Study Period Report

Privacy Engineering Framework (PEF)

Rapporteur : Antonio Kung
Co-rapporteur: Mathias Reinis

Outline

- Reminder on TOR
- Jaipur 2nd Call for Contribution
- Overview of Contributions
- Options for continuation
  - NWIP on TR Privacy Engineering
  - Others
- Discussion
- Conclusion

Reminder on TOR (Kuching)

- Taken into account
  - ISO/IEC 29100, 29101, 29134, 27034
  - ISO/IEC 42010 (instead of 42001), 15288, 12207
  - CNIL methodology for privacy risk management
  - NIST Interagency Report on Privacy Engineering (draft forthcoming)
  - PRIPARE project methodology
  - OASIS Privacy Management Reference Model and Privacy by Design Documentation for Software Engineers
  - EDPS Internet Privacy Engineering Network
  - MITRE Privacy Engineering Framework
  - Centre for Information Policy Leadership research on Privacy Risk Management
- Establish a Study Period to review the emerging field of privacy engineering starting in May 2015 and

Reminder on TOR (Kuching)

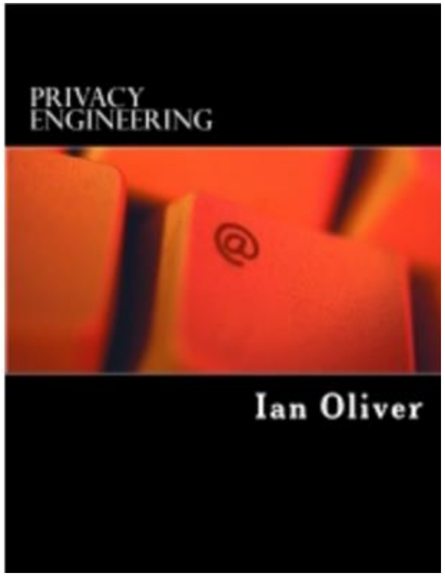
- task the rapporteurs of the Study Period
  - to review privacy engineering terms, definitions, methodologies, frameworks, objectives, and principles to develop a high-level description of the privacy engineering process (taking into account the existing spectrum of models from traditional to agile models);
  - to review the relationship between privacy engineering and other privacy, security, and risk management standards, as appropriate;
  - to identify possible improvements to existing privacy impact assessment and management standards;
  - to potentially provide (a) New Work Item Proposal(s) and/or other input material to the Work Group, depending on the outcome of this assessment.

Further Contributions Requested (Jaipur)

- Refine work on engineering
  - Requirements domain
  - Architecture roles and practice
  - Link with 15288
- Quality management
- Assurance
  - Taking into account assurance e.g. ISO 19608, 29190, Europrise privacy seals…
- Supplier's viewpoint
- Cultural influence / Different legal domains
- Further work on organisational support
- Further work on lifecycle support
  - Includes Consent
  - Existing methodologies (e.g. NIST, OASIS, LINDDUN, CNIL,…)
    - Principles VS Specifics
  - Link to existing standards (29101,29191, 29134, 29151, HL7)
  - Role of supplier
- Draft PEF
- WG5 Roadmap
- Consider other relevant aspects of WG5 (e.g. SP on privacy notice)

Contribution 1 (Japan)

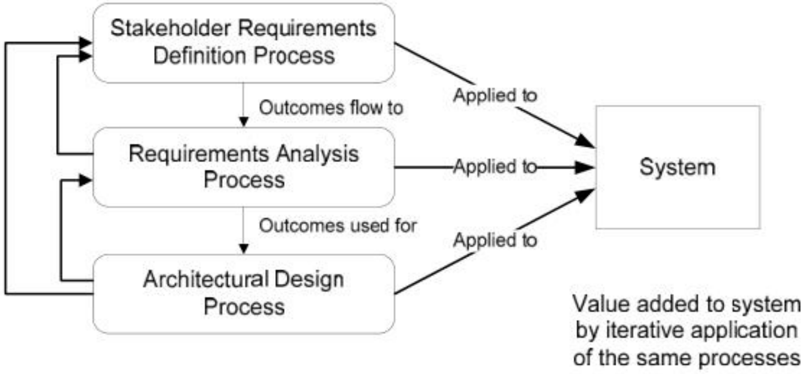
- Kouichi Ito
  - Reference: Ian Oliver, Privacy Engineering
  - Three requirements viewpoints
    - Security requirements: e.g. storage encryption
    - Information Type requirements: e.g. credit card information, personal ID or session ID
    - Personal data requirements: e.g. child protected by COPPA



Requirements Engineering
Need for viewpoints in body of knowledge

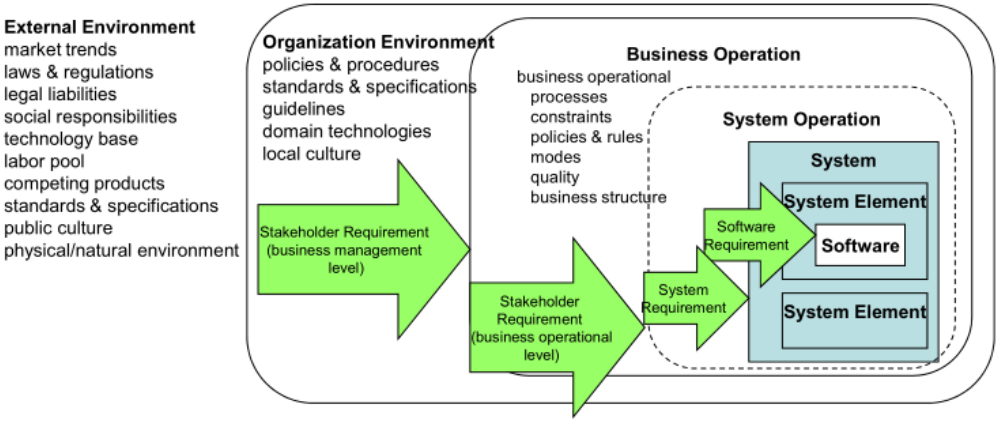
Contribution 2 (Pripare)

- Requirements Engineering in Privacy Engineering
  - Use ISO 29149 as a reference



Stakeholder Requirements Definition Process
Outcomes flow to
Requirements Analysis Process
Outcomes used for
Architectural Design Process
Applied to
Applied to
Applied to
System
Value added to system by iterative application of the same processes

Requirement Engineering Processes



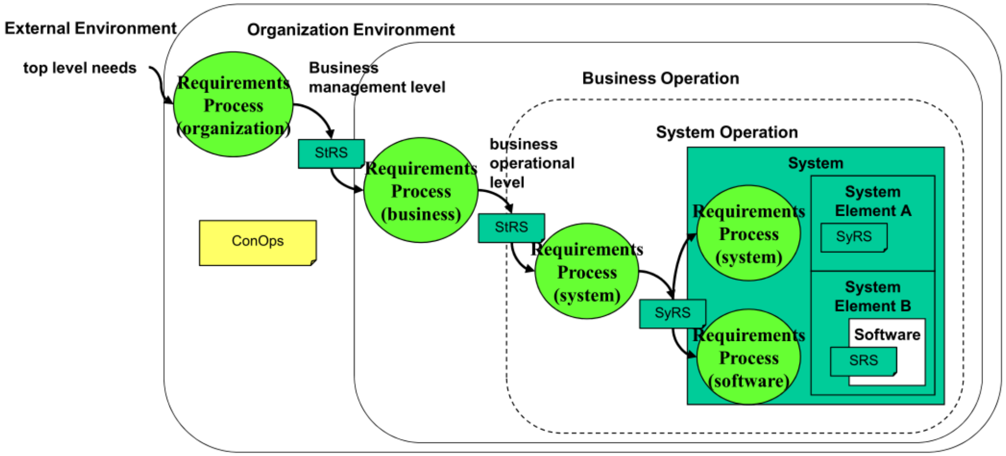
Requirement Scope in a Business Context

Using ISO 29149 or privacy engineering

Need for guidelines and viewpoints in body of knowledge

Contribution 2 (Pripare)

- Requirements Engineering in Privacy Engineering
  - Use ISO 29149 as a reference


External Environment
top level needs
Organization Environment
Requirements Process (organization)
Business management level
StRS
ConOps
Requirements Process (business)
Business Operation
business operational level
StRS
System Operation
Requirements Process (system)
SyRS
System
Requirements Process (system)
Requirements Process (software)
System Element A
SyRS
System Element B
Software
SRS

Requirement Scope in a Business Context

Using ISO 29149 for privacy engineering

Need for guidelines and viewpoints in body of knowledge

Contribution 2 (Pripare)

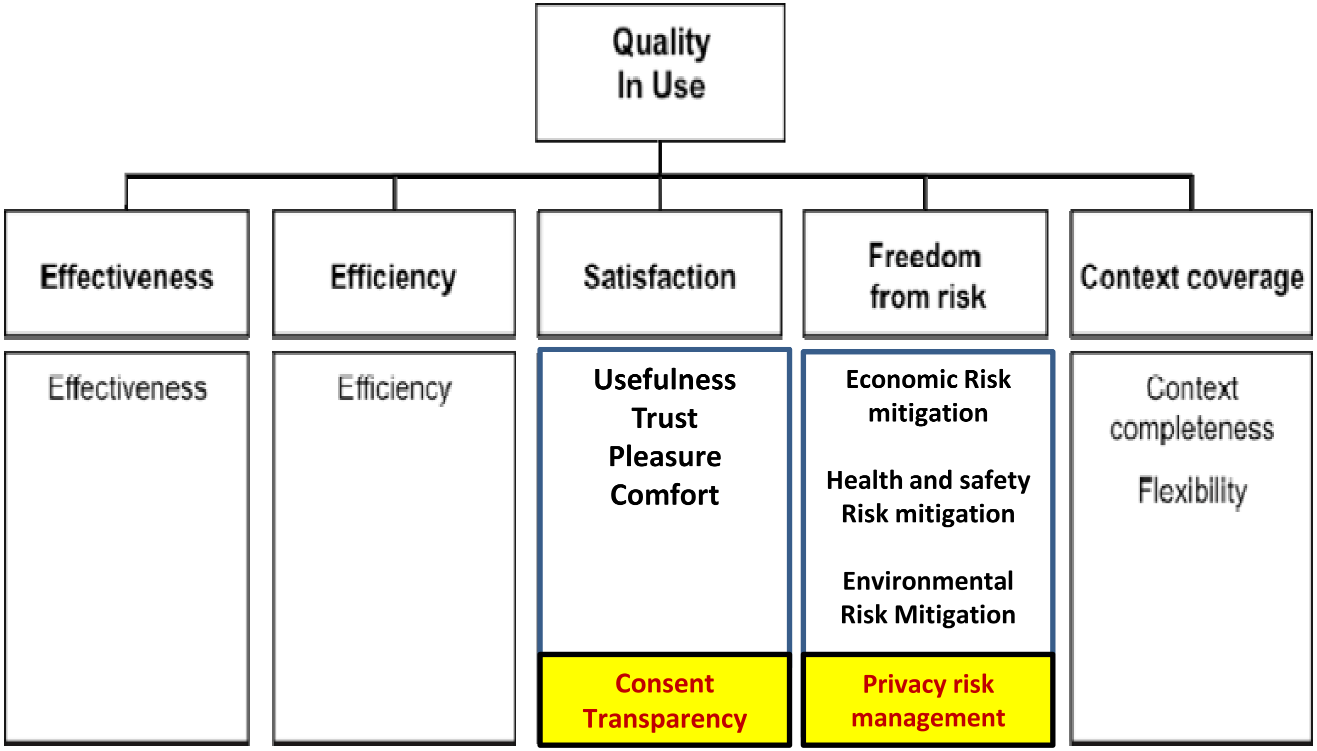
- Requirements Engineering in Privacy Engineering
  - Use ISO 19608 (Security techniques — Guidance for developing security and privacy functional requirements based on ISO/IEC 15408)
    - select and specify Security Functional Requirements or SFRs from ISO/IEC 15408-2 to protect PII
    - develop Privacy Functional Requirements or PFRs as extended components based on privacy principles defined in ISO/IEC 29100 through the paradigm described in ISO/IEC 15408-2

Usabling ISO19608 for privacy engineering

Need for guidelines and viewpoints in body of knowledge

Contribution 2 (Pripare)

- Quality Management in Privacy Engineering
  - ISO 25010 (Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE))



Quality In Use

Effectiveness: Effectiveness

Efficiency: Efficiency

Satisfaction: Usefulness, Trust, Pleasure, Comfort; Consent, Transparency

Freedom from risk: Economic Risk mitigation, Health and safety Risk mitigation, Environmental Risk Mitigation; Privacy risk management

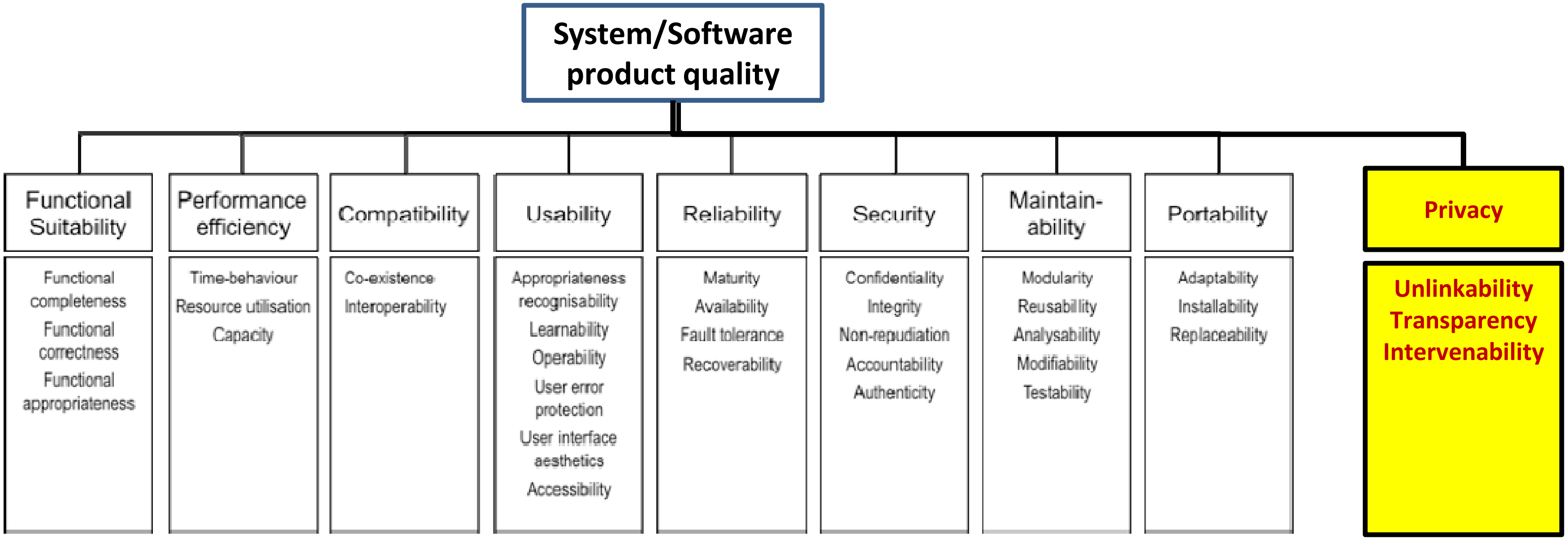
Context coverage: Context completeness, Flexibility

Model for Quality in use

Extension for Privacy engineering

Contribution 2 (Pripare)

- Quality Management in Privacy Engineering
  - ISO 25010 (Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE))



System/Software product quality

Functional Suitability	Performance efficiency	Compatibility	Usability	Reliability	Security	Maintain-ability	Portability	Privacy
Functional completeness Functional correctness Functional appropriateness	Time-behaviour Resource utilisation Capacity	Co-existence Interoperability	Appropriateness recognisability Learnability Operability User error protection User interface aesthetics Accessibility	Maturity Availability Fault tolerance Recoverability	Confidentiality Integrity Non-repudiation Accountability Authenticity	Modularity Reusability Analysability Modifiability Testability	Adaptability Installability Replaceability	Unlinkability Transparency Intervenability

Extension for Privacy engineering

Contribution 2 (Pripare)

- Quality Management in Privacy Engineering
  - ISO 25010 (Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE))
  - Defines following stakeholders
    - Primary user: person who interacts with the system to achieve the primary goals.
    - Secondary users who provide support
    - Indirect user: person who receives output, but does not interact with the system

    - Does not cover data subject

Extension for privacy engineering

Contribution 2 (Pripare)

- Architecture in Privacy Engineering
  - ISO 42020 (Architecture processes) is a standard in development, can be used as a reference
  - ISO 42030 (Architecture evaluation) is a standard in development, can be used as a reference provided ISO 25010 is extended
    - Must cover the data quality management for privacy engineering
  - It would be of interest to include specific quality attributes to privacy engineering
    - minimization, enforcement, accountability and modifiability

Usable for privacy engineering

Need for guidelines and viewpoints in body of knowledge

Contribution 2 (Pripare)

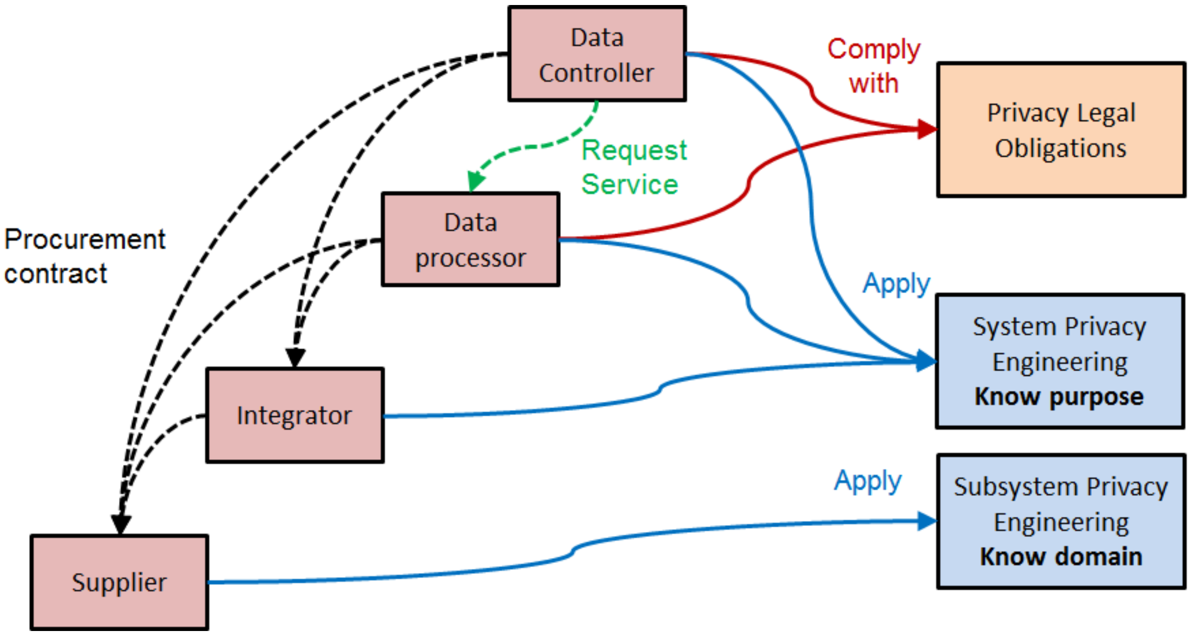
- Assurance in Privacy Engineering
  - ISO 19608 Security techniques — Guidance for developing security and privacy functional requirements based on ISO/IEC 15408
    - Not an standard for assurance but will help being prepare
  - ISO 29190 (Information technology – Security techniques -- Privacy capability assessment model
    - Could be used by organisation

Usable for privacy engineering

Need for guidelines and viewpoints in body of knowledge

Contribution 2 (Pripare)

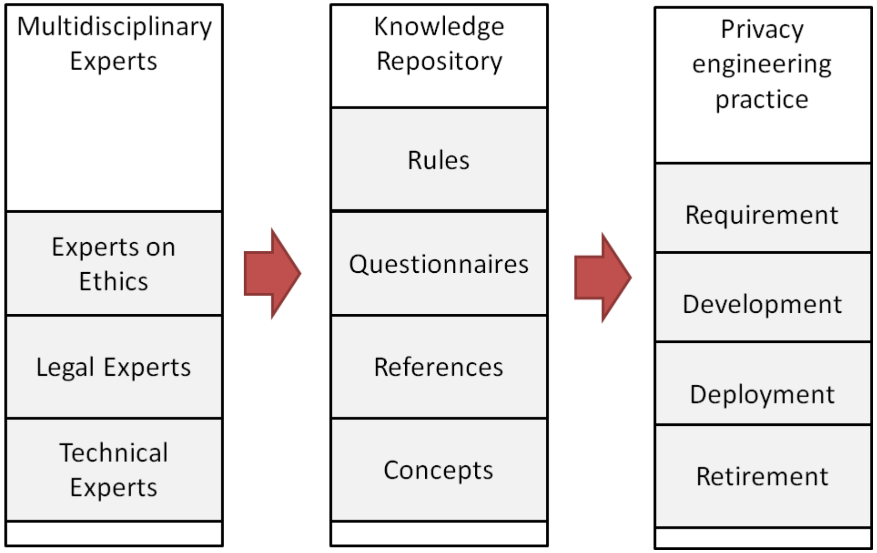
- Supplier Viewpoint


Data Controller
Comply with
Privacy Legal Obligations
Request Service
Data processor
Procurement contract
Apply
System Privacy Engineering **Know purpose**
Integrator
Apply
Subsystem Privacy Engineering **Know domain**
Supplier

Not covered in Standards?
Need for guidelines and viewpoints in body of knowledge

Contribution 2 (Pripare)

- Cultural and Legal Influence on Privacy Engineering
  - Need for multidisciplinary body of knowledge



Needed for privacy engineering / No input in standard?
Need for guidelines and viewpoints in body of knowledge

Contribution 2 (Pripare)

- Enterprise Size impact on Privacy Engineering
  - ISO 29110 set of standards (Software engineering — Lifecycle profiles for Very Small Entities (VSEs))

- From first period
  - ISO 12207 - Software Life Cycle Processes
  - ISO 15288 - System Life Cycle Processes

Usable for privacy engineering

Need for guidelines and viewpoints in body of knowledge

Conclusion

- Privacy Engineering can rely on many standards
  - Many can be just reused
  - Some might need extensions (e.g. 25010)
  - Supplier viewpoint missing
  - Multicultural viewpoint missing

- Needs for
  - understanding privacy engineering
  - guidelines and viewpoint in body of knowledge

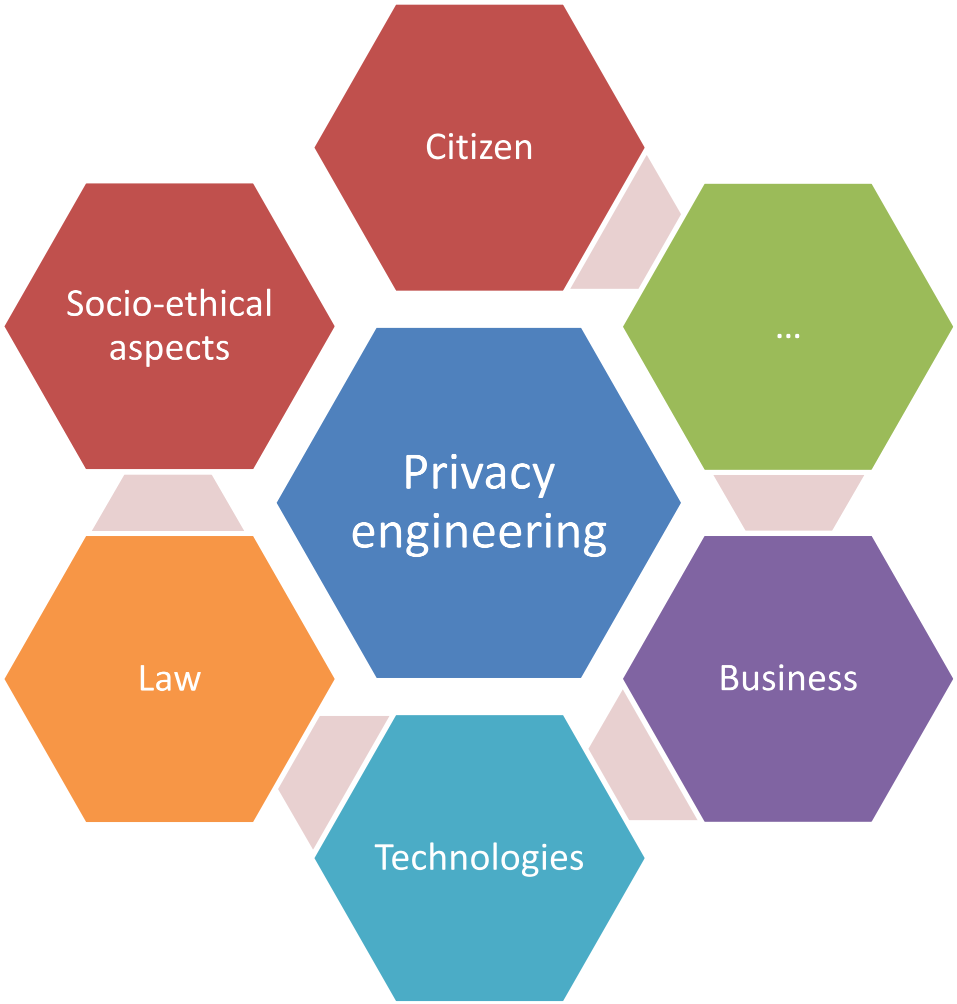
Proposed Options

- NWIP: TR for Privacy Engineering
- Others

Scope

- Explains discipline of privacy engineering / Explain how to engineer capabilities for privacy beyond security
  - Privacy engineering ecosystem and terminology
    - Engineering for privacy
    - Privacy engineering as subdiscipline of engineering
  - Definition of actors and roles in the engineering of systems processing personally identifiable information (PII),
  - Measurable outcomes
  - Considerations on engineering privacy safeguards, taking into account ISO/IEC 29100, ISO/IEC 29134 (draft) and ISO/IEC 29151 (draft)
- Provides guidelines and viewpoints taking into account existing standards, on different aspects such as
  - Requirement elicitation
  - Risk analysis
  - Design and Architecture process
  - Quality management, Assurance
  - Education and personnel certification programmes (in accordance to ISO/IEC 17024)
- Examples of practice in a number of application domains

Understanding Privacy Engineering Context



Citizen

…

Socio-ethical aspects

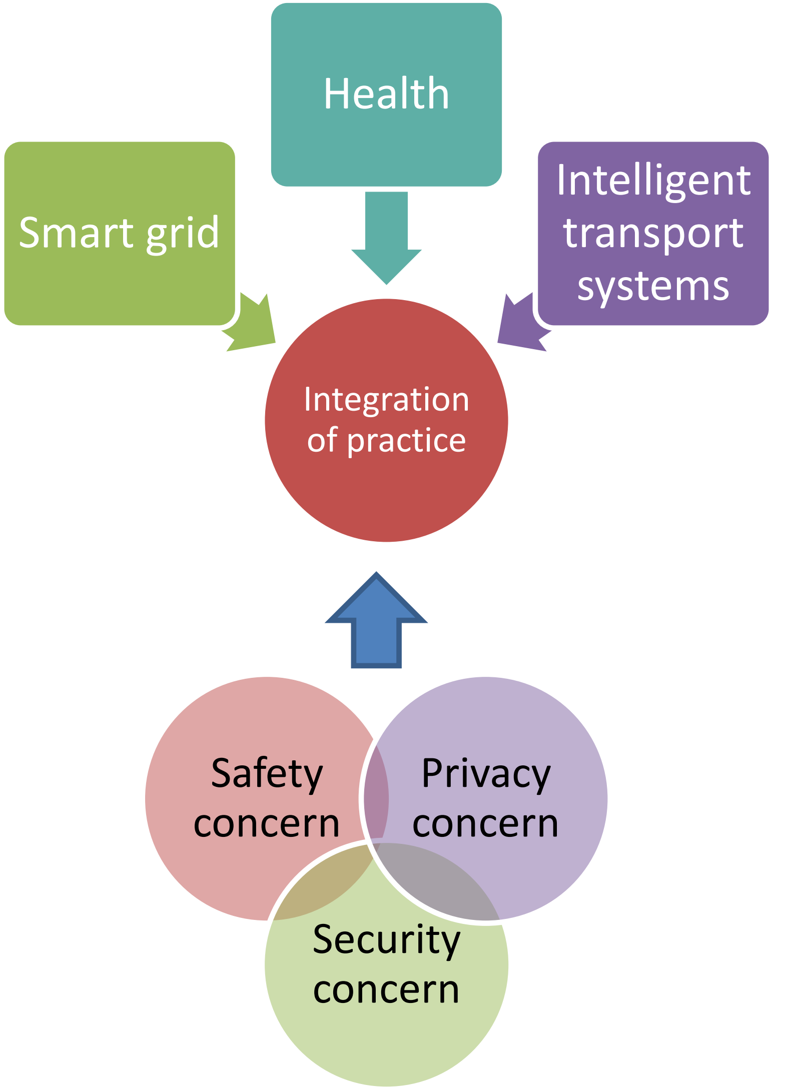
Privacy engineering

Law

Business

Technologies

Integrating Privacy Engineering



Health

Smart grid

Intelligent transport systems

Integration of practice

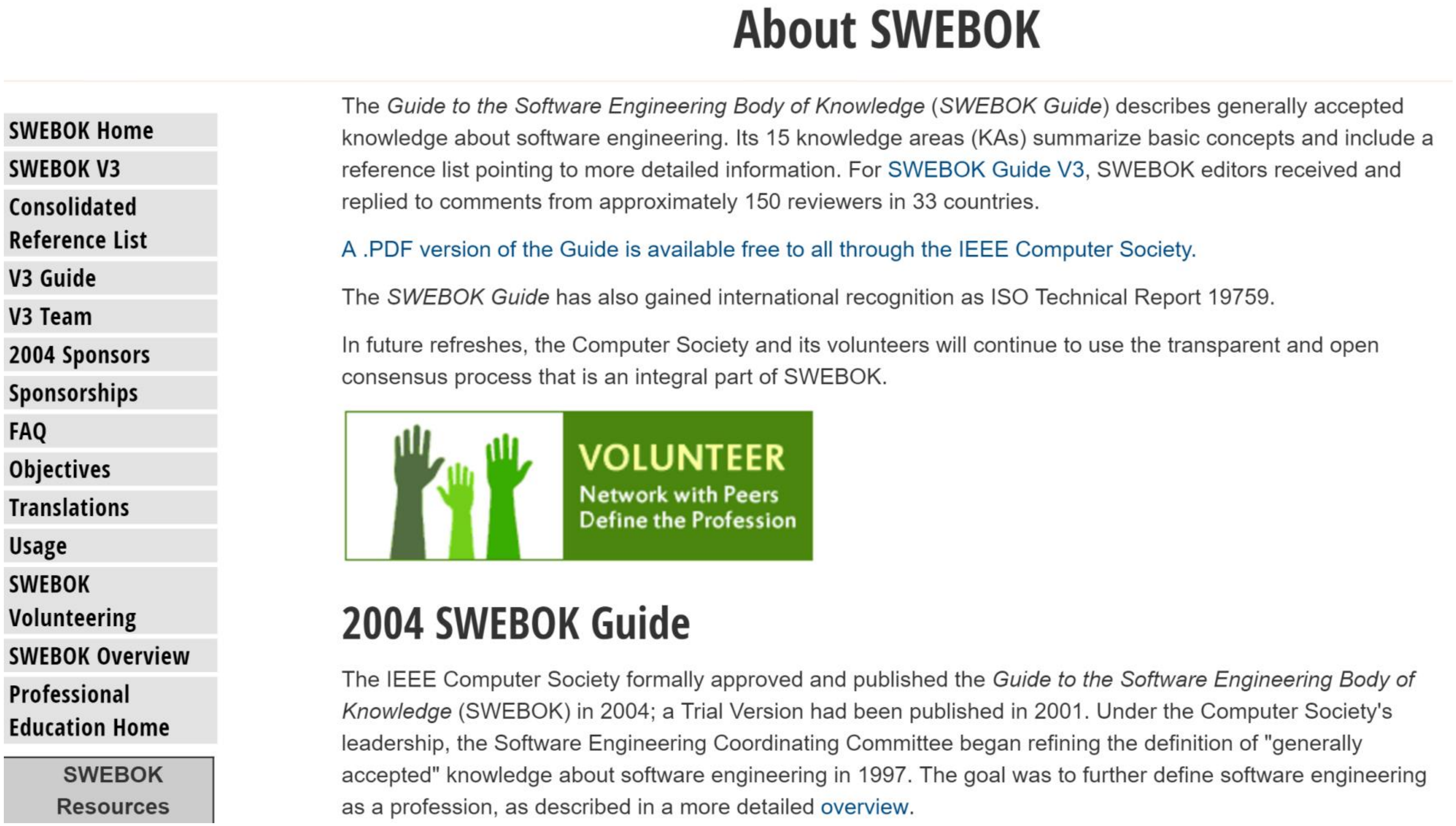
Safety concern

Privacy concern

Security concern

Towards Privacy Engineering Body of Knowledge?

- Example of SWEBOK (Software Engineering Body of Knowledge)
  - https://www.computer.org/web/swebok/index



About SWEBOK

- SWEBOK Home
- SWEBOK V3
- Consolidated Reference List
- V3 Guide
- V3 Team
- 2004 Sponsors
- Sponsorships
- FAQ
- Objectives
- Translations
- Usage
- SWEBOK Volunteering
- SWEBOK Overview
- Professional Education Home

SWEBOK Resources

The *Guide to the Software Engineering Body of Knowledge* (*SWEBOK Guide*) describes generally accepted knowledge about software engineering. Its 15 knowledge areas (KAs) summarize basic concepts and include a reference list pointing to more detailed information. For SWEBOK Guide V3, SWEBOK editors received and replied to comments from approximately 150 reviewers in 33 countries.

A .PDF version of the Guide is available free to all through the IEEE Computer Society.

The *SWEBOK Guide* has also gained international recognition as ISO Technical Report 19759.

In future refreshes, the Computer Society and its volunteers will continue to use the transparent and open consensus process that is an integral part of SWEBOK.

2004 SWEBOK Guide

The IEEE Computer Society formally approved and published the *Guide to the Software Engineering Body of Knowledge* (SWEBOK) in 2004; a Trial Version had been published in 2001. Under the Computer Society's leadership, the Software Engineering Coordinating Committee began refining the definition of "generally accepted" knowledge about software engineering in 1997. The goal was to further define software engineering as a profession, as described in a more detailed overview.

Discussion and Conclusion

Privacy Engineering

Discussion and Conclusions

- System engineering approach
  - Privacy engineering as a sub-discipline
  - Focus on (measurable) outcomes
  - Engineering: focus on the problems that the engineer has to solve
- Problem with term
  - Privacy engineering

Conclusion

- Concerns voice
  - Text book orientation
  - Unclarity of scope
- Next action
  - Straw poll
    - Two persons unfavourable to the NWIP because scope is unclear
    - One person favouring to follow a text book path with the current scope
    - Delegates from 5 countries supporting the NWIP
  - Attempt to rework the scope
    - Clarify
      - Problem to solve
      - Target audience
      - What is out of scope
    - Outline with some examples