Trust in Data and AI

Gyu Myoung Lee (WP3/13 Co-Chair)

Data and Trust

Who are we comfortable sharing personal data from smart devices with?

- 14% Ad Companies
- 22% Supermarkets
- 26% Boss
- 41% Close Friends
- 63% Spouse/Significant Other
- 40% Health Professionals
- 30% Police
- 28% Insurance Companies
- 20% Energy Companies
- 14% Government

Source: 2014 Internet of Things Privacy Infographic
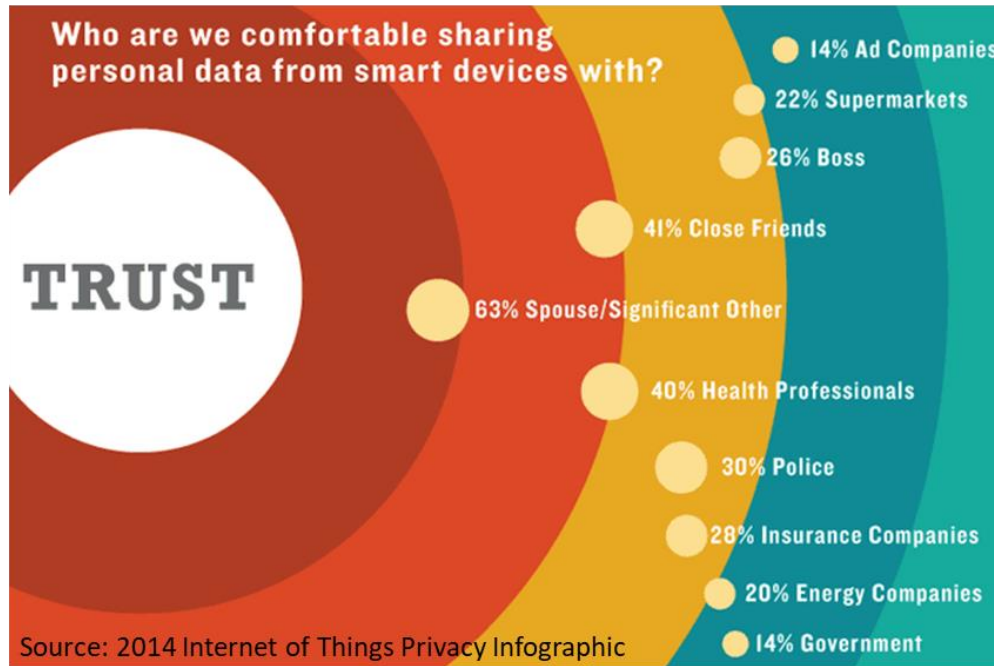
Volume – Data at Rest

Variety – Data in Many Forms

Velocity – Data in Motion

Variability – Data in Change

Veracity – Data in Doubt

Understanding of Trust
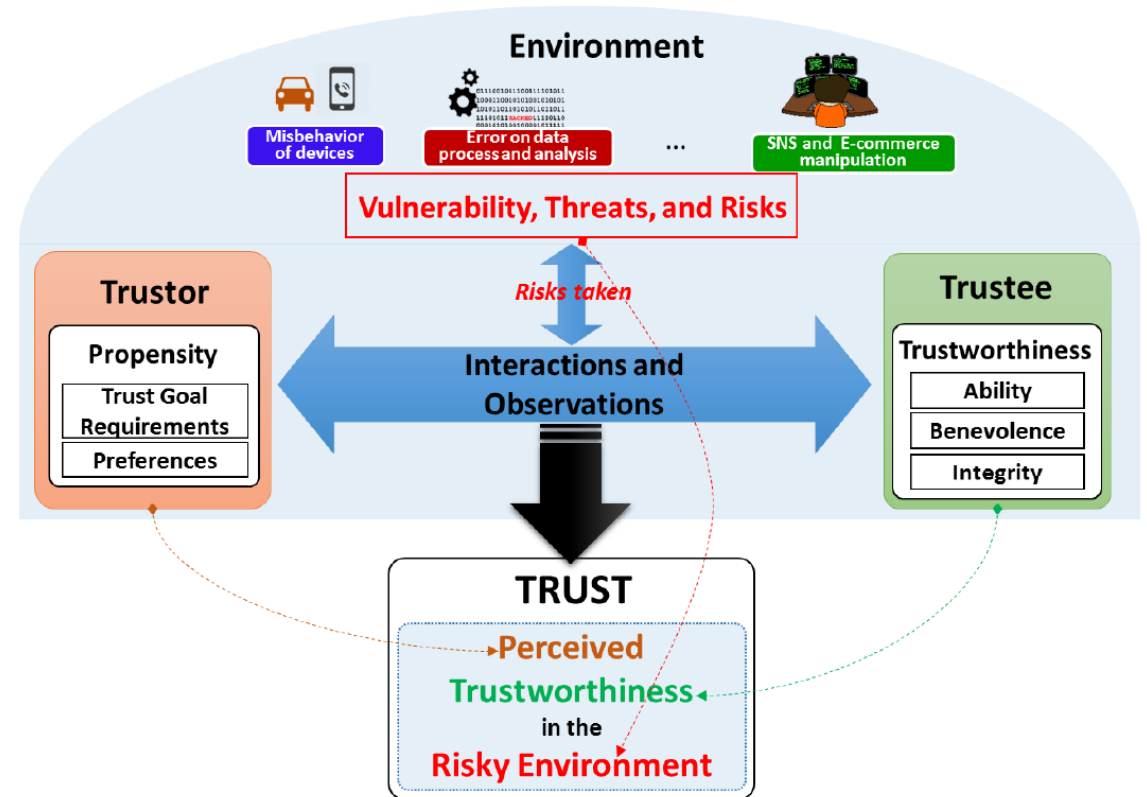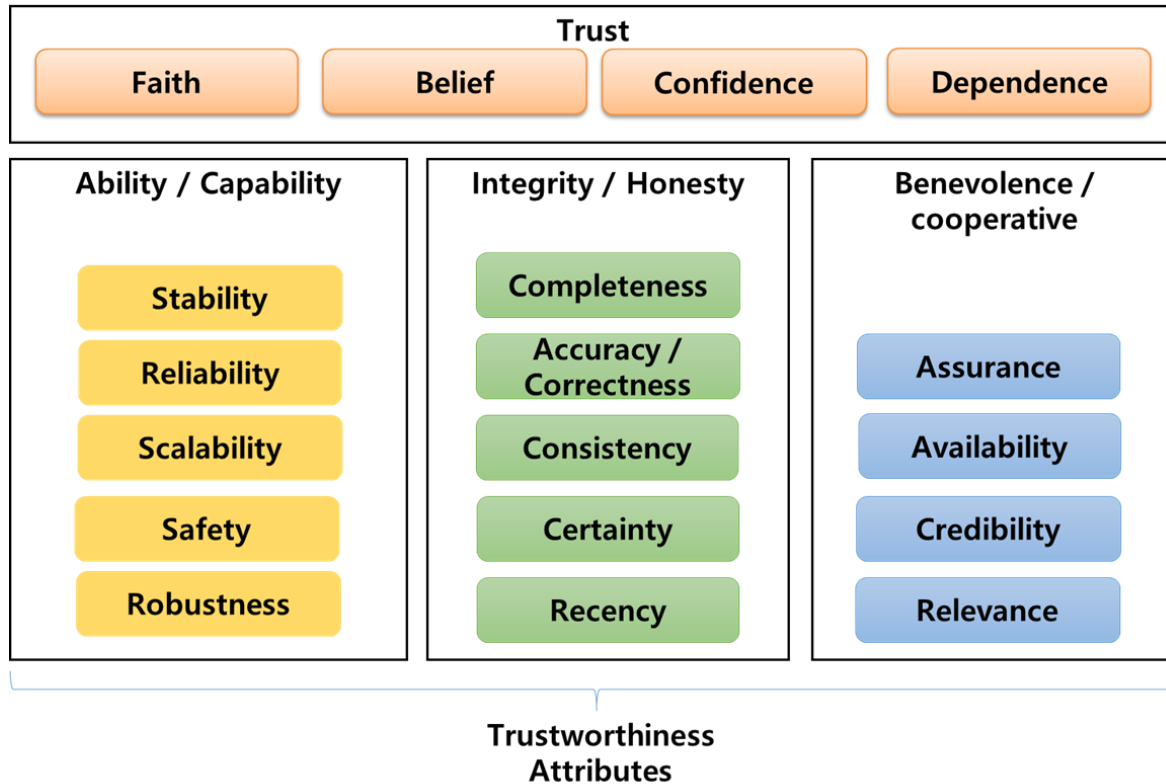
Definition of Trust

Trust of a party **A** to a party **B** for a given task **S** is the measurable belief of **A** in that **B** accomplishes S dependably for a specified period **P** within a particular trust context T (in relation to the task **S**)

Trust is **relative** to a specific task (a service). Different trust relationships appear in different business contexts

The measurement may be **absolute** (e.g. probability) or **relative** (e.g. Level of Trust)

This period may be in the **past** (history), the **duration of the service** (from now and until end of service), **future** (a scheduled or forecasted critical time slot), or always

Dependability is deliberately understood broadly to include **availability, reliability, safety, confidentiality, integrity and serviceability**

Security, Privacy and Trust
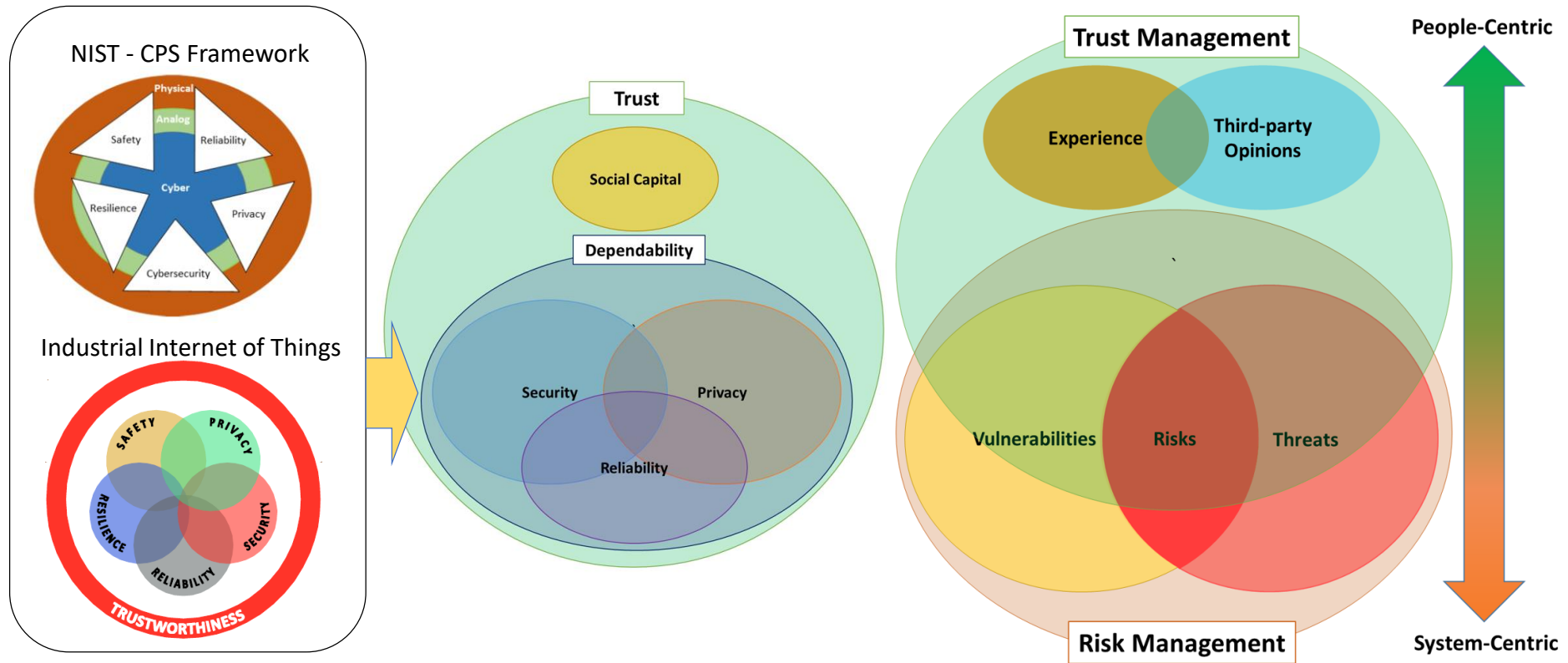
Trust Evaluation – Trust Index
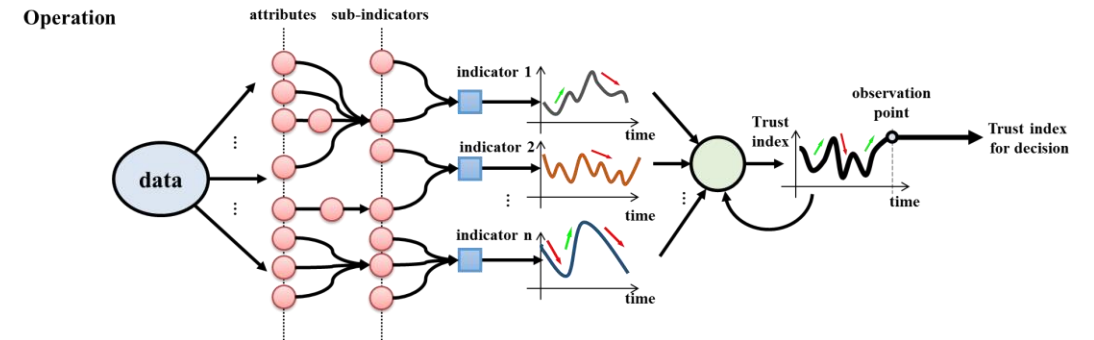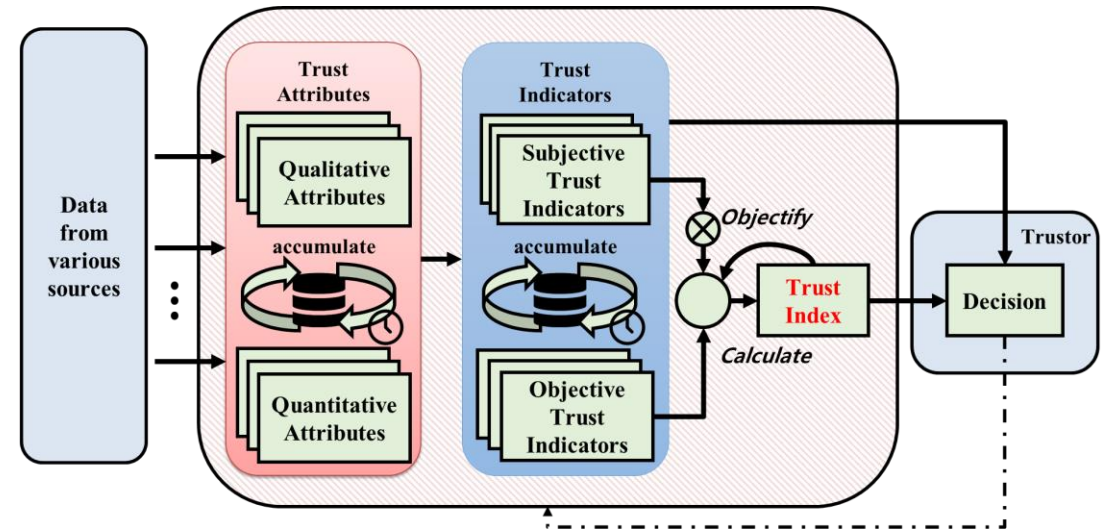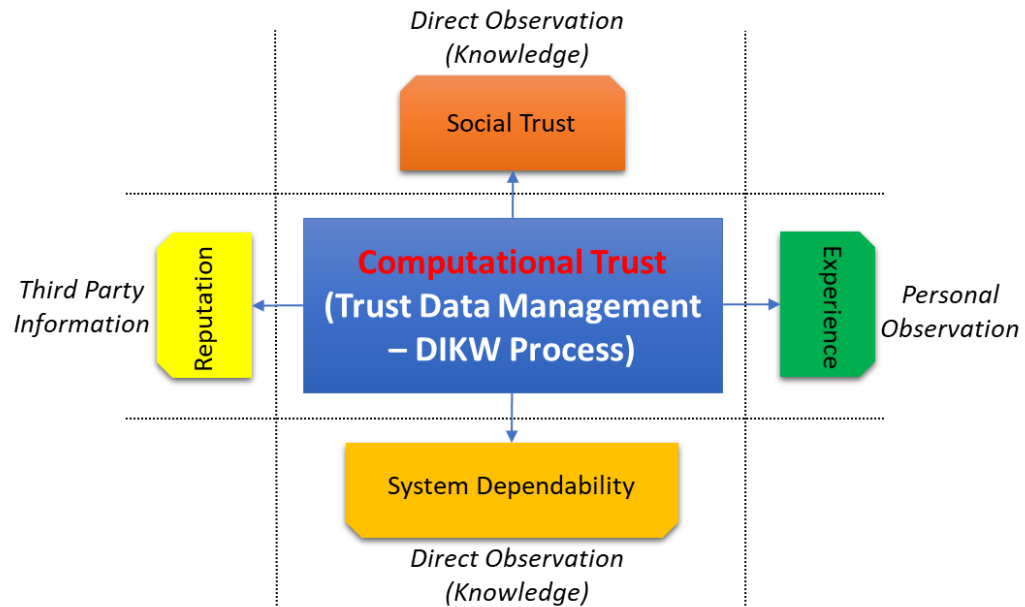
Goal: Trust in Data and AI for Data Driven Services

- An intelligent nerve that facilitates the **data trading**, **data exchange** and **data management** that facilitates the **business** development, at the same time that satisfies the **regulations**

- Build a **Data Economy Ecosystem** that offers **lawfully and GDPR compliance by default**
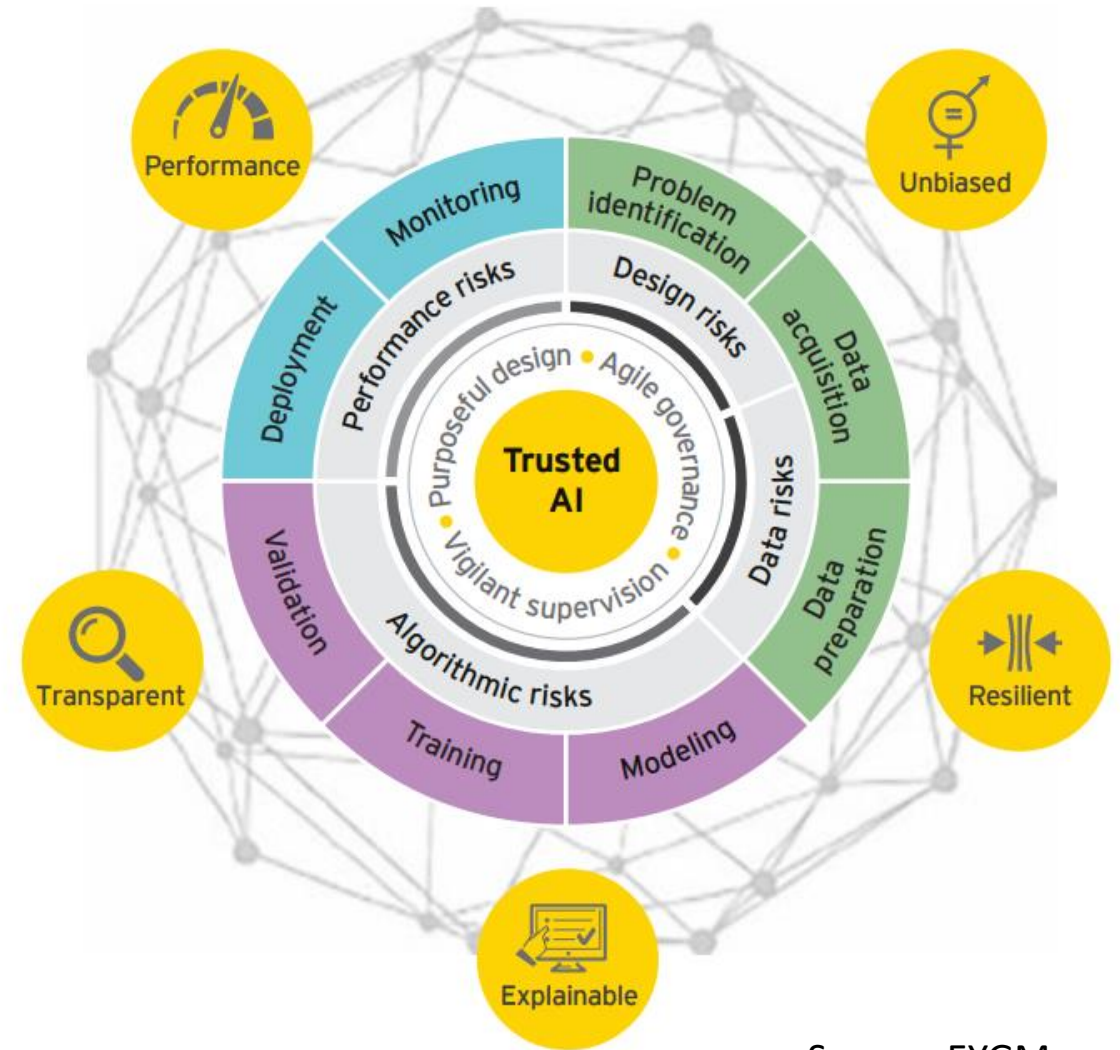
Key Topic – Trusted Data

An integrated requirements framework for technical enablers to promote trusted data (source: FG-DPM D4.3)
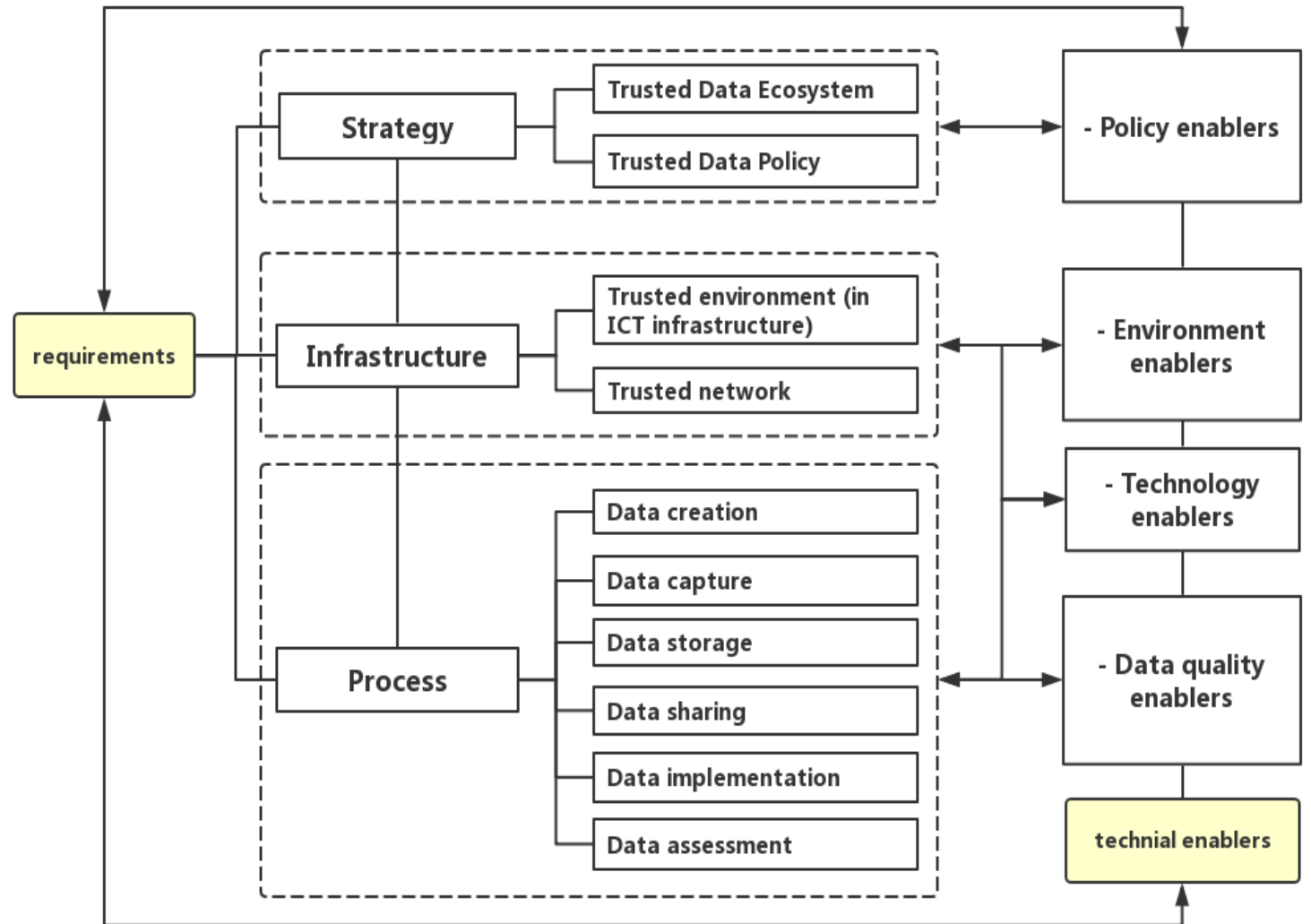
Key Topic – Trusted AI

- ## Responsible AI
  - Taking responsibility **in** Design, **by** Design and **for** Design(ers)
- ## Four conditions
  - Ethics
  - Social responsibility
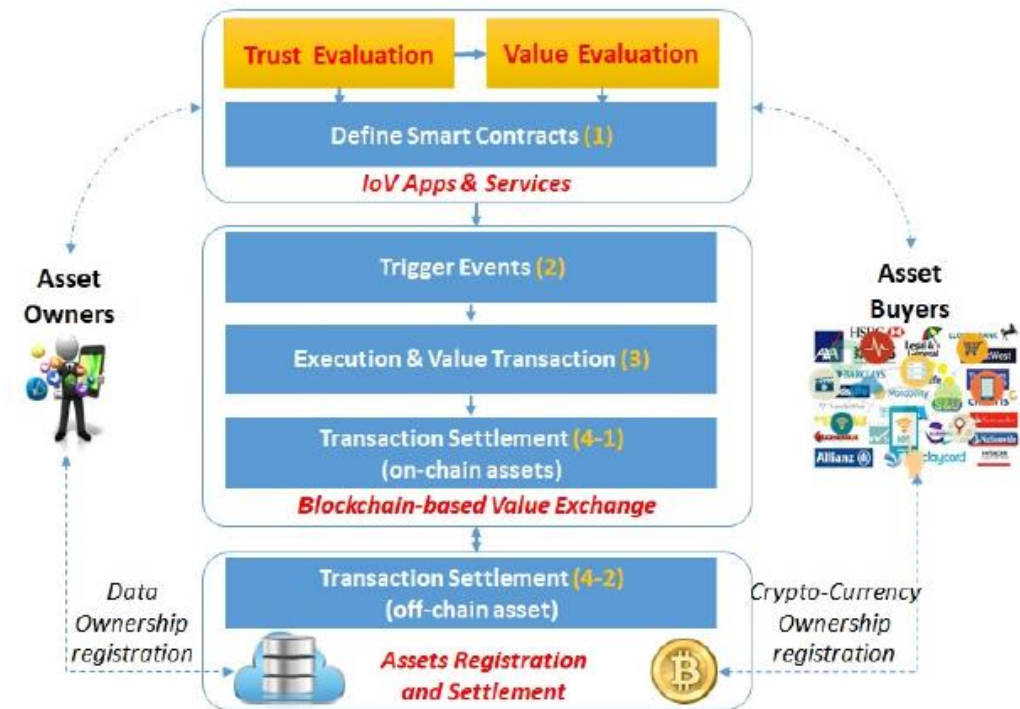 - Accountability and explainability
  - Reliability

Source: EYGM

Key Topic - Blockchain

"It is a machine for creating trust." (Source: The Economist)

- building trust, reducing costs and accelerating transactions

- Blockchain-based Internet of Value

Trust standardization in ITU-T SG13

Published Recommendations

- **Y.3051** (The basic principles of trusted environment in ICT infrastructure)
- **Y.3052** (Overview of trust provisioning for ICT infrastructures and services)
- **Y.3053** (Framework of trustworthy networking with trust-centric network domains)
- **Y.3054** (Framework of Trust-based Media Services)

Draft Recommendations

- **Y.SNS-trust** (Framework for Evaluation of Trust and Quality of Media in Social Networking Services)
- **Y.trust-arch** (Functional architecture for trust enabled service provisioning)
- **Y.trust-index** (Trust index for ICT infrastructures and services)
- **Y.trust-pdm** (Framework for Trust based Personal Data Management Platform)

Trust standardization in other SDOs

- IEEE
  - DIITA: Digital Inclusion, Identity, Trust & Agency
  - Ethically Aligned Design in Autonomous and Intelligent Systems

- ISO/IEC
  - SC 42/WG 3: trustworthiness working group
  - NP TR 24028 (AI - - Overview of trustworthiness in Artificial Intelligence)

Strategic direction to be taken by ITU-T

- Related groups in this study period
  - SG13: Q16/13 (Knowledge-centric trustworthy networking and services)
  - SG17: Security
  - SG20: Q6/20 (Security, privacy, trust and identification for IoT and SC&C)
- It's right time to focus on Trust in Data and AI
  - Necessary to create a new group for Data and AI

Questions for SGLA discussion

- Correct understanding of trust?
  - Vary over time with the different context

- Work scope of trust?
  - Technical vs. non-technical aspects

- Responsibility of relevant groups in ITU-T?
  - Trust solutions in specific domains such as networks, IoT, data and AI, etc.
  - Commonly applicable solutions vs. adoption of trust solutions in a specific domain

All SGs should consider the "Trust by Design" principle.

Conclusion - Beyond Conventional Security Soultions

- Transparency
- Data protection
- Privacy preserving
- Policy and regulatory issues
- Ethics

"**Trust** is the **oxygen** which will breathe life into the IoT. Industry needs to show **data** is safe and that it is properly treated." (source: www.techuk.org.)