PRIPARE Proposal for a ISO/IEC JTC 1/SC 27/WG 5 Study Period on

Privacy Engineering Framework

Proposing WG 5 Expert: Antonio Kung

Trialog

www.trialog.com

PRIPARE

PReparing **I**ndustry to **P**rivacy-by-design by supporting its **A**pplication in **RE**search

SEVENTH FRAMEWORK PROGRAMME

Outline

- PRIPARE
- Proposal for a privacy engineering study period
- Context
  - Privacy engineering
  - Examples of engineering terms and concepts
  - Examples of lifecycle terms and concepts
- Position w.r.t standardisation
- Proposed TOR

PRIPARE

- FP7 Support action on privacy-by-design
- France
  - Trialog, INRIA, American University in Paris
- Spain
  - ATOS, Gradiant, University P. Madrid
- UK
  - Trilateral research
- Germany
  - U.Ulm, Fraunhofer SIT
- Ireland
  - Watford TSSG
- Belgium
  - KU Leuven

Proposal

- Definition of a privacy engineering framework.
  - Takes into account on-going work related to privacy engineering and privacy-by design
  - Need to ensure convergence and alignment of terms and concepts
- Will pave the way to future standards for privacy engineering
- Proposing expert willing to act as rapporteur

Privacy Engineering

From Mitre Privacy Engineering Framework Presentation

A systematic, risk-driven process that operationalizes the Privacy by Design philosophical framework within IT systems …

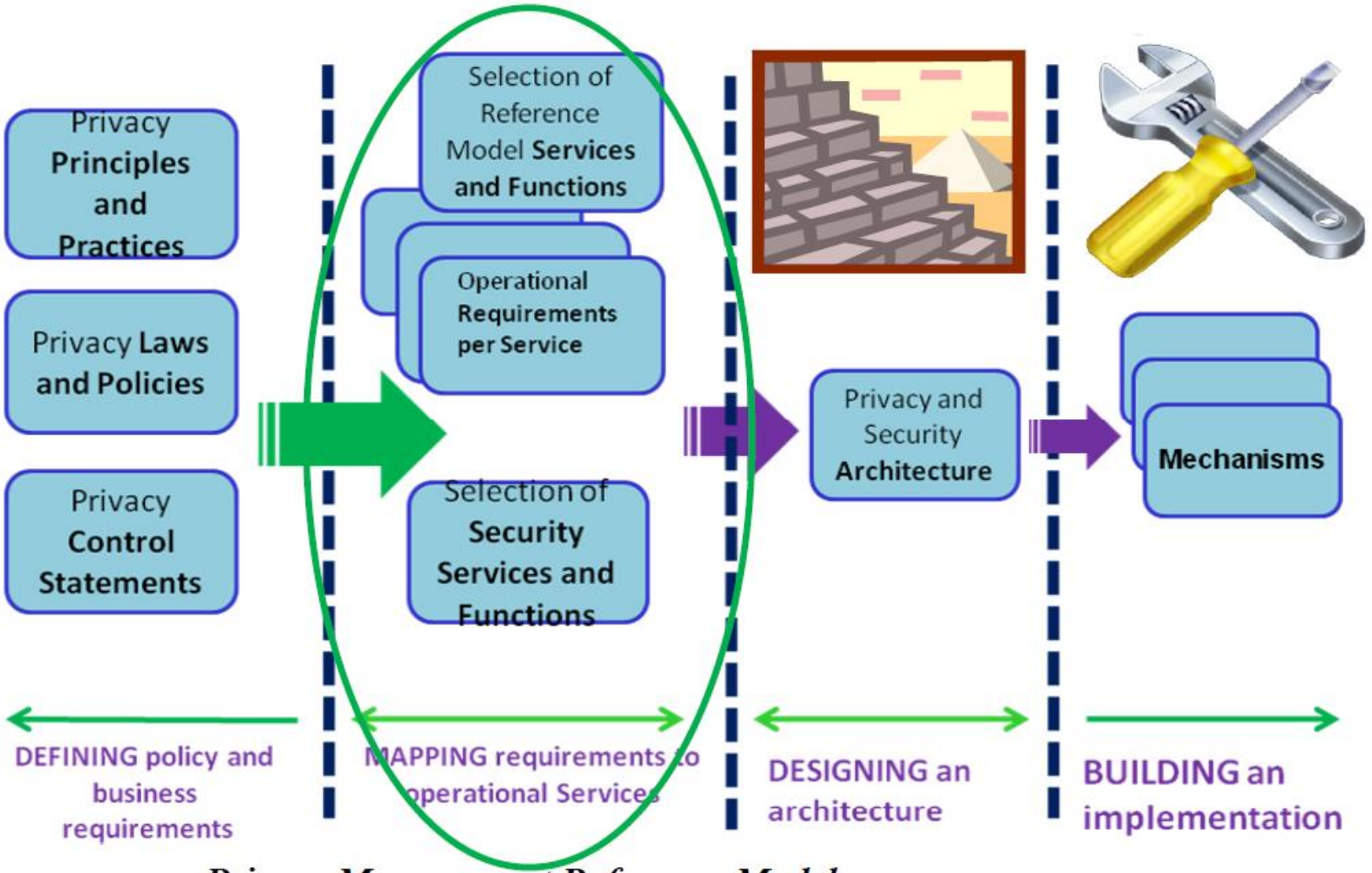
…Privacy is integrated into systems as part of the systems engineering process

Engineering Concepts and Terms

Terms in red could be part of a privacy enginering framework

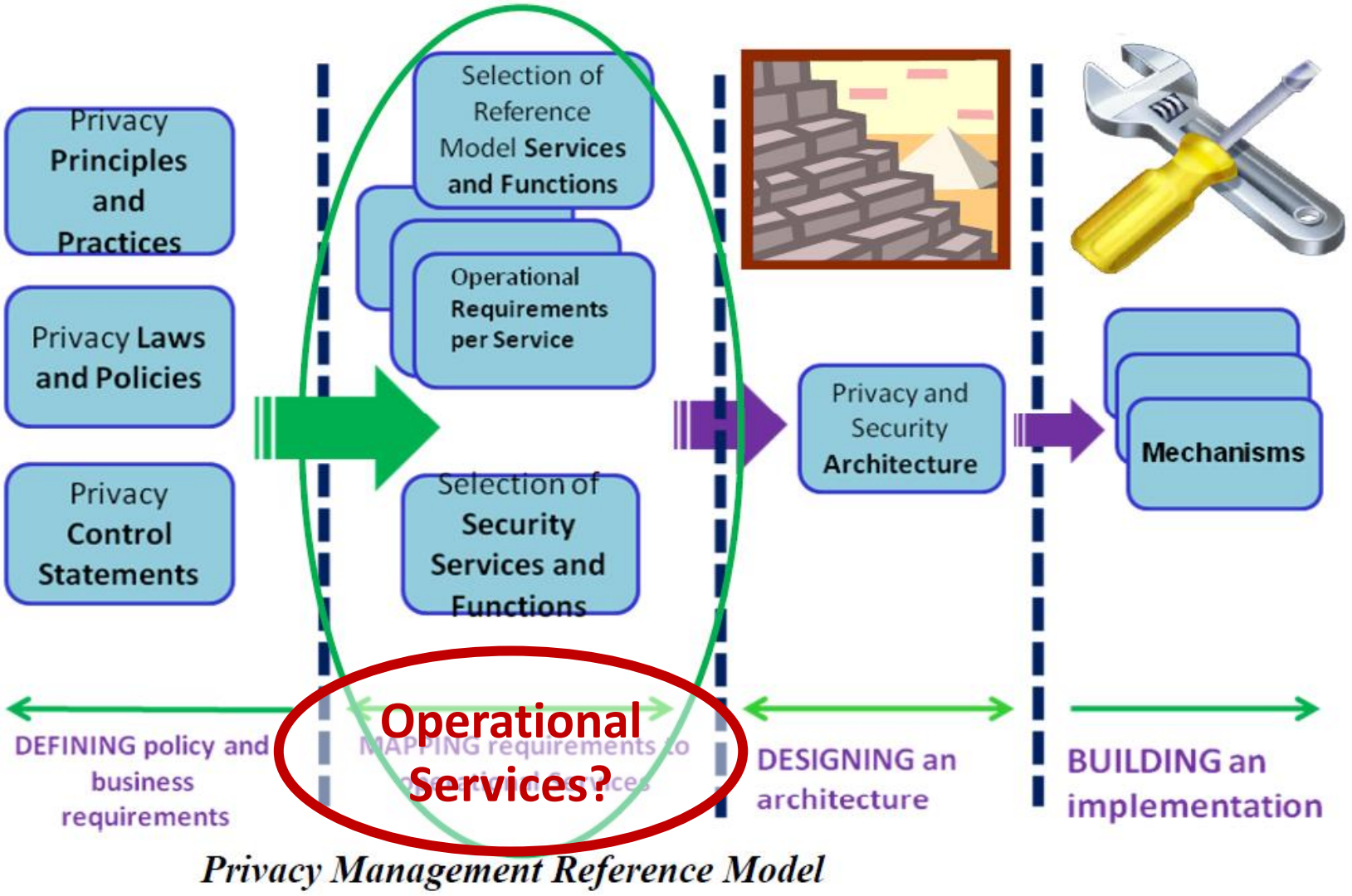
- Principles and concepts
  - Pbd Seven principles (Cavoukian)
  - Privacy-by-architecture/privacy-by-policy (Spiekermann09)
  - Data minimisation (Guerses11)
  - Minimisation, enforcement, transparency (Kung11)
    - Privacy Enhancing Architectures (Pears)
  - Minimise, Hide, Separate, Aggregate, Inform Control, Enforce, Demonstrate (Hoepman 14)
    - Design strategies

Existing Privacy Engineering Standard: OASIS PMRM



Privacy Management Reference Model

Existing Privacy Engineering Standard: OASIS PMRM



Privacy Management Reference Model

OASIS PMRM: Operational Services

	Service	Purpose
From OASIS PMRM	Agreement	Management of permissions and rules
	Usage	Controlling personal data usage
	Validation	Checking personal data
	Certification	Checking stakeholders credentials
	Enforcement	Monitor operations and react to exceptions
	Security	Safeguard privacy information and operations
	Interaction	Information presentation and communication
	Access	Data subject access to their personal data
From PRIPARE	Accountability	Log and audit management

OASIS PMRM: Operational Services

	Service	Purpose
From OASIS PMRM	Agreement	Management of permissions and rules
	Usage	Controlling personal data usage
	Validation	Checking personal data
	Certification	Checking stakeholders credentials
	Enforcement	Monitor operations and react to exceptions
	Security	Safeguard privacy information and operations
	Interaction	Information presentation and communication
	Access	Data subject access to their personal data
From PRIPARE	Accountability	Log and audit management

Operational Services?

PRIPARE Privacy Enhancing ARchitectures

Antonio Kung. PEARs: Privacy Enhancing ARchitectures. Annual Privacy Forum. Lecture Notes in Computer Science Volume 8450, 2014

Strategy		Tactics Examples
1 Minimization	Collection of personal information should be kept to a strict minimum	• Anonymize credentials (e.g. Direct anonymous attestation) • Limit processing perimeter (e.g. client processing, P2P processing)
2 Enforcement	Provide maximum protection of personal data during operation	• Enforce data protection policies (collection, access and usage, collection, retention) • Protect processing (e.g. storage, communication, execution, resources)
3 Transparency and accountability	Maximum transparency provided to stakeholders on the way privacy preservation is ensured	• Log data transaction • Log modifications (policies, crypto, protection) • Protect log data
4 Modifiability	Cope with evolution needs	• Change Policy • Change Crypto Strength and method • Change Protection Strength

PRIPARE Privacy Enhancing ARchitectures

Antonio Kung. PEARs: Privacy Enhancing ARchitectures. Annual Privacy Forum. Lecture Notes in Computer Science Volume 8450, 2014

Strategy		Tactics Examples
1 Minimization	Collection of personal information should be kept to a strict minimum	• Anonymize credentials (e.g. Direct anonymous attestation) • Limit processing perimeter (e.g. client processing, P2P processing)
2 Enforce data protection	Provide maximum protection of personal data during operation	• Enforce data protection policies (collection, access and usage, collection, retention) • Protect processing (e.g. storage, communication, execution, resources)
3 Transparency and accountability	Maximum transparency provided to stakeholders on the way privacy preservation is ensured	• Log data transaction • Log modifications (policies, crypto, protection) • Protect log data
4 Modifiability	Cope with evolution needs	• Change Policy • Change Crypto Strength and method • Change Protection Strength

Architecture Strategies?

Architecture Tactics?

Hoepman: Design Strategies

Jaap-Henk Hoepman. Privacy design strategies . In ICT Systems Security and Privacy Protection - 29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco

Design Strategy		Patterns Examples
1 Minimization	Amount of processed personal data restricted to the minimal amount possible	• select before you collect • anonymisation / pseudonyms
2 Hide	Personal data, and their interrelationships, hidden from plain view	• Storage and transit encryption of data • mix networks • hide traffic patterns • attribute based credentials • anonymisation / pseudonyms
3 Separate	Personal data processed in a distributed fashion, in separate compartments whenever possible	• Not known
4 Aggregate	Personal data processed at highest level of aggregation and with least possible detail in which it is (still) useful	• aggregation over time (used in smart metering) • dynamic location granularity (used in location based services) • k-anonymity • differential privacy
5 Inform	Transparency	• platform for privacy preferrences • Data breach notification
6 Control	Data subjects provided agency over the processing of their personal data	• User centric identity management • End-to-end encryption support control
7 Enforce	Privacy policy compatible with legal requirements to be enforced	• Access control • Sticky policies and privacy rights management
8 Demonstrate	Demonstrate compliance with privacy policy and any applicable legal requirements	• privacy management systems • use of logging and auditing

Hoepman: Design Strategies

Jaap-Henk Hoepman. Privacy design strategies . In ICT Systems Security and Privacy Protection - 29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco

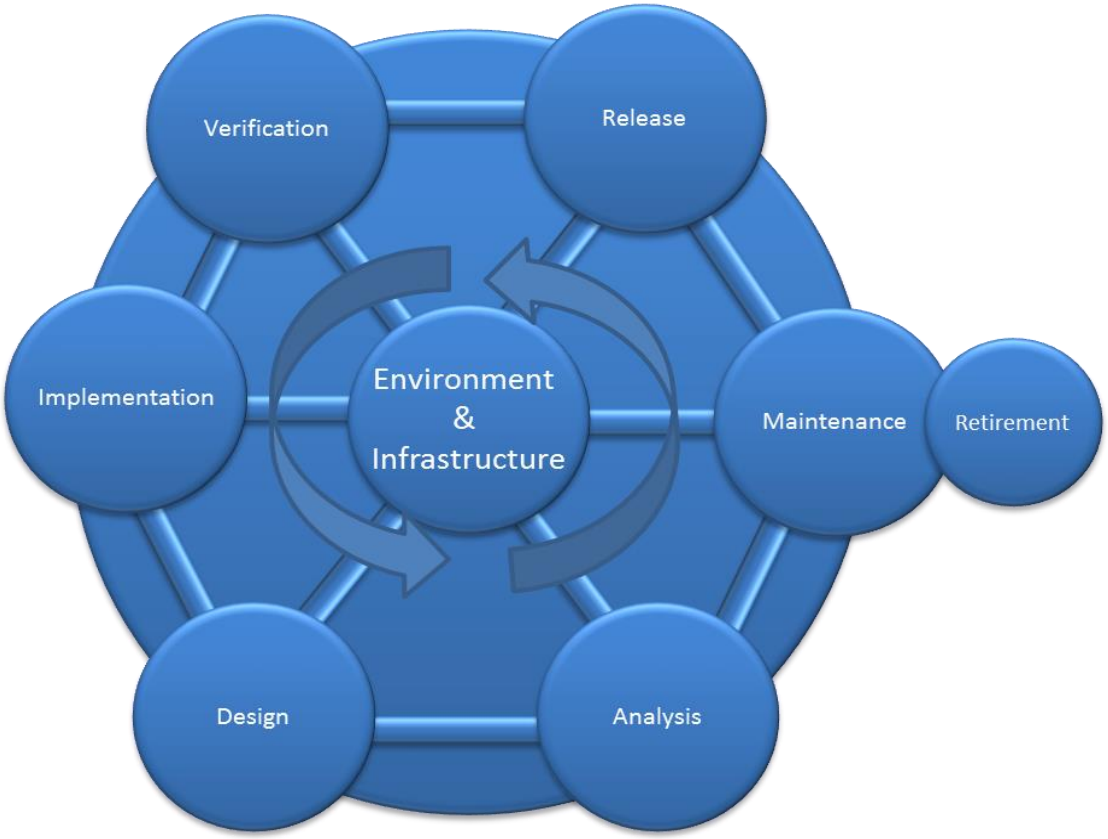
Design Strategy		Patterns Examples
1 Minimization	Amount of processed personal data restricted to the minimal amount possible	• select before you collect • anonymisation / pseudonyms
2 Hide	Personal data, and their interrelationships, hidden from plain view	• Storage and transit encryption of data • mix networks • hide traffic patterns • attribute based credentials • anonymisation / pseudonyms
3 Separate	Personal data processed in a distributed fashion, in separate compartments whenever possible	• Not known
4 Aggregate	Personal data processed at highest level of aggregation and with least possible detail in which it is (still) useful	• aggregation over time (used in smart metering) • dynamic location granularity (used in location based services) • k-anonymity • differential privacy
5 Inform	Transparency	• platform for privacy preferrences • Data breach notification
6 Control	Data subjects provided agency over the processing of their personal data	• User centric identity management • End-to-end encryption support control
7 Enforce	Privacy policy compatible with legal requirements to be enforced	• Access control • Sticky policies and privacy rights management
8 Demonstrate	Demonstrate compliance with privacy policy and any applicable legal requirements	• privacy management systems • use of logging and auditing

Patterns?

Design Strategies?

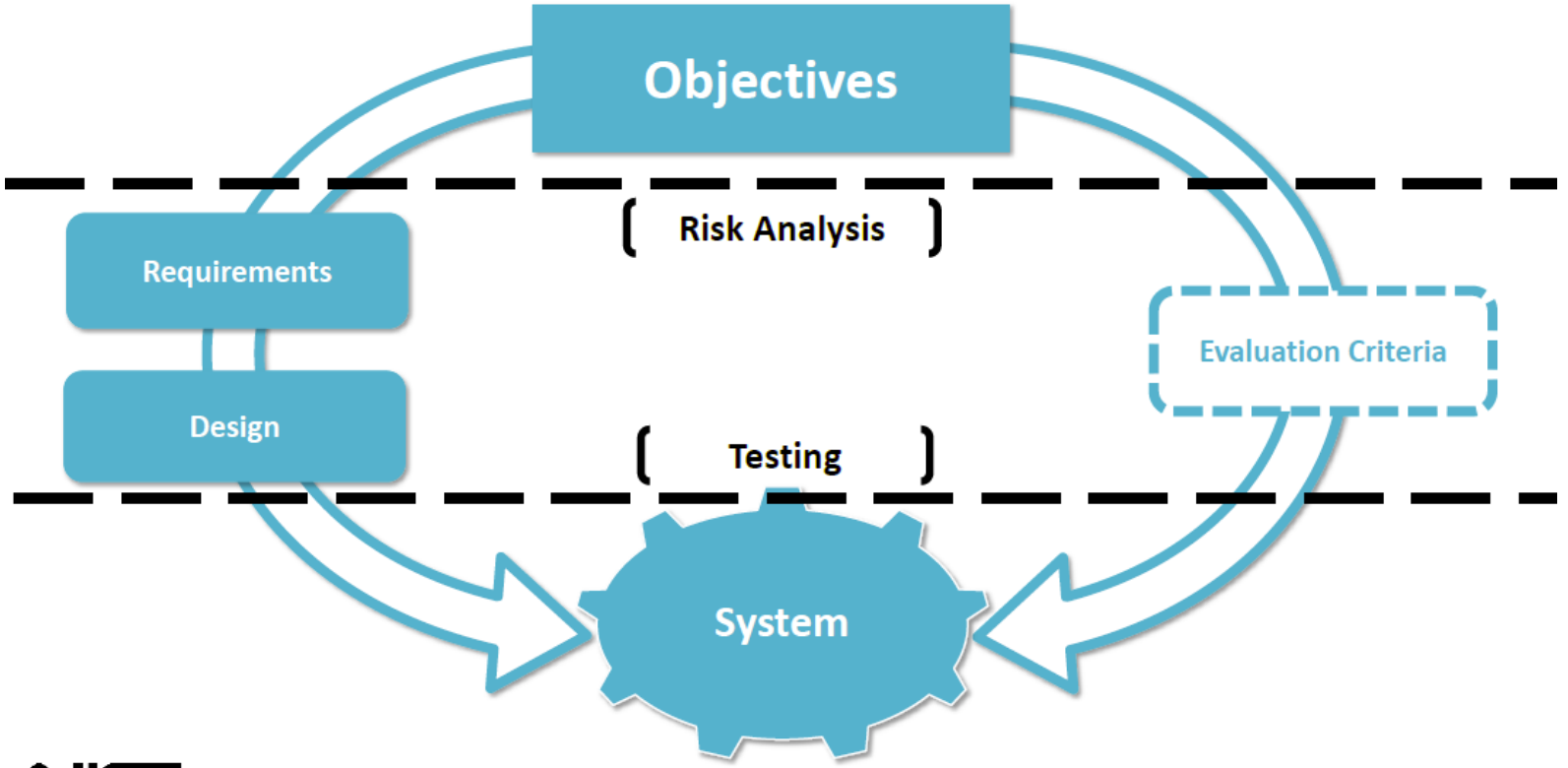
Life Cycle Concepts and Terms

- PRIPARE focus on Risk analysis (CNIL) and Architectures (Pears)



Life Cycle Concepts and Terms

- NIST: Focus on risk analysis

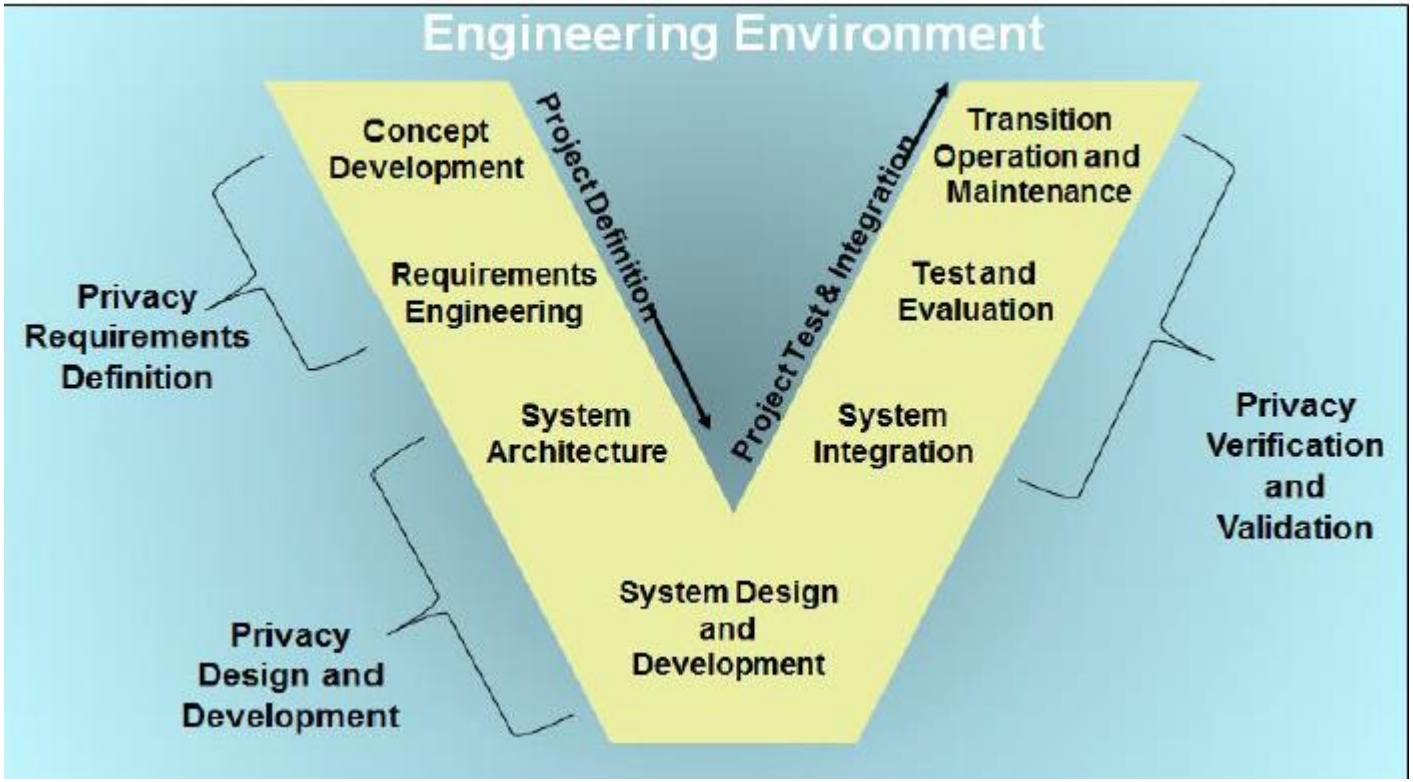


NIST

DISCUSSION DRAFT – NOT FINAL

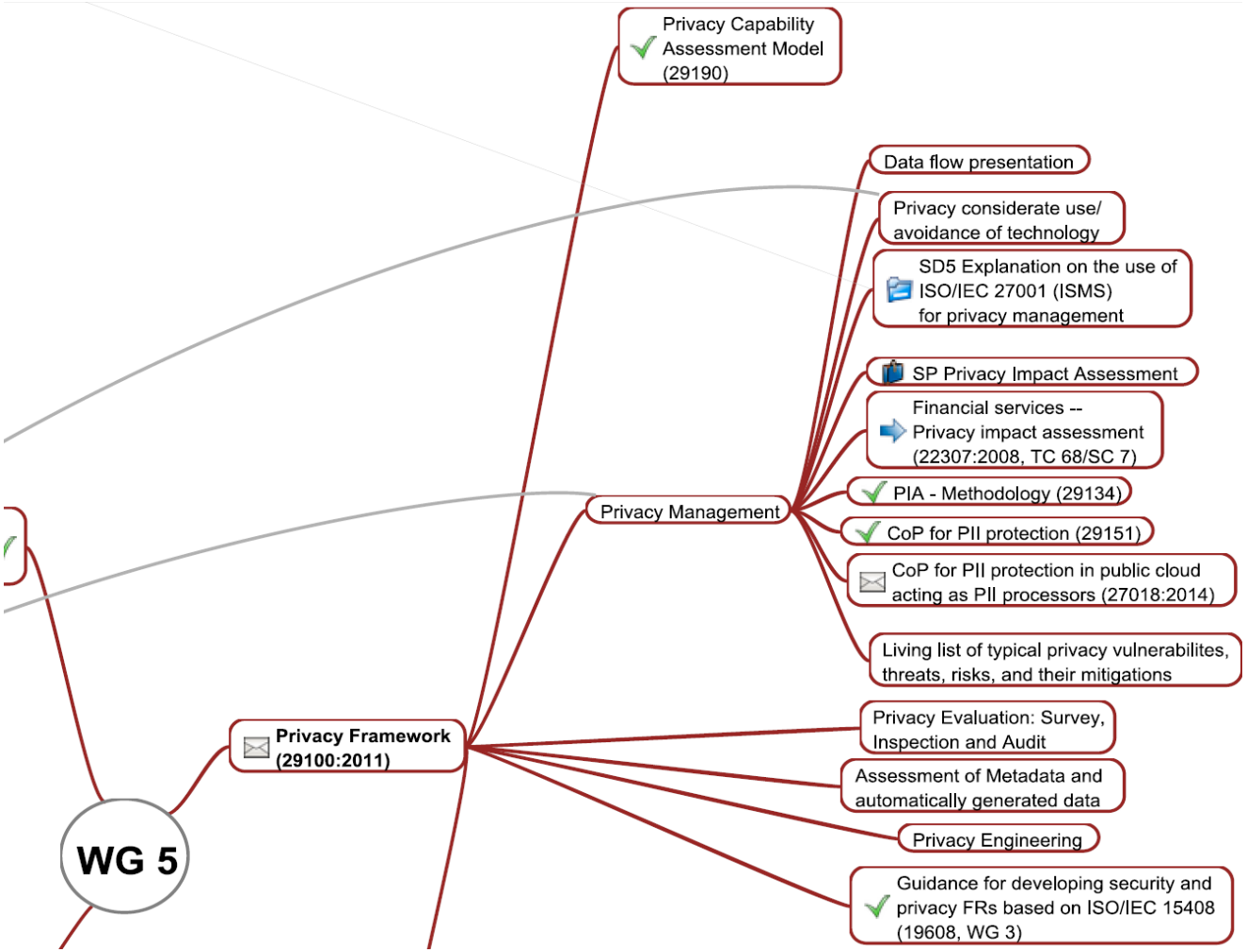
Life Cycle Concepts and Terms

- MITRE Engineering Environment



Positioning w.r.t. Standardisation

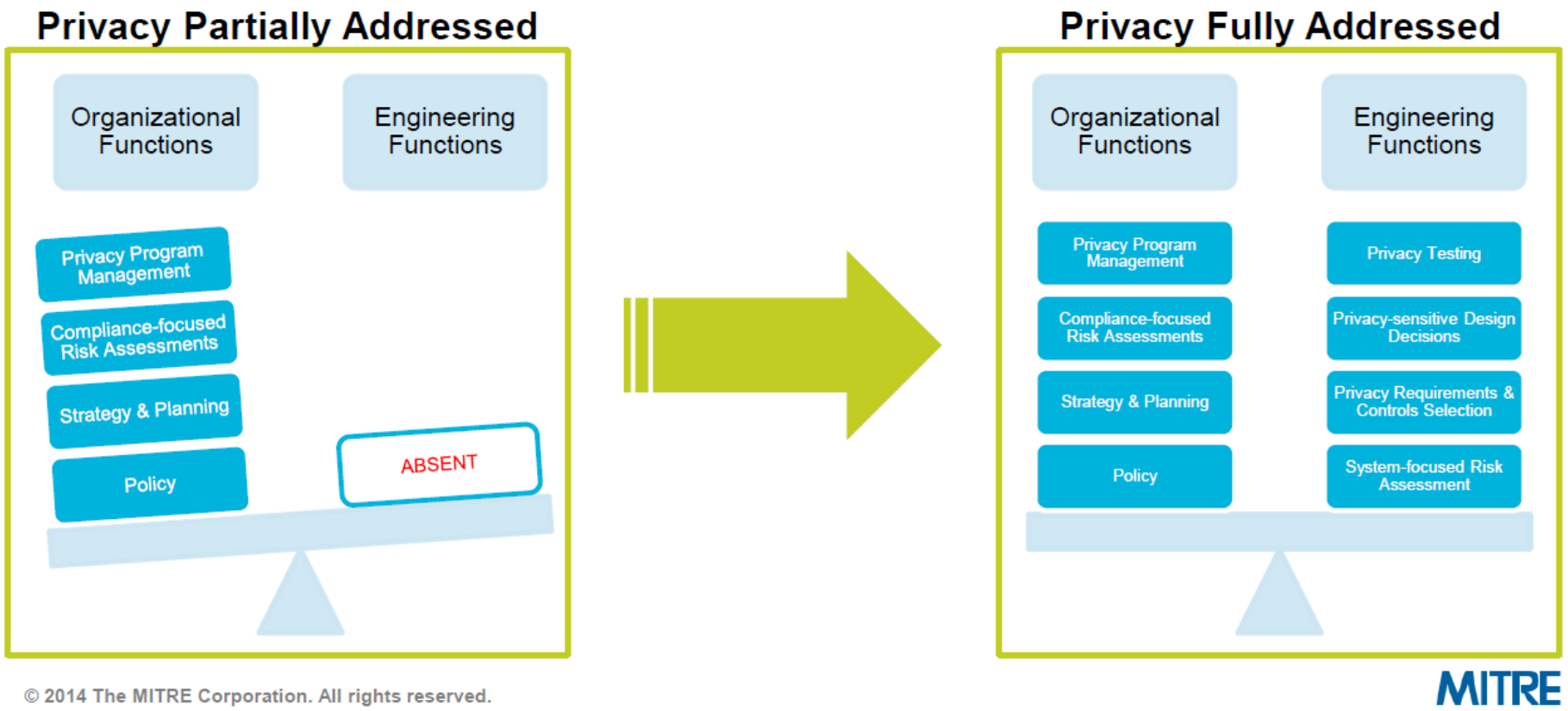
- Management and Compliance orientation



Other standards input

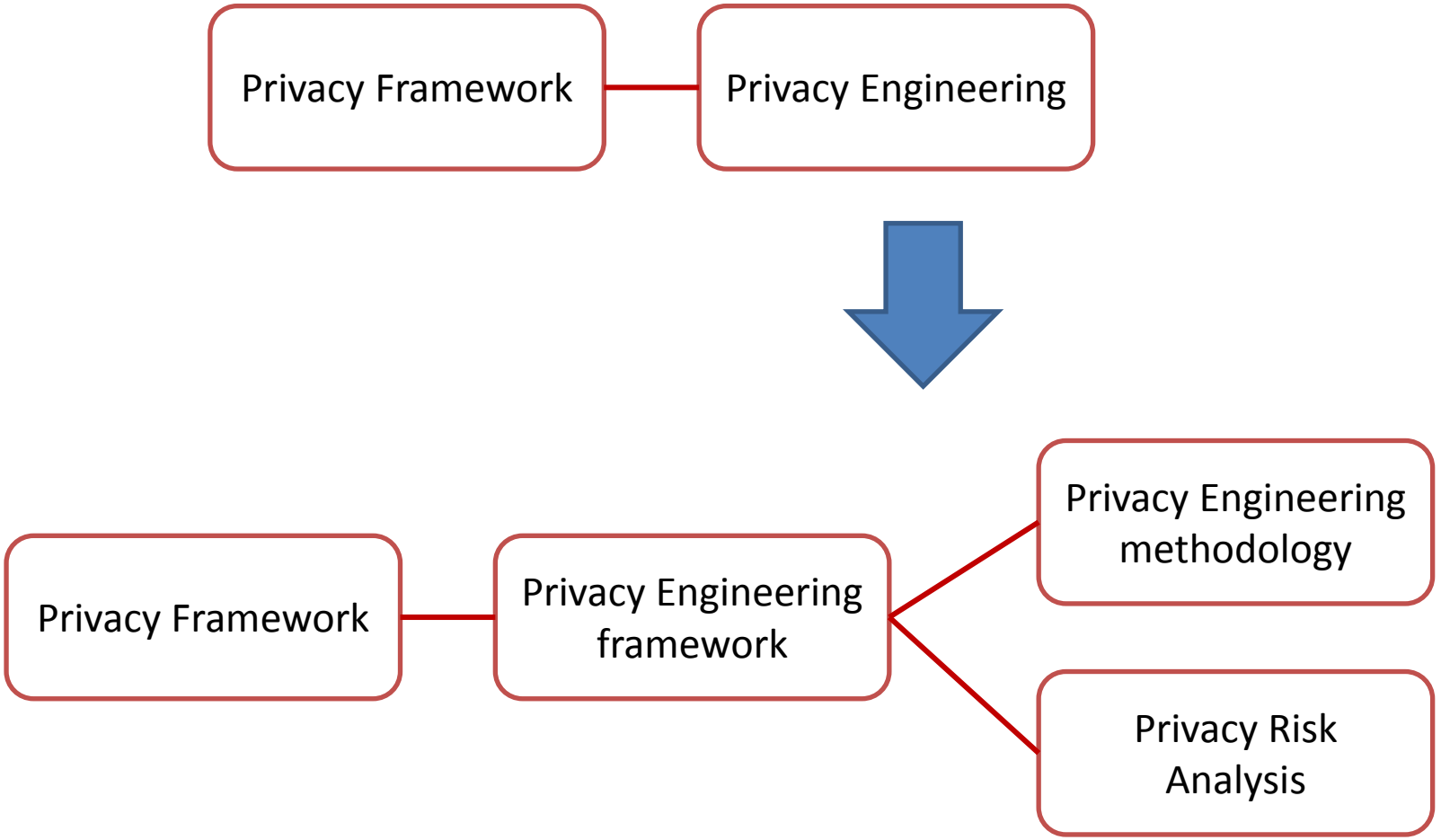
- ISO/IEC JTC 1/SC27/WG5
  - 29134
    - 6.3.4.2 Privacy Risk Analysis
    - Annex A (informative) Scale criteria on the level of impact and on the likelihood
  - 29151
    - Annex A Extended control set for PII protection
- ISO/IEC JTC 1/SC7 Software and systems engineering
  - 42001 Architecture description
  - 15288 Systems and software engineering – System life cycle processes
  - 12207 Systems and software engineering – Software life cycle processes
- ISO/IEC 27034 Application security

Mitre Analysis



MITRE

Paving the Way to Future Standards



Terms of Reference (Proposed by US expert)

- Taken into account
  - ISO/IEC 29100, 29101, 29134, 27034
  - ISO/IEC 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

Terms of Reference (Proposed by US expert)

- task the rapporteurs of the Study Period
  1. 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)
  2. to review the relationship between privacy engineering and other privacy, security, and risk management standards, as appropriate.
  3. to propose possible updates to existing privacy impact assessment and management standards.
  4. 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.

Terms of Reference (Proposed by US expert)

- A first call for contributions will be circulated after the Malaysia Meeting and the National Bodies are requested to provide their contributions by 15 September 2015. The National Body contributions received in response to this call for contributions will be discussed at the ISO/IEC JTC 1/SC 27 Working Group 5 Meetings in October 2015 in Jaipur, India. A second call for contributions might be circulated after the India Meeting.

Thanks

PRIPARE

PReparing **I**ndustry to **P**rivacy-by-design by supporting its **A**pplication in **RE**search

SEVENTH FRAMEWORK PROGRAMME