ITU Workshop on "Future Trust and Knowledge Infrastructure", Phase 2
Geneva, Switzerland
1 July 2016

Overview - Trust in ICT Infrastructure and Services

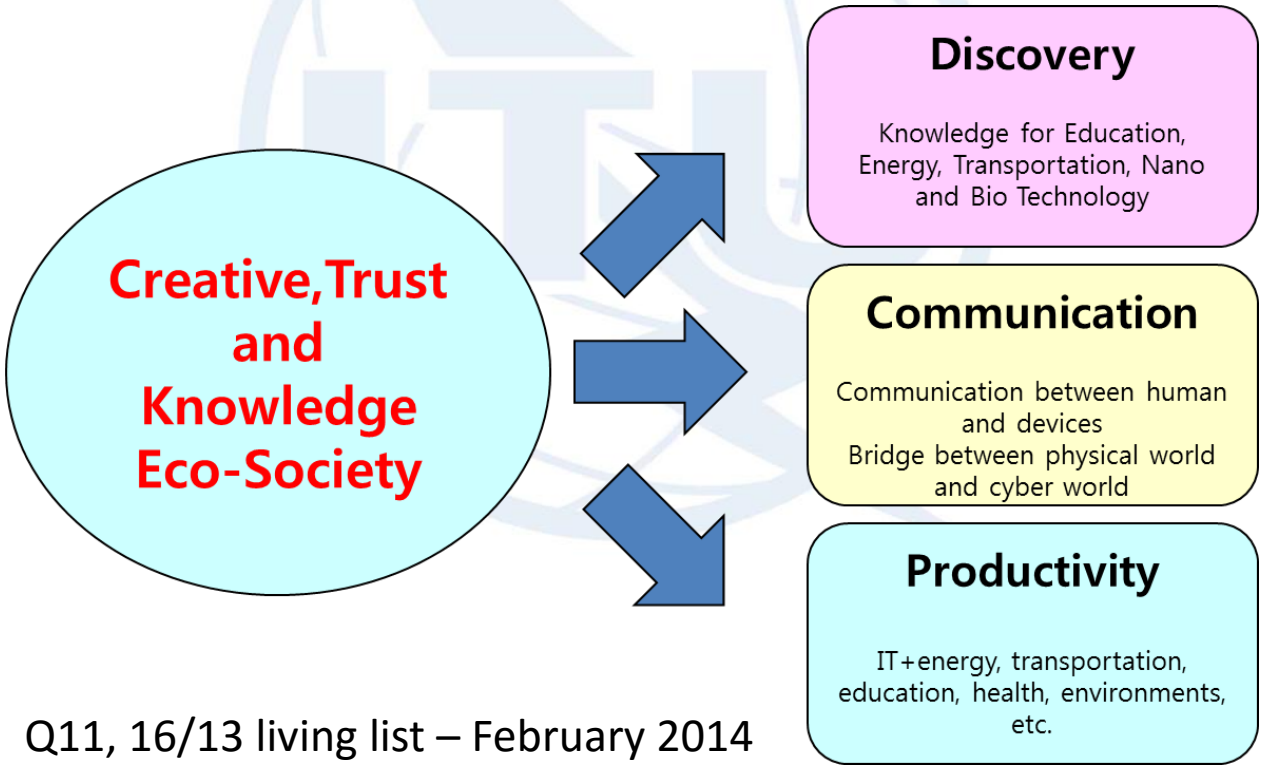
Gyu Myoung Lee
ITU-T WP3/13 Co-chair, Q11/13, Q16/13 and Q4/20 Rapporteur
LJMU UK/ KAIST Korea
gmlee@kaist.ac.kr

Contents

- Introduction
- ITU Workshop on “Future Trust and Knowledge Infrastructure”, Phase 1
- Correspondence Group on Trust (CG-Trust) Activities
- CG-Trust Technical Report
  - ICT & Knowledge Society
  - Trust concepts and key technical issues
  - Architectural overview
- Strategies for Future Standardization on Trust
- Conclusion

Introduction

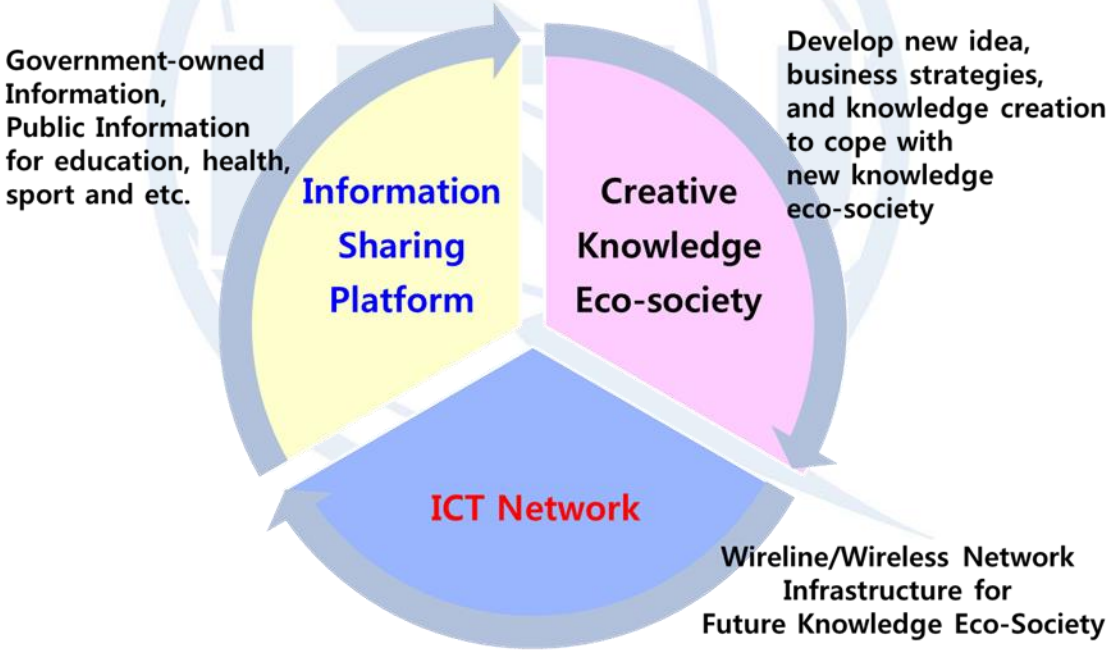
- Future ICT infrastructure



Q11, 16/13 living list – February 2014

Trust and Knowledge

- **Future trust and knowledge infrastructure**



ITU Workshop on "Future Trust and Knowledge Infrastructure", Phase 1 (1)

- **Phase 1 workshop – 24 April 2015**
- Aims of the workshop
  - Define the strategic and technical priorities for future ICT infrastructure;
  - Clearly identify the current socio-economic trends of markets and services driven by social networking services, mobile services and cloud computing platforms;
  - Articulate visions of the future Information Society, including the required form of infrastructure from the perspectives of knowledge and trust; and
  - Identify areas ripe for standards- development work to realize future trust and knowledge ICT infrastructure.

ITU Workshop on "Future Trust and Knowledge Infrastructure", Phase 1 (2)

- **4 key sessions**
  - Data Science for the Knowledge Society
  - Requirements and Expectations for Future ICT Infrastructure
  - The "Open and Secure" Paradox
  - Open Data Platforms

- **Panel session: action plans for future ICT infrastructure**
  - What is trust? – Different views on trust
  - What is needed? - SDO's views
  - Action items - A collaboration team (basic term, achieve trust)

Workshop programme:
http://www.itu.int/en/ITU-T/Workshops-and-Seminars/24042015/Pages/Programme.aspx

ITU Workshop on "Future Trust and Knowledge Infrastructure", Phase 1 (3)

- Key outcome
  - **Q16/13** – Requested the creation of **CG-Trust** for preliminary work on trust standardization
  - Approved at the SG13 meeting on 1 May 2015

- Planned the Phase 2 workshop

Challenges

1. Understanding of trust
2. Trust relationships
3. Trust management
4. Measure & calculate
5. Decision making
6. Autonomy
7. Constraint environment
8. T-SCPI architecture
9. New business models
10. Standardization

ITU-T CG-Trust Activities

- Terms of Reference
  - Develop a technical report which contains:
    - Definition, use cases, functional classification
    - Challenges, technical issues related to trust
    - Overall strategies of standardization for trust provisioning
  - The lifetime: 1 year
- The CG-Trust reported its activities to the SG13 meeting (April 2016)

ITU-T CG-Trust Activities

- 7 CG-Trust meetings in total
  - 1st meeting (e-meeting, 17 June 2015): 4 contributions;
  - 2nd meeting (Geneva, 13 – 23 July 2015): 5 contributions;
  - 3rd meeting (e-meeting, 2 September 2015): 5 contributions;
  - 4th meeting (Geneva, 17-18 October 2015): 6 contributions;
  - 5th meeting (Geneva, 30 November – 11 December 2015): 12 contributions;
  - 6th meeting (e-meeting, 24 February 2016) : 3 contributions;
  - 7th meeting (Geneva, 18 – 29 April 2015): 6 contributions.

- 41 contributions in total

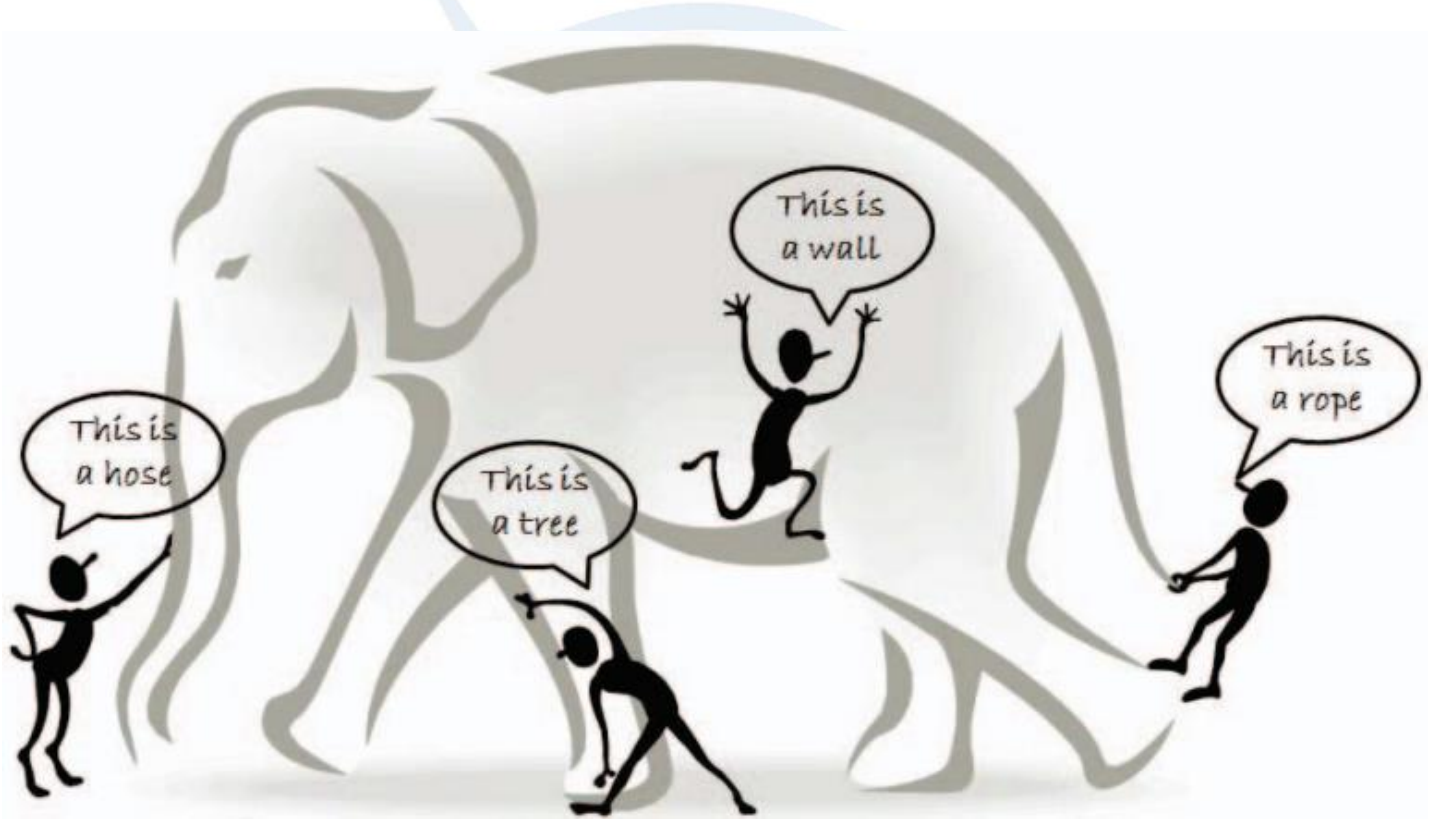
ITU-T CG-Trust Activities

- CG-Trust Technical Report
  - The importance and necessity of trust toward knowledge societies;
  - Concepts and key features of trust;
  - Key challenges and technical issues for trusted ICT infrastructures;
  - Architectural overviews of trusted ICT infrastructures;
  - Trust based ICT service models;
  - Summary of use cases for trusted ICT infrastructures;
  - Strategies for future standardization on trust.

CG-Trust Technical Report

"Trust provisioning for future ICT infrastructures and services"

The blind men and the giant elephant



The localized (limited) view of each blind man leads to a biased conclusion

Xindong Wu, et. al., "Data mining with big data," IEEE TR on Knowledge and data engineering, Jan. 2014.

From Information to Wisdom

- Challenges
  - How to **collect** these information?
  - How to **compute** and **storage** these information?
  - How to **use** these information?
  - How about the **relationship** between these information?

In the **Information explosion** but **lack of Knowledge**,
Internet is changing from sale of information to sale of knowledge.

ICT is a Basis of Knowledge Society

- ICT evolution affects the means of knowledge creation and processing
- If knowledge is exploited for malicious intentions, it could suffer from irreparable damage and uncertain dangers.
- Identify and prevent risks of knowledge in the complicated ICT infrastructure.

Potential risks in ICT infrastructures

- Risks on **Data Integrity**
  - Maintain the accuracy and consistency of data.
- Risks of the **Operation of Systems**
  - The advent of S/W and H/W accelerates the deployment of autonomic processing and operation of systems.
- **Social Networking** Risks
  - False knowledge propagation gives rise to great confusion in societies.

Trust for future ICT infrastructures and services

- **Trust**
  - A key issue in the processing and handling of data, as well as the provisioning of services which comply with users' needs and rights.
- The Aim
  - To create a trusted ICT infrastructure for sharing information and creating knowledge, and
  - To stimulate activities for future standardization on trust with related SDOs.

Increasing Intelligence

- Behave intelligently and rationally to
  - Sense real-world behaviour
  - Perceive the world using information models
  - Adapt to different environments and changes
  - Learn and build knowledge
  - Act to control their environments

Control vs. Trust

Trust Definitions

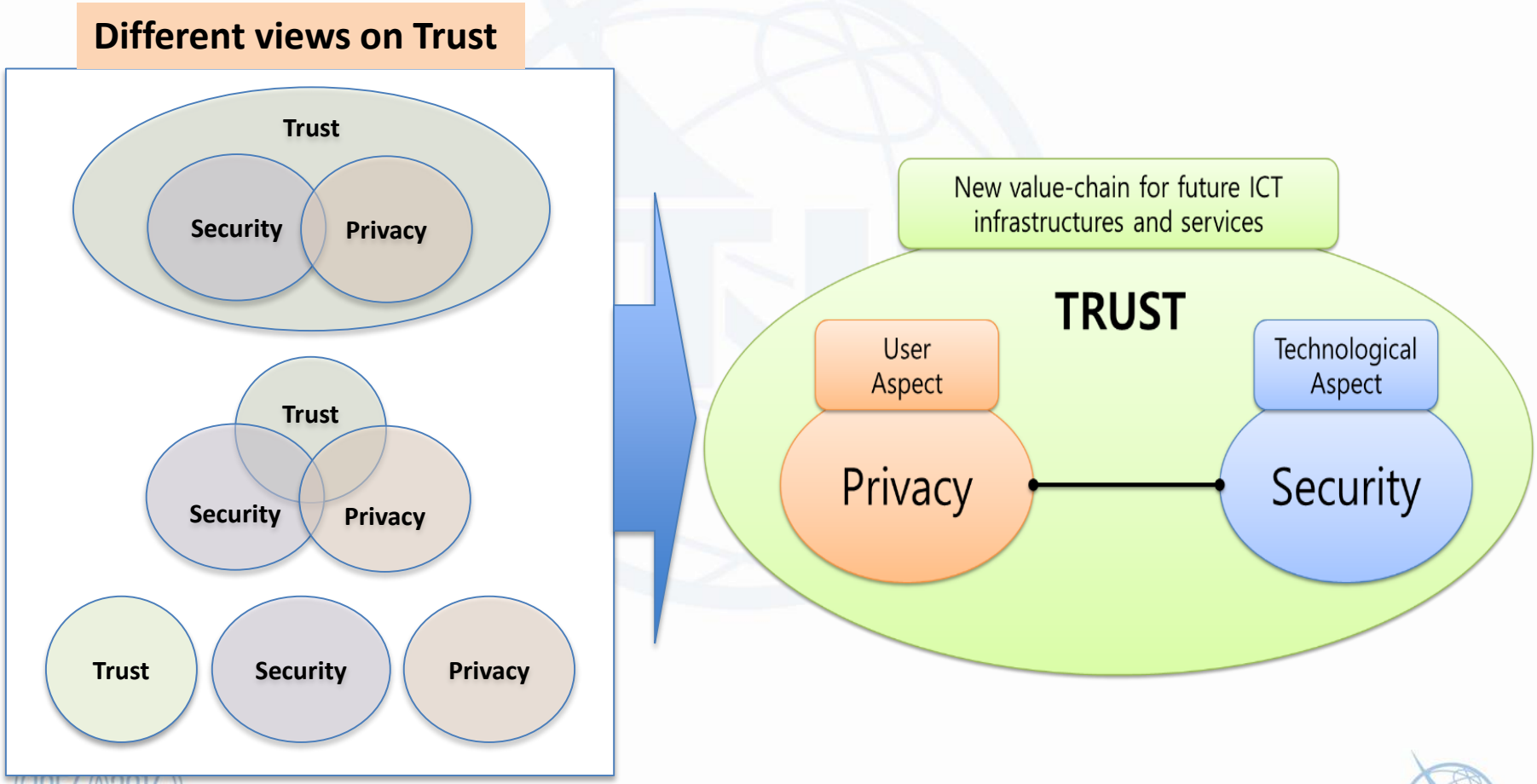
	Definitions
Lexical-semantic	Reliance on the integrity, strength, ability, surety, etc., of a person or thing; confidence
	Reliance on and confidence in the truth, worth, reliability, etc., of a person or thing; faith
General aspects	**Trust is a measure of confidence** that an entity will behave in an expected manner, despite the lack of ability to monitor or control the environment in which it operates.
Psychology	Trust is considered to be a psychological state of the individual, where the trustor risks being vulnerable to the trustee based on positive expectations of the trustee's intentions or behaviour.
	Trust is considered to have three aspects: **cognitive, emotive, and behavioural**.

	Definitions
Computer Science	Trust in computer science in general can be classified into two broad categories: "user" and "system". The notion of **"user" trust** is derived from psychology and sociology, with a standard definition as "a subjective expectation an entity has about another's future behaviour".
	"System" trust is "the expectation that a device or system will faithfully behave in a particular manner to fulfil its intended purpose".
	System trust is "an attitude of confident expectation in an online situation of risk that one's vulnerabilities will not be exploited"
Specific context (Trust in IoT)	**Interpersonal trust** is a relationship between a trustor and a trustee arising in uncertain and (potentially) risky situations, affecting trustors behaviour, emotion and cognition. It is evoked by the perception of trustworthy characteristics (such as ability, benevolence and integrity) of the trustee.
	In the context of IoT, **trust** is reliance on the integrity, ability or character of an entity. Trust can be further explained in terms of confidence in the truth or worth of an entity.
	Trust is an internal status of the user that may possibly become in the users behaviour as well as in the users' affect and cognition and therefore is partly accessible. Furthermore, trust is evoked by trustworthiness characteristics of the technology.
	Trust is **"a user's confidence in an entity's reliability, including user's acceptance of vulnerability in a potentially risky situation".**

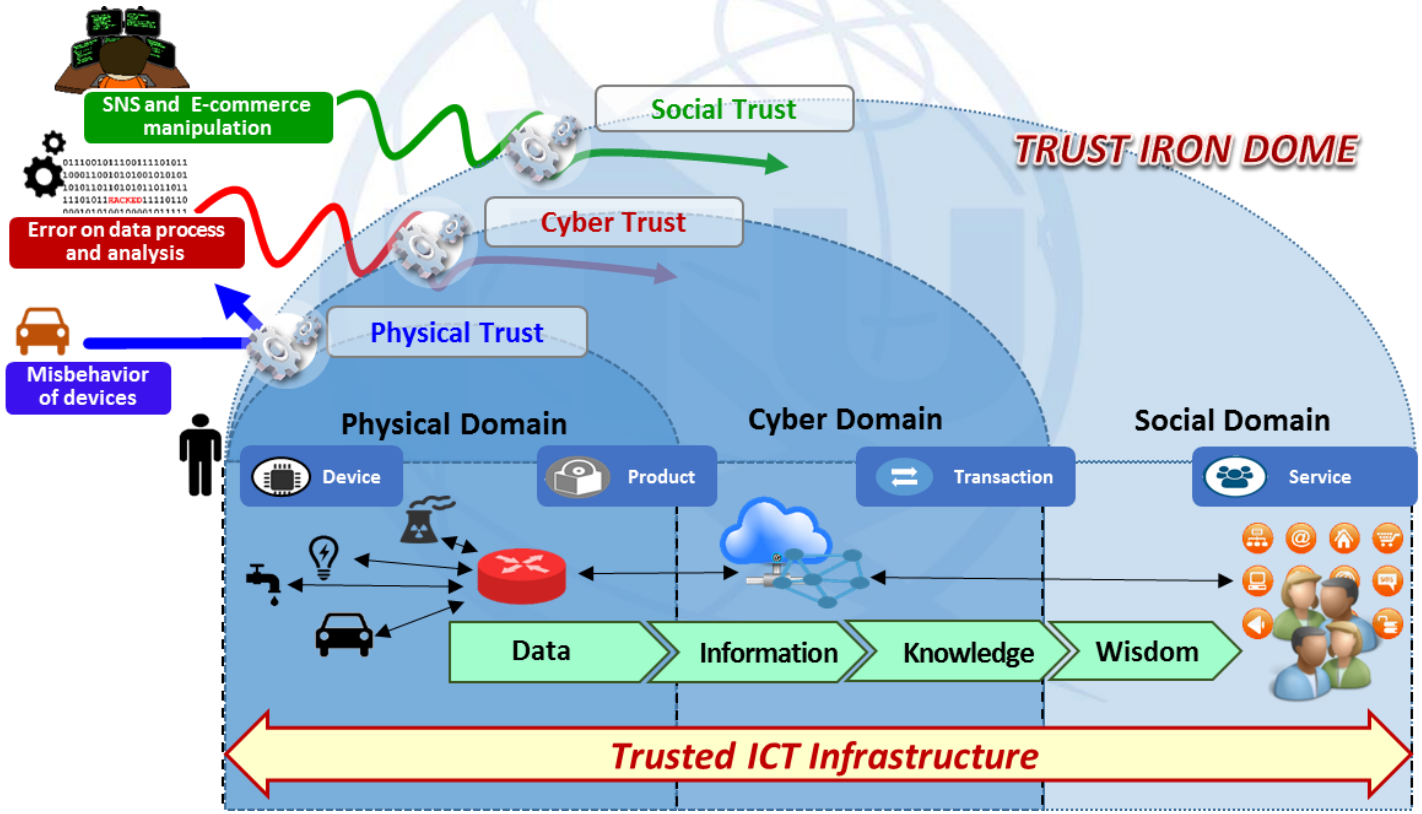
Trust Definitions

- **CG-Trust Technical Report**
  - Trust is an accumulated value from history and the expecting value for the future.
  - Trust is quantitatively and/or qualitatively calculated and measured, which is used to evaluate values of physical components, value-chains among multiple stakeholders, and human behaviours including decision making.
  - Trust is applied to social, cyber and physical domains.

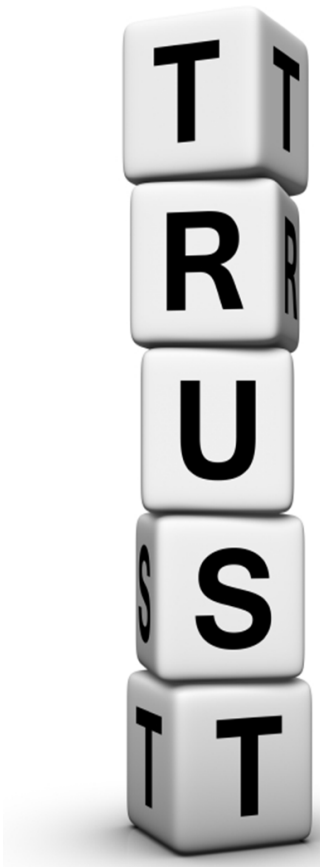
Relationship among security, privacy and trust with different aspects



Trusted ICT infrastructure



Attributes for Trust



Social domain		
Confidence	Dependence	Goodness
Belief	Ability	Honesty
Expectation	Faith	Integrity
Surety	Reputation	Assurance
Cyber domain		
Correctness	Completeness	Credibility
Relevance	Accuracy	Confidentiality
Physical domain		
Stability	Dependability	Reliability
Scalability	Reconfigurability	Availability

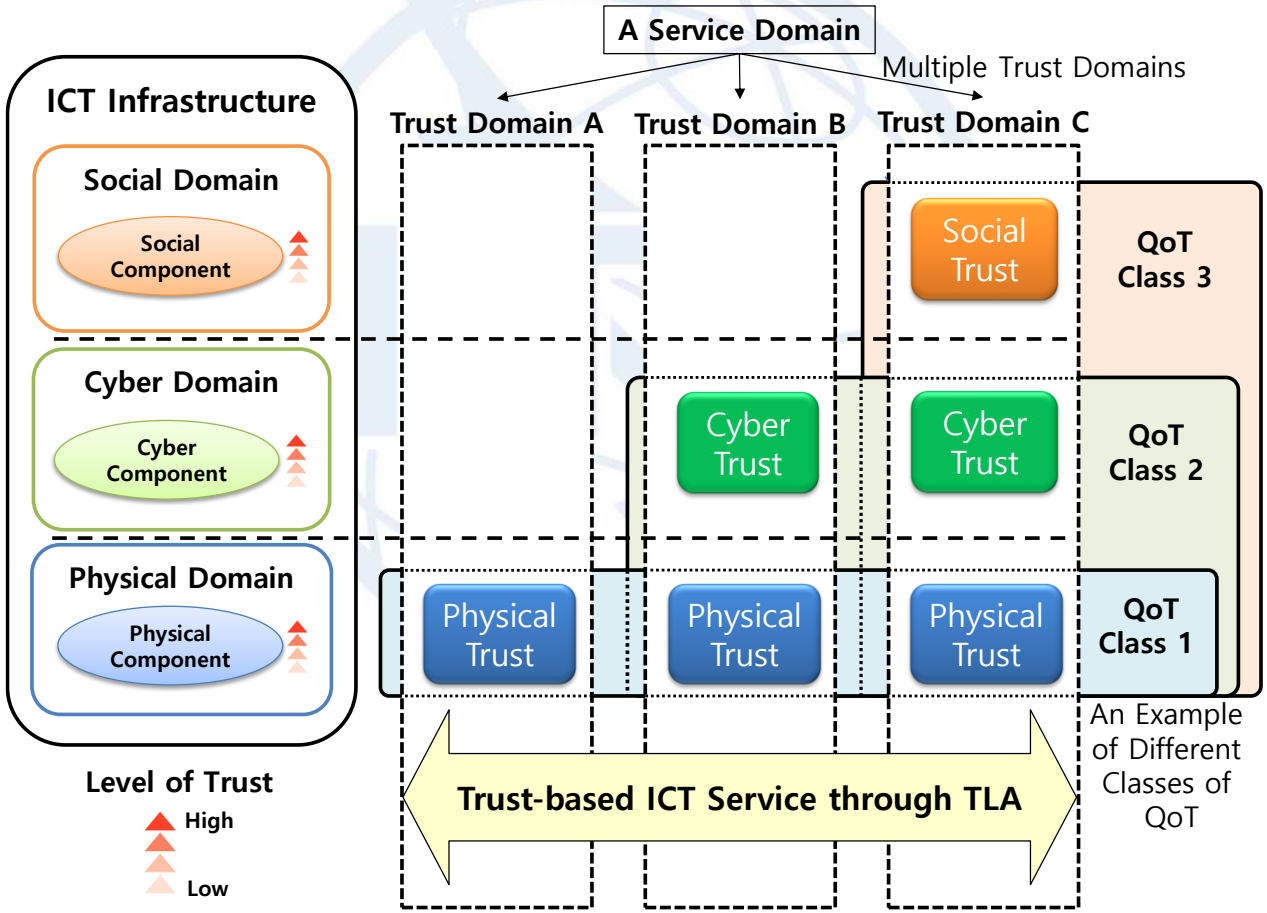
Trust Characteristics (1)

- Trust is **dynamic**
  - As it applies only in a given time period and maybe change as time goes by.
- Trust is **context-dependent**
  - Trust applies only in a given context. The degree of trust on different contexts is significantly different.
- Trust is **not transitive** in nature but maybe transitive within a given context.
- Trust is an **asymmetric** relationship.
  - Trust is a non-mutual reciprocal in nature.

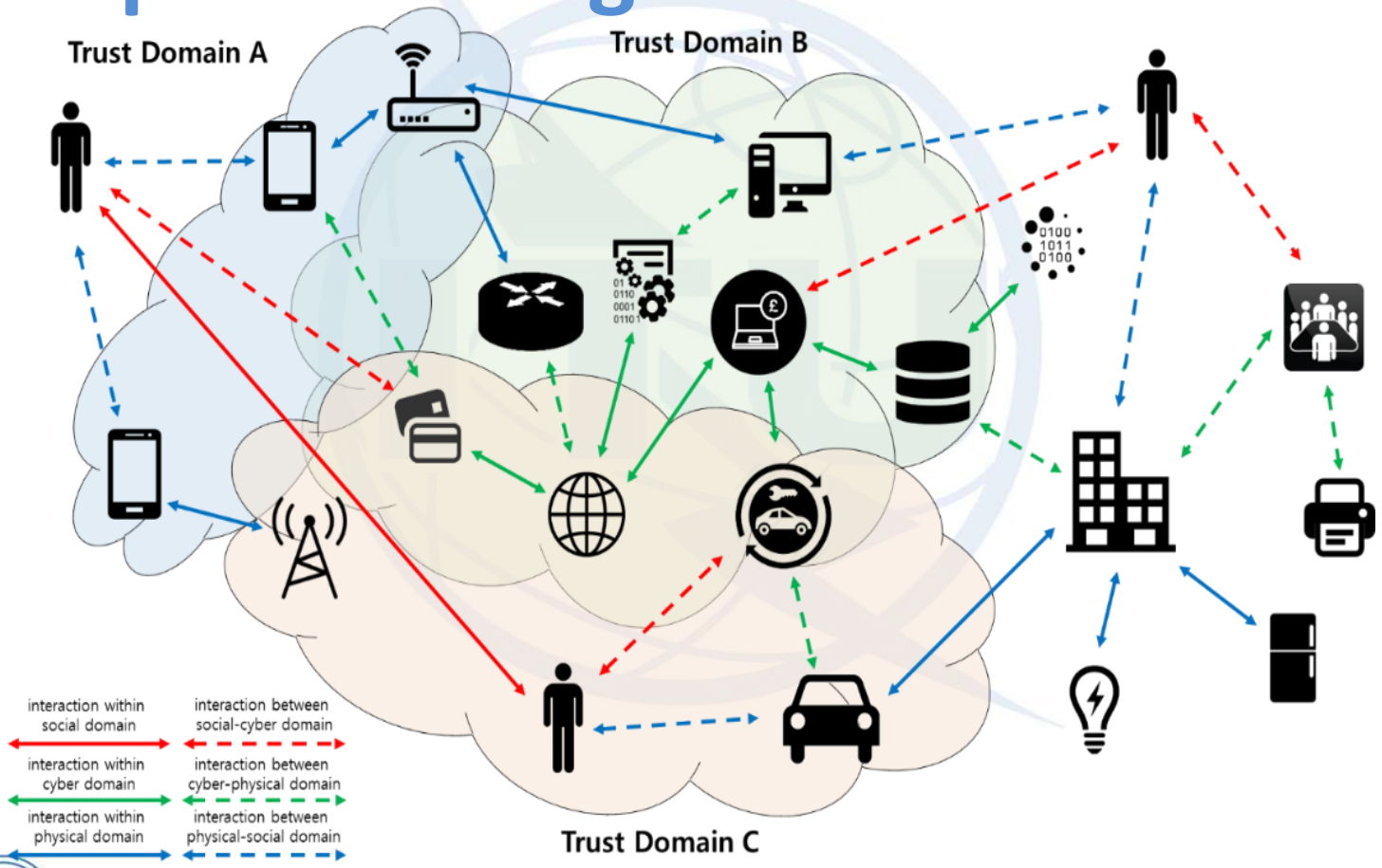
Trust Characteristics (2)

- Implicit
  - It is hard to explicitly articulate the confidence, belief, capability, context, and time dependency of trust.
- Antonym
  - The articulation of trust context in two entities may differ based on the opposing perspective.
- Asynchrony
  - The time period of trusting relationship may be defined differently between the entities.
- Gravity
  - The degree of seriousness in trust relationships may differ between the entities.

QoT and TLA among multiple trust domains

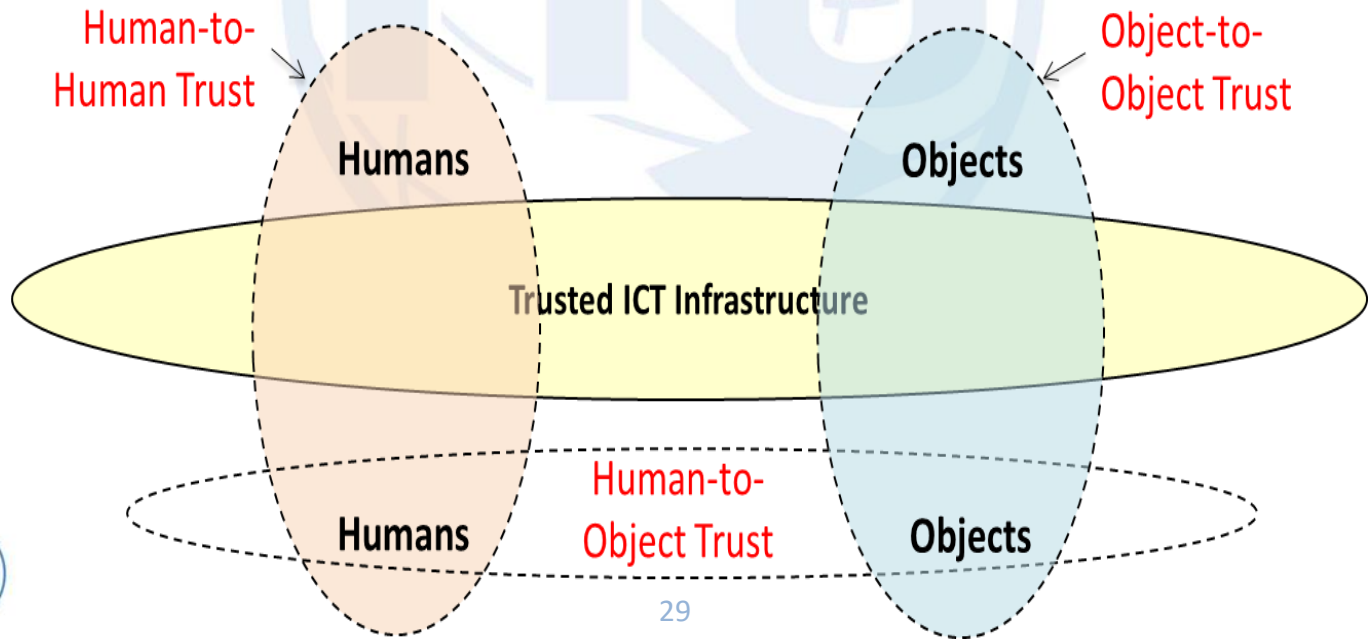


Interactions among entities for trust provisioning in a real world



Key challenges for trust provisioning (1)

- Trust Relationship
  - **Social** trust among humans and things
  - From **individual** trust to **community** trust



Key challenges for trust provisioning (2)

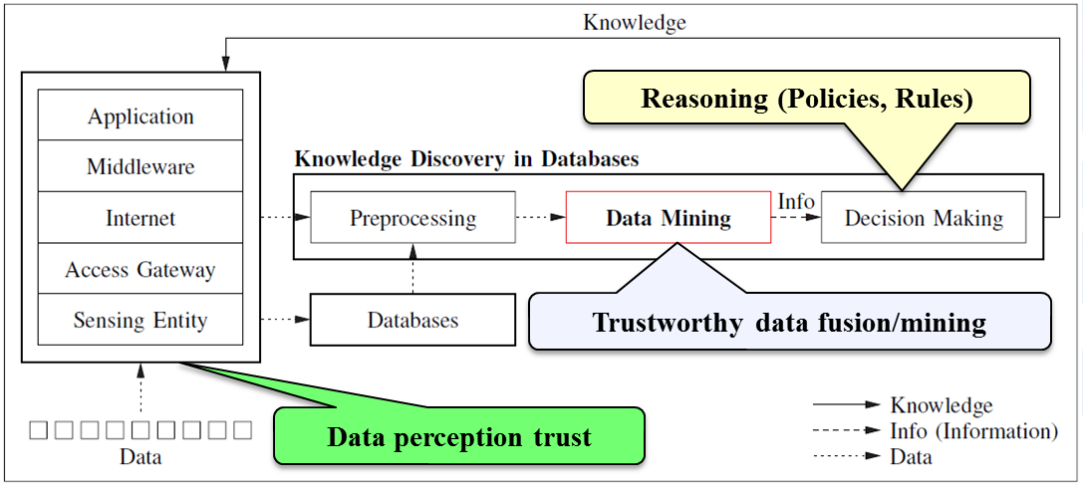
- Highly interconnected ICT infrastructure
  - A new kind of **complex system**
- Assuring continuous trustworthiness
  - Trust is situation-specific and trust changes over time
- Scalability and complexity
  - Trust, security and privacy become tightly coupled
  - **A unified approach** towards trust, security and privacy co-analysis, design, implementation and verification
- Inter-domain trust provisioning
  - Social-cyber-physical trust relationships

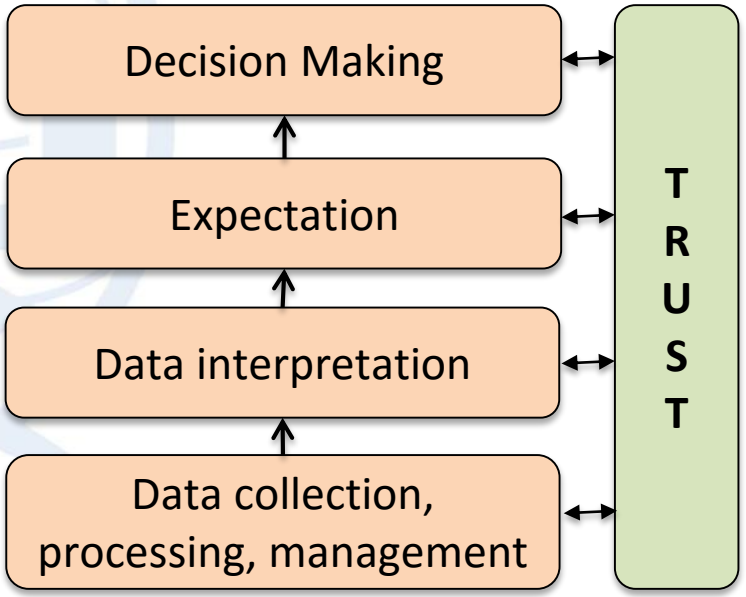
Technical Issues (1)

- Trustworthy data collection and aggregation
- Trustworthy data process and analysis
- Trust metric and modelling
- Trust index
- Dissemination of trust information
- Trustworthy system lifecycle management

Technical Issues (2)

- Trust management in a holistic manner





Technical Issues (3)

- **Trust metric**
  - A measure to evaluate a level of trust by which a human or an object can be judged or decided from trustworthiness.
  - Key issue – to describe qualitative and quantitative metrics across the domains, to determine the attributes in the different domains
- Trust model
  - A method to specify, build, evaluate and ensure trust relationships among entities.
  - Used for the processing trust data.
  - Key issue – to select a suitable trust model for a particular domain.

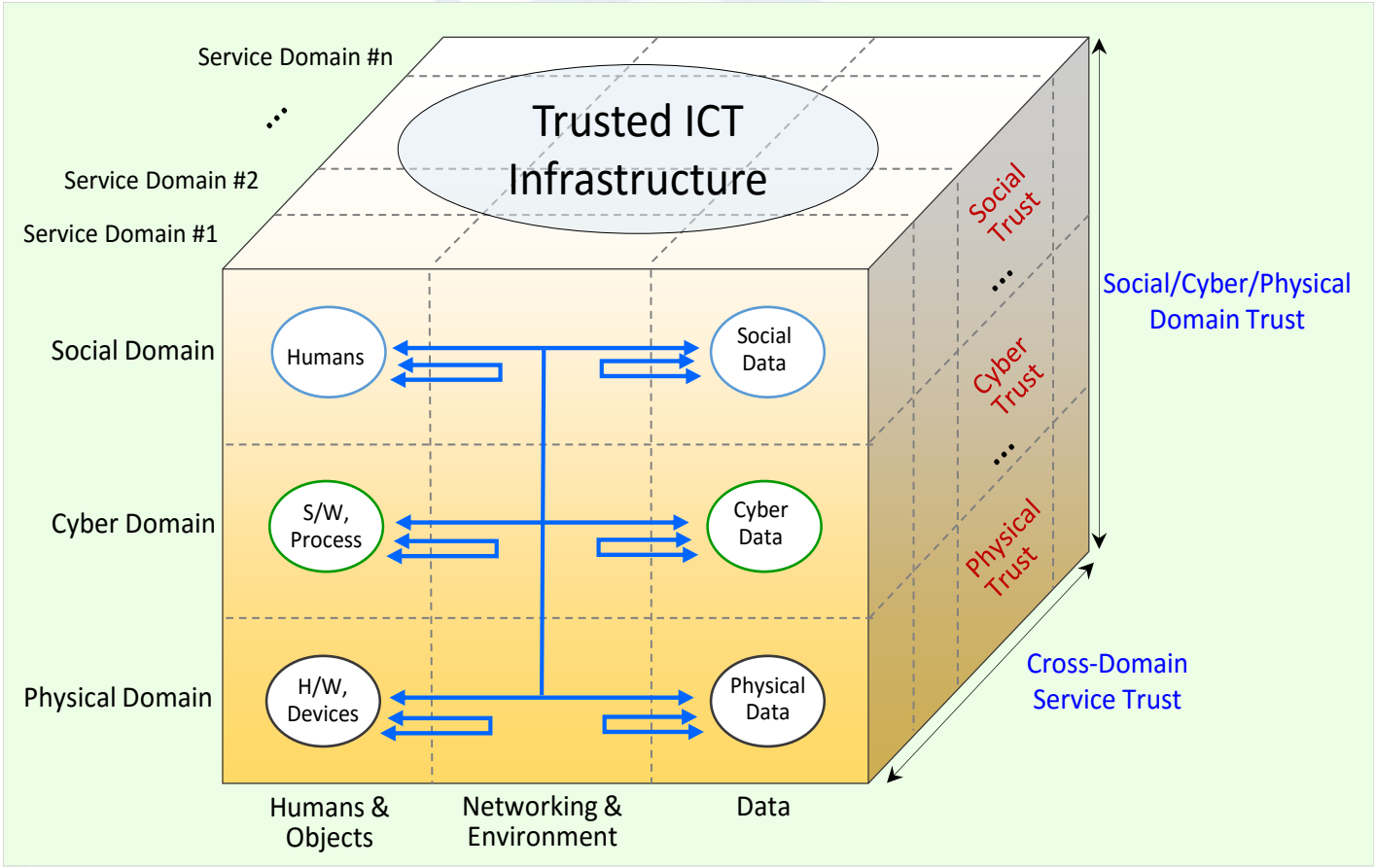
Technical Issues (4)

- **Trust Index**
  - A composite and relative value that combines multiple trust related indicators (e.g., objective trust metrics and subjective trust attributes) into one benchmark measure
    - Similar to ICT Development Index (IDI) or stock market index.
  - Used to compare trust among stakeholders when they create a new trust relationships or a trust value chain.

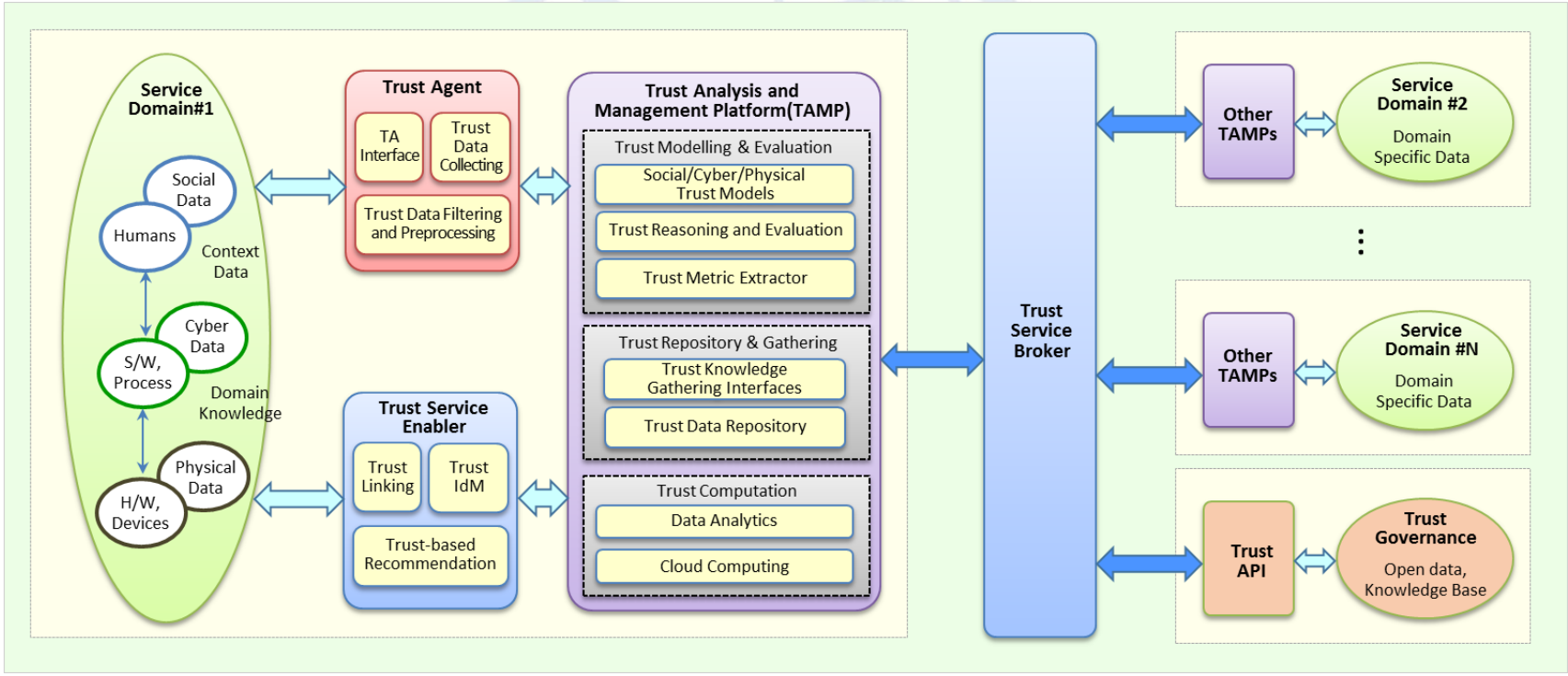
Architectural Overview

- The model developed in CG-Trust
  - Three different vertical domains (i.e., social, cyber and physical domains)
  - Three different horizontal components (i.e., humans & objects, networking & environment and data)
  - Multiple service domains for supporting a multiplicity of applications.
- Intends to illustrate the complex relationships and required roles for trust provisioning between and across domains which are associated with an individual entity of ICT infrastructures and services.

A Generic ICT Trust Model



Architectural Framework

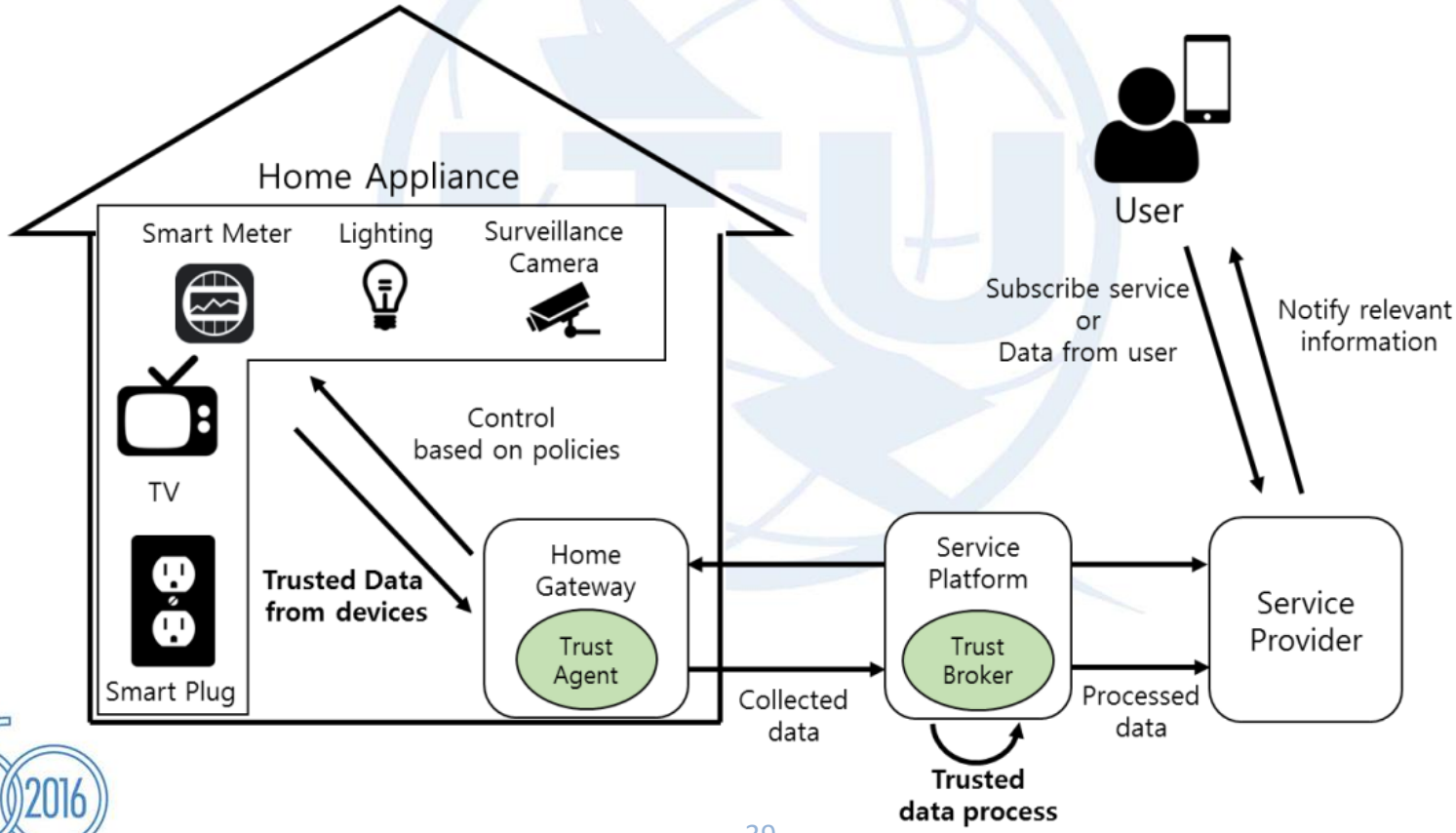


Use Cases – Summary

No	Use case	Purpose	Method
1	**Trustworthy smart home service**	Managing home facilities	Trustworthy home-related data → Providing personal information to service platform
2	**Trustworthy smart office service**	Managing office facilities	Trust level of users → Determining facility usage right
3	**Trustworthy document sharing service**	Sharing document with appropriate users	Trust level between users → Determining authority of accessing document
4	**Device selection for data transmission**	Selecting trustful device for D2D communication	Trust level between devices → Selecting appropriate device for transmission
5	**Trustworthy car sharing service**	Promoting trustworthy car sharing	Trustworthy data about a shared car and users' data → Providing an information of shared car and its user
6	**Trustworthy used car transaction service**	Mediating transparent used car transaction	Trustworthy data about a used car → Providing transparent car history information

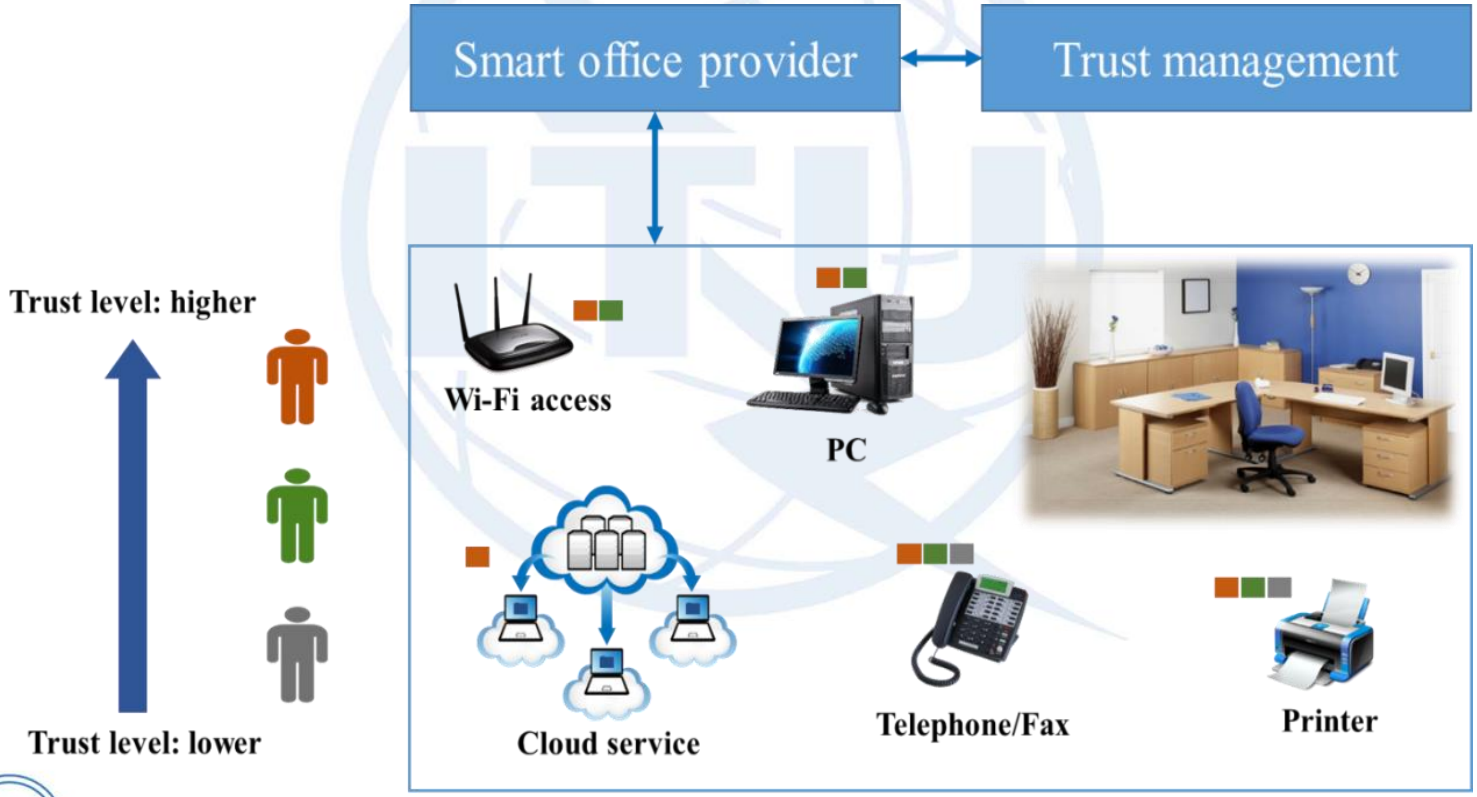
Use Case – Smart Home Service

Enables users to monitor and manage the home appliances remotely and safely.



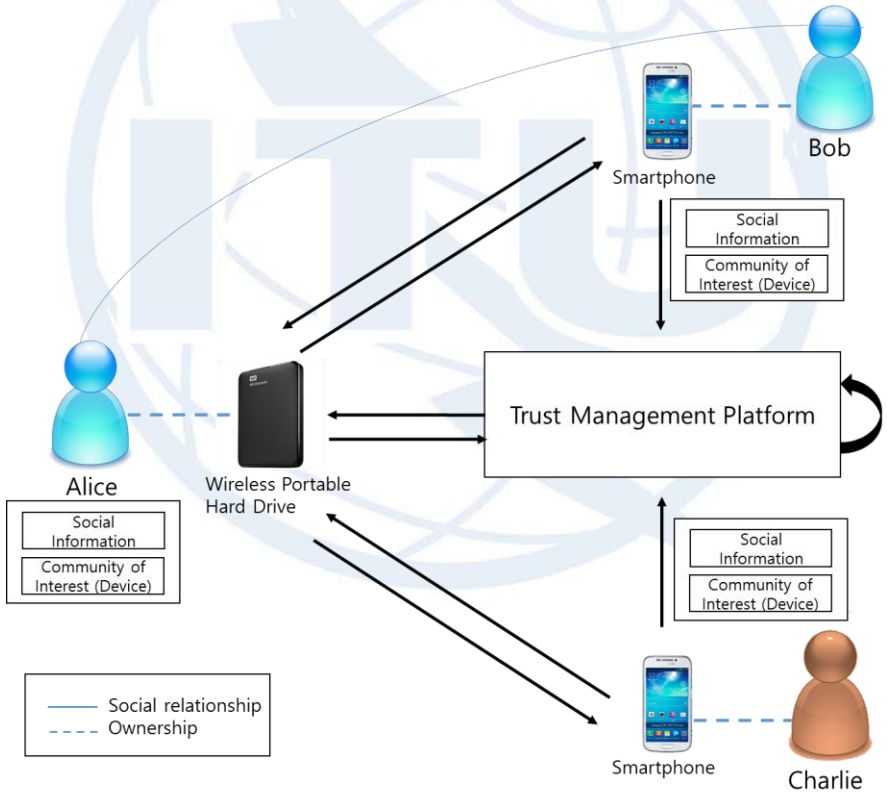
Use Case – Smart Office Service

Allows users utilizing various facilities in office based on the trust level of users.



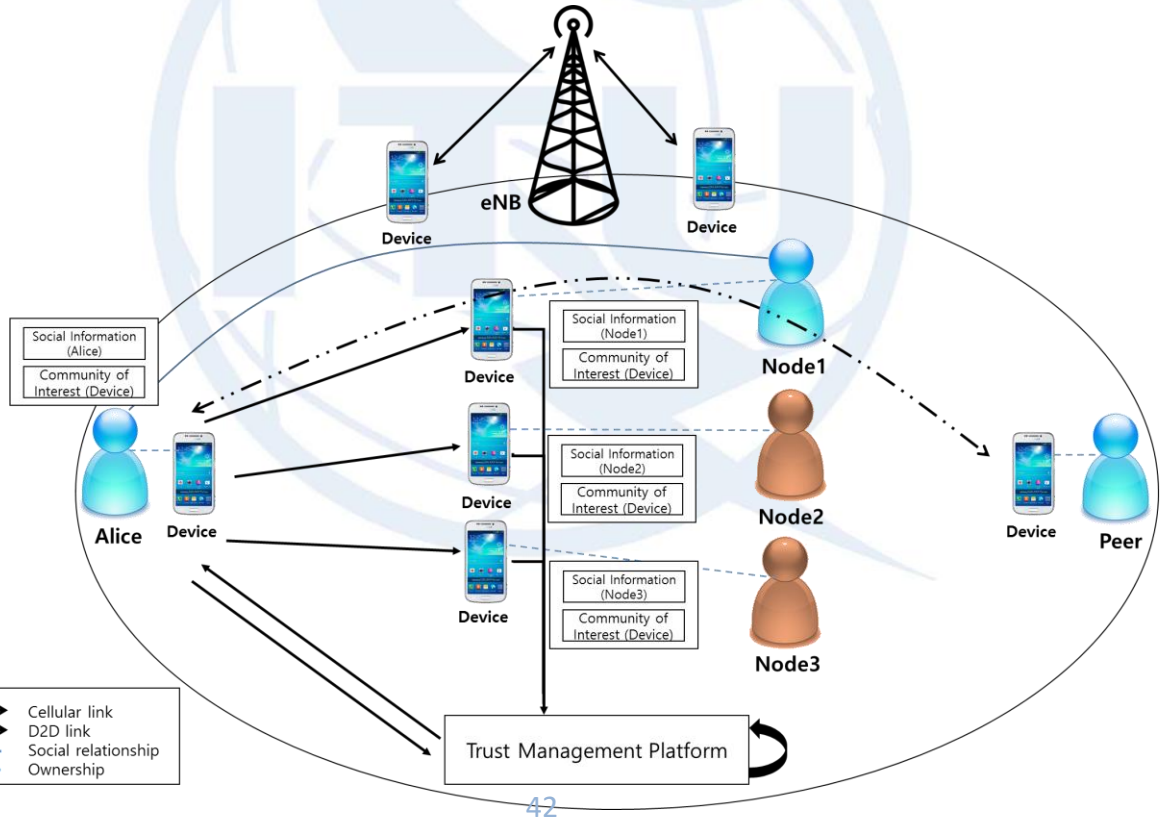
Use Case – Document Sharing Service

Sharing the document among co-workers using social trust value among them.



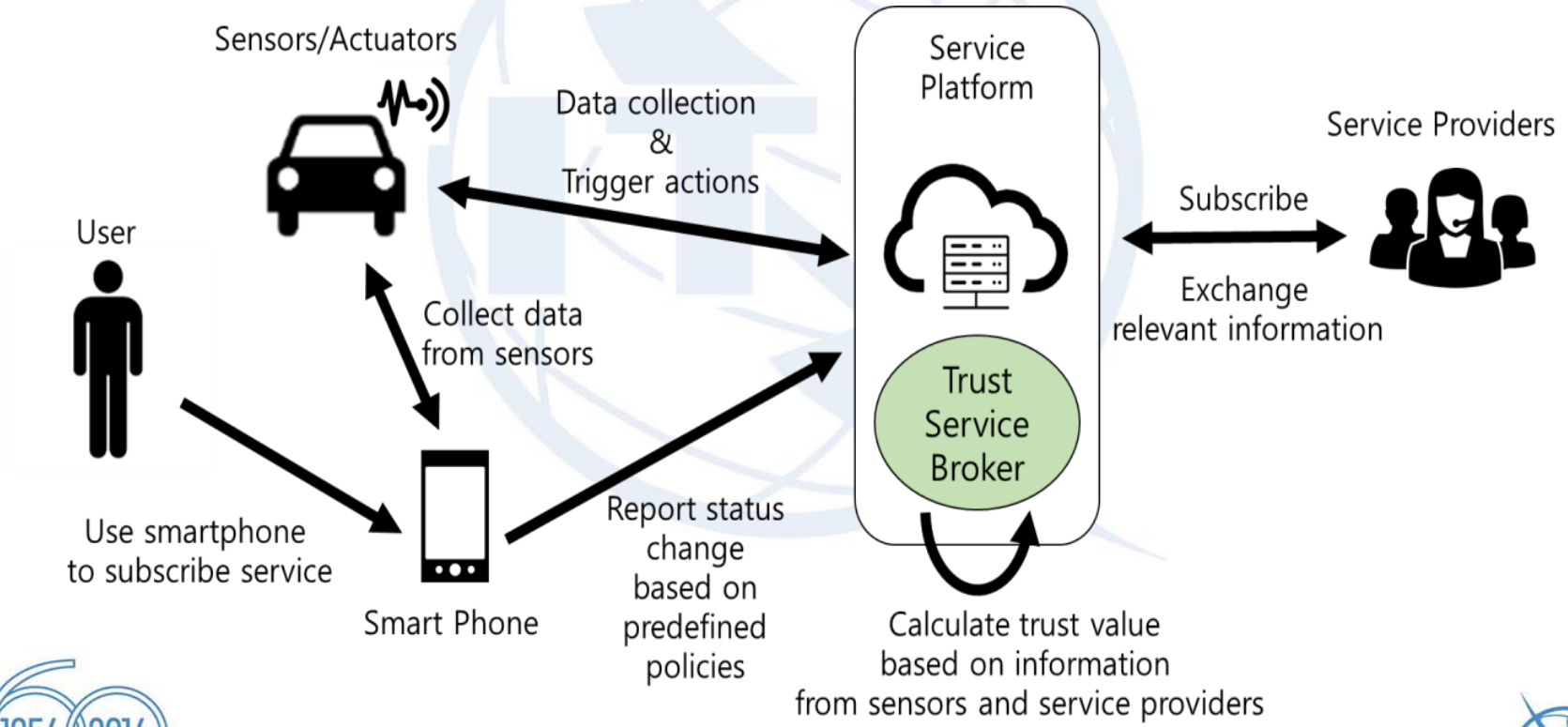
Use Case – Device Selection for Data Transmission

Selecting the device for data transmission in multi-hop Device-to-Device (D2D) environment using social trust value among devices.



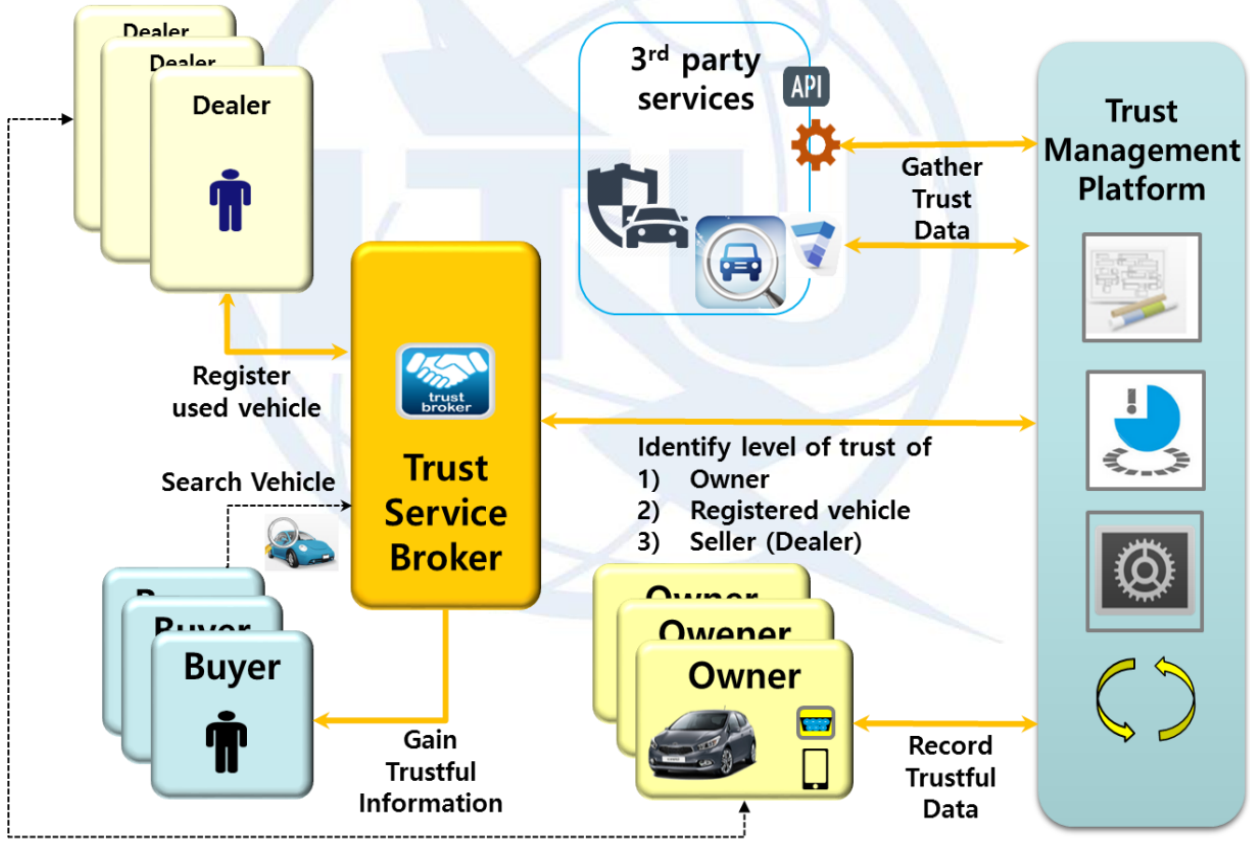
Use Case – Car Sharing Service

Provides reliable transaction in consideration of trustworthiness of users and cars.



Use Case – Used Car Transaction Service

Buying a used car in trustworthy procedure.



Strategies for Future Standardization on Trust

Trust Standardization (1)

- ITU-T SG13 - Correspondence Group on Trust
  - Started new work on **future trusted ICT infrastructures** to cope with emerging trends in ICT while also considering social and economic issues.
  - Completed to develop a technical report on **trust provisioning for future ICT infrastructures and services**.

Trust Standardization (2)

- Other SDOs
  - Until now, focusing on **network security and cybersecurity**
    - To be expanded to take into consideration trust issues
  - **Online Trust Alliance**, **Trusted Computing Group**
    - Still limited to social trust between humans
    - Further consideration on trust between humans and objects as well as across domains of SCP and services

Future Standardization on Trust (1)

- **New work Items** on Trust in ITU-T
  - Overview of trust in ICT;
  - Service scenarios and capabilities;
  - Requirements for trust provisioning;
  - Architectural framework and functional architectures;
  - Technical solutions for trust provisioning;
  - Trust provisioning for convergence applications;
  - Trust provisioning for cloud computing.

Future Standardization on Trust (2)

- Incorporate trust issue into related SGs activities in ITU-T
  - **SG17**: A liaison with SG17 activities on security matters
  - **SG20**: Trust in IoT applications, services and platforms as well as smart cities infrastructure
  - **Others**: The identification issue with SG2, trust in financial services with Focus Group on Digital Financial Services
- Closely collaborate with **other SDOs**
  - **Existing security solutions**: IETF, W3C
  - **IoT**: oneM2M, FI-WARE, Open Connectivity Foundation, AllSeen Alliance
  - **Cloud Computing**: TCG, Cloud Security Alliance
  - **Other groups**: OTA

ITU-T Next Study Period – 1

- SG13
  - Future networks, with focus on IMT2020, cloud computing, big data and **trust in ICT**
- Lead study group on
  - Future networks
  - IMT2020 networks (non radio related) including softwarization
  - Mobility management
  - Cloud computing/big data and **trust in ICT**

ITU-T Next Study Period – 2

- Question G/13 - **Knowledge-centric trustworthy networking and services** (Continuation of Question 11/13 and 16/13)
  - Development of new Recommendations related to:
    - Knowledge-centric **trustworthy networking and services**;
    - Environment-aware networking and services for reducing energy consumption and energy efficiency management;
    - **Socio-economic** aware networking and services for **trusted ICT infrastructures**;
    - Interworking between other networks (including specific networks, e.g., networks for vehicular, smart grid and healthcare, etc.) and services considering heterogeneous and constraint networking environments in end user side;
    - End user networks and their specific applications/services in end users perspective (e.g., enhancement of home networks, personal area networks, etc.).

Conclusion

Trust considerations as an important item for standardization

- **ITU-T**
  - Lead future knowledge societies in terms of standardization.
  - Initiate new work methods for future knowledge information infrastructures including pre-standardization and conceptual framework.
  - A strong leadership to collaborate with private sectors and academia which are outside of ITU-T.


ITU


1956
2016
CCITT / ITU-T