ISO/TC 268/SC 1
Smart community infrastructures

Email of secretary: h_yoshida@jsa.or.jp
Secretariat: JISC (Japan)

ISO/IEC TS 27570, Privacy Guidelines for Smart Cities

Document type: Other meeting document

Date of document: 2019-04-30

Expected action: INFO

Background: ISO/TC 268/SC 1 Plenary meeting was held on 11th of April in Paris, France. In this meeting, as the liason report of JTC 1/SC 27/WG 5 (Identity management and privacy technologies), the presentation concerning ISO/IEC TS 27570 * was made by Mr. Antonio Kung, the one of the Project Leader of ISO/IEC TS 27570. This document is the presentation material.
* ISO/IEC TS 27570, Information Technology -- Security Techniques -- Privacy guidelines for Smart Cities

Committee URL: https://isotc.iso.org/livelink/livelink/open/tc268sc1

ISO/IEC TS 27570 Privacy Guidelines for Smart Cities

TC268/SC1/WG4 Liaison Presentation

Antonio Kung, Editor ISO/IEC 27570

Context

- JTC1/SC27 Security techniques
  - WG1 Information security management systems
  - Cryptography and security mechanisms
  - Security evaluation, testing and specification
  - Security controls and serivces
  - Identity management and privacy techniques
- Privacy for smart cities Study period
  - October 2015 - First Study period (18 months) initiated by India
  - June 2017 – Second Study period (6 months) Initiated by France further to contribution from JTC1/WG11 smart cities
- Privacy guidelines for smart cities ISO/IEC 27570 TS
  - Editors
    - Antonio Kung – France
    - Heung Youl Youm – Korea
  - 20 June 2018 – Registration – 1st WD
  - October 2018 – 2nd WD
  - April 2019 – 2nd WD disposition of comments

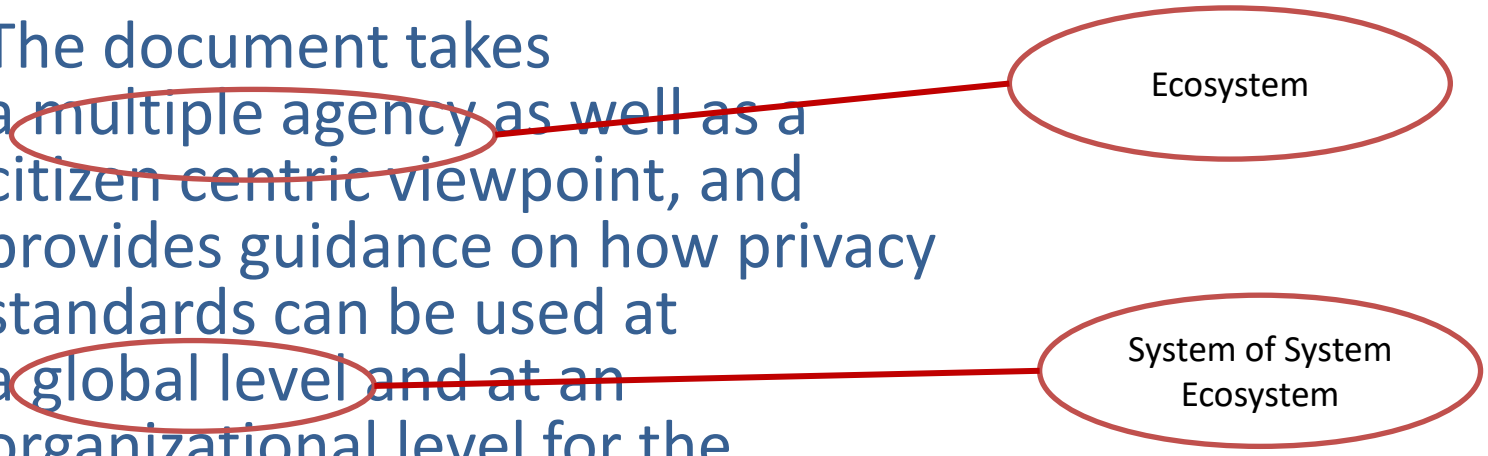
ISO/IEC 27570 Timeline

- 4 April 2019 – 2nd WD disposition of comments
- 20 May 2019 – 1st CD - PDTS

Stage	Version	Description	Target date	Limit date	Started
10.00	1	Proposal for new project registered			2017-12-04
10.20	1	New project ballot initiated	2017-12-04		2017-12-04
10.60	1	Close of voting	2018-02-26		2018-02-28
10.99	1	New project approved			2018-06-20
20.00	1	New project registered in TC/SC work programme			2018-06-20
20.20	1	Working draft (WD) study initiated			2018-07-06
20.60	1	Close of comment period			2018-08-31
20.20	2	Working draft (WD) study initiated			2018-11-06
20.60	**2**	**Close of comment period**	**2019-02-24**		**2019-02-25**
30.00		Committee draft (CD) registered	2019-04-01		
50.00		Final text received or FDIS registered for formal approval	2020-09-01		
60.60		International Standard published	2020-12-01	2021-06-20	

Reminder: Scope

- The document takes a multiple agency as well as a citizen centric viewpoint, and provides guidance on how privacy standards can be used at a global level and at an organizational level for the benefit of citizens.
- This document is applicable to all types and sizes of organizations, including public and private companies, government entities, and not-for-profit organizations that provide services in smart city environments



Presentation of 2nd Draft

Smart Cities experts

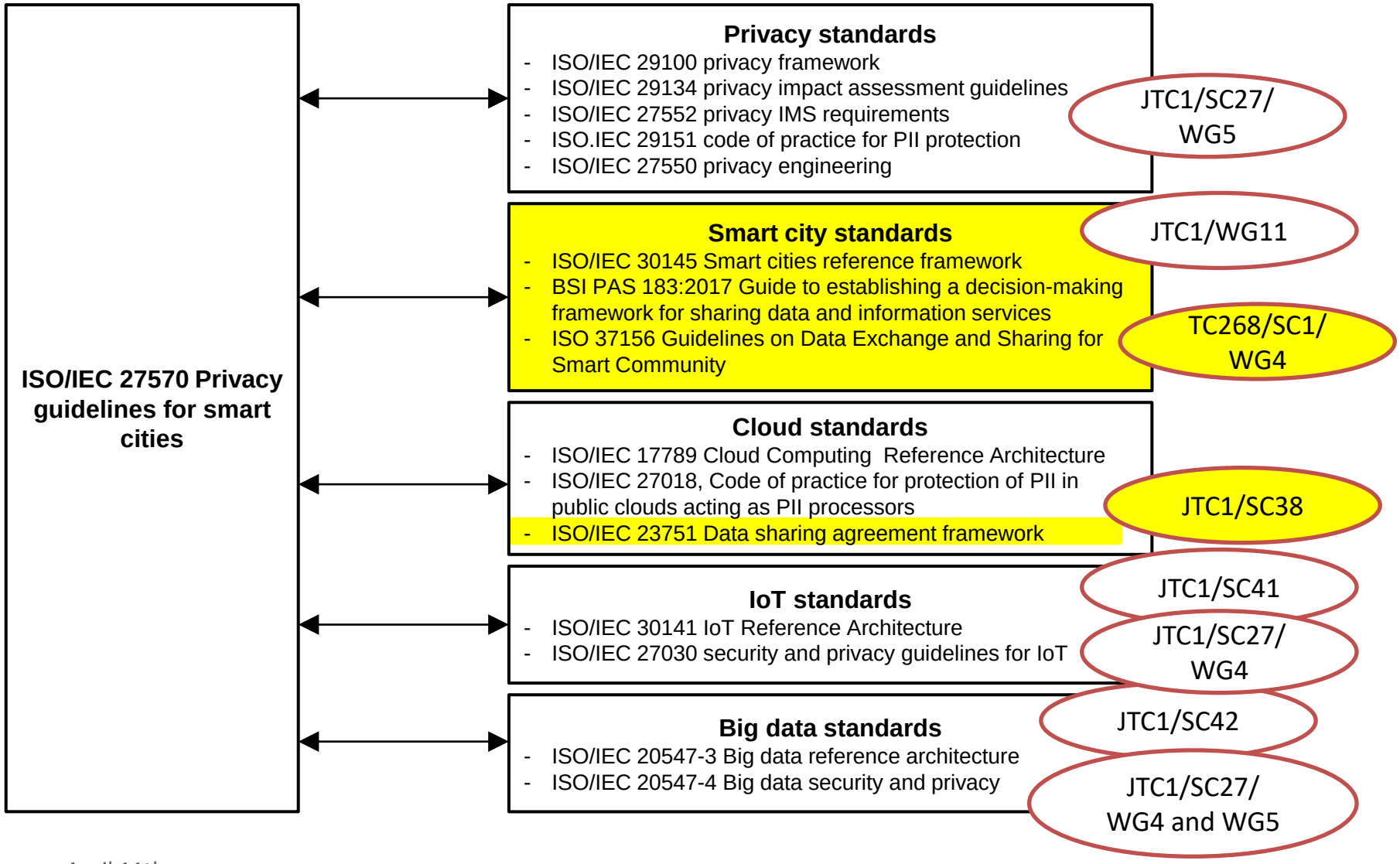
Smart Cities experts

SC27 experts

SC27 and smart cities experts

SC27, SC38, smart cities experts

Need to integrate privacy standards with other standards



Presentation of 2nd Draft

Smart Cities experts

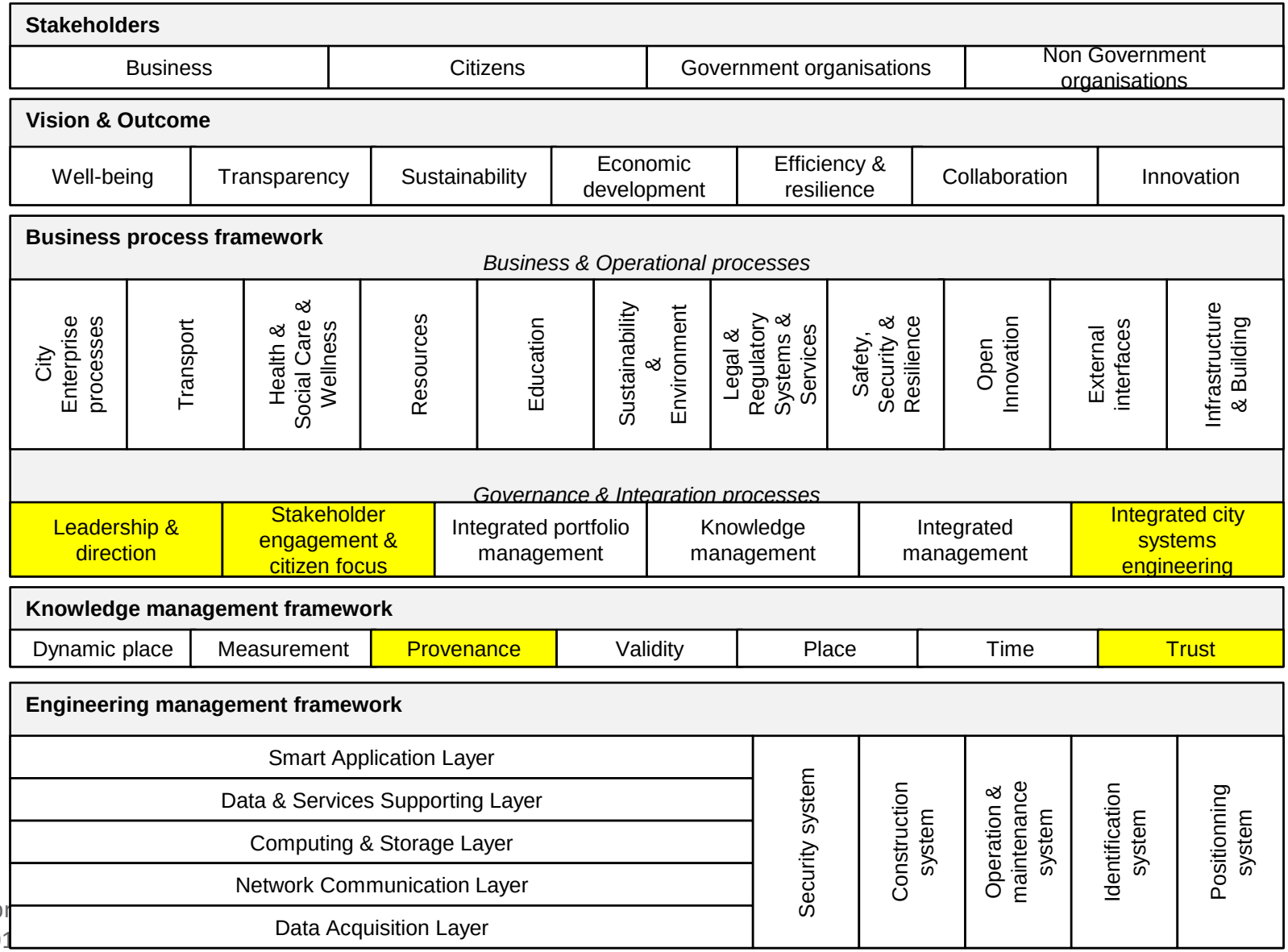
Smart Cities experts

SC27 experts

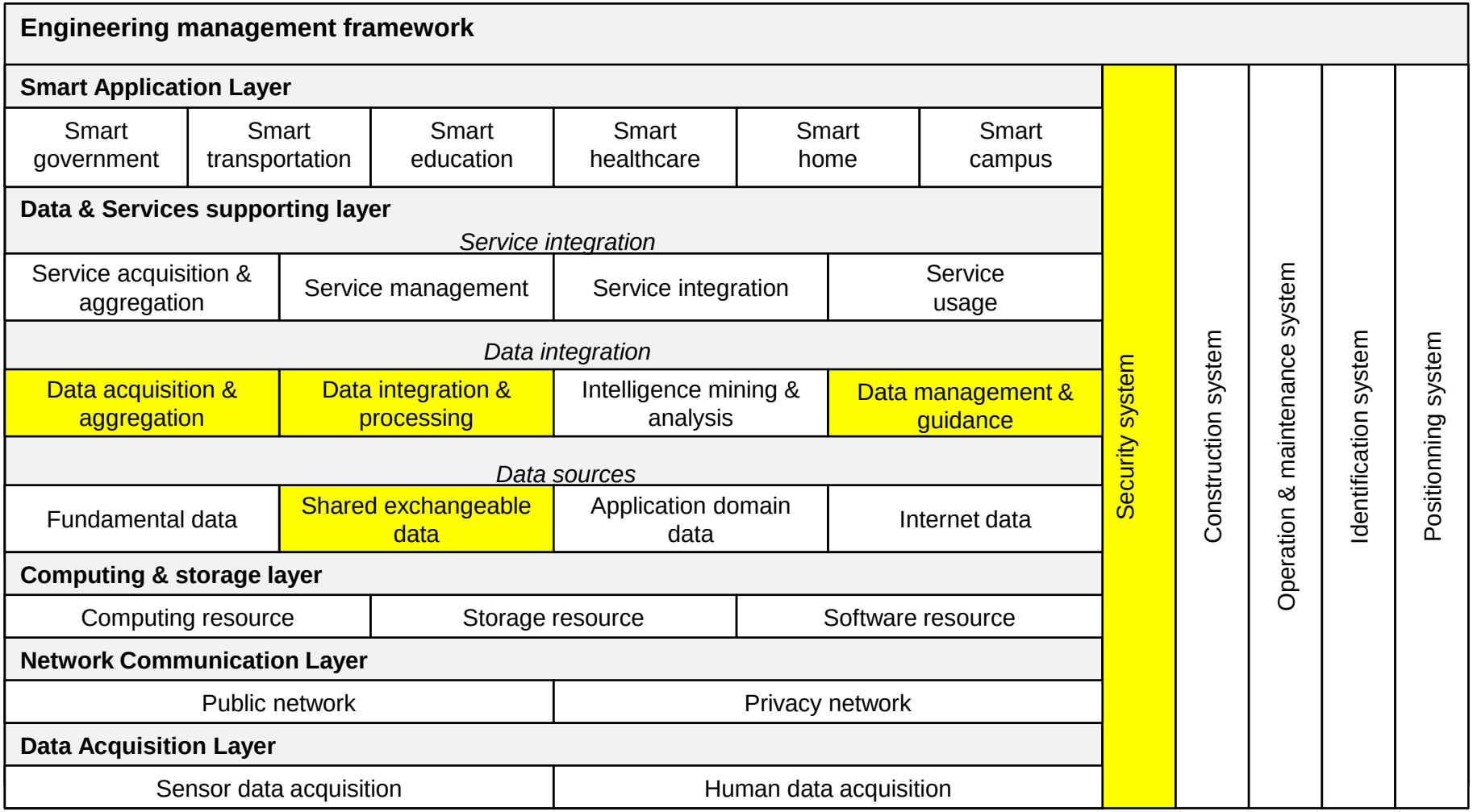
SC27 and smart cities experts

SC27, SC38, smart cities experts

Smart cities: use 30145 Smart cities ICT reference framework



Smart cities: use 30145 Smart cities ICT reference framework



Presentation of 2nd Draft

Smart Cities experts

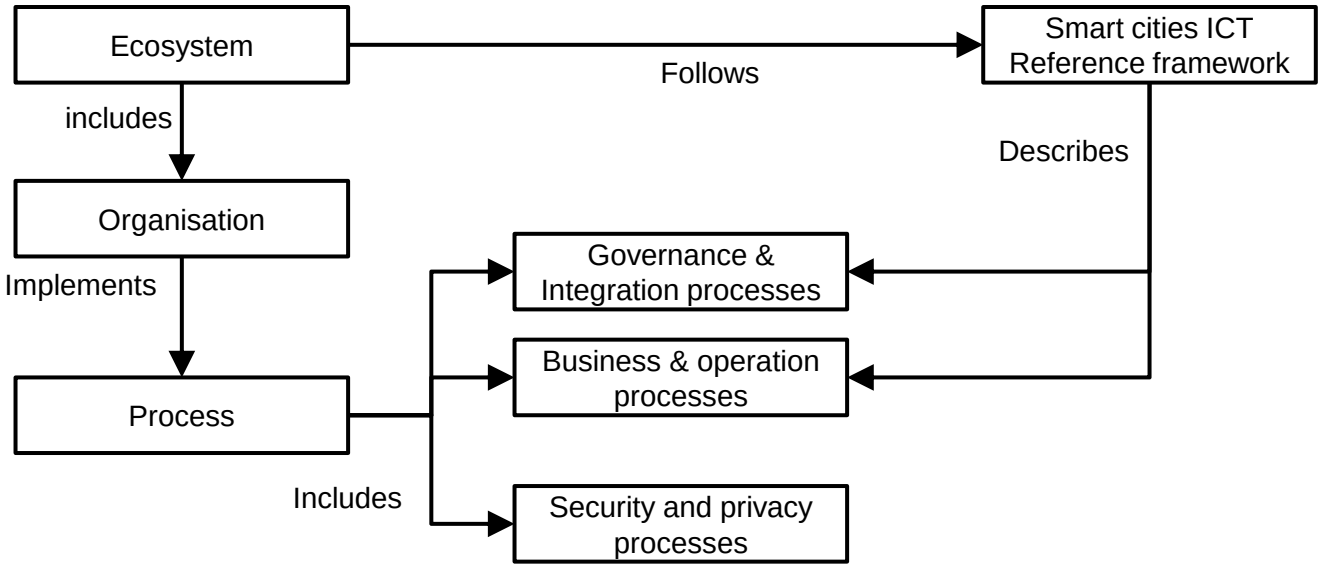
Smart Cities experts

SC27 experts

SC27 and smart cities experts

SC27, SC38, smart cities experts

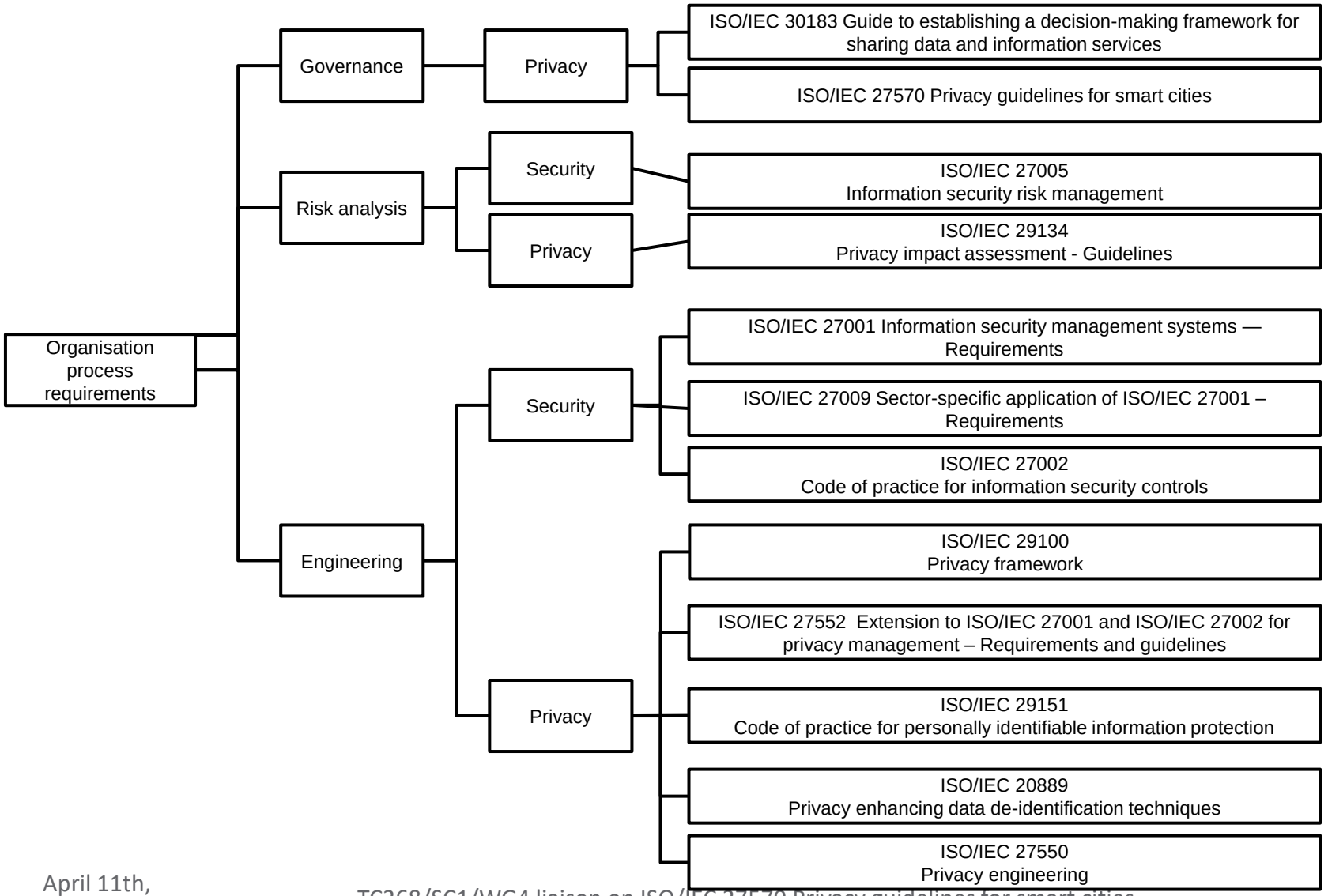
Smart City Ecosystems



Requirements on ecosystems

	Example of Vulnerabilities
Governance chain requirements	Smart city is not able to track all PII controllers or PII processors For instance, a smart city is not able to identify the PII controllers or PII processors that caused a breach.
	Smart city is not able to enforce privacy policies in the governance chain
Supply chain requirements	Supplier provides an ICT technology component that includes privacy controls that are not properly implemented Privacy impact assessments made by PII controllers or PII processors are subsequently incorrect.
	PII controllers or PII processors rely on suppliers of components that do not support some desired privacy controls.
Data sharing chain requirements	Lack of awareness from stakeholder in the data sharing chain of its obligations.
	Wrong assessment from a stakeholder that it is not a PII controller or PII processor For instance publishing open data that is not properly anonymized, or combining two datasets which do not contain PII into a dataset which contains PII.

Standards for smart cities



Presentation of 2nd Draft

Smart Cities experts

Smart Cities experts

SC27 experts

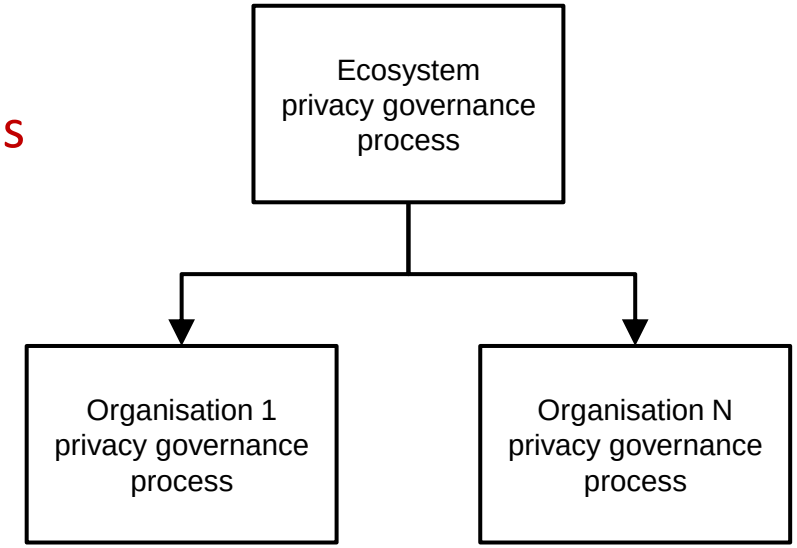
SC27 and smart cities experts

SC27, SC38, smart cities experts

Governance process

Must be consistent with standards on governance

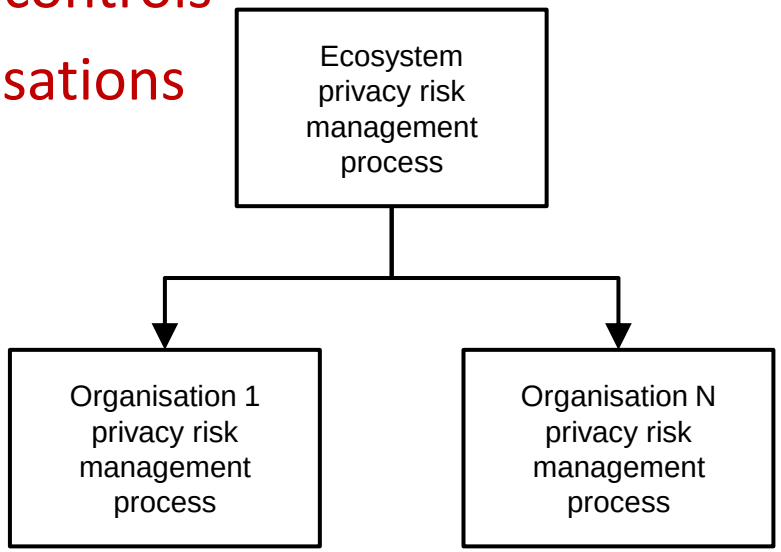
- Description of activities
  - establishment of privacy policies
  - monitoring of their implementation in smart city service
- Guidelines for ecosystem coordination
  - rules and policies of for chain of privacy governance;
  - specify supervision requirements
  - Specify supervision process
  - Identify supervised organizations
  - apply the supervision process
- Guidelines for organizations
  - Enrolment
  - Implement of rules and policies
  - Apply supervision process



Risk management process

Must be consistent with standards on risk management

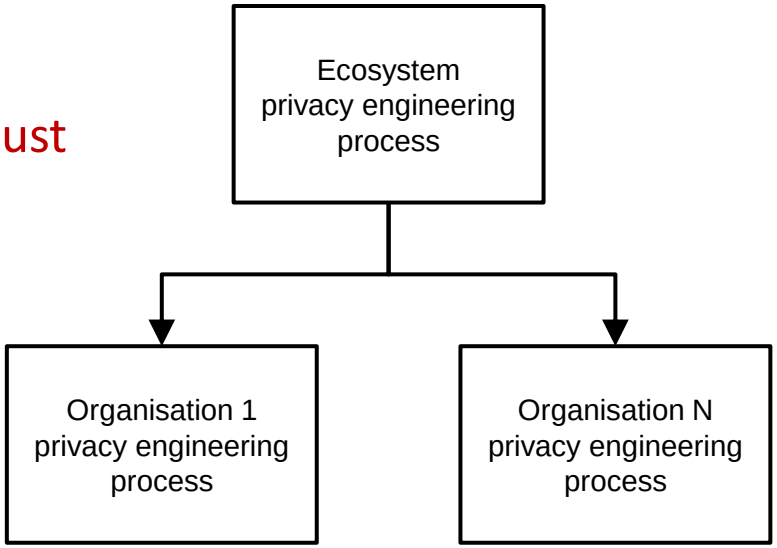
- Description of activities
  - System of system risk management
  - System-level risk management
- Guidelines for ecosystem coordination
  - SoS risk analysis leading to SoS controls
  - Mapping SoS controls to organisations
- Guidelines for organizations
  - System risk analysis leading to system controls
  - Implement controls
  - Apply risk mgt process



Engineering process

Must be consistent with privacy engineering standards

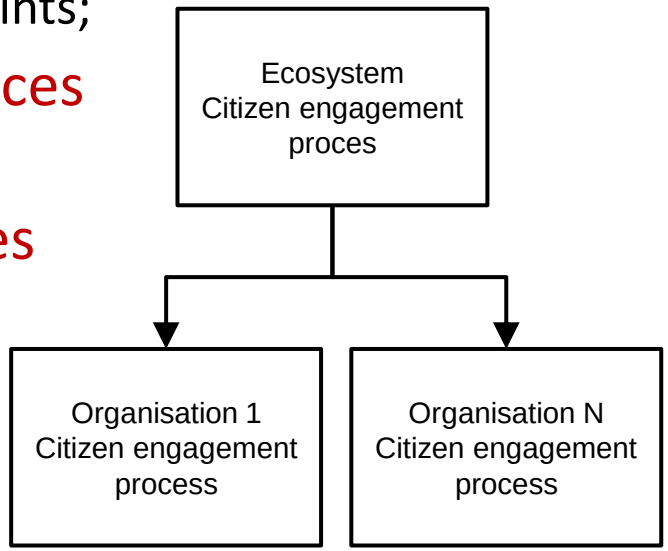
- Description of activities
  - activities for privacy related to the lifecycle of a smart city service
- Guidelines for ecosystem coordination
  - identify data processing operational requirements
  - identify security and privacy requirements
  - identify activities where privacy must be taken into account;
  - map activities to the organizations of the ecosystem;
  - establish coordination schemes
- Guidelines for organizations
  - identify activities where privacy must be taken into account;
  - identify the controls to be implemented
  - establish the lifecycle process in accordance with coordination scheme



Citizen Engagement process

Must be consistent with citizen engagement standards

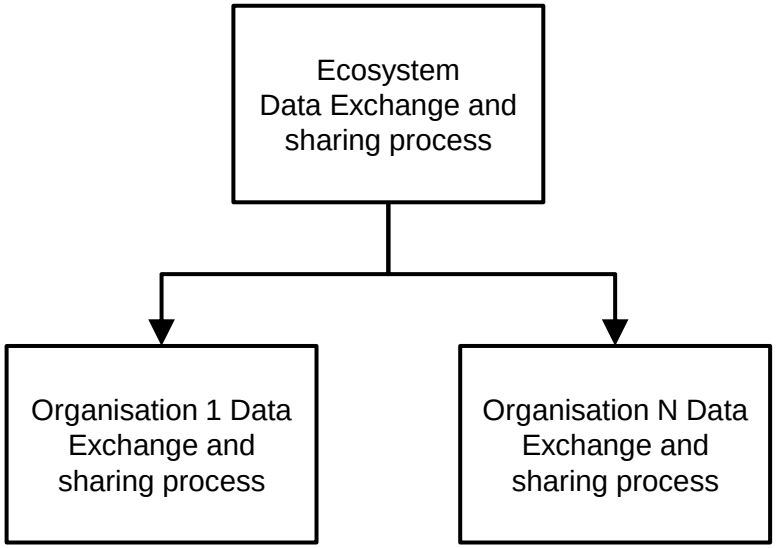
- Description of activities
  - concertation with smart city citizens
- Guidelines for ecosystem coordination
  - establish a citizen concertation process on privacy
  - establish a citizen interaction process
    - Information, enquiries and complaints;
  - Establish review process of services involving citizens
  - Periodic citizen review of services
  - Establish coordination schemes
- Guidelines for organizations
  - Apply concertation support activities



Data Exchange and sharing process

- Description of activities
  - Integration of privacy in data exchange and sharing
  - monitoring at smart city level
- Guidelines for ecosystem coordination
  - specify the privacy impact assessment and sharing agreement templates to use
  - establish security and privacy coordination schemes
    - measures for compliance, assurance and audit of practice.
- Guidelines for organizations
  - Use templates
  - carry out data exchange and sharing activities in accordance with coordination scheme.

Must be consistent with 37156 (TC268) and 23751 (JTC1/SC38)



Conclusion

- Request for a copy of current version of 37156
- Request for contribution
  - 2nd WD and 2nd WD Doc Available
- Interested experts can informally contact editor. informal contributions accepted before submission of 1st PDTS (May 20th)