Status of Privacy Engineering Standardisation

Antonio Kung

Trialog, 25 rue du Général Foy 75008 Paris

antonio.kung@trialog.com

Outline

- Speaker
- Ecosystem viewpoint: big change in standardisation
- Privacy engineering: new standards in the pipe
- IPEN in the loop: recommendation for best practice sharing on privacy engineering

Speaker

- Engineering background
  - **Coordinator PRIPARE (pripareproject.eu) 2013-2015**
    - Liaison with ISO/IEC JTC1/SC27/WG5
    - Member of OASIS (Privacy Management Reference Model - PMRM)
- Active participation in privacy standards
  - **Privacy by design principles**
    - Privacy by design for consumer goods and services (ISO 31700)
  - **Privacy engineering**
    - Privacy engineering (ISO/IEC 27550 – to be published)
    - Big data – Security and privacy fabric (ISO/IEC 20547-4)
    - Smart cities - Privacy guidelines for smart cities (ISO/IEC 27570)
    - IoT - Security and privacy guidelines for IoT (ISO/IEC 27030)
    - Privacy preference management (ISO/IEC 27556)
    - Privacy engineering models - study

Administrator of IPEN wiki

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

Page Discussion

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 • IETF Activities • IEEE standards • ISO/IEC • ITU standards • OASIS • OpenID Foundation • W3C Activities • National Level Standards	• APP Pets (ULD project) • AN.ON-Next (ULD project) • CREDENTIAL (EC project completed) • DNT Guide • PARIS (EC project completed) • PDP4E (EC project on-going) • PRIPARE (EC project completed) • PRISMACLOUD (EC project completed) • Privacy framework (NIST project on-going) • Privacypatterns • Signatu	• DPIA and PIA guidelines • Studies • OWASP • Business Process Cookbook • Events • Presentations

More info on privacy standards [Expand]
More info on privacy engineering projects. [Expand]
More info on reports, events, presentations [Expand]

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

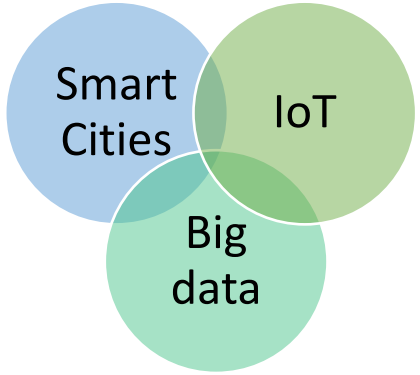
Contents [hide]

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
  4.5 27030 IS Security and Privacy for the Internet of Things
  4.6 27045 IS Big Data Security and Privacy - Processes
  4.7 27550 TR Privacy engineering for system lifecycle processes
  4.8 27551 IS Requirements for attribute-based unlinkable entity authentication
  4.9 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)

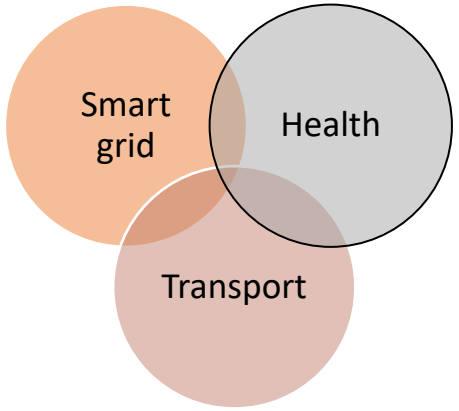
The ecosystem viewpoint

Big change in standardisation

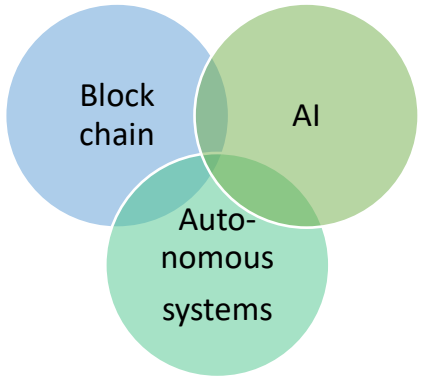
The Ecosystem Viewpoint



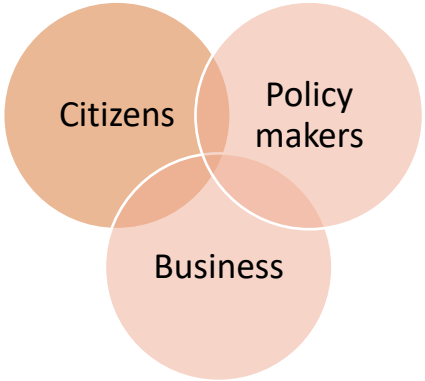
Ecosystems



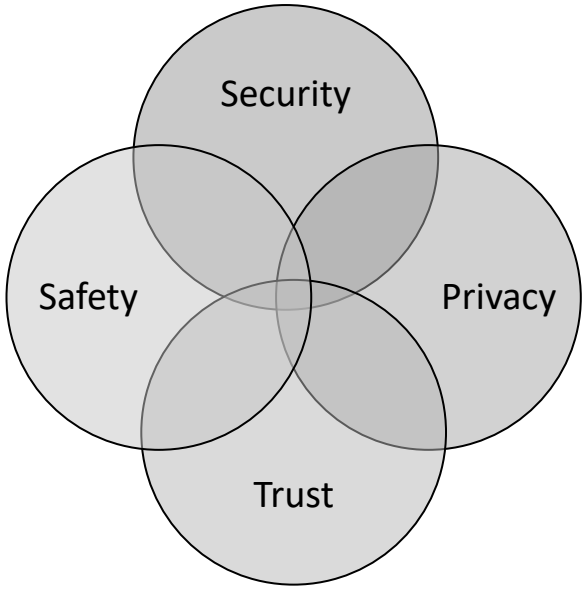
Domains



Technologies

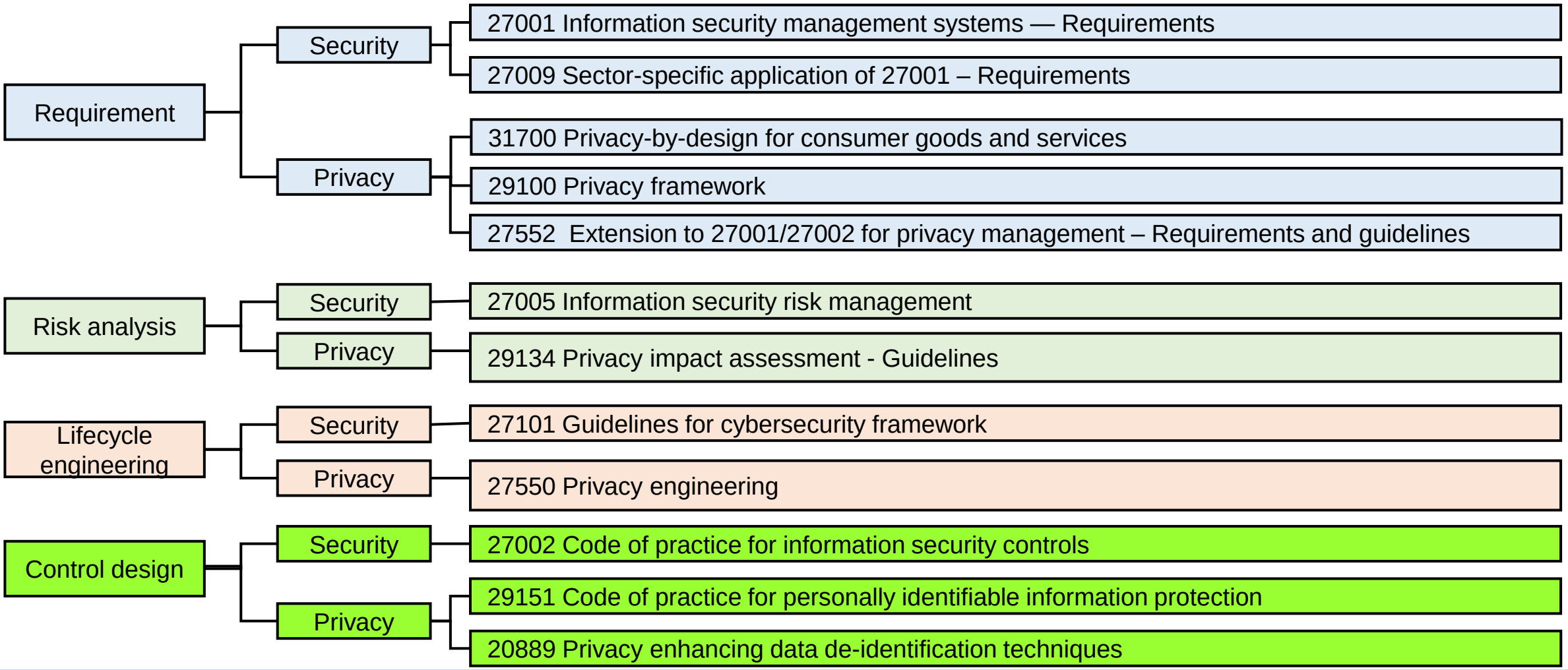


Stakeholders



Concerns

An Integration Issue of Transversal Concern: Example of Security and Privacy



Trends in Standards: Ecosystem Guidance

ISO/IEC 17789 Cloud computing Reference Architecture

ISO/IEC 23751 Data sharing agreement

Cloud service customer	Ecosystem guidance
Cloud service partner	
Cloud service provider	

ISO/IEC 30141 IoT Reference Architecture

ISO/IEC 27030 Security and privacy guidelines for IoT

Iot user	Ecosystem guidance
IoT service developer	
IoT service provider	

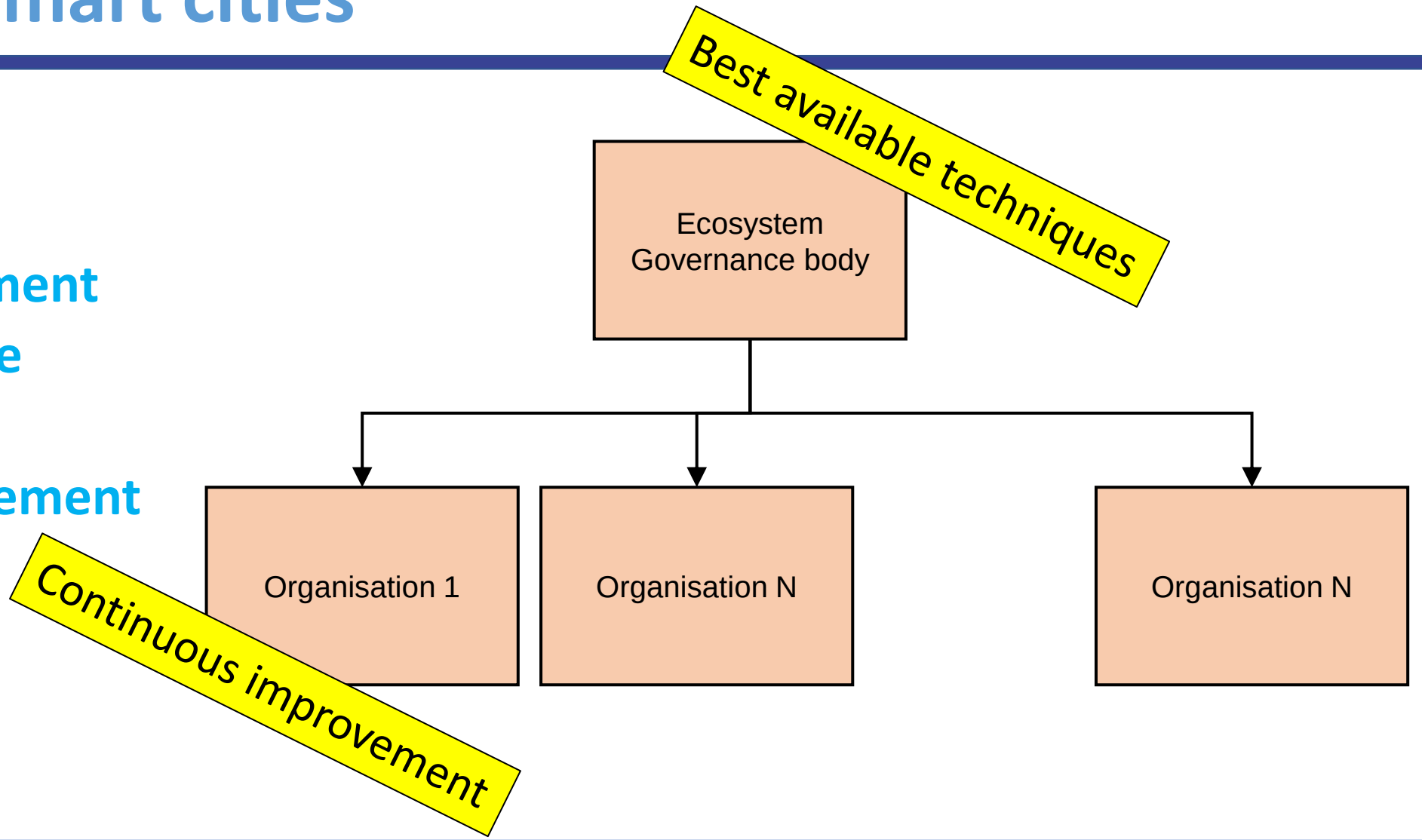
ISO/IEC 20547-3 Big data Reference Architecture

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	

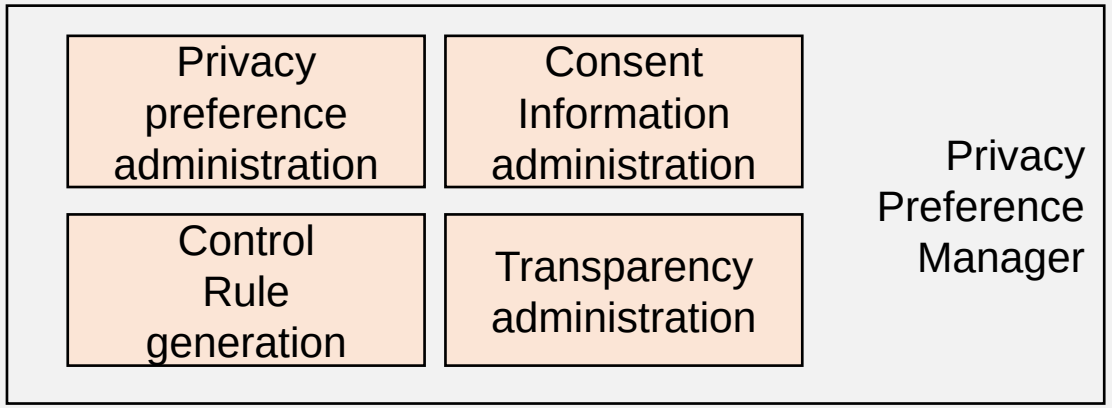
ISO/IEC 27570 Privacy guidelines for smart cities

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

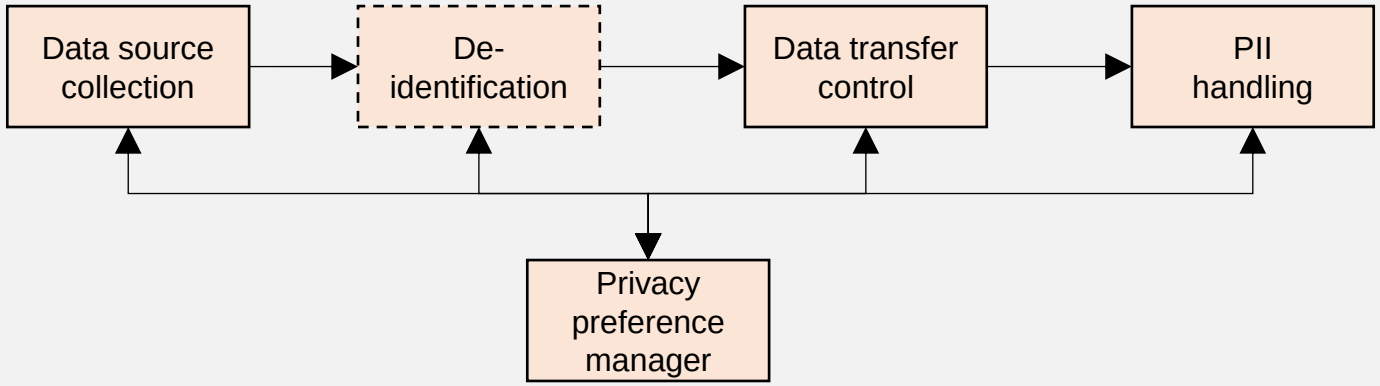


Example of 27556 Privacy Preference management

Functional Viewpoint



Ecosystem Viewpoint



What is next?

- ISO/IEC JTC1 SG6 « Meta Reference Architecture » Workshop Montreal 20-22 August
- Will gather standard editors on important standards
  - **Architecture (system, cloud, big data, IoT, smart city)**
  - **Cross cutting concern (security, privacy, safety, trust…)**
  - **Governance and continuous improvement**
- Objective
  - **Reach common understanding**
  - **Define shape of convergent standards**
  - **Define roadmap**

Privacy engineering standards

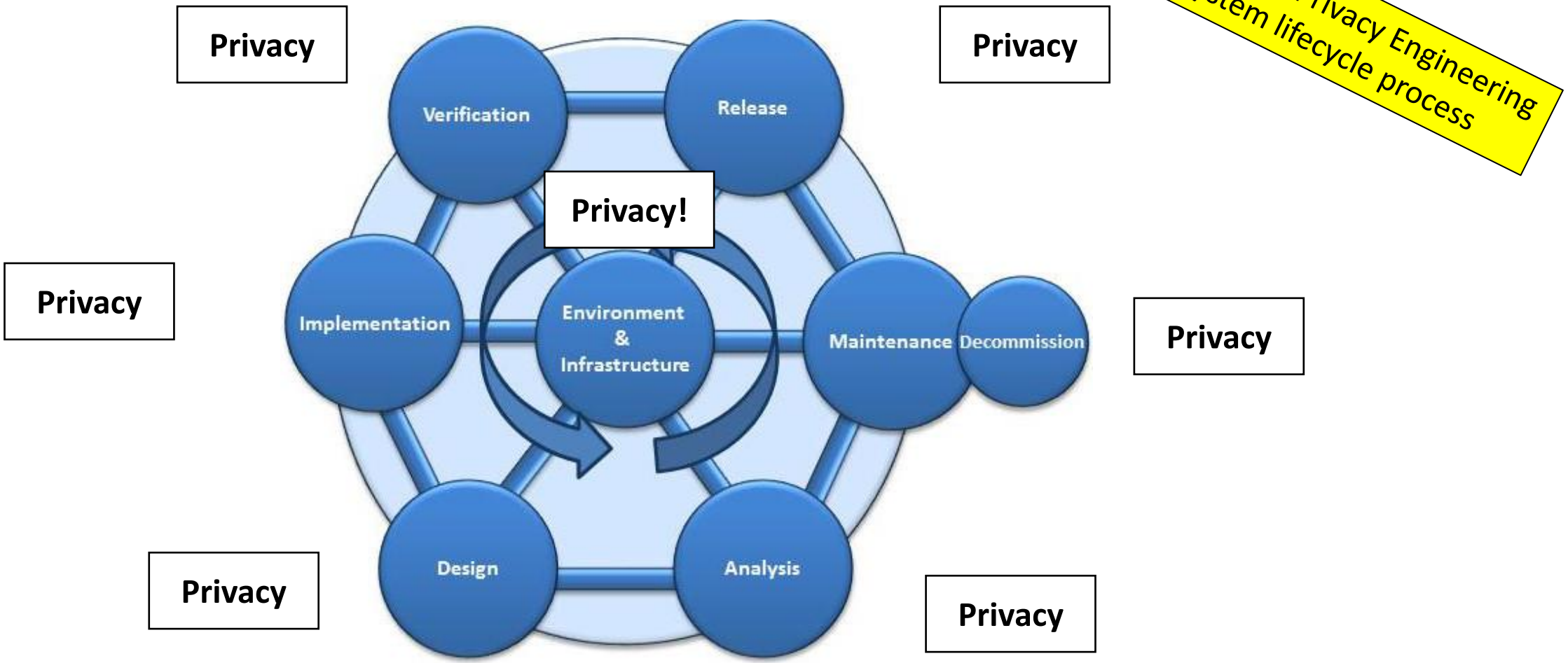
New standards in the pipe

Current work

Principles	ISO 37100	Privacy-by-design for consumer goods and services	Pending
	ISO/IEC 29100	Privacy framework	Published (free)
Mechanism	ISO/IEC 20889	Data de-identification terminology and classification of techniques	Published
	ISO/IEC 29184	Online privacy notices and consent	Pending
Organisation practice	ISO/IEC 27550	Privacy engineering for system life cycle processes	2019
	ISO/IEC 27552	Privacy information management -- requirements and guidelines	2019
	ISO/IEC 27555	Establishing a PII deletion concept in organisations	Pending
	ISO/IEC 27556	User-centric framework for privacy preference management	Pending
	ISO/IEC 29134	Privacy impact assessment guidelines	Published
	ISO/IEC 29151	Code of practice for PII protection	Published
	ISO/IEC 29190	Privacy capability assessment model	Published
Ecosystem practice	ISO/IEC 20547-4	Big data security and privacy	Pending
	ISO/IEC 27030	Security and privacy guidelines for IoT	Pending
	ISO/IEC 27570	Privacy guidelines for smart cities	Pending
	ISO/IEC 23751	Data sharing agreements	Pending

Privacy Engineering: Integrating privacy concerns

ISO/IEC 27550 Privacy Engineering for system lifecycle process

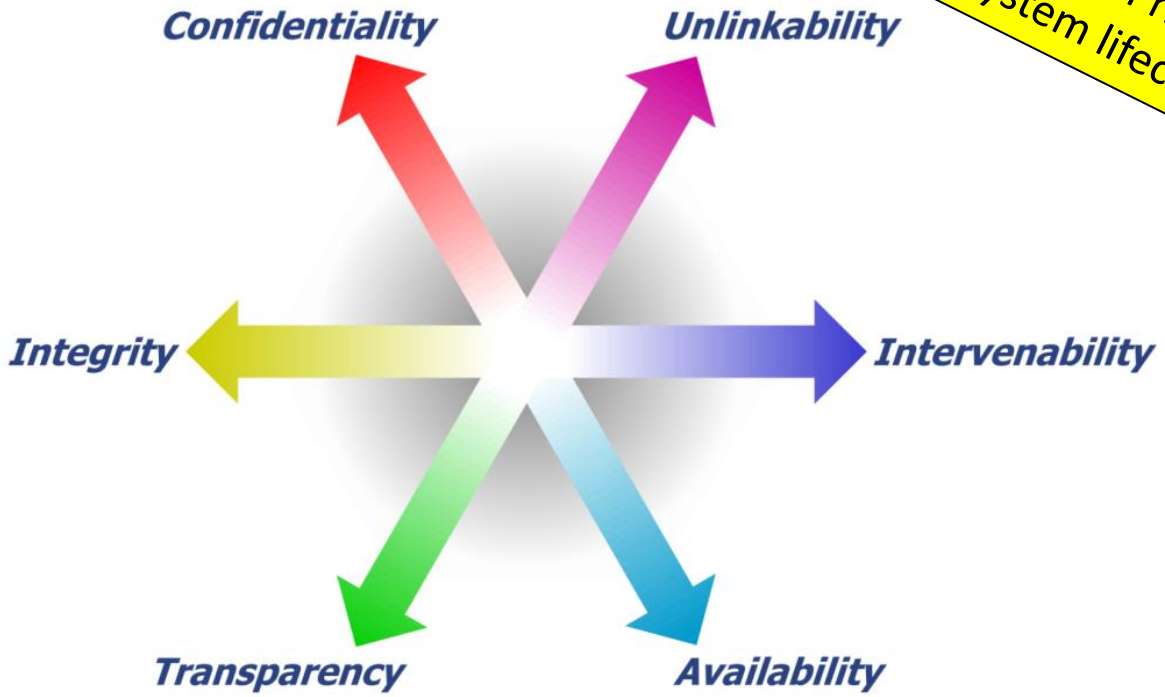


Beyond CIA

ISO/IEC 27550 Privacy Engineering for system lifecycle process

- Confidentiality
- Integrity
- Availability

- Unlinkability
- Intervenability
- Transparency



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

Privacy threats analysis: LINDDUN

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

	Property	Threat
Hard privacy	Unlinkability	Linkability
	Anonymity	Identifiability
	Plausible deniability	Non-repudiation
	Undetectability and unobservability	Detectability
Security	Confidentiality	Disclosure of information
Soft Privacy	Content awareness	Unawareness
	Policy and consent compliance	Non compliance

ISO/IEC 27550 Privacy Engineering for system lifecycle process

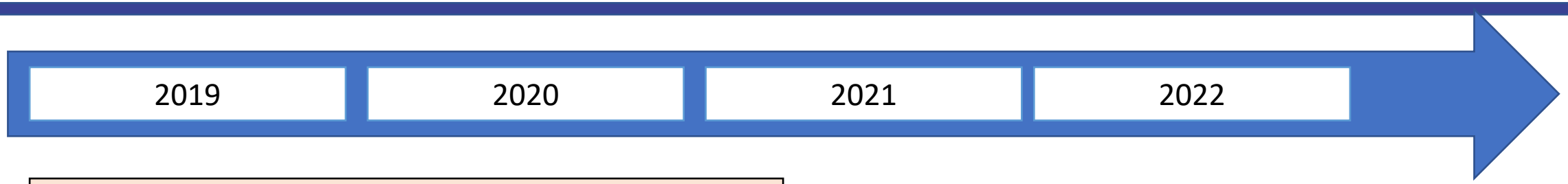
Design Strategy (J.H.Hoepman)

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

ISO/IEC 27550 Privacy Engineering for system lifecycle process

Design strategy		Description
Data oriented strategies	Minimize	Limit as much as possible the processing of PII
	Separate	Distribute or isolate personal data as much as possible, to prevent correlation
	Abstract	Limit as much as possible the detail in which personal data is processed, while still being useful
	Hide	Prevent PII to become public or known.
Process oriented strategies	Inform	Inform PII principals about the processing of PII
	Control	Provide PII principals control about the processing of their PII.
	Enforce	Commit to PII processing in a privacy friendly way, and enforce this
	Demonstrate	Demonstrate that PII is processed in a privacy friendly way.

What is next? New standards in the pipe
A possible scenario



ISO 31700
Privacy by design for consumer goods and services principles

SC27/WG5 study
Privacy engineering models

Privacy engineering
(IS)

27550 Edition 2
(from TR to IS)

Participation to Standardisation

❑Liaison category C with ISO/IEC JTC1/SC27/WG5

Sujet: Establishment for a category C Liaison between PRIPARE and JTC1/SC27/WG5
De : Blandine GARCIA <GARCIAB@iso.org>
Date : 21/10/2014 00:29
Pour : Antonio kung <antonio.kung@trialog.com>
Copie à : Passia Krystyna Mrs <krystyna.passia@din.de>

Dear Mr. Kung,

We are pleased to announce you the establishment of the Liaison C with JTC1/SC27/WG5 and your registration in our Global Directory, as Liaison officer.

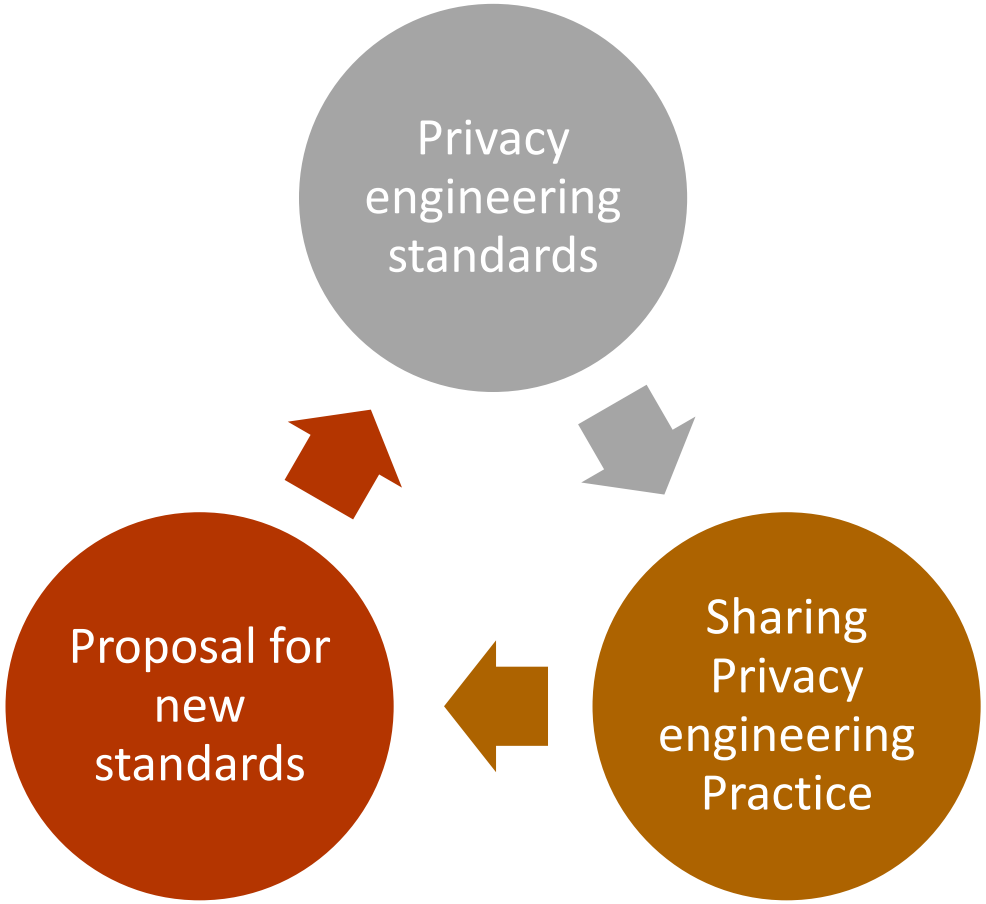
Best regards,

Mrs Blandine GARCIA
ISO/IEC Information Technology Task Force
ISO/IEC Project Manager
Standard Department

IPEN in the Loop: Recommendation for best practice sharing on privacy engineering

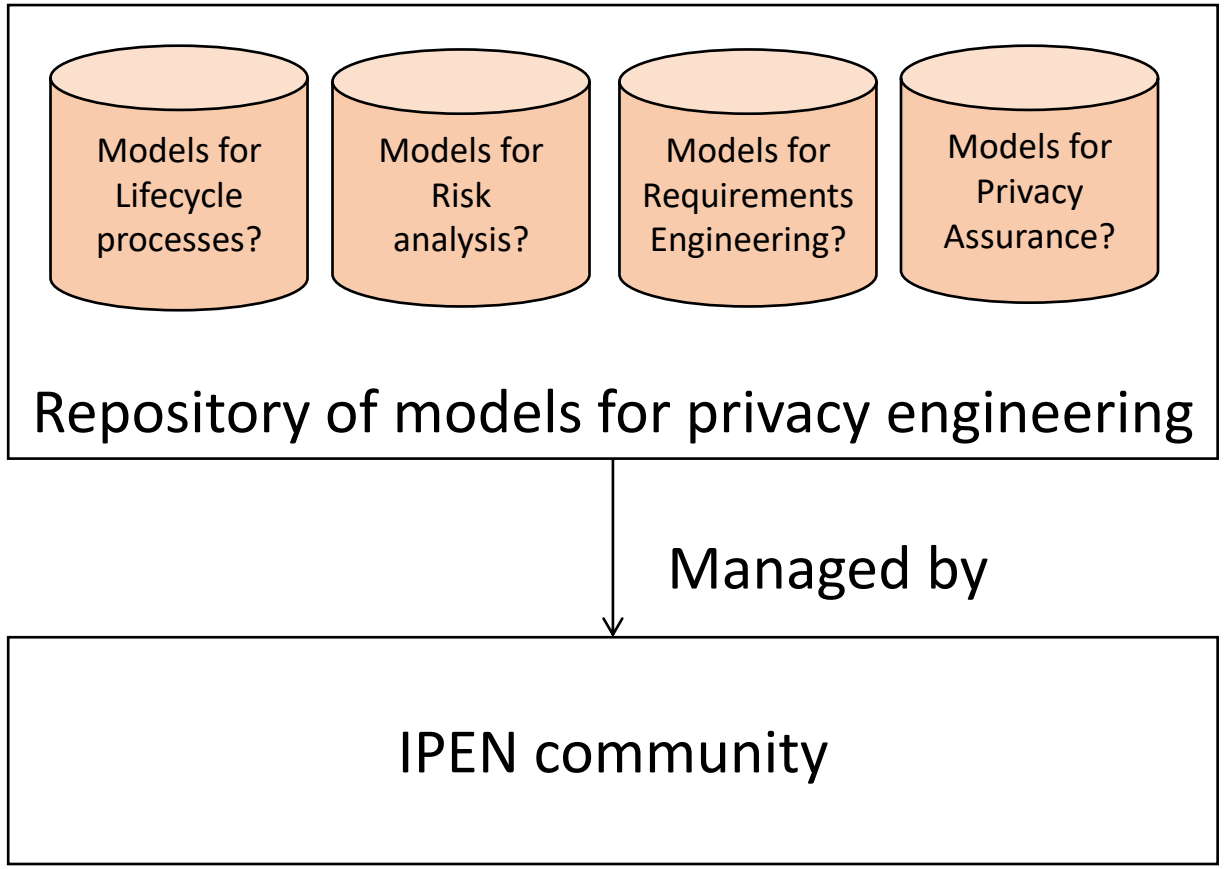
Creating a Virtuous Cycle

- Best practice sharing on privacy engineering will drive new standards
- Conditions
  - **Community participation**
    - e.g. H2020 cluster of GDPR projects
  - **Repository operation**
  - **Content**
    - Textual information (use case like)
    - Models
  - **Management**
    - Editorial and acceptance process



PDP4E Contribution to Best Practice Sharing

- Models for privacy engineering
  - IPR free
  - Guidelines for use
- Possible contributions
  - Use case for smart grid big data
  - Use case connected vehicles (C-ITS)



Question?

antonio.kung@trialog.com

www.trialog.com