consumer Protection - Privacy-by-design fo consumer goods and services

5 On-going Study Periods
- 5.1 Privacy consideration in practical workflows (Started in April 2018)
- 5.2 Additional Privacy-Enhancing Data De-identification standards (Started in April 2018)

Privacy from a Policy Maker Viewpoint

Example of smart cities

They Deal with Complex Ecosystems



Smart Cities

IoT

Big data

Ecosystems

Smart grid

Health

Transport

Domains

Block chain

AI

Auto-nomous systems

Technologies

Security

Safety

Privacy

Concerns

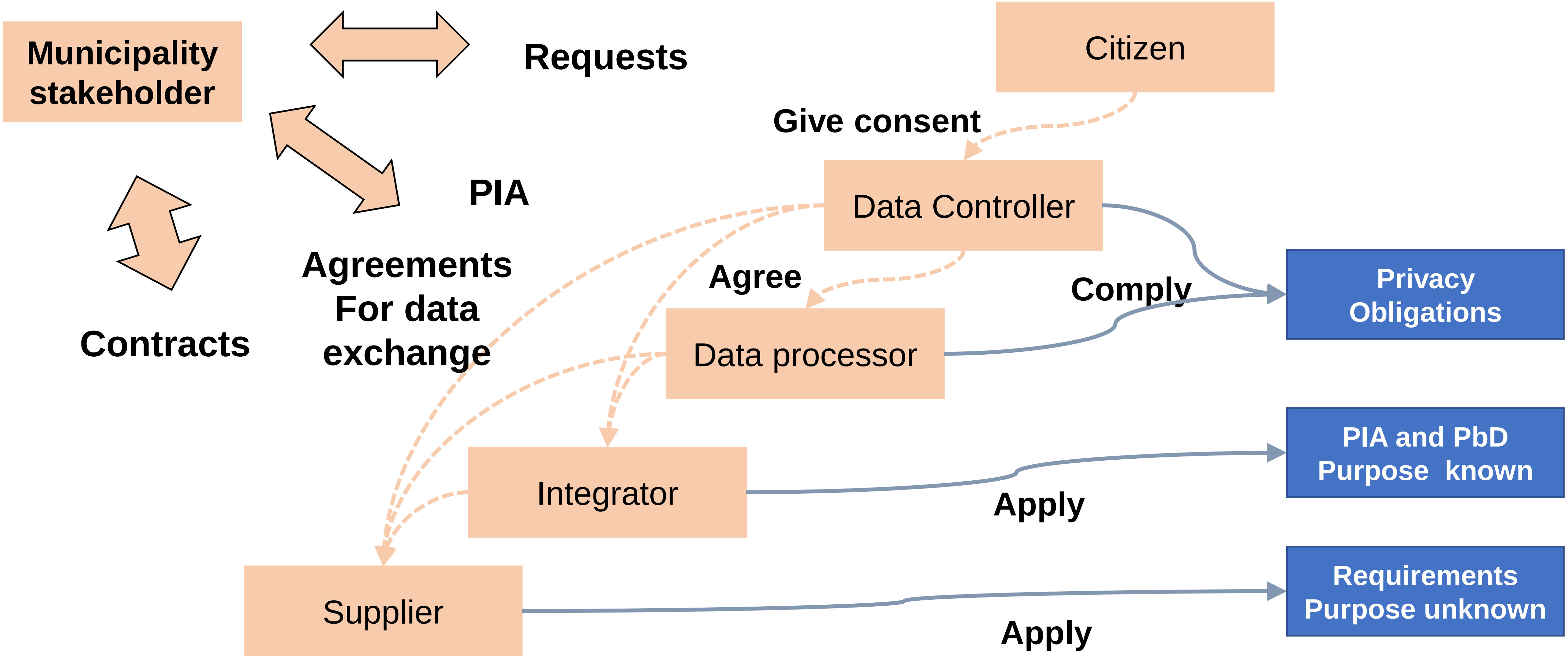
Citizens

Policy makers

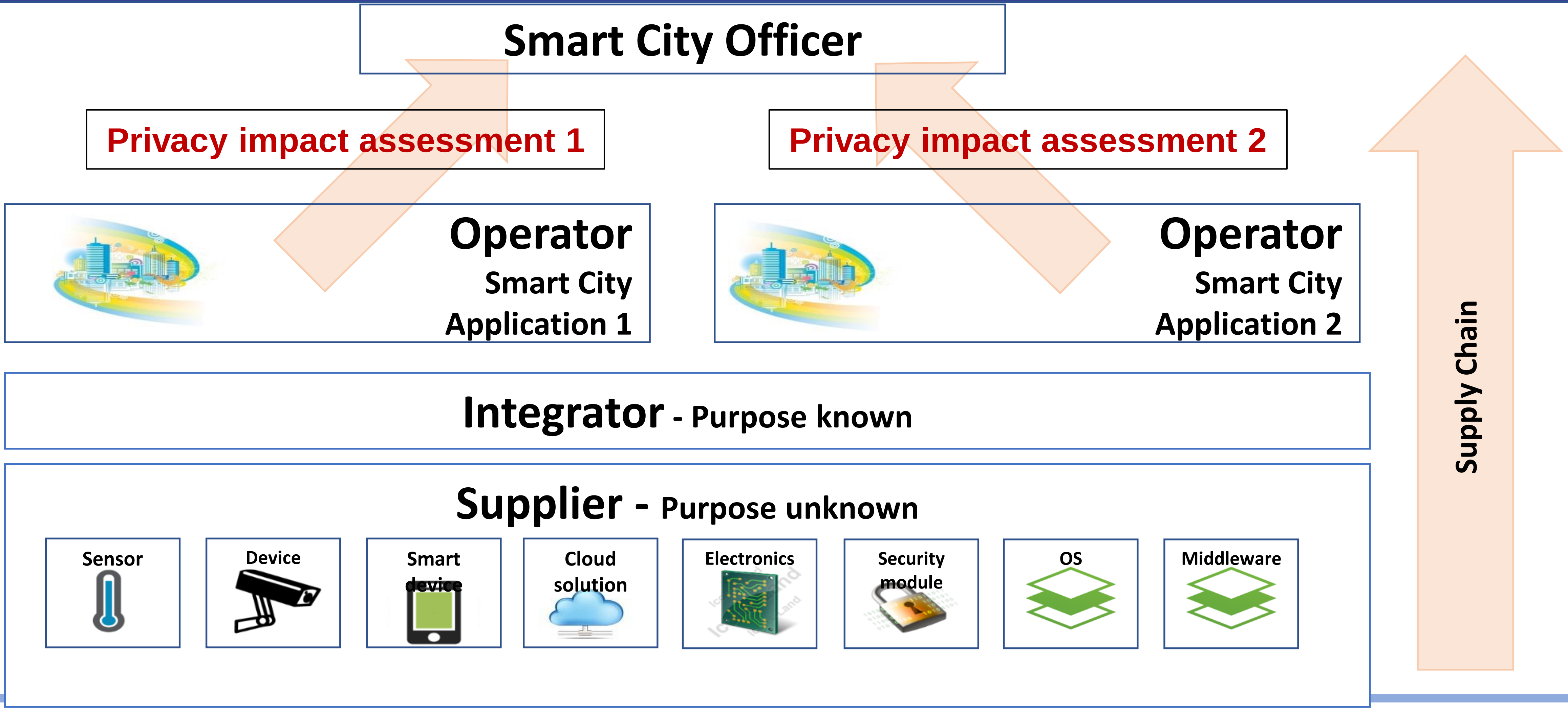
Business

Stakeholders

They Manage Privacy for these Ecosystems



Including a Supply Chain Vision



Smart City Officer

Privacy impact assessment 1

Privacy impact assessment 2

Operator
Smart City
Application 1

Operator
Smart City
Application 2

Integrator - Purpose known

Supplier - Purpose unknown

Sensor

Device

Smart device

Cloud solution

Electronics

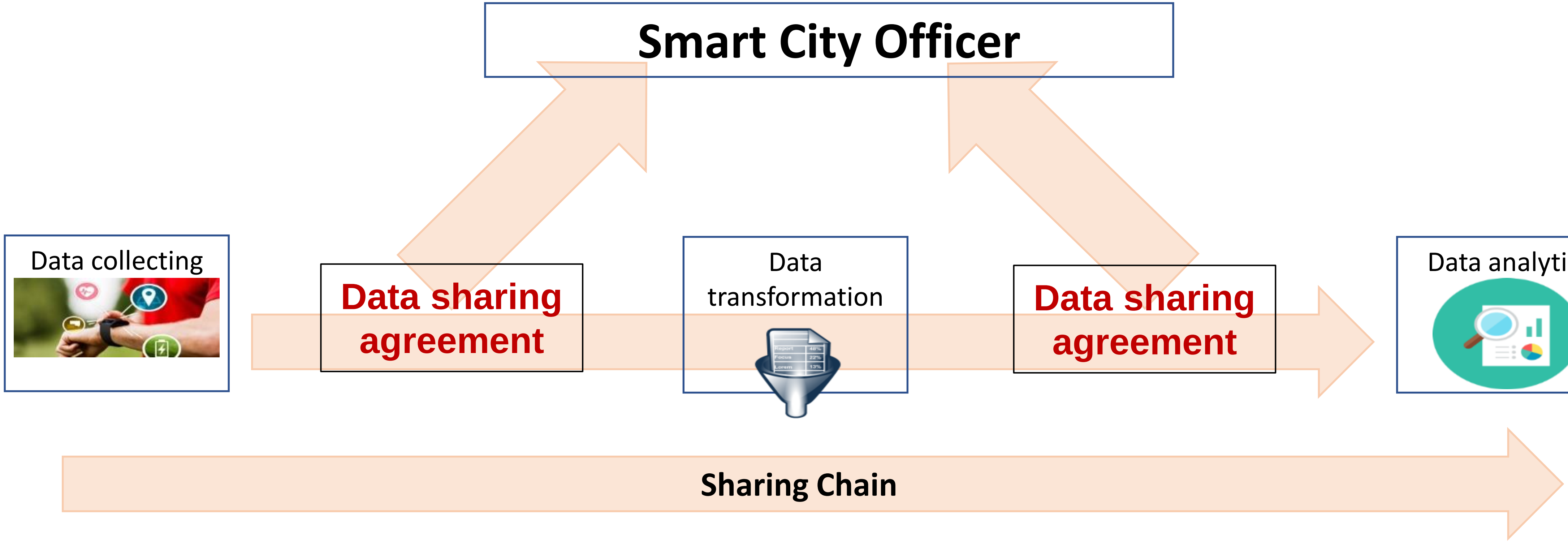
Security module

OS

Middleware

Supply Chain

Including a Sharing Chain Vision

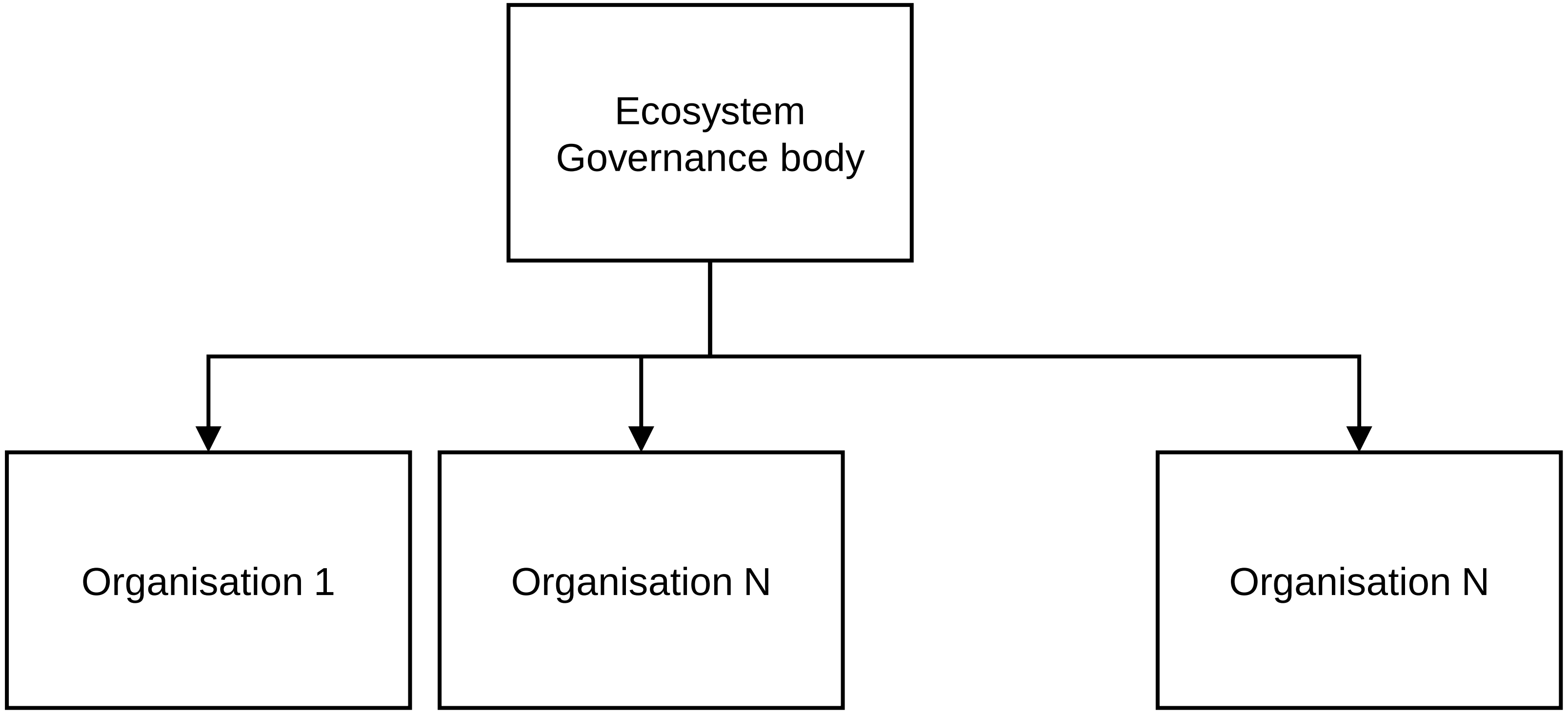


Several Types of Concerns

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

Ecosystem Management of Privacy

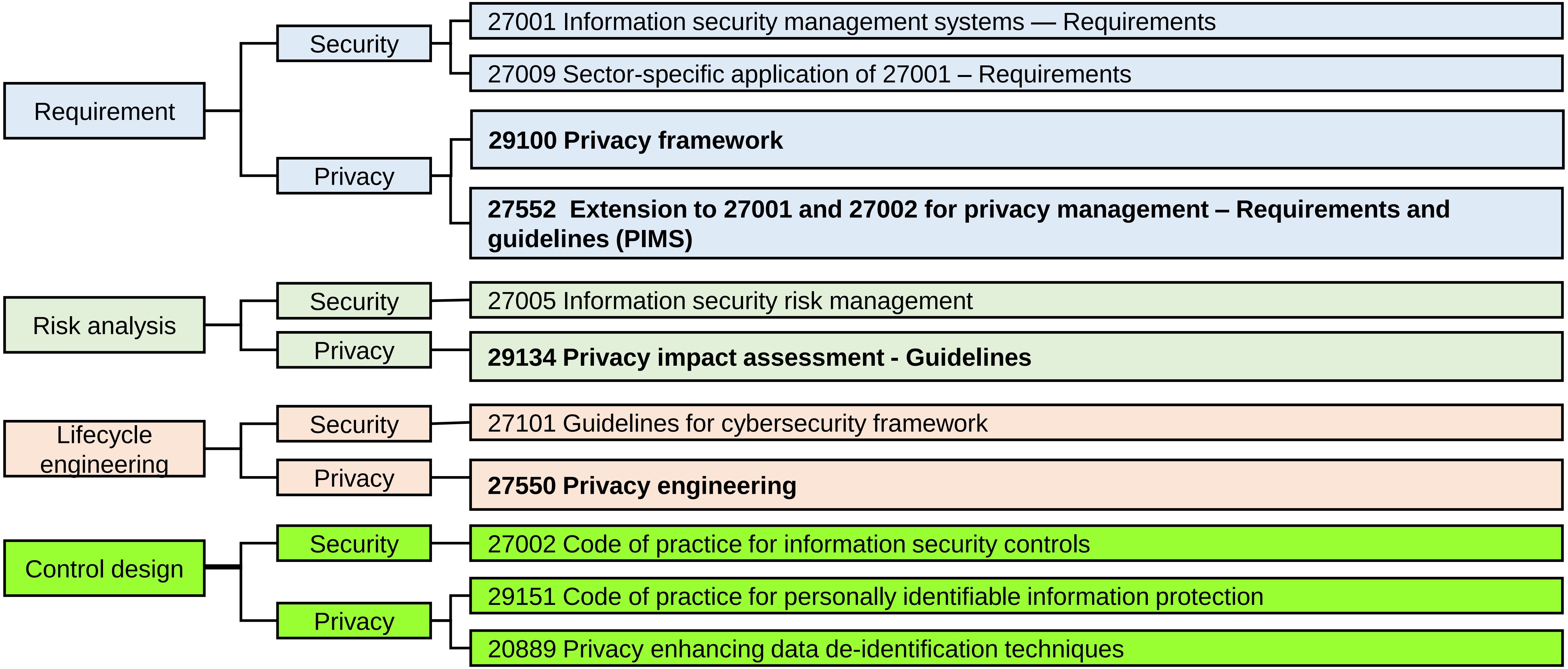
- ❑ Five processes
  - ❑ **Governance**
  - ❑ **Risk management**
  - ❑ **Data exchange**
  - ❑ **Engineering**
  - ❑ **Citizen engagement**



Overview of Work on Standardisation

Several Viewpoints

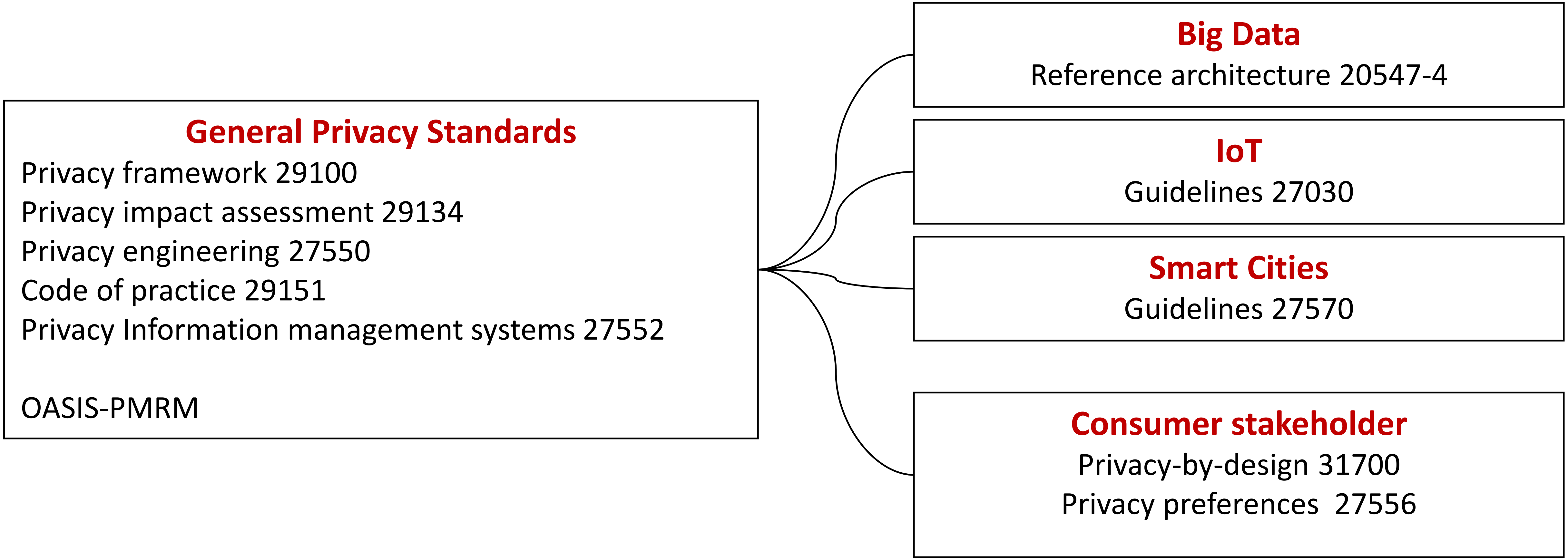
Security and Privacy Viewpoint: an Integration Issue



- Requirement
  - Security
    - 27001 Information security management systems — Requirements
    - 27009 Sector-specific application of 27001 – Requirements
  - Privacy
    - **29100 Privacy framework**
    - **27552 Extension to 27001 and 27002 for privacy management – Requirements and guidelines (PIMS)**
- Risk analysis
  - Security
    - 27005 Information security risk management
  - Privacy
    - **29134 Privacy impact assessment - Guidelines**
- Lifecycle engineering
  - Security
    - 27101 Guidelines for cybersecurity framework
  - Privacy
    - **27550 Privacy engineering**
- Control design
  - Security
    - 27002 Code of practice for information security controls
  - Privacy
    - 29151 Code of practice for personally identifiable information protection
    - 20889 Privacy enhancing data de-identification techniques

Ecosystem Viewpoint

Ecosystem guidelines



General Privacy Standards

Privacy framework 29100

Privacy impact assessment 29134

Privacy engineering 27550

Code of practice 29151

Privacy Information management systems 27552

OASIS-PMRM

Big Data

Reference architecture 20547-4

IoT

Guidelines 27030

Smart Cities

Guidelines 27570

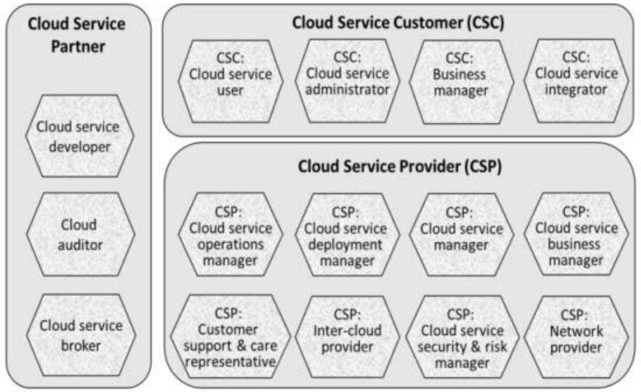
Consumer stakeholder

Privacy-by-design 31700

Privacy preferences 27556

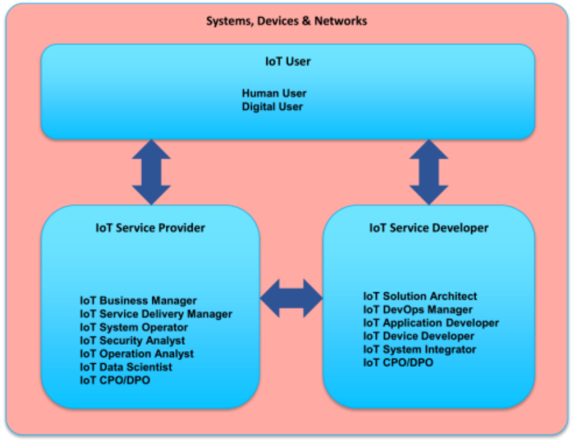
Trends in Standards: Ecosystem Guidance

ISO/IEC 17789 Cloud computing roles


Cloud Service Partner
Cloud service developer
Cloud auditor
Cloud service broker
Cloud Service Customer (CSC)
CSC: Cloud service user
CSC: Cloud service administrator
CSC: Business manager
CSC: Cloud service integrator
Cloud Service Provider (CSP)
CSP: Cloud service operations manager
CSP: Cloud service deployment manager
CSP: Cloud service manager
CSP: Cloud service business manager
CSP: Customer support & care representative
CSP: Inter-cloud provider
CSP: Cloud service security & risk manager
CSP: Network provider

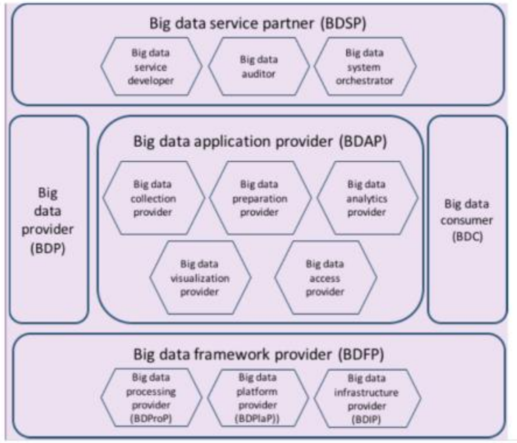
ISO/IEC 23751 Data sharing agreement	
Cloud service customer	Ecosystem guidance
Cloud service partner	
Cloud service provider	

ISO/IEC 30141 IoT roles



ISO/IEC 27030 Security and privacy guidelines for IoT	
Iot user	Ecosystem guidance
IoT service developer	
IoT service provider	

ISO/IEC 20547-3 Big data roles

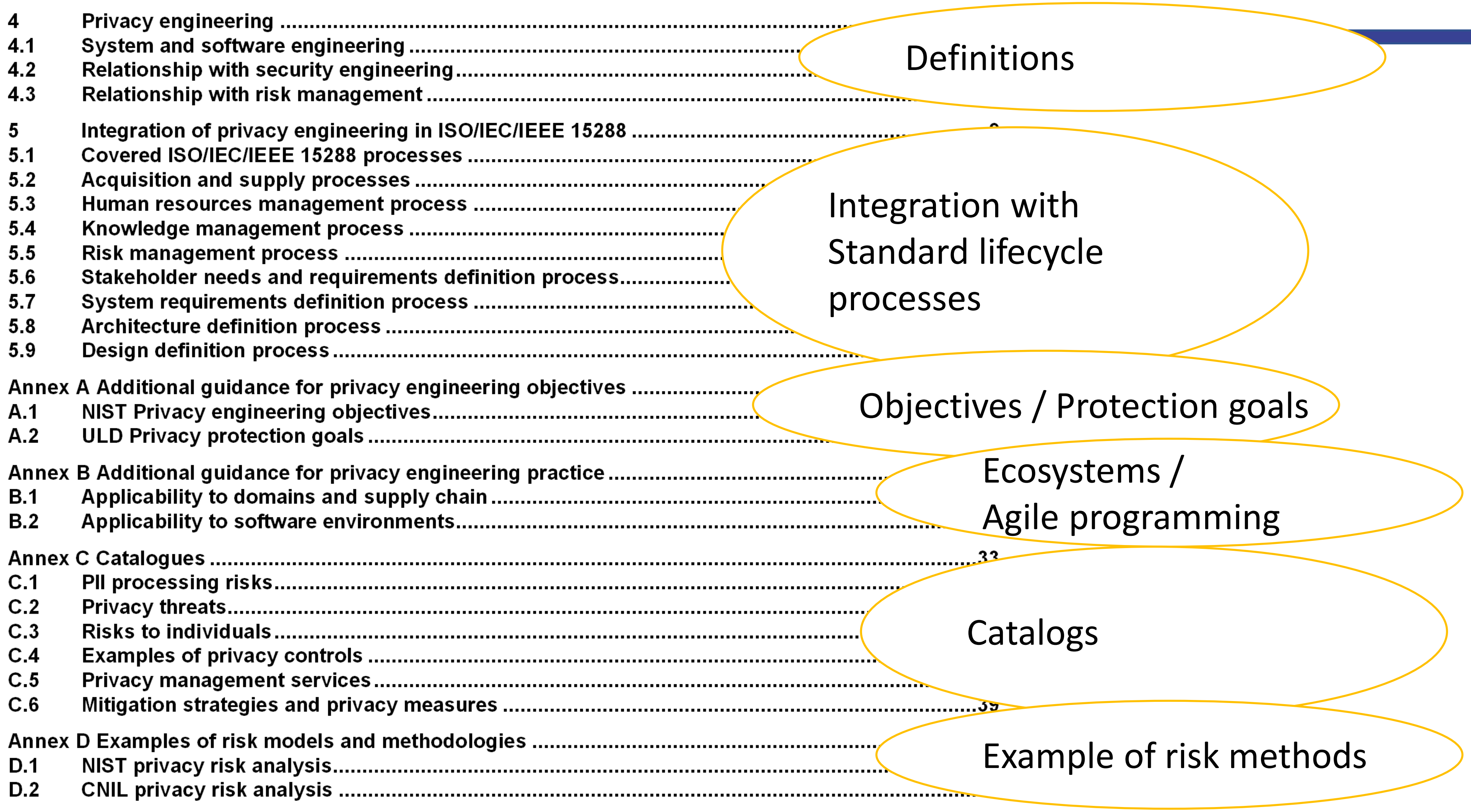

Big data service partner (BDSP)
Big data service developer
Big data auditor
Big data system orchestrator
Big data provider (BDP)
Big data application provider (BDAP)
Big data collection provider
Big data preparation provider
Big data analytics provider
Big data visualization provider
Big data access provider
Big data consumer (BDC)
Big data framework provider (BDFP)
Big data processing provider (BDProP)
Big data platform provider (BDPlaP))
Big data infrastructure provider (BDIP)

ISO/IEC 20547-4 Big data security and privacy	
Big data service partner	Ecosystem guidance
Big data application provider	
Big data provider	
Big data consumer	
Big data framework provider	

ISO/IEC 27550

Privacy Engineering for system lifecycle process

Structure



Definitions

Integration with Standard lifecycle processes

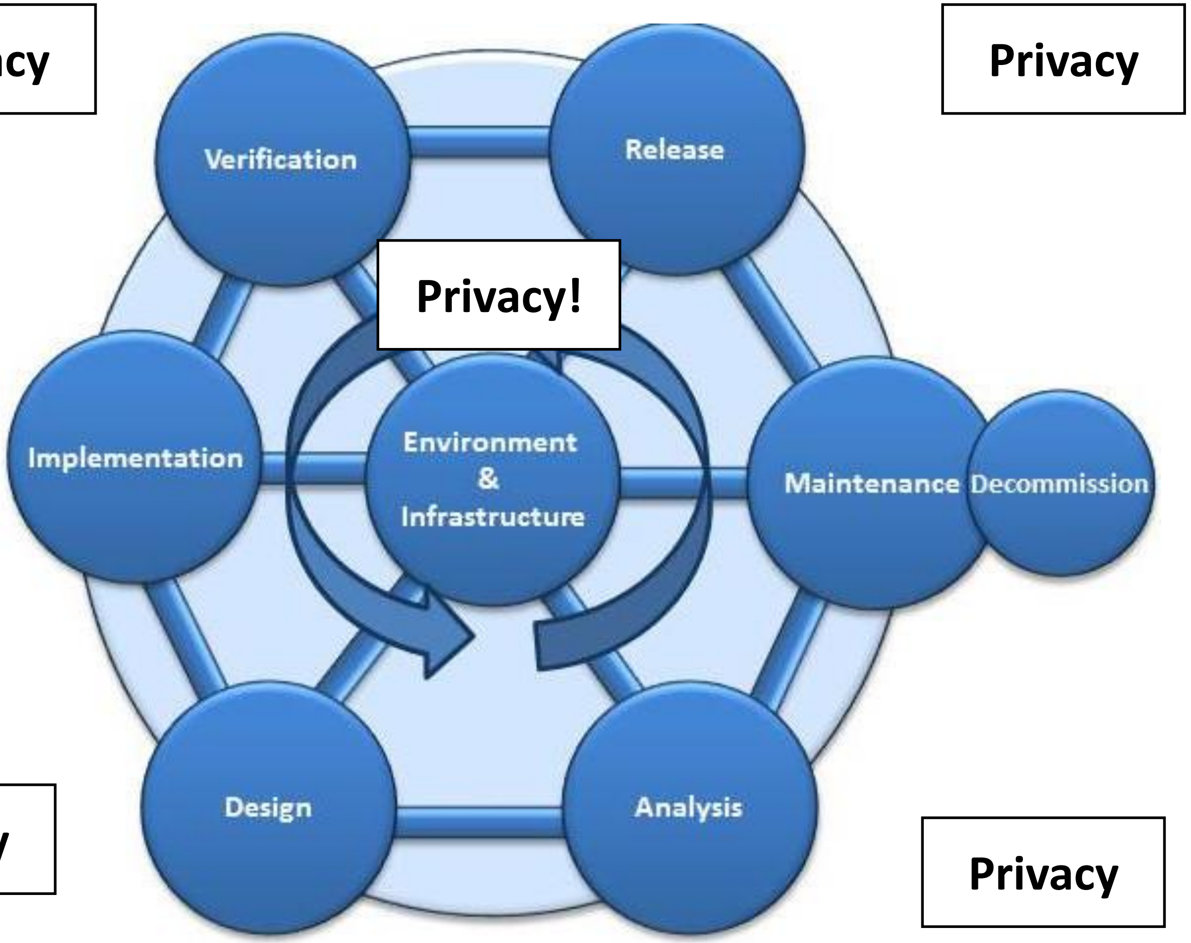
Objectives / Protection goals

Ecosystems / Agile programming

Catalogs

Example of risk methods

Privacy Engineering: Integrating privacy concerns



Privacy

Privacy

Privacy!

Privacy

Privacy

Privacy

Privacy

Beyond CIA

❑Confidentiality

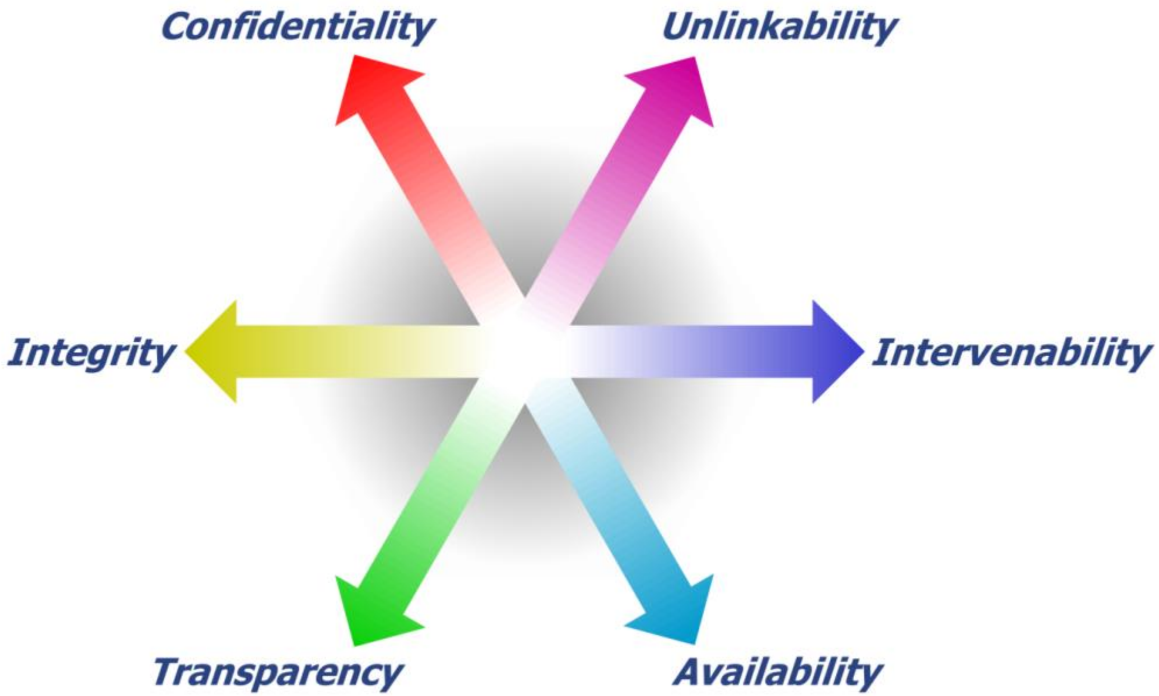
❑Integrity

❑Availability

❑Unlinkability

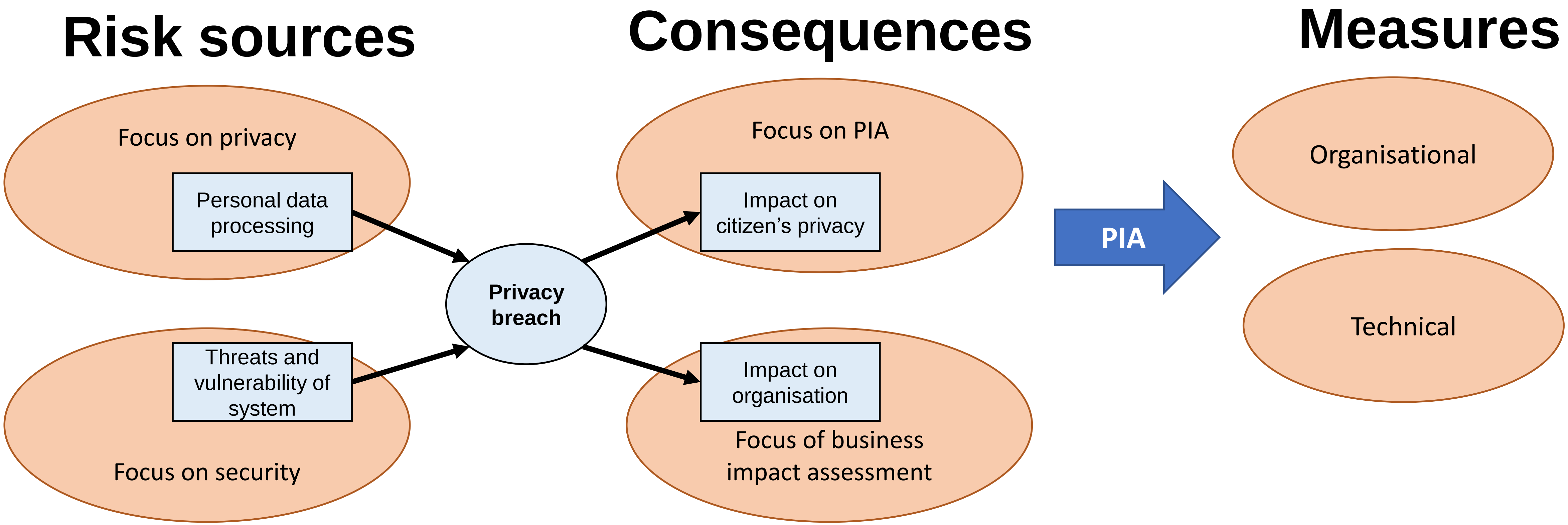
❑Intervenability

❑Transparency



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

Privacy Impact Assessment (PIA)



From security properties to security threats: STRIDE

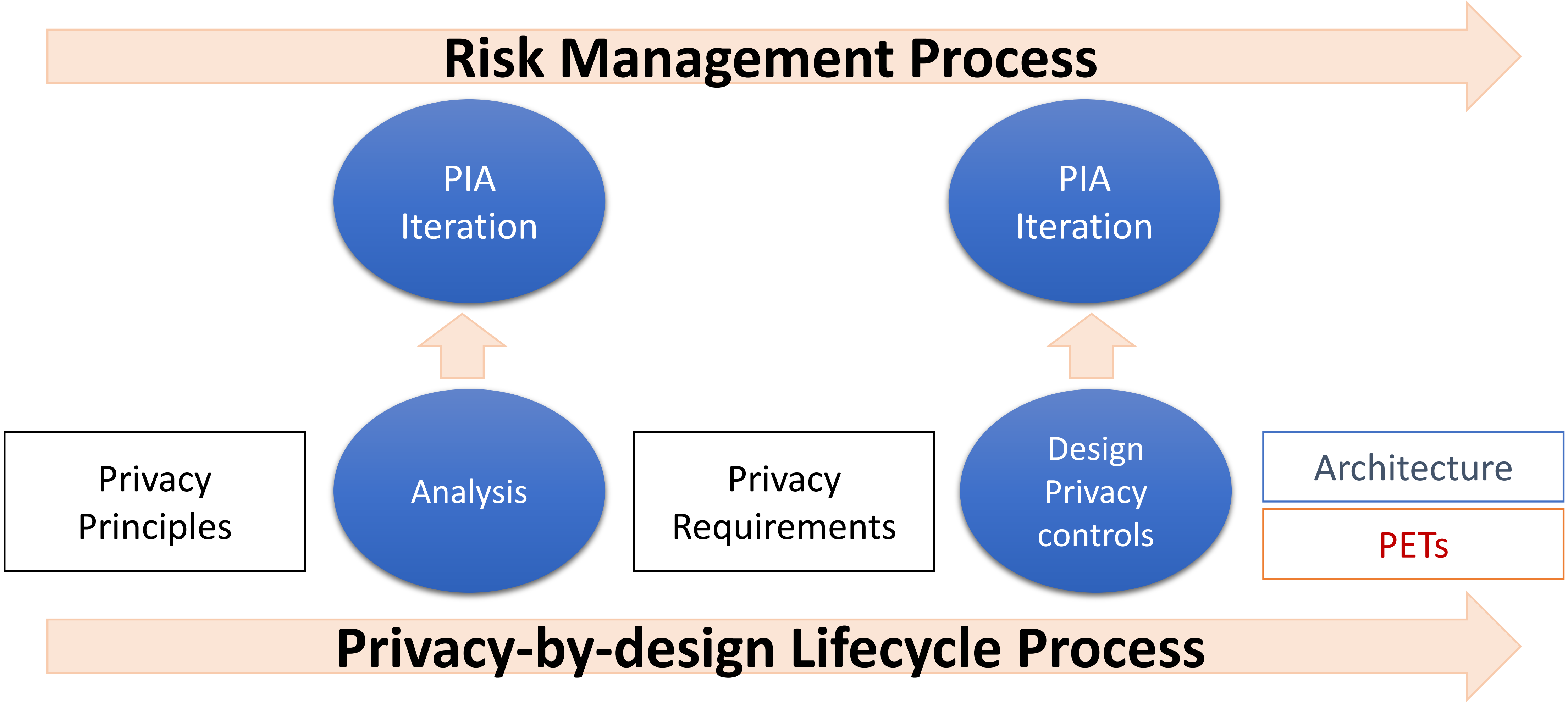
Property	Description	Threat
Authentication	The identity of users is established (or you’re willing to accept anonymous users).	**S**poofing
Integrity	Data and system resources are only changed in appropriate ways by appropriate people.	**T**ampering
Nonrepudiation	Users can’t perform an action and later 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

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

Type	Property	Description	Threat
Hard privacy	Unlinkability	Hiding the link between two or more actions, identities, and pieces of information.	Linkability
	Anonymity	Hiding the link between an identity and an action or a piece of information	Identifiability
	Plausible deniability	Ability to deny having performed an action that other parties can neither confirm nor contradict	Non-repudiation
	Undetectability and unobservability	Hiding the user’s actvities	Detectability
Security	Confidentiality	Hiding the data content or controlled release of data content	Disclosure of information
Soft Privacy	Content awareness	User’s consciousness regarding his own data	Unawareness
	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	Non compliance

Privacy-by-design



Design Strategy (J.H.Hoepman)

https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport

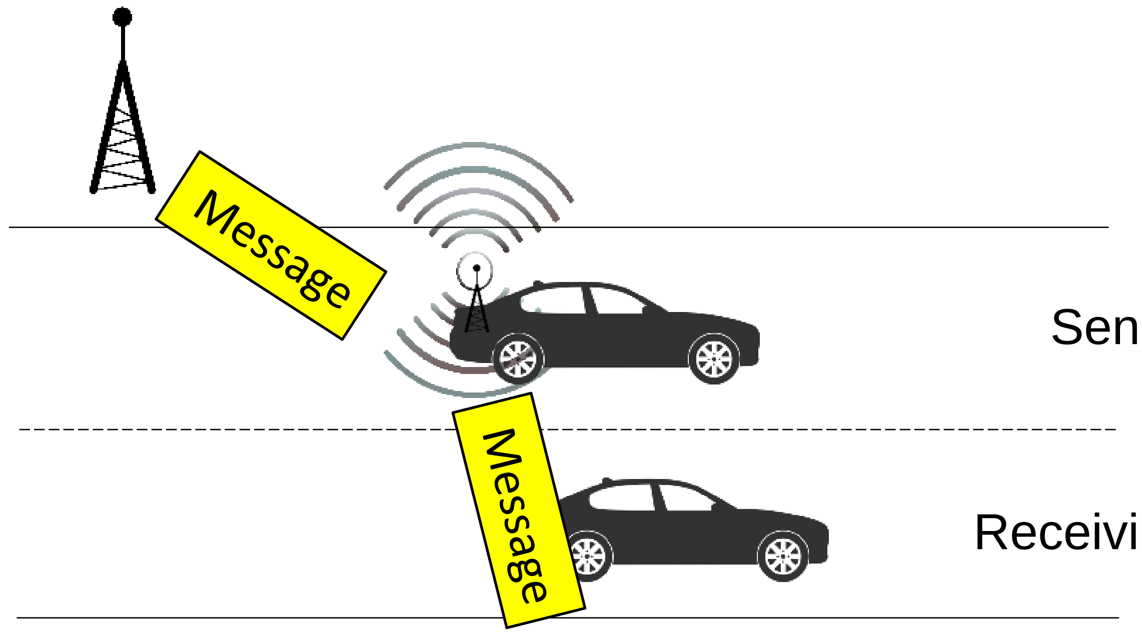
Design strategy		Description	Privacy control examples
Data oriented strategies	Minimize	Limit as much as possible the processing of PII	Selection before collection, Anonymization
	Separate	Distribute or isolate personal data as much as possible, to prevent correlation	Logical or physical separation, Peer-to-peer arrangement, Endpoint processing
	Abstract	Limit as much as possible the detail in which personal data is processed, while still being useful	Aggregation over time (used in smart grids), Dynamic location granularity (used in location based services), k-anonymity
	Hide	Prevent PII to become public or known.	Encryption, Mixing, Perturbation (e.g. differential privacy, statistical disclosure control), Unlinking (e.g. through pseudonymisation), Attribute based credentials
Process oriented strategies	Inform	Inform PII principals about the processing of PII	Privacy icons, Layered privacy policies, Data breach notification
	Control	Provide PII principals control about the processing of their PII.	Privacy dashboard, Consent (including withdrawal)
	Enforce	Commit to PII processing in a privacy friendly way, and enforce this	Sticky policies and privacy rights management, Privacy management system, Commitment of resources, Assignment of responsibilities
	Demonstrate	Demonstrate that PII is processed in a privacy friendly way.	Logging and auditing, Privacy impact assessment, Design decisions documentation

Privacy management in C-ITS

C-ITS Environment

- Position of vehicle
- Movement of vehicle (speed, acceleration, steering angle, …)
- Static information about the vehicle: type and size
- Pseudonym
- Recent Path (limited to the last 30 seconds at maximum)

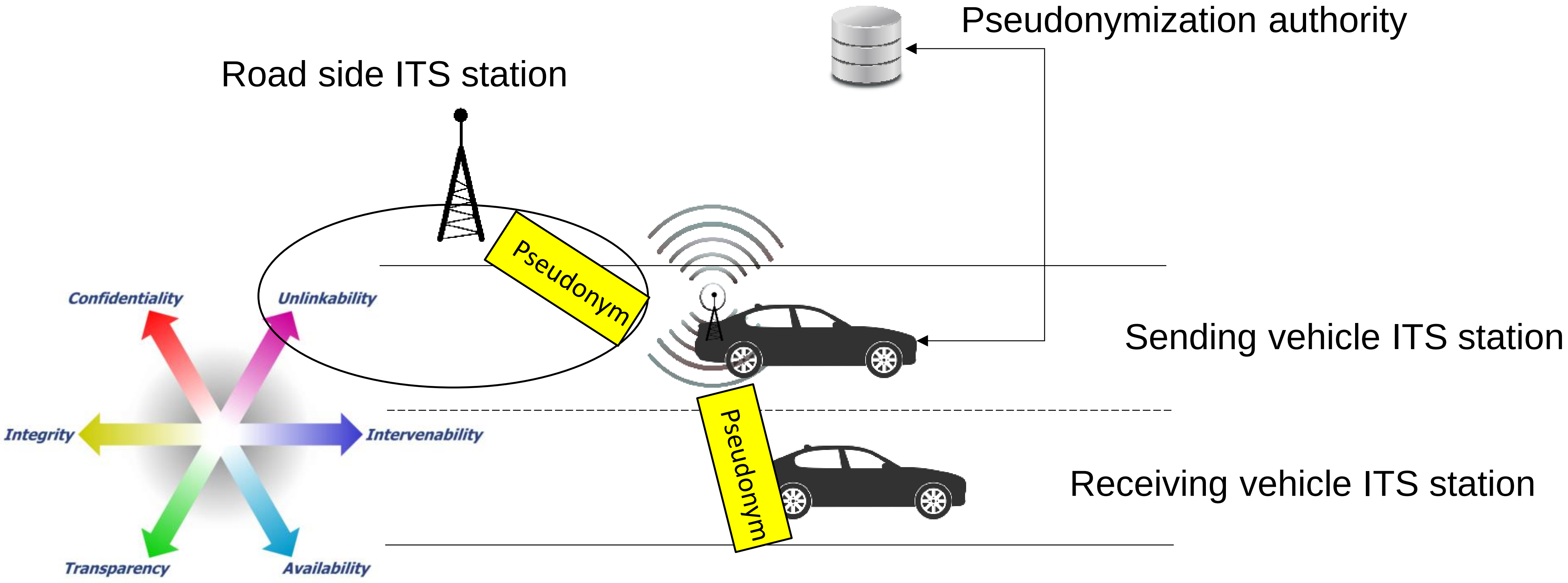
Road side ITS station



Sending vehicle ITS station

Receiving vehicle ITS station

C-ITS Environment



Pseudonymization authority

Road side ITS station

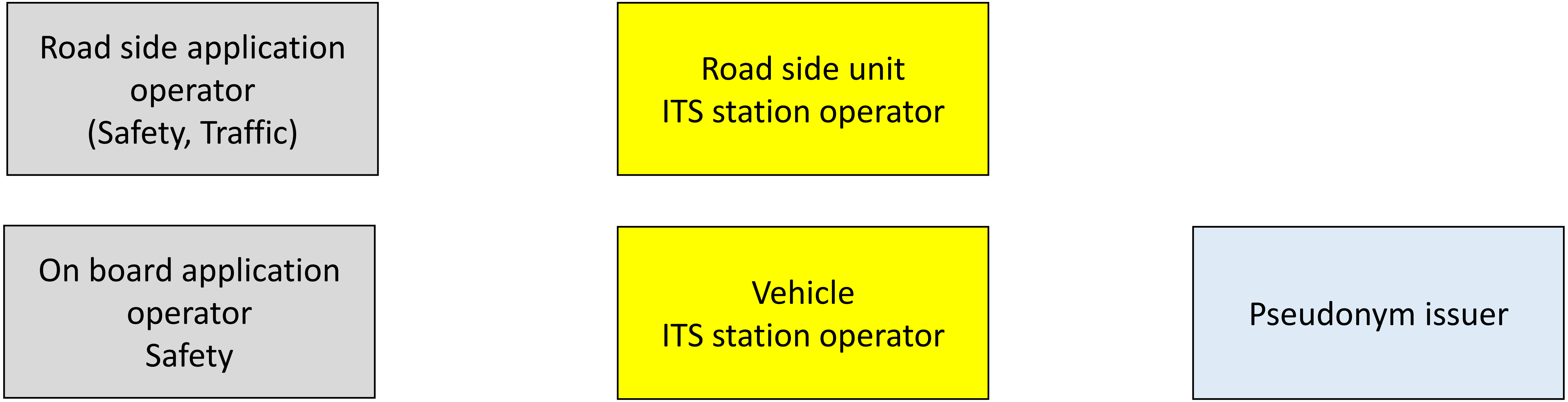
Pseudonym

Sending vehicle ITS station

Pseudonym

Receiving vehicle ITS station

Generic Viewpoint of Ecosystem



Road side application operator (Safety, Traffic)

Road side unit ITS station operator

On board application operator Safety

Vehicle ITS station operator

Pseudonym issuer

C-ITS management requirements

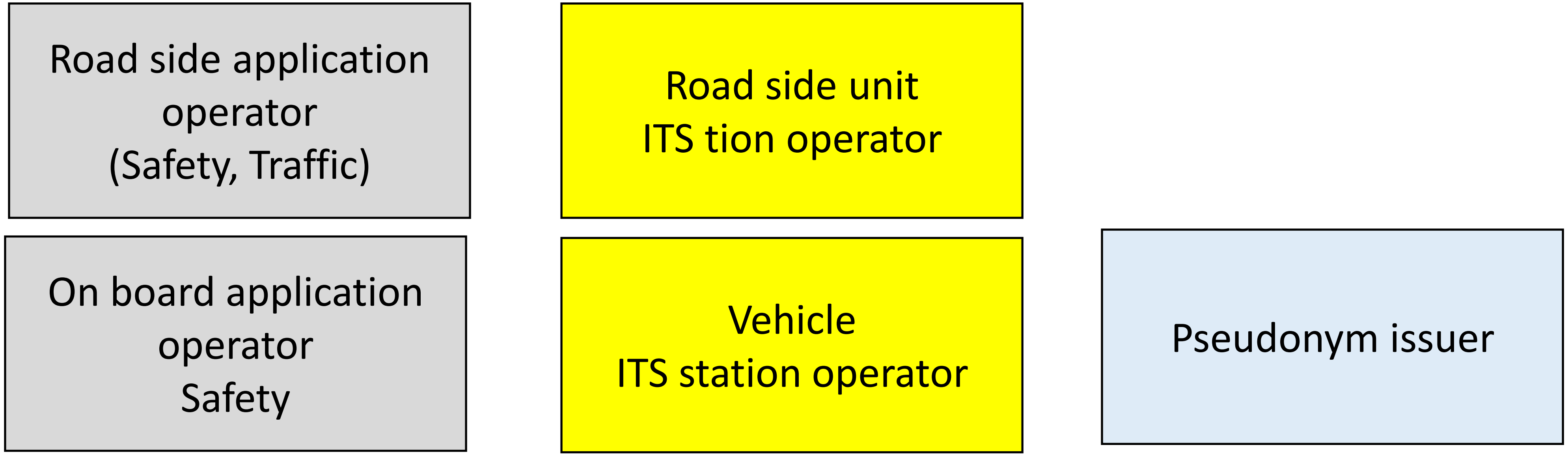
Chain	Requirements
Governance	Enforcing privacy compliance in the organisational chains
	Identifying and enrolling all data controllers and processors
Supply chain	Ensuring that suppliers have a minimum level of competence concerning privacy and privacy-by-design
Data sharing chain	Ensuring that members of the chain meet their obligations Stay within purpose Inform governing body when data is transmitted to third party
	Ensuring that organizations inform the governing body when they discover a breach or a threat that may lead to a breach

Privacy Risks

Road side application operator On board application operator	Road side unit operator Vehicle ITS station operator	Ecosystem Pseudonym issuer
Risks Outside purpose • Applications which are not in the purpose Re-identification scheme	De-identification • Compute trajectory • Identify driving behaviour • Identify driving offence Pseudonym unlinkability degradation • New guessing approaches • Minority of vehicles use PKI B	De-identification • Reveal vehicle id and allocated pseudonyms
Measures Breach management Continuous improvement	C-ITS station update Breach management Continuous improvement	Segregation of duties • Registering a vehicle • Supplying pseudonym to vehicle Breach management Continuous improvement

Governance for privacy?

- □ Which stakeholder
  - □ **Data protection authority (At european level, at national level)**
  - □ **Ministry of transport**
  - □ **Association**
- □ PKI issuer?



Road side application operator (Safety, Traffic)

Road side unit ITS tion operator

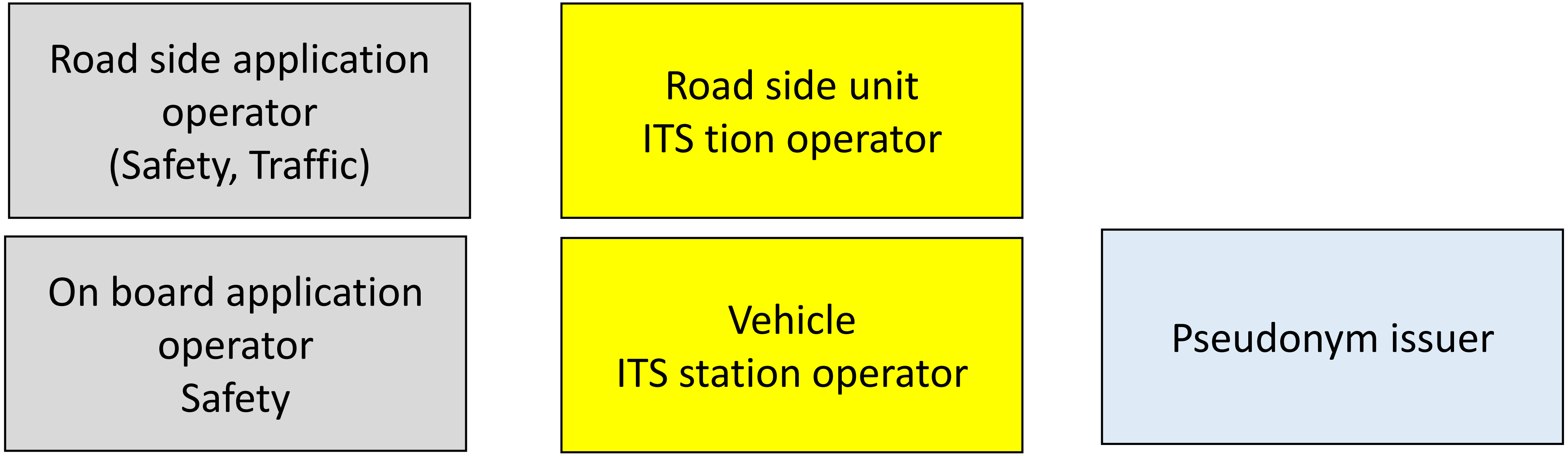
On board application operator Safety

Vehicle ITS station operator

Pseudonym issuer

Risk management for privacy?

- □ Access to common risk data base
- □ Ensuring that operators have the same assessment
  - □ **Interoperability and consistency of risk management**
- □ Issue how do operators trust each other?



Road side application operator (Safety, Traffic)

Road side unit ITS tion operator

On board application operator Safety

Vehicle ITS station operator

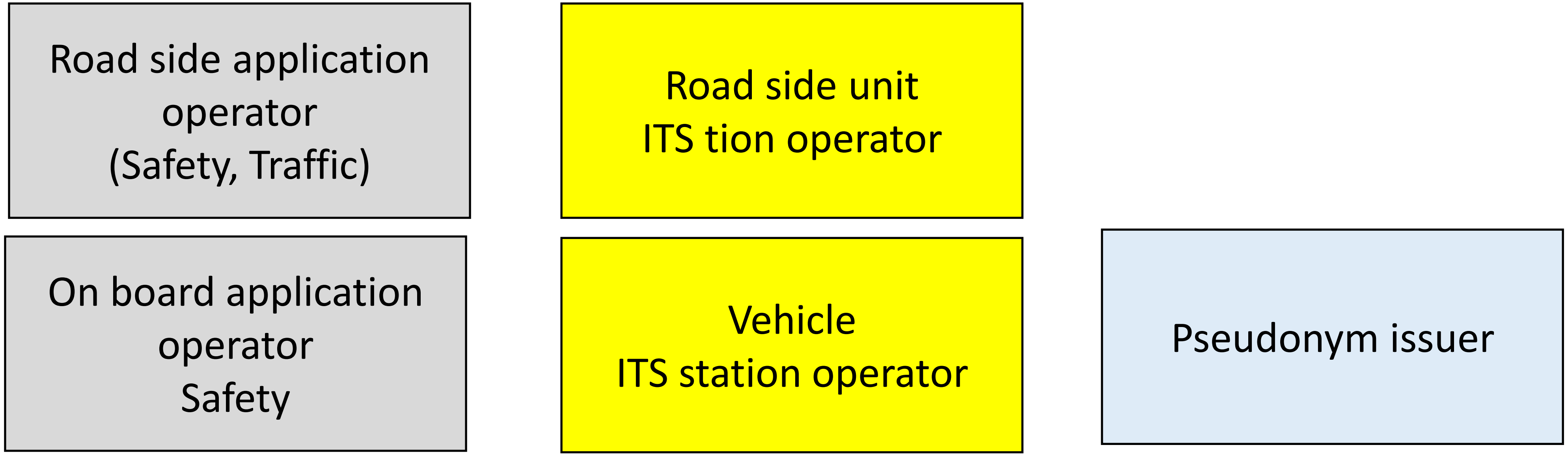
Pseudonym issuer

Engineering for privacy?

□Sharing design, privacy specific components

□Same solutions?

□Alliance or observation to select



Road side application operator (Safety, Traffic)

Road side unit ITS tion operator

On board application operator Safety

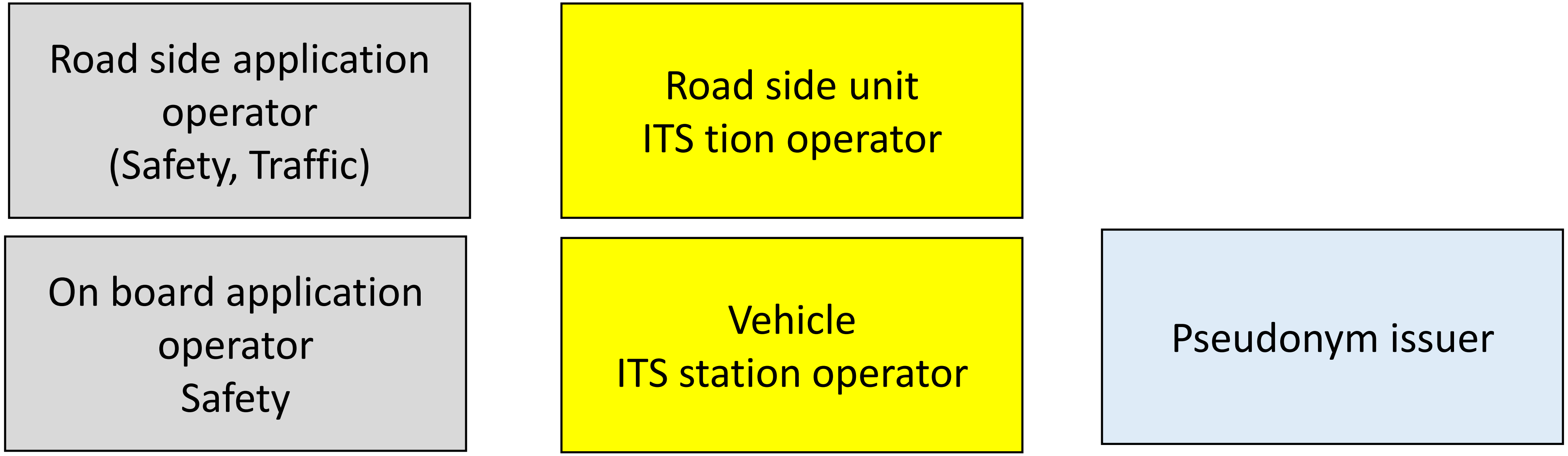
Vehicle ITS station operator

Pseudonym issuer

Data sharing agreements for privacy?

□ Using the same template?

□ Tracking the list of stakeholders?



Road side application operator (Safety, Traffic)

Road side unit ITS tion operator

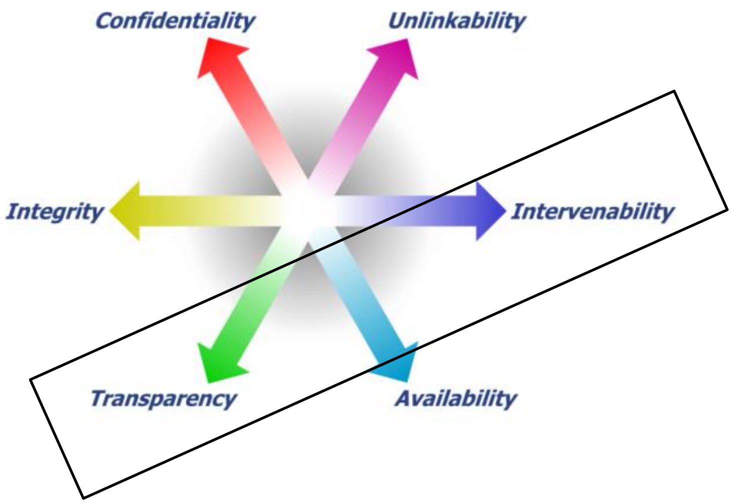
On board application operator Safety

Vehicle ITS station operator

Pseudonym issuer

Citizen engagement for privacy?

- □ Same transparency / intervenability requirements?



Road side application operator (Safety, Traffic)

Road side unit ITS tion operator

On board application operator Safety

Vehicle ITS station operator

Pseudonym issuer

Question?

antonio.kung@trialog.com

www.trialog.com