International Telecommunication Union

ITU-T Technical Report

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(29 April 2016)

Trust Provisioning for future ICT infrastructures and services

Summary

This technical report provides an overview of trust provisioning for future ICT infrastructures and services. It describes the importance and necessity of trust from potential risks toward knowledge societies in terms of ICT and provides the concepts and key features of trust. After identifying key challenges and technical issues, it also presents architectural overview of trusted ICT infrastructures. And then, it introduces trust based ICT service models and summary of use cases, and it proposes strategies for future standardization on trust. The trust related activities in other standardization bodies, backgrounds for ICT service model analysis framework and detailed use cases are also provided in informative appendices.

Keywords

Trust provisioning, ICT infrastructure, ICT service, Knowledge society

Change Log

None

Forward

This Technical Report has been developed by Mr Hyeontaek Oh, Mr Tai-won Um, Mr Jun Kyun Choi.

CONTENTS

Page

List of Tables

List of Figures

Technical Report ITU-T

Technical Report ITU-T
Trust Provisioning for future ICT infrastructures and services

Summary

This technical report provides an overview of trust provisioning for future ICT infrastructures and services. It describes the importance and necessity of trust from potential risks toward knowledge societies in terms of ICT and provides the concepts and key features of trust. After identifying key challenges and technical issues, it also presents architectural overview of trusted ICT infrastructures. And then, it introduces trust based ICT service models and summary of use cases, and proposes strategies for future standardization on trust. The trust related activities in other standardization bodies, backgrounds for ICT service model analysis framework and detailed use cases are also provided in informative appendices.

1 Scope

This technical report provides an overview of trust provisioning for future trusted ICT infrastructures and services. More specifically, this technical report covers the following:

- 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.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in the text of this technical report form basis and help understanding the topic of trust provisioning in ICT. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; readers are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

[ITU-T M.3410] Recommendation ITU-T M.3410 (2008), *Guidelines and requirements for security management systems to support telecommunications management.*

[ITU-T X.509] Recommendation ITU-T X.509 (2012), *Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks*

[ITU-T X.1163] Recommendation ITU-T X.1163 (2015), *Security requirements and mechanisms of peer-to-peer-based telecommunication networks.*

[ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions.*

[ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1.*

[ITU-T Y.2720] Recommendation ITU-T Y.2720 (2009), *NGN identity management framework.*

3 Terms and definitions

3.1 Terms defined elsewhere

This Technical Report uses the following terms defined elsewhere:

3.1.1 Cloud computing [b-ITU-T X.1601]: A paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with on-demand self-service provisioning and administration.

3.1.2 Internet of Things [b-ITU-T Y.2060]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

NOTE 2 – From a broader perspective, the IoT can be perceived as a vision with technological and societal implications.

3.1.3 Knowledge society [b-UN]: The knowledge society is one in which institutions and organizations enable people and information to develop without limits and open opportunities for all kinds of knowledge to be mass-produced and mass-utilized throughout the whole society.

3.2 Terms defined here

3.2.1 Trust: Trust is an accumulated value from history and the expecting value for 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.

NOTE 1 - Trust is applied to social, cyber and physical domains.

NOTE 2 – Trust [ITU-T X.509]: Generally, an entity can be said to "trust" a second entity when it (the first entity) assumes that the second entity will behave exactly as the first entity expects. The key role of trust is to describe the relationship between an authenticating entity and an authority; an entity shall be certain that it can trust the authority to create only valid and reliable certificates.

NOTE 3 – Trust [ITU-T X.1163]: The relationship between two entities where each one is certain that the other will behave exactly as it expects.

NOTE 4 – Trust [ITU-T X.1252]: The firm belief in the reliability and truth of information or in the ability and disposition of an entity to act appropriately, within a specified context.

NOTE 5 – Trust [ITU-T Y.2701]: Entity X is said to trust entity Y for a set of activities if and only if entity X relies upon entity Y behaving in a particular way with respect to the activities.

NOTE 6 – Trust [ITU-T Y.2720]: A measure of reliance on the character, ability, strength, or truth of someone or something.

4 Abbreviations

API Application Programming Interface

B2B	Business-to-Business
B2C	Business-to-Customer
CoI	Community of Interest
CPS	Cyber-Physical System
D2D	Device-to-Device
DDoS	Distributed Denial-of-Service
DIKW	Data, Information, Knowledge and Wisdom
DPI	Deep Packet Inspection
IaaS	Infrastructure-as-a-Service
ICT	Information and Communication Technology
IdM	Identity Management
IETF	Internet Engineering Task Force
IoT	Internet of Things
ITU	International Telecommunication Union
LBS	Location Based Service
M2M	Machine-to-Machine
NFC	Near Field Communication
OAM&P	Operations, Administrations, Maintenance, and Provisioning
OBD	On-Board Diagnostics
OIC	Open Interconnect Consortium
OS	Operating System
OTA	Online Trust Alliance
PaaS	Platform-as-a-Service
PIN	Personal Identification Number
QoE	Quality of Experience
QoS	Quality of Service
QoT	Quality of Trust
SaaS	Software-as-a-Service
SDO	Standards Development Organization
SG	Study Group
SLA	Service Level Agreement
SNS	Social Network Service
TA	Trust Agent
TAMP	Trust Analysis and Management Platform
TCG	Trusted Computing Group

TLA	Trust Level Agreement
TSB	Trust Service Broker
TSE	Trust Service Enabler
WAN	Wide Area Network
WSIS	World Summit on the Information Society
WWW	World Wide Web
W3C	World Wide Web Consortium

5 Introduction to Trust toward Knowledge Societies

5.1 Toward knowledge societies

At the 15th International Telecommunications Union (ITU) Plenipotentiary Conference, year 1999, the World Summit on the Information Society (WSIS) was created to develop the information society. During the first phase of the WSIS, the debates on the information society are mainly focused on information and communication technology (ICT) infrastructures. The concept of knowledge societies is more all-embracing and more conducive, which is simply "opens the way to humanization of the process of globalization." The notion of knowledge is central to changes of education, science, culture, and communication. Knowledge is recognized as the object of huge economic, political and cultural stakes, to the point of justifiably qualifying the societies currently emerging.

Knowledge is defined as a familiarity, awareness or understanding of someone or something such as facts, information, description or skills. Knowledge is acquired through experience or education by perceiving, discovering and learning. It can refer to theoretical or practical understandings of a subject that is implicit (as with practical skill or expertise) or explicit (as with theoretical understanding of a subject). It can be more or less formal or systematic.

In the networked society, knowledge is a source of all human being including behaviours and building a society. The networking of knowledge and the speeding up of information processing open up new possibilities for work on databases, irrespective of their size, their use and their ultimate purpose. The current Internet as a public network gives fresh opportunities to achieve equal and universal access to knowledge. Like Internet, new ICTs have created for emergence of knowledge societies [b-UNESCO]. Future knowledge societies will be built on the basis of ICT infrastructures since it is not only for delivery of digital data, but also provides the eco-platform to share data, information, and knowledge.

Accordingly, as a top level standard organization relating to ICTs as well as the United Nations agency, the ITU should concern about future knowledge societies.

5.2 Potential risks in ICT infrastructures

Knowledge societies will have to cope with instability and insecurity since the accelerated spread of knowledge will be confronted with risks in ICT infrastructures. There are many potential risks in ICT infrastructures as follows.

- **In nature**
  - **New technology development**: Any scientific progress and technology development may incur potential risks. New technologies may not be stable without guarantee of stability and reliability. Without acceptable confidence, it may cause unexpected

accident and destroy the existing value chain of business. The development of new technologies may be sometimes undesirable if the certain levels of controllability and credibility are not guaranteed. Furthermore, the adaptation of new technologies may cause instability and insecurity since new technologies always have uncertainty. In the ICT infrastructure, new technological revolution may provide great advantages for utilizing networking resources. However, it confronts unidentified risk beforehand.

- **Human behaviours**
  - **Human-human interactions**: If there is no trust among peoples, their interactions (e.g., exchanging data and information) have meaningless due to lack of confidence with each other. If the people are not trustworthy, personal interactions do not invoke any response. The unclear decision making or unrealistic situation may be happening from low or broken trust in human relationships.
  - **Human-machine interactions**: When a human cannot trust a machine (e.g., delivering imprecise data from a machine to a human), human-machine interactions cannot be established and potential benefits on system performance will be lost. The human-machine systems have always proved unpredictable and fallible, whereas the nature of the system is to function normally. It relies on technological dependency which accentuates risks.
  - **Human interactions in cyber-physical system (CPS) environments**: The CPS cannot be fully operable if a physical world and a cyber world have some mismatch. If the malfunction of a physical system does not notify at the responsible entities in a cyber world, there are some risks to prevent safety in a physical world. An intelligent human in a cyber world can avoid or reduce the risk of failures and minimize the unacceptable situation in a physical world. The time critical convergence applications such as smart grid and intelligent transportation systems require high trust between a cyber world and a physical world. Greater openness, in combination with hiding one's real identity in a physical world and making a false object in a cyber world, increases the risks that people are becoming victims of deception. They also include identity theft and exposure to inappropriate actions.
  - **Human errors**: Without recognizing a set of rules and external conditions of a physical system, human actions may result on risks or failures. Human errors may be a primary cause or a contributing factor in risks and accidents. Intentional or unintentional human errors may cause serious problems in ICT infrastructures.
- **Complexity of ICT infrastructures**
  - **A numerous number of ICT resources**: Risks threaten us to cope with complexity of interactions and mechanisms of ICT infrastructures. The access of a large number of ICT resources causes irreparable damages and creates unpredictable dangers. It is essential to make ICT resources accessible to all the people with promises but with unknown dangers.
  - **Complexity of network operation**: There are a lot of algorithms for network resource optimization including efficient routing, congestion avoidance, and guaranteeing Quality of Service (QoS)/Quality of Experience (QoE). When the unpredictable situations are happened in a network, the out-of-service possibility is increasing. Natural disaster and distributed denial-of-service (DDoS) attacks are also a part of risks. While network control functions can arrange the by-pass or de-tour route to cope with overflowed traffic, the unexpected side effects like traffic fluctuation and domino effect may bring additional risks. To increase network survivability during network operation, networking protocols and OAM&P (Operations, Administrations,

Maintenance, and Provisioning) functions should be re-designed to be trustworthy. Moreover, when a network infrastructure includes a cloud platform with large volume of storage and processing capabilities, network instability is not coming only from traffic congestion. The operation of the cloud platform and high level applications are additional harmful sources to increase network risks. The existing security functions including firewall and Deep Packet Inspection (DPI) may be replaced to provide the certain level of trust, through the implementation by a trust gateway system and trust-guaranteed network OAM functions.

- **Data, information and knowledge process**: Since future ICT infrastructures should provide data, information and knowledge process, the trust provisioning is quite essential. Data integrity refers to maintain and assure the accuracy and consistency of data. The failure of data aggregation is coming from any unintended changes to data as the results of storage, retrieval and processing operation for further information and knowledge. For example, if data stored in a cloud platform are shared by anonymous users, there may be a possibility to happen undesirable situations. With a certain level of trust, data delivery and cognitive data, information, knowledge and wisdom (DIKW)1 process may be effective and meaningful.
- **Complexity of convergence services and applications**: ICT based services and applications will continue to be heterogeneous, and this may lead to increase a number of convergence services that cover multiple service domains. Especially, in Internet of Things (IoT) and CPS environments, people, platforms and devices will be highly inter-connected by a dynamic network of networks and operated in heterogeneous environments. These kinds of highly connected environments increase the complexity of services and applications (which consume data and information from connected sensors, devices, etc.), and the unknown potential risks may be incurred due to complex interactions. As ICT based applications and services will scale over multiple domains and involves multiple stakeholders, methods for assessing trust are needed to enable the users to have confidence to these services and applications.

5.3 Trust for future ICT infrastructures and services

For evolving toward knowledge societies, ICT will be mainly used for the creation, dissemination and utilization of knowledge in an open and collaborative manner. Although recent advances in ICT have brought changes to our everyday lives, various problems exist due to the lack of trust. The large scale collection and analysis of data from sensors and devices in physical spaces imposes difficult issues, ranging from the risks of unanticipated uses of consumer data to the potential discrimination enabled by data analytics and the insights offered into the movements, interests and activities of an individual. If knowledge is exploited for malicious intentions, it could suffer from irreparable damage and uncertain dangers. However, it is difficult to identify and prevent risks of knowledge in complicated ICT infrastructures.

The convergent services have been required to obtain reliable knowledge from raw data. As an aim of intelligent service provision is to make autonomous decisions without human intervention, trust has been highlighted as a key issue in the processing and handling of data, as well as the provisioning

---

1 DIKW (Data, Information, Knowledge and Wisdom): This refers loosely to a class of models for representing purported structural and/or functional relationships between data, information, knowledge, and wisdom. "Typically information is defined in terms of data, knowledge in terms of information, and wisdom in terms of knowledge". (Source: https://en.wikipedia.org/wiki/DIKW_Pyramid)

of services which comply with users' needs and rights. Therefore, we need to find a way to minimize the unexpected risks and maximizing the survivability of future knowledge societies. Within certain reliability and predictability, the ICT infrastructure can be operating in a controlled environment. It should be robust to unexpected conditions and adaptable to system failures.

Based on the significant efforts made to build converged ICT services and a reliable information infrastructure, ITU-T has recently started new work on future trusted ICT infrastructures. These infrastructures will be able to accommodate emerging trends in ICT, while taking into account social and economic considerations. Thus, this report addresses trust provisioning for future ICT infrastructures and services which act as the glue for integrating physical, cyber and social worlds with ICT as a basis for knowledge societies. It provides the trust conceptual model and the trust architectural framework to cope with potential risks due to the lack of trust. The aim is to create a trusted ICT infrastructure for sharing information and creating knowledge and to stimulate activities for future standardization on trust with related Standards Developing Organizations (SDOs).

6 Understanding of Trust

6.1 Generic definitions of trust

As a lexical-semantic, trust means reliance on the integrity, strength, ability, surety, etc., of a person or object. Generally trust is used as 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.

Trust concept itself is a complicated notion with different meanings depending on both participators and situations and influenced by both measurable and non-measurable factors. There are various kinds of trust definitions leading to difficulties in establishing a common, general notation that holds, regardless of personal dispositions or differing situations. Generally, trust is considered as a computational value depicted by a relationship between trustor and trustee, described in a specific context and measured by trust metrics and evaluated by a mechanism.

Previous research has shown that trust is the interplay among human, social sciences and computer science, affected by several subjective factors such as social status and physical properties; and objective factors such as competence and reputation [b-Alcalde]. The competence is measurement of abilities of the trustee to perform a given task which is derived from trustee's diplomas, certifications and experience. Reputation is formed by the opinion of other entities, deriving from third parties' opinions of previous interactions with the trustee.

Trust revolves around assurance and confidence that people, data, entities, information or processes will function or behave in expected ways. At the deeper level, trust is regarded as a consequence of progress towards security or privacy objectives.

Trust is crucial that it affects the appetite of an entity to use services or products offered by another entity. This trust may come from our past experience of using these brands' products (termed "belief") or from their reputations that are perceived from people who bought items and left their opinions about those products (termed "reputation"), or from suggestions of your surrounding such as families and friends (termed "recommendation").

It is challenging to concisely define "trust" of an entity due to its uniqueness to each individual entity. From a sociological point of view, trust is defined as the trusting behaviour that one person has on another person in a situation where an ambiguous path exists. In such definition, trust is used to mitigate the risks of the dealings with others. Trust is also considered as the capacity and belief of an entity that the other entity would meet its expectations.

6.2 Trust in ICT Environments

As trust can be interpreted in different ways, there are various meanings from literature for more clear views on trust in terms of telecommunication systems and ICT.

The term trust in the context of ICT world differs from the concept of trust among people. This notion of trust stands in contrast to some more intuitive notions of trust expressing that someone behaves in a particular well-behaved way. Trust in ICT is an important concept in the sense that a trusted resource is one that you are forced by necessity to trust. The failure of this resource would compromise the function, integrity or security of a system which are not in expected ways.

Nevertheless, trust is an important feature in the decision-making process not only used by humans in daily life but also by applications and services in ICT environment.

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."

Trust in an on-line transaction can be divided into two types: direct (personal) trust and third party trust. Direct trust is a situation where a trusting relationship is nurtured by two entities. This type of trust is formed after these entities have interacted with each other. The entity A inherently trusts entity B after a number of successful transactions that involved both entities. On the contrary, third-party trust is a trust relationship of an entity that is formed from the third party recommendations. For example, entity A trusts entity B because B is trusted by entity C and C recommends that B is trustful. In this example, entity A derives trust of B from C, and A also trusts entity C does not lie to him.

Due to dynamics of network configuration and resources, trust issue occurs not only in the human to human network, but also in machine to machine and human to machine and vice versa. In other words, trust is needed not only for people to maintain social network service benefit, but also for machine to be connected safely to network. System/network-related trust is the beliefs that a specific technology has the attributes necessary to perform as expected in a given situation in which negative consequences are possible [b-McKnight].

Trust is a broad concept used in many disciplines and subject areas but until now, there is no commonly agreed definition. Therefore, ITU-T CG-Trust has newly defined the terms "trust" Clause 3.2.1. As per the definition, trust in the ICT world is defined as "Trust is an accumulated value from history and the expecting value for 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 value is applied to social, cyber and physical domains. Figure 6-1 shows various related attributes for trust in social, cyber and physical domains.

NOTE 1 – Clause 7 presents the details of social, cyber and physical domains.

NOTE 2 – Appendix I provides the summary of trust definitions from various viewpoints.

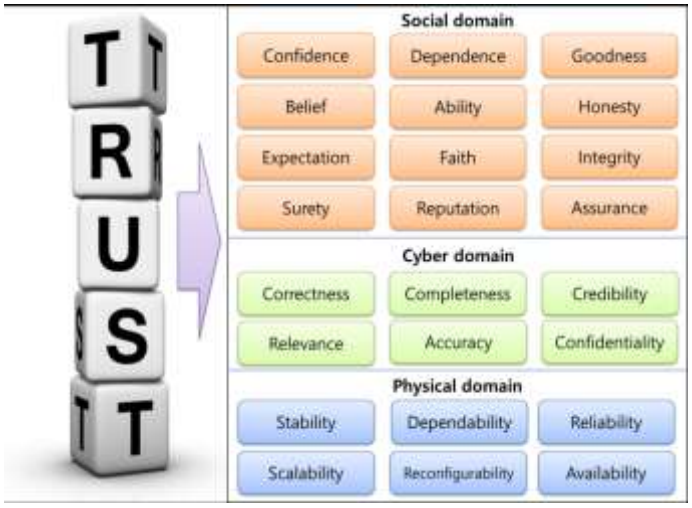

Figure 6-1: Attributes for trust

6.3 Relationship among security, privacy and trust

– **Security**: systems need a variety of methods to prevent behaviours with malicious intents. Security mainly concerns technological aspects such as the confidentiality, availability and integrity. It also includes attack detection and recovery/resilience.

– **Privacy**: users need the protection of their personal information related to their behaviours and interactions with other people, services and devices. Privacy mainly concerns user aspects to support anonymity and restrictive handling of personal user data.

– **Trust**: trust is broader concept that can cover security and privacy (Figure 6-2). Trust revolves confidence that people, data, devices will function or behave in expected ways. Trust can be used to build new value-chain for future ICT infrastructure and services.

For example, security and privacy have controlled a system and data securely in social-cyber-physical domains. However, traditional secure system concerns about how to authorize the entities as well as how to provide data to the authorized entities. Trust can give reliability to security and privacy as a parameter by measuring a discrepancy between observation and objective or subjective expectation of the reliable entities and data.

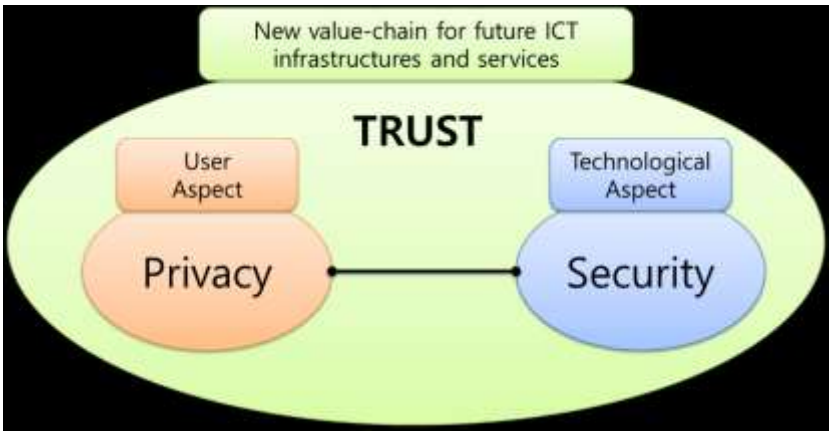

Figure 6-2: Relationship among security, privacy and trust with different aspects

6.4 Relationship between knowledge and trust

To understand trust, it is required to analyse the collected data from entities, extract the necessary information for trust, understand the information, and then create the trust-related knowledge.

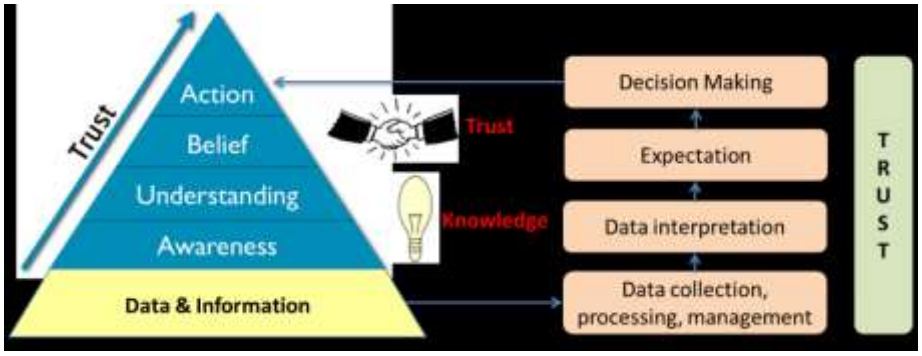

Figure 6-3: Knowledge and Trust[2]

The social and economic value of data is mainly reaped during two moments: first when data is transformed into knowledge (gaining insights) and then when it is used for decision making (taking action). The knowledge is accumulated by individuals or systems through data analytics over time. So far data processing, management and interpretation for awareness and understanding have been considered as fundamental processes for obtaining the knowledge. As shown in left hand side of Figure 6-3, trust is strengthened from accumulated knowledge and it mainly has a significant role as a belief between knowledge (i.e., awareness and understanding) and action. It means that the expectation process for trust should be additionally considered before decision making. As shown in the right hand side of Figure 6-3, trust should be further considered to the whole process from data collection to decision making.

7 Features, Challenges and Technical Issues for Trusted ICT infrastructures

7.1 Trusted ICT infrastructure

Figure 7-1 shows high-level overview for a trusted ICT infrastructure. A physical domain mainly consists of physical devices which interwork with each other through information and communication networks. A cyber domain is responsible for the delivery, storage and processing of data and information. A social domain has become popular to people for sharing and showing their knowledge and become a new medium for connecting people in cyberspace.

[2] Illustration compiled from trust pyramid: http://www.johnhaydon.com/how-make-people-trust-your-nonprofit/

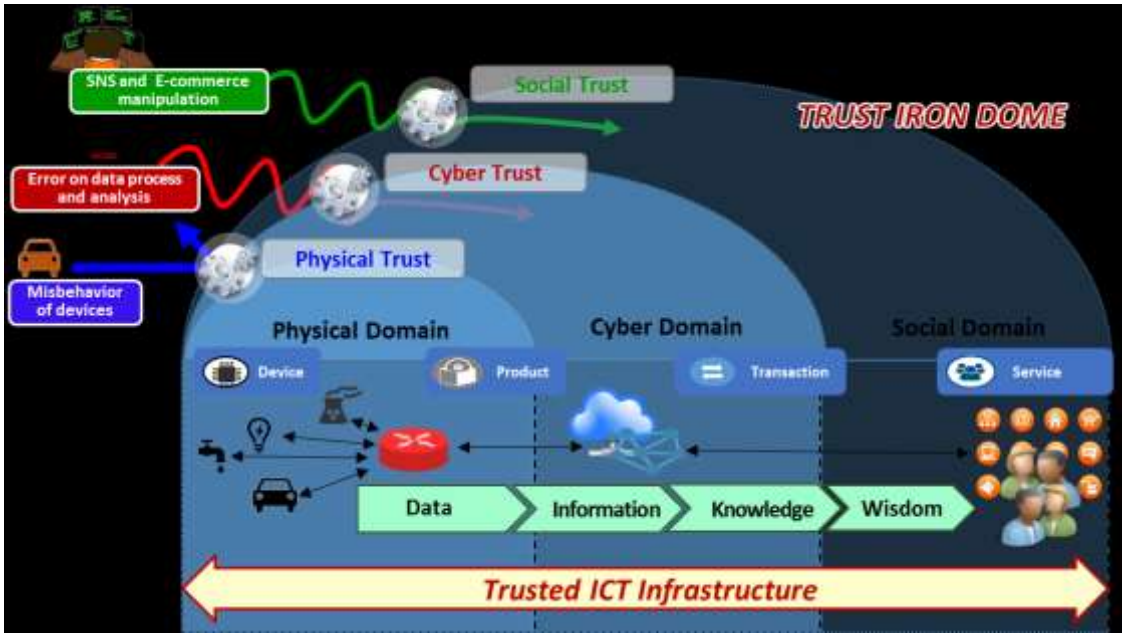

Figure 7-1: High-level overview of a trusted ICT infrastructure

The trusted ICT infrastructure comprise objects from the physical domain (physical objects), the cyber domain (virtual objects) and the social domain (humans with attached devices), which are capable of being identified and integrated into information and communication networks. All of these objects have their associated information, which can be static and dynamic.

NOTE – Clause 8.1 provides detailed explanations on physical trust, cyber trust and social trust.

7.2 Key features of trust

- **Trust** characteristics

There are several important characteristics of trust that further enhance our understanding about trust digital environments.

– **Trust is dynamic**: as it applies only in a given time period and maybe change as time goes by. For example, for the past one year Alice highly trusts Bob. However, today Alice found that Bob lied to her, consequently, Alice no longer trusts Bob.

– **Trust is context-dependent**: trust applies only in a given context. The degree of trust on different contexts is significantly different. For example, Alice may trust Bob to provide financial advice but not for medical advice.

– **Trust is not transitive in nature but maybe transitive within a given context**. That is, if entity A trusts entity B, and entity B trusts entity C then entity A may not trust entity C. However A may trust any entity that entity B trusts in a given context although this derived trust may be explicit and hard to be quantified.

– **Trust is an asymmetric relationship**. Thus, trust is a non-mutual reciprocal in nature. That means if entity A trust entity B, then the statement "entity B trusts entity A" is not always true.

The nature of trust is fuzzy, dynamic and complex. Besides asymmetry and transitivity, there are additional key characteristics of trust: implicitness, antonym, asynchrony, and gravity [b-Chang-2005, b-Chang-2006].

– **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. For example, entity A trusts entity B in the context of "buying" book, however from entity B to entity A the context is "selling" book.

– **Asynchrony**: The time period of trusting relationship may be defined differently between the entities. For example, entity A trusts entity B for 3 years, however, entity B may think that the trust relationship only last for the last 1 year.

– **Gravity**: The degree of seriousness in trust relationships may differ between the entities. For example, entity A may think that its trust with entity B is important, however, entity B may think it differently.

• **Trust among multiple trust domains**

Trust domain is a set of information and associated resources consisting of users, networks, data repositories, and applications (or services) that manipulate the data in those data repositories. For providing a trust-based service, multiple trust domains are involved. Different trust domains may share the same social-cyber-physical components. Also, a single trust domain may employ various levels of trust, depending on what the users need to know and the sensitivity of the information and associated resources [ITU-T M.3410].

– **Quality of Trust (QoT)**: Due to the diversity of applications and their inherent differences in nature, trust is hard to be formalized in a general setting. However, it is important to quantify a level of trust in ICT infrastructures. A certain level of trust should be derived from the associated devices, services, applications and users of trust. The level of trust can be measured and classified objectively or subjectively. The concept of QoT, which is similar with QoS as an objective manner (e.g., measured quantitatively) or QoE as a subjective manner (e.g., counted qualitatively), represents different classes in terms of levels of trust in multiple domains (e.g., physical, cyber, and social domains). It can be used to understand the degree of trust among multiple trust domains.

– **Trust Level Agreement (TLA)**: Depending on what QoT the users need, including those related to sensitivity of information and associated resources, there may be a lot of TLAs – similar to the concept of Service Level Agreement (SLA).

Figure 7-2 shows an example of different classes of QoT among multiple trust domains in an ICT infrastructure. A service domain may consist of multiple trust domains (e.g., three trust domains in this figure). Depending on levels of trust for each component, a trust domain may have different classes of QoT. For example, trust domain A provides physical trust (QoT Class 1), trust domain B provides physical and cyber trust (QoT Class 2), and trust domain C provides physical, cyber and social trust (QoT Class 3). Then, TLA is established, based on the agreement of all involved trust domains using the QoT information to provide a trust-based ICT service.

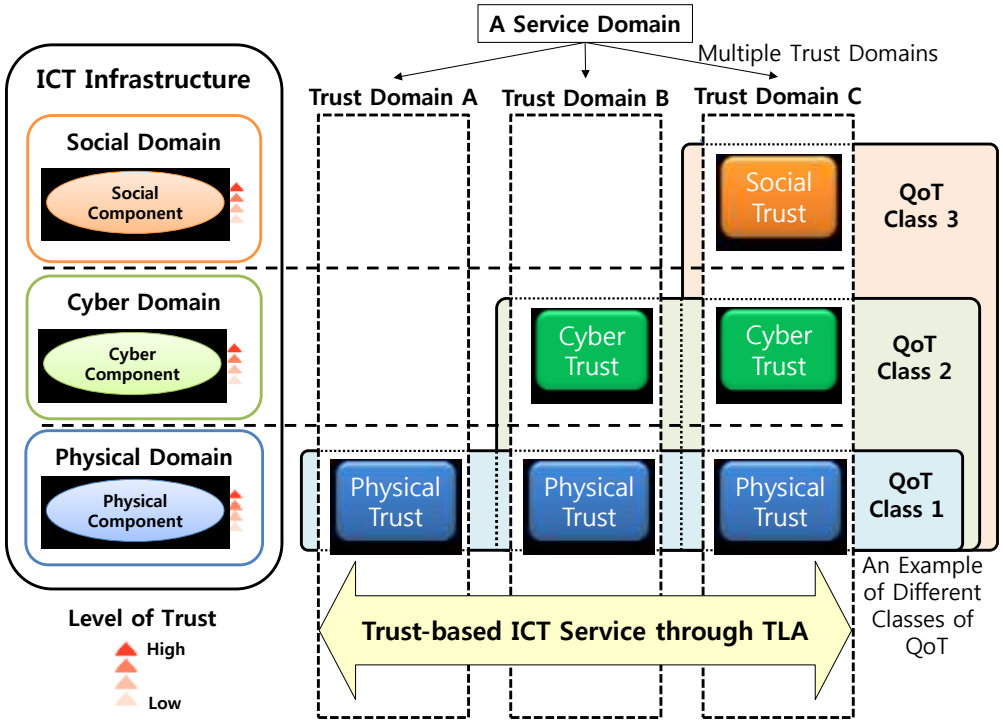

Figure 7-2: An example of QoT and TLA among multiple trust domains

From the concepts of trust domains in the previous figure, Figure 7-3 illustrates several interactions among entities for trust provisioning in a real world. These interactions are based on trust relationships of each entity in social, cyber and physical domains according to different classes of QoT.

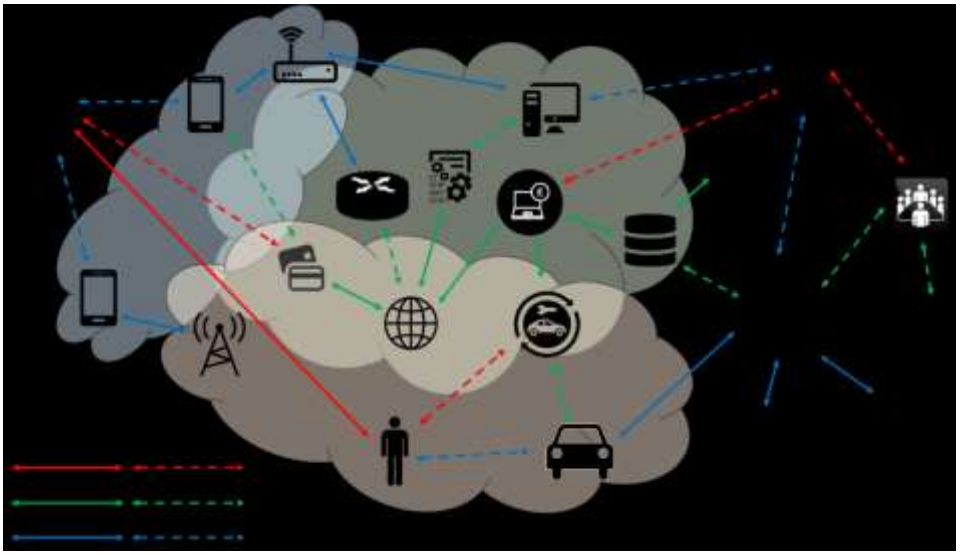

Figure 7-3: Illustration of interactions among entities for trust provisioning in a real world

7.3 Key challenges for trust provisioning

This clause describes key challenges for trust provisioning for ICT infrastructures.

Trust relationship may be human to human, object to object (e.g., handshake protocols negotiated), human to object (e.g., when a consumer reviews a digital signature advisory notice) or object to human (e.g., when a system relies on user input and instructions without extensive verification) as shown in Figure 7-4. For social-cyber-physical relationships, trust is taking into consideration coexistence, connectivity, interactivity and spatio-temporal situations across domains.

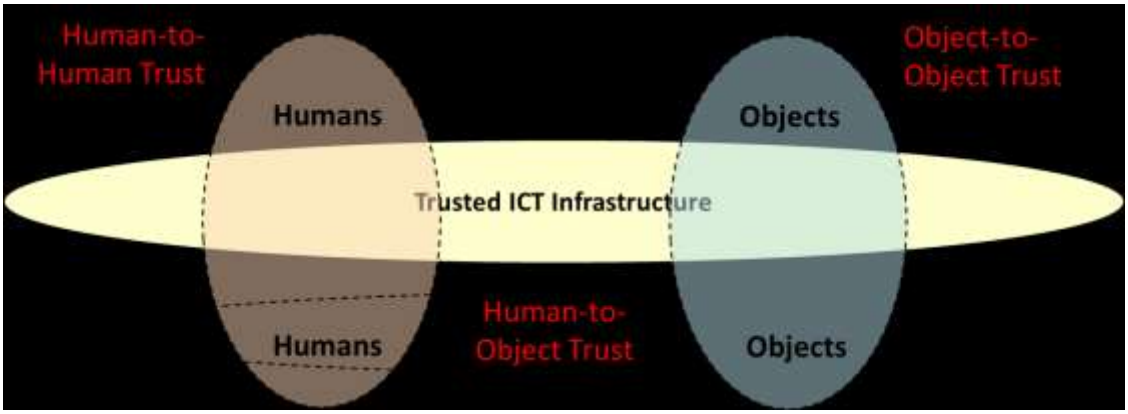

Figure 7-4: Trust relationships in a trusted ICT infrastructure

In this highly interconnected ICT infrastructure, a number of independently developed, operated and managed objects are autonomously networked, yielding a new kind of complex system that provides various services. Furthermore, services and applications are now open their platform through common interfaces. Such characteristics of interconnected systems lead to the introduction of security vulnerabilities that can be very hard to find and analyse. If it is not properly handled, the stability and safety of the overall system can be seriously threatened.

Assuring continuous trustworthiness, taking into account such characteristics for trusted ICT infrastructures with highly interconnected systems, is becoming a key challenge. Trust must be addressed and evaluated in all services and infrastructures, as well as in all system and component levels, in a holistic manner. Trust management is required to apply between heterogeneous systems and stakeholders, while focusing on the relationships and dependencies between them. Also, the state of objects changes dynamically in the ICT infrastructure, (e.g., sleeping and waking, connected/disconnected, and node failure etc.) as does their context, including location and speed. Moreover, the number of entities also fluctuates. That is, trust is situation-specific and trust changes over time.

On the other hand, for scalability and complexity of ICT infrastructures due to the huge number of different links and interactions, trust, security and privacy become tightly coupled because system features increasingly depend on networks, computation and processing. Trustworthiness requires cooperation and co-engineering with security and privacy. It is not sufficient to address one of them in isolation, nor is it sufficient simply to combine components of trust, security and privacy. In order to address these issues, a unified approach is needed towards trust, security and privacy co-analysis, design, implementation and verification. In case of small-size sensor devices, because of its severe resource constraints and dynamics, conventional security approaches cannot fully cover security demands of the IoT domain, and trust technologies can be used as additional complementary features to support the security demands.

Trust provisioning is desirable to combine features from different domains for developing inter-domain trust provisioning which is able to cover social-cyber-physical trust relationships. For trust provisioning for ICT infrastructures, these key challenges are considered to new trust provisioning technology.

7.4 Technical issues for trust provisioning

This clause describes technical issues for trust provisioning for ICT infrastructures. Following technical issues should be considered: i) trustworthy data collection and aggregation, ii) trustworthy

data process and analysis, iii) trust metric and modelling, iv) dissemination of trust information, v) trust index and vi) trustworthy system lifecycle management.

7.4.1 Trustworthy data collection and aggregation

As the number of data sources and types are dramatically increased, the trustworthiness of data itself is regarded as important. Because collection and aggregation of false data will lead to a degradation of service quality and waste of system resources, it is a significant issue to detect wrong or polluted data. Trust metrics and models can be used as criteria for checking trustworthiness to achieve trusted data collection and aggregation.

7.4.2 Trustworthy data process and analysis

When the huge amounts of data are collected to a system, these data should be processed and analysed in trustworthy ways. Data process and analysis mainly occurs in cyber domain (e.g., utilizing cloud computing for big data analysis), however, it also can be done in a physical domain as well as a social domain. Each domain has its own intelligence to process incoming data to create new useful information. This information is usually propagated to different entities and domains, so there are some ways to check whether given data process and analysis mechanism is trustworthy or not. Measurable trust value should be defined to analyse trust of entities, and it is also important to find appropriate trust evaluation mechanisms for analysing trust values for a specific domain.

7.4.3 Trust metric and modelling

A trust metric is a measure to evaluate a level of trust by which a human or an object can be judged or decided from trustworthiness. It can be differently defined in each human or each object. Trust metrics might be separately defined in each of domains, but the key issue is to describe qualitative and quantitative metrics across the domains, to determine the attributes in the different domains. For measurable trust, some mechanisms and solutions may be established by defining trust metric. There are several attributes social-cyber-physical domains for trust provisioning. Attributes in each domain of Figure 6-1 are examples. Depending on the services and applications, the required attributes of trust may vary.

A trust model is the method to specify, build, evaluate and ensure trust relationships among entities. The trust model is used for the processing trust data. Most existing trust models are based on the understanding of trust characteristics, accounting for factors influencing trust. Trust modelling is domain-specific and there exists numerous ways to define trust model for each domain. It is a critical issue to select a suitable trust model for a particular domain.

7.4.4 Trust index

A trust index is a composite and relative value that combines multiple trust related indicators (e.g., objective trust metrics and subjective trust attributes) into one benchmark measure, which is similar to ICT Development Index (IDI) or stock market index. It can be used to compare trust among stakeholders when they create a new trust relationships or a trust value chain. The trust index should be designed to quantify a trust value of each stakeholder, and the methodology used to compute trust index should be clearly defined. In order to apply the trust index to a real world, common indicators for covering different stakeholder characteristics and comparing methods for trust indices of different stakeholders should be developed.

7.4.5 Dissemination of trust information

Trust dissemination means to distribute or broadcast trust information. There could be many ways of disseminating trust information in different domains. In case of a social domain, recommendation and

visualization methods are considered as main approaches to disseminate trust information [b-Sherchan]. The efficient, effective and suitable trust dissemination methods should be developed.

7.4.6 Trustworthy system lifecycle management

In order to achieve trustworthy systems, we need a systematic methodology to cover all relevant trust aspects of operation life cycle. At the design phase, the definition, metrics and goals of trust for the target system should be determined and the system should be developed while trust measures are considered to fulfil the design goals in the development phase. The maintenance phase has to properly monitor the normal operation of the running of a trustworthy system and the dynamics of the execution environment to verify the trust provisions at runtime.

8 Architectural overview for trust provisioning for ICT infrastructures

8.1 Generic ICT trust conceptual model

From the concept of trust provisioning for a trusted ICT infrastructure described in Clause 7, a generic ICT trust conceptual model is shown in Figure 8-1 to clarify architectural overview for trust provisioning for ICT infrastructures. The model comprises three different domains vertically (i.e., social, cyber and physical domains) and three different horizontal components (i.e., humans & objects, networking & environment and data). In addition, there are multiple service domains for supporting a multiplicity of applications. This model 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.

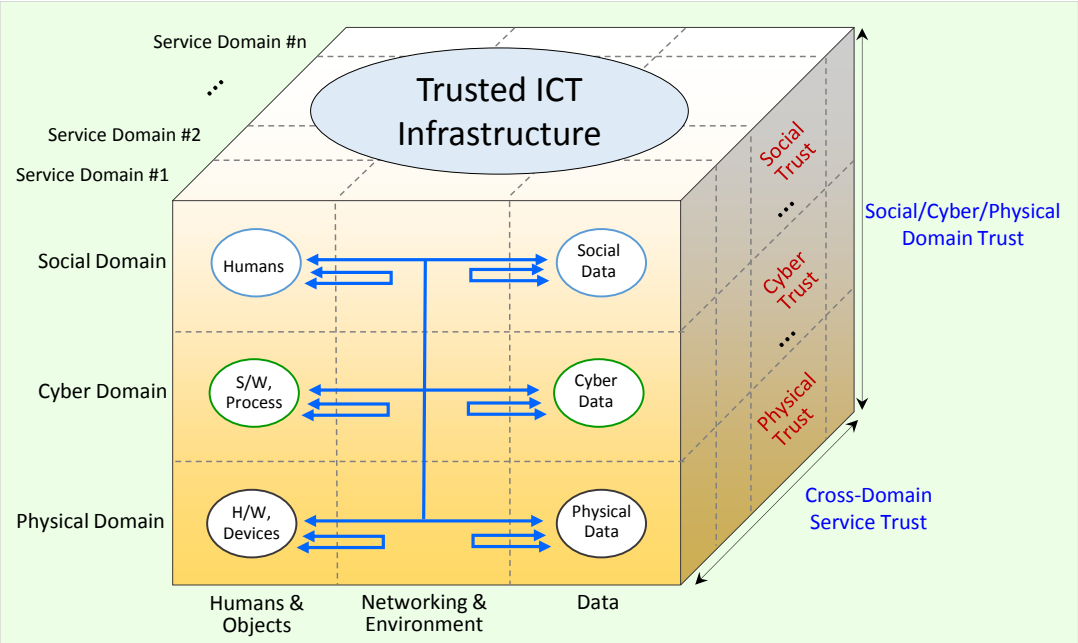

Figure 8-1: A generic ICT trust conceptual model

Physical trust

A physical domain contains a huge number of objects (i.e., H/W or device) including sensors, actuators, mobile terminals, which generate data by using sensing technologies to sense physical objects and their behaviours within their environments (e.g., temperature, pressure, etc.). Collecting

secure and reliable data from physical objects is the first step to provide trustworthy ICT services and applications because the propagation and process of false data will cause service degradation and waste system resources.

In order to detect trust problems in the physical domain such as injections of obstructive signals, malfunctions of systems, shutdowns or accidents, the operations of the physical objects and their data must be examined. Since many data are created from constrained devices, lightweight trust mechanisms are needed for data processing trust (e.g., efficiency, accuracy, reliability, etc.).

Cyber trust

A cyber domain includes virtual objects such as software agents, services and applications working over computing, storage and networking components. These virtual objects are seamlessly interconnected and cooperated for data coding, transmission, fusion, mining and analysing to provide information and knowledge to humans independent of location in fixed/mobile environments.

In order to safely cooperate between virtual objects, they have to distinguish malicious and non-malicious objects. One way to resolve this challenge is to evaluate the trust with their specific goal to decide which virtual objects to cooperate with. On the other hand, when huge amount of data is collected in the cyber domain, they should be processed and analysed accurately and transparently.

Data should be also transmitted and communicated in a reliable way via networking systems. Existing advances in networking and communications can be applied in order to achieve data transmission and communication trust. In particular, the trustworthy networking and communication protocols can support heterogeneous and specific networking contexts.

Social trust

Social networks are popular for sharing information and knowledge. Trust is an important feature in social networks because it relies on the level of trust that users have with each other, as well as with the service provider. Social trust actually depends on the behaviour and interactions of humans in the social networks. If humans fail to build trust, then they may not wish to share their experience and knowledge with others because of anxiety that their knowledge and privacy will be misused.

Social-Cyber-Physical domain trust

In the ICT infrastructure, there are interactions among the social, cyber and physical objects, as well as data transmission between them. Actually, the objects in the physical and cyber domain interoperate closely with each other and form a system organization around its user (human) in the social domain. Human interactions with cyber-physical objects should be performed in a trustworthy way.

Furthermore, because most smart devices are human-related or human-carried devices, the social relationships between humans can spread through their devices. To define and manage trust among physical, cyber and social domains, appropriate trust models for the interactions among social, information and communication networks are required while taking into account the severe resource constraints, and dynamics. Trust evaluation and trust management are especially challenging issues in the social-cyber-physical domain trust.

Cross-domain service trust

Trust management is service and domain specific, and it may be desirable to combine features from different trust management systems for developing cross-service trust management which is able to cover social-cyber-physical trust relationships between different service domains.

To disseminate trust information from one service domain to another service domain, a trust service brokering mechanism can be used for efficient, effective and suitable trust dissemination.

8.2 Trust Architectural Framework

Based on the generic ICT trust conceptual model, an architectural framework for strengthening trust in the ICT infrastructure is presented in Figure 8-2. It consists of four major parts as follows.

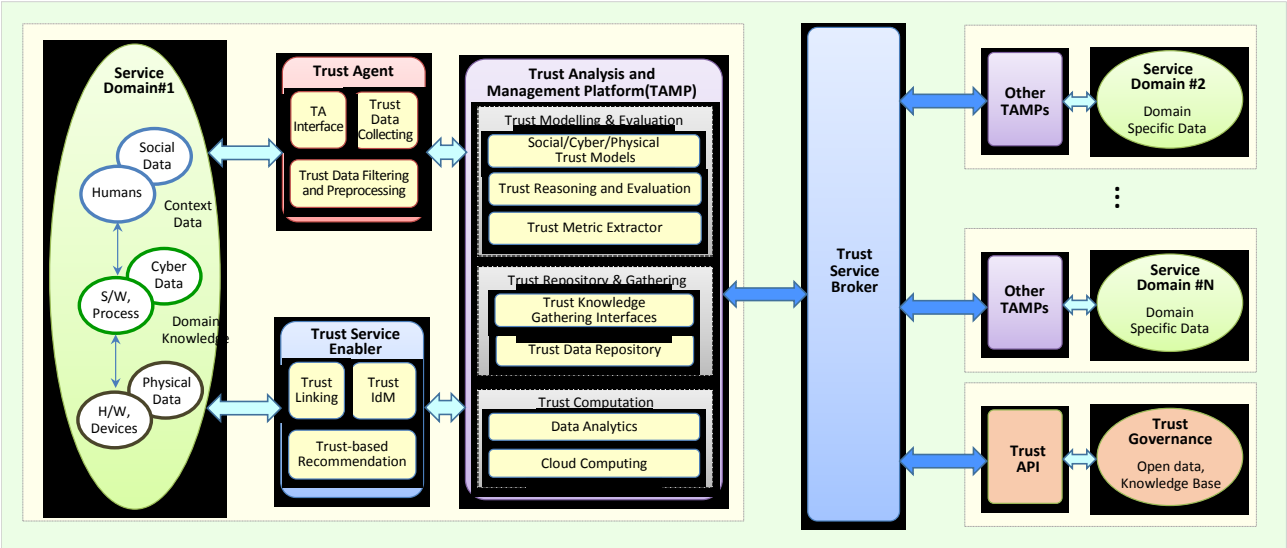

Figure 8-2: An architectural framework for trust provisioning for ICT infrastructure

8.2.1 Trust Agent (TA)

TA is used to collect trust-related data from the social-cyber-physical environments with the following modules.

– **TA Interface**: TA provides lightweight interfaces to collect trust-related data from various types of objects. Furthermore, TA interfaces need to be easily connected to existing platforms and devices in order to extract the required data.

– **Trust Data Collection**: This module is responsible for gathering the data required for evaluating a trust level of an object. The Trust Analysis and Management Platform identifies the required trust metrics for the object and informs to this module.

– **Trust Data Filtering and Pre-processing**: This module is used to refine trust data sets without including other data that can be repetitive, irrelevant or even sensitive for trust evaluation.

8.2.2 Trust Analysis and Management Platform (TAMP)

TAMP is used for modelling, reasoning and managing trust data collected from TAs to check whether social-cyber-physical objects satisfy certain trust criteria.

– **Trust Modelling**: A trust model is used to specify, annotate and build trust relationships between objects for the purpose of reasoning trust data. Trust modelling is social-cyber-physical and service domain-specific, and there are social, cyber and physical trust models to define a trust model for each domain in the ICT infrastructure. According to its domain and a particular service domain, a suitable trust model is selected and applied for trust modelling. The trust-related data collected from TAs can be transformed to structured and

annotated formats by using semantic and ontology technologies through this trust modelling module.

- **Trust Reasoning and Evaluation**: Trust evaluation is used to analyse and assess trust levels based on the trust model. There are various types of reasoning methods which depend on the social-cyber-physical domains, and a proper reasoning method will be chosen for the specific object. For example, policy-based trust reasoning makes a binary decision according to which an object is trusted or not. Because trust status could change with time and circumstantial context, a trust reasoning method must handle such dynamics of trust.
- **Trust Metric Extractor**: The trust metric extractor recognizes trust characteristics, accounts for factors influencing trust and determines proper trust metrics for the trust modelling and reasoning by analysing the metadata or semantic ontologies.
- **Trust Knowledge Gathering Interface:** This module is used to gather related trust knowledge regarding on object's trust aspects from related service domains via the Trust Service Broker.
- **Trust Data Repository**: The trust data including operations of objects and the history of interactions between objects can be maintained in the trust data repository. For trust evaluation, the necessary data will be loaded from this repository to the computation module.
- **Trust Computation**: This module is used for data processing for trust evaluation. Trust computation happens when the state of an object is changed or an interaction occurs between objects. To process a large amount of data related to trust evaluation, it can adopt data analytics and cloud computing technologies for calculation of the trust level of objects according to the change of the trust state of objects based on direct observation.

8.2.3 Trust Service Enabler (TSE)

TSE is used to provide trust knowledge of social-cyber-physical objects for a service based on the ICT infrastructure. It also provides trust-adapting capabilities to enable effective and efficient adaptation of trust knowledge to services.

- **Trust Linking**: Trust linking is a module capable of creating a link between social-cyber-physical objects based on trust metrics.
- **Trust IdM**: The identity management (IdM) can be used to manage digital identification/authentication of social-cyber-physical objects. Trust IdM assures the identity of trustworthy objects and support trust-based services.
- **Trust-based Recommendation**: This module provides recommendations to other objects. This module aims at providing a recommendation for selecting a suitable object that meets the required level of trust.

8.2.4 Trust Service Broker (TSB)

An object has a number of trust aspects which are related to other service domains in general. For instance, a human may have different trust levels at home, office, bank, social communities, etc. Each service domain has an effective trust evaluation mechanism specialized to analyse the domain-specific trust-related data. TSB provides a brokering service to share and disseminate domain-specific trust knowledge across service domains. TSB also provides a brokering service from trust governance information through trust API. When various kinds of trust aspects of a certain object are needed to investigate and judge their multifaceted trustworthiness, TAMP can gather an object's trust

knowledge of other service domains from TSB and evaluate the whole trust knowledge to determine the object's multifaceted trustworthiness.

9 Trust based ICT Service Models

Today, it is known that almost everything can get hacked. If someone is going to get our data, tools like encryption and tokenization of that data become important defence methods. Any users including enterprises needs to follow some simple best practices to protect themselves online. Therefore, many business opportunities may exist if we further consider trust.

Trust based new ICT service models are a good positioning that builds trust with ICT service users by enabling them to control and leverage their own personal data. In doing so, trust based ICT service models give ICT service providers a sustainable business strategy for disrupting current ICT "Big Data primes" as well as delivering a permission-based personal data pipeline and services. A trust based ICT service model is a "game-changing" disruptive strategy that enables firms using big data to provide incremental trust improvements to existing big data deployment. To exploit customer data more comprehensively, businesses must develop a much greater level of trust with their customers. The primary concern is to overcome the gap between the personal controllability of privacy and business benefits of ICT services in terms of human and service related trust.

This clause firstly discusses some mistrust drivers in current ICT environments. Then, it presents a framework for analysing trust based ICT service models on new market disruption and symmetric ICT environment based on a new market disruptive innovation model.

9.1 Mistrust in current ICT environments

There are some mistrust drivers in current ICT environments:

- **Privacy infringements and errors**: The endless supply of so-called big brother stories is slowly shifting people's views on privacy and personal data, making them more open to tracking blockers and privacy products. Government agencies' programs used to collect ICT users' materials, including searches, the content of emails, file transfers, instant messages, and live chats. This puts the "Safe Harbor" agreement with the EU at risk [b-EU-Safeharbor]. In a company level, corporate annexation of consumer rights can be as easy as a new sentence in a company's privacy policy.
- **Security breaches**: The growing regularity of news reports about online security breaches is likely to lead a higher proportion of the population to change their behaviours. Consumers are now looking for improved security. It provides richer opportunities for security and privacy players.
- **Government mass surveillance**: A surveillance software provides users worldwide with the tangible evidence that comprehensive, population-wide surveillance is systemic in many countries. The surveillance covers every medium, and has been almost totally outsourced to a dozen of ICT major service providers.

The result of 'mistrust' is the "asymmetric ICT environment" as follows:

- **Information asymmetries**: Firms have an overload of user information, but consumers suffer from information scarcity in terms of their own data.
- **Solution asymmetries**: Firms have sophisticated analytics for optimizing customer lifetime value, but consumers have no analytics for minimizing vendor lifetime cost.
- **Control asymmetries**: Consumers are comparatively powerless to control the collection and use of their personal data. In some cases, firms have full control on personal data which firms have.

NOTE – Appendix III describes theoretical and industrial backgrounds about trust based ICT service models.

9.2 A framework for analysing a trust based ICT service model

A trust based ICT service model is a positional strategy building trust not only with consumers by defending their social economy and by enabling their control of their own devices and data, but also making ecosystem with business partners by defending their sharing economy and by enabling creation of their products and services. In doing so, trust gives a new business strategy for disrupting the legacy economy and delivers a more high-quality, permission-based data pipeline and profitable services with trust attributes (e.g., integrity, ability, benevolence, reliability, and helpfulness, etc.). This analysis framework is focusing on three major asymmetries:

- **Information asymmetries**: Companies have an overload of user information (mostly social and transaction data), but consumers suffer information scarcity in terms of their own data and that relating to companies. It is trust about product and service **(product and service level)**.
- **Solution asymmetries**: Companies have sophisticated analytics for optimizing customer lifetime value, but consumers have no analytics for minimizing vendor lifetime cost, which is the flip side of customer lifetime value. It is trust about log, social and business transactions, etc. **(software level)**.
- **Control asymmetries**: Consumers are comparatively powerless to control the collection of their data and the operating system (OS), but corporations have full control of data storage and OS which they provide. It is trust about data source, storage, network, and software **(software and network level)**.

Trust attributes of product & service, customer and process of ICT service models based on the theoretical background, new value chains of markets are as follows:

- **Product & Service**: Privacy, Safeness, Security, Convenience, Simplicity, etc.;
- **Customer & Market**: Satisfaction, Life cycle of service, Developer ecosystem, etc.;
- **Business model process** (infrastructure): Mobile, Social, Cloud, Data analytics, Interoperability, Standardization, etc.

With these backgrounds, this clause intends to categorize new market disruption into three platform types of products, market and software. In fact, on the road of disruptive innovation, the related researches are almost about the platform strategies and the meaning of platform business has been expanded from the products & services to market & software ecosystem. In these three types of platforms, there are rationalities specific for each platform as follows [b-Sandberg] and the rationalities are related to the trust attributes [b-Mayer, b-McKnight]:

- **Rationality of product platform** (Integrity, ability and functionality): Modularity allows re-use and decreases complexity, standardization of platform combined with customization allows economies of scale and scope. The overarching goal is product efficiency and functionality;
- **Rationality of market platform** (Integrity, ability and benevolence): Re-use of infrastructure allows efficient transactions. Focus on market efficiency and transaction costs. Competitive advantages are achieved by attracting a large number of providers and customers through strategic decisions;
- **Rationality of software ecosystem platform** (Integrity, reliability and helpfulness): Shared functionality in codebase allows specialization, distribution of development costs

and access to users. Commonality achieved through shared platform rather than application area.

Based on disruptive model theory and ICT symmetry following Table 9-1 is presented, and detailed examples are shown in Appendix III.

Table 9-1 A framework for analysing a trust based ICT service model

Types of Symmetric ICT	New Market Disruptions (platform type)		
	Products & Services (Product platform)	**Customer & market (Market platform)**	**Business model Process (Software platform)**
Information Symmetries	Ability	Ability	Reliability
Solution Symmetries	Functionality	Benevolence	Helpfulness
Control Symmetries	Integrity	Integrity	Integrity

10 Use cases of Trust Provisioning for ICT infrastructures and services

This clause discusses six use cases of trust provisioning for ICT infrastructures and services. The use cases can be shown in wide range of service domains requiring trust. Although each use case has different purposes and consists of different actors, it is true that trust can play an important role of mitigating risks of violation of security as well as privacy and mediating interactions among actors.

Use case #1: Trustworthy smart home service

Trustworthy smart home service is a service to monitor, control and manage home appliances and smart devices by using trust information. This use case focuses on a trust provisioning at home. The home gateway collects personal data from the household devices. After aggregating the personal data, the home gateway sends data to the remote service platform and service platform generates trust information from data and provides trust information to service providers for managing home appliances and other devices.

Use case #2: Trustworthy smart office service

This use case allows users utilizing various facilities in office based on the trust level of users. For the trust management, various properties like social/business relationship and membership of each user can be considered to determine each user's trust level. Smart office provider offers office facilities to users based on the users' trust level estimated by trust management platform.

Use case #3: Trustworthy document sharing service

This use case focuses on sharing the document among co-workers using social trust value among them. Trust management platform estimates social trust values between co-workers by using the collected social data from intermediate entities (e.g., smartphone) of co-workers and then, these values will be used to judge whether the receiver has enough qualification to get the document or not. If the document receiver has enough qualification to get the document, an entity transfers the document to receiver.

Use case #4: Device selection for data transmission

This use case focuses on selecting the device for data transmission in multi-hop Device-to-Device (D2D) environment using social trust value among devices. Trust management platform calculates the trust value using the collected social data from intermediate entities of users and then, these trust

value will be used to judge whether that device has enough reliability to receive and transmit data or not.

Use case #5: Trustworthy car sharing service

The car sharing service offers a new business model for automobile transportation. This use case is particularly designed for two user groups – first of all, people who live in cities but do not drive a car every day, and secondly tourists who travel in cities but do not bring their car. Thus, people who need a car at short period can take this alternative without purchasing it. Trust management platform can provide the evaluated trust levels of users or cars by using collected data of cars as well as users who use the car sharing service.

Use case #6: Trustworthy used car transaction service

This use case focuses on buying a used car in trustworthy procedure. Buying a used car involves high levels of uncertainty and risk because there exists inevitable distrust in used car transactions between entities. Trust management platform can play an important role in mediating entities who participate in a used vehicle market by sharing trustworthy information between entities in a transaction. Trust management platform evaluates each actor's trust by collected data from various sources such as insurance company, public organization, social network services, and vehicle itself.

NOTE – The detail features and operations of each use case are described in Appendix IV.

Table 10-1 summarizes six use cases discussed in Appendix IV. In Table 10-1, it is observed that the uncertainty and risks can be mitigated by providing trust information.

Table 10-1: Summary of use cases

No	Use case	Purpose	Method	Actors
1	Trustworthy smart home service	Managing home facilities	Trustworthy home-related data → Providing personal information to service platform	- User - Service provider - Service platform - Home gateway - Home appliance
2	Trustworthy smart office service	Managing office facilities	Trust level of users → Determining facility usage right	- User - Smart office - Smart office provider - Trust mgmt. platform
3	Trustworthy document sharing service	Sharing document with appropriate users	Trust level between users → Determining authority of accessing document	- User A - A's Device - User B - B' device - Trust mgmt. platform
4	Device selection for data transmission	Selecting trustful device for D2D communication	Trust level between devices → Selecting appropriate device for transmission	- User A - A's device - User B - B's device - Trust mgmt. platform
5	Trustworthy car sharing service	Promoting trustworthy car sharing	Trustworthy data about a shared car and users' data → Providing an	- User A - A' device - Sensor attached in sharing car

			information of shared car and its user	- Service platform - Service provider
6	Trustworthy used car transaction service	Mediating transparent used car transaction	Trustworthy data about a used car → Providing transparent car history information	- Seller (User A) - Seller's car - Service broker - Trust mgmt. platform - Buyer (User B)

11 Strategies for future standardization on trust

Until now, a number of standards focusing on network security and cybersecurity technologies have been developed in various standardization bodies including Internet Engineering Task Force (IETF). The scope of these standards needs to be expanded to take into consideration trust issues in future ICT infrastructures. There are a few preliminary activities taking place, for instance in Online Trust Alliance (OTA) and Trusted Computing Group (TCG). However, as existing research and standardization activities on trust are still limited to social trust between humans, trust relationships between humans and objects as well as across domains of social-cyber-physical domains should also be taken into account for trustworthy autonomous networking and services.

Based on this, we need to first find various use cases considering user confidence, usability and reliability in ICT ecosystems for new business models which reflect sharing economy. Then, a framework for trust provisioning including requirements and architectures should be urgently specified in relation to the relevant standards. In addition, global collaborations with related SDOs are required to further stimulate trust standardization activities.

More specifically, the following key items are identified as future work for standardization on trust.

- **Overview of trust in ICT**

It aims to provide a clear understanding of trust from different perspectives and identify key differentiations compared to security and privacy. It also highlights the importance of trust in future ICT infrastructures towards knowledge societies.

- **Service scenarios and capabilities**

From various use cases analysis, considering sharing economy, it is necessary to develop service scenarios for trust provisioning and define required capabilities to support trust in ICT.

- **Requirements for trust provisioning**

From key challenges and technical issues, it is necessary to specify detailed requirements in terms of different viewpoints and various stakeholders.

- **Architectural framework and functional architectures**

It targets to identify core functions for future trusted ICT infrastructures and develop architectural models, including detailed functional architectures. Relevant trust models should be based on key concepts of trust domains, levels of trust, TLA and trust index, taking into account social, cyber and physical domains.

- **Technical solutions for trust provisioning**

It covers some methodologies for specifying and measuring trust metrics. It also needs to develop protocol specifications for trust provisioning, and mechanisms for data gathering, filtering, analytics, reasoning and decision making.

- **Trust provisioning for convergence applications**

For trust provisioning, it is necessary to develop specific technical solutions applicable to convergence applications (e.g., smart grid, healthcare, intelligent transport systems, and logistics, etc.).

- **Trust provisioning for cloud computing**

For trust provisioning, it is necessary to develop specific technical solutions applicable to the processing and analysis of the large amount of data through cloud computing.

Additionally, we need to incorporate trust issue into related Study Groups' (SGs) activities in ITU-T.

– **SG17**: As trust is tightly associated with security issues, a liaison with SG17 activities on security matters is **required**.

– **SG20**: As the **recently** established SG20 is targeting IoT applications, services and platforms as well as smart cities infrastructure, SG20 should consider trust in IoT.

– **Others**: Depending on specific topics, a collaborative work is needed, for instance, the identification issue with SG2, trust in financial services with Focus Group on Digital Financial Services.

Finally, we need to closely collaborate with other SDOs and forums listed below.

– **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 has a responsibility to get a consensus for trust and knowledge information infrastructures. ITU-T may have a leadership to introduce future knowledge societies by getting global consensus of future ICT infrastructures. Standards for future all the industries as well as ICT industries are critical to realize knowledge eco-societies.

Finally, ITU-T may get a chance to lead future knowledge societies in terms of standardization. As a top level of formal standard body, ITU-T may initiate new work methods for future knowledge information infrastructures including pre-standardization and conceptual framework. Also, ITU-T may have a leadership to collaborate with private sectors and academia which are outside of ITU-T.

Appendix I
Trust definitions

This appendix provides various trust definitions from different viewpoints as shown in Table I-1.

Table I-1: Trust definitions

	Definitions	References
Lexical-semantic	**Reliance** on the integrity, strength, ability, surety, etc., of a person or thing; **confidence**	Dictionary
	Reliance on and confidence in the truth, worth, reliability, etc., of a person or thing; **faith**	Dictionary
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.	[b-Sherchan]
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.	
Sociology	**Trust** is defined as "a bet about the future contingent actions of the trustee". This bet, or expectation, is considered to be trust only if it has some consequence upon the action of the person who makes the bet (i.e., trustor).	
	Trust is considered from two viewpoints: individual and societal. At individual level, similar to the perspective from psychology, the vulnerability of the trustor is a major factor.	
	Trust is differentiated from cooperation in the presence of assurance (a third party overseeing the interaction and providing sanctions in case of misbehaviour). However, cooperation in the presence of the shadow of the future (i.e., fear of future actions by the other party) is considered to be trust. In this respect, social trust has only two facets, cognitive and behavioural, with the emotive aspect building over time as trust increases between two individuals.	
	At societal level, **trust** is considered to be a property of social groups and is represented by a collective psychological state of the group. **Social trust** implies that members of a social group act according to the expectation that other members of the group are also trustworthy and expect trust from other group members. Thus, at societal level, social trust also has the institutional or system aspect of trust.	
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"	[b-uTRUSTit]
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".	

Appendix II
Standardization Activities on Trust in related SDOs

This appendix introduces standardization activities on trust in related SDOs such as IETF, OTA and TCG.

1. Activities in Internet Engineering Task Force (IETF) for Internet Trust

To discuss a trust and knowledge ICT infrastructure, it is required to review a data lifecycle – its production, process and consumption. Therefore, it is important to deal with trust issues focusing on Internet. For this purpose, this clause introduces IETF's activities on trust to identify trends and main issues from perspective of Internet.

In IETF, currently 11 working groups (WG) are dealing with issues on trust.

– DNSOP (Domain Name System Operations)
– DNSSEC (Domain Name System Security Extensions)
– DNSExt (Domain Name System Extensions)
– NEA (Network Endpoint Assessment)
– OAUTH (Web Authorization Protocol)
– HTTPbis (HyperText Transfer Protocol)
– WPKOPS (Web Public Key Infrastructure Operations)
– ECRIT (Emergency Context Resolution with Internet Technologies)
– SDNRG (Software Defined Networking Research Group)
– ICNRG (Information Centric Networking Research Group)\
– SIDR (Secure Inter-Domain Routing)

Figure II-1 shows individual WGs and its related OSI layer.

Figure II-1: Classification of IETF WG based on OSI Layer

Figure II-2 shows a brief categorization of WGs into trust technical issues.

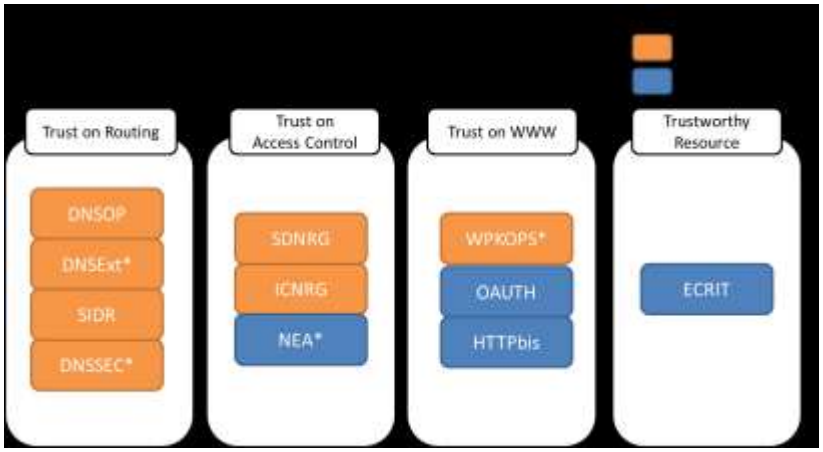

Figure II-2: Trust domains of IETF WGs

2. Activities in Online Trust Alliance (OTA) for IoT

OTA is a non-profit organization with the mission to enhance online trust and address IoT risks comprehensively. The framework presents guidelines for IoT manufacturers, developers and retailers to follow when designing, creating, adapting and marketing connected devices in two key categories: home automation and consumer health and fitness wearables.

Through extensive research, this taskforce concluded that the safety and reliability of any IoT devices, Apps or services depend equally on security and privacy, as well as a third, often overlooked component: sustainability.

Although the IoT framework of OTA has identified various requirements, most of them can be seen as reinterpretation of traditional security and privacy issues. Therefore, it is noticed that trust in OTA includes more broad range of scope covering security and privacy as well as regulatory issues [b-Gilson, b-OTA-2015].

3. Activities in Trusted Computing Group (TCG) for Interoperable Trusted Computing Platforms

TCG is a not-for-profit organization formed to develop, define and promote open, vendor-neutral, global industry standards, supportive of a hardware-based root of trust, for interoperable trusted computing platforms.

TCG technologies do not provide an immediate solution to all IoT device and service security needs, but they enable existing and new IoT solutions to be fundamentally far more robust than today's state-of the art.

Solutions developed by TCG includes authentication, cloud security, data protection, IoT, mobile security and end-to-end security. Similar to OTA, TCG has also focused on various solutions from existing security and privacy issues while taking into account additional concepts of trust.

TCG has provided the following concepts for trust related terminologies in the architecture's guide for cyber security [b-TCG 2013, b-TCG 2015].

- Trusted Network Connect (TNC)

TCG's TNC network security architecture and open standards help businesses create and enforce security policies as well as facilitating communication between security systems. Using TNC standards, network managers gain better visibility into who and what is on their network, and whether

devices remain compliant with policies. More than two dozen vendors of commercial and open source products support TNC standards in their products.

- Self-Encrypting Drive (SED)

Self-Encrypting Drives silently and automatically encrypt all user and system data, making sure this information doesn't fall into the wrong hands if the device or drive gets lost. Such drives may also be remotely wiped if they're lost or stolen.

- Trusted Platform Module (TPM)

The Trusted Platform Module is a hardware security component built into a computing device that provides a hardware root of trust for user and device identity, network access, data protection, and more. TPMs are built into more than half a billion end systems, including many laptops and mobile devices.

Appendix III
Backgrounds for Trust based ICT Service models

This appendix describes some theoretical and industrial backgrounds about a framework for analysing trust based ICT service models in business perspective.

Many firms already see and manage high volumes of security incidents, breaches, malware, and hackers and early security offerings tended to focus on the network (e.g., WAN and Internet service security), but such managed security services are expanding now into other areas like Internet data, mobile, web, and cloud-based ICT, IoT services and business models.

Especially, people are connected with each other and with objects as well, and expect always-on connectivity. It is expected to see 'trusted ICT infrastructures from all parts of the ICT ecosystem, not only devices and networks, but also applications and services. The EU (European Union)'s focus on Trust & Security in "Europe 2020 Strategy," researches about 'trust' in projects of FP7's uTRUSTit, ABC4Trust, and USA's application of 'Trust & Security' on the industry level (NIST & DARPA), research about trust technology in projects like Smart America, and HACMS (High-Assurance Cyber Military Systems) are verifying the importance of the trust and security in the emerging business models in e-commerce, Social Network Service (SNS), IoT services and so on.

In business area, some leading firms also are pursuing the same way in financial technology area. Despite of such efforts of leading companies, recent big data based business models are not trusted by personal consumers. There is 'mistrust' in many ICT service domains. Some companies launched permission-based business models to use personal data, a more sustainable strategy to put consumers in control of their personal data. It is a kind of disruptive innovation in the new market.

Human/service-related trust is beliefs that the other party has suitable attributes for performing as expected in a specific situation irrespective of the ability to monitor or control that other party [b-Mayer]. It composed to three attributes of integrity, ability and benevolence. The integrity refers to the beliefs that the trustee adheres to a set of principles that the trustor finds acceptable. The ability is the beliefs that the trustee has the group of ability, skills and characteristics that enable them to have influence within some specific domain [b-Mayer, b-McKnight 2002]. Lastly, the benevolence is the beliefs that the trustee will want to do good to the trustor, aside from an egocentric profit motive.

There are three innovation models to creating new-growth businesses: 1) sustaining innovation, 2) low-end disruption, and 3) new market disruption: [b-Christensen]

1) **Sustaining innovation model**: A sustaining innovation does not create new markets or value networks but rather only evolves existing ones with better value, allowing the firms within to compete against each other's sustaining improvements.

- **Disruptive innovation model**: An innovation that creates a new market by applying a different set of values, which ultimately (and unexpectedly) overtakes an existing market.

2) **Low-end disruption**: targets customers who do not need the full performance valued by customers at the high end of the market.

3) **New market disruption**: targets customers who have needs that were previously unserved by existing incumbents.

The characteristics of each innovation models are presented in Table III-1.

Table III-1: Three approaches to creating new-growth businesses

Dimension	Sustaining innovations	Low-end disruption	New market disruption
Targeted performance of the product or service	Performance improvement in attributes most valued by the industry's most demanding customers. These improvements may be incremental or break-through in character.	Performance that is good enough along the traditional metrics of performance at the low end of the mainstream market.	Lower performance in "traditional" attributes, but improved performance in new attributes - typically simplicity and convenience.
Targeted customer or market application	The most attractive (i.e., profitable) customers in the mainstream markets who are willing to pay for improved performance.	Over-served customers in the low end of the mainstream market.	Targets non-consumption: customers who historically lacked the money or skill to buy and use the product.
Impact on the required business model (processes and cost structure)	Improves or maintains profit margins by exploiting the existing processes and cost structure, and making better use of current competitive advantages	Utilizes a new operating or financial approach or both, a different combination of lower gross profit margins and higher asset utilization that can earn attractive returns at the discount prices required to win business at the low end of the market.	Business model must make money at lower price per unit sold, and at unit production volumes that initially will be small. Gross margin dollars per unit sold will be significantly lower.

Several studies have examined the conditions or rules of the platform and its effects on competitive strategy in a variety of industrial contexts. Recently, it is suggested that digitizing and its affordance of convergence is one of the primary drivers for platform change [b-Yoo 2012]. They note "from one perspective, in order to harness the convergence and generativity made possible by pervasive digital technology, firms now innovate by creating platforms rather than single products." The penetration of digital technologies into products and services and their success as witnessed by the history of existing online markets has heightened the role of platform strategies in firms' innovation activities [b-Yoo 2010, b-Tilson 2010]. Also, [b-Sandberg] complements this understanding of platform evolution by analysing qualitative changes in platforms rules and architecture and how they relate to strategy (i.e., how the platform is positioned with regard to its use and production contexts).

More innovative firm tends to be platform providers in order to harness the convergence made possible by digital technology, firms innovate by creating platforms rather than single products [b-Yoo 2012]. The firm needs to source its products or services across multiple innovation domains (e.g., devices, networks, contents, and services) in order to increase its innovation complexity and diversity [b-Yoo 2010]. Platform evolution has been also explored in the context of market-based

competition on two-sided markets [b-Eisenmann], and related concerns for strategy management [b-Gawer].

In Table III-2, an example of use case (or business model) analysis framework is shown.

Table III-2: An example of use case analysis framework

Types of Symmetric ICT	New Market Disruptions		
	Products & Services	**Customer & Market**	**Business model Process**
Information Symmetries	Reputation service	Messaging service	Identity management as SaaS
Solution Symmetries	IoT device whose goal is efficiency and functionality	IoT based application service for specific market allowing efficiency and transaction cost	IoT PaaS, IoT server security as PaaS, IoT SaaS, IoT IaaS, etc. allowing shared functionality in codebase. Commonality can be achieved through shared platform.
Control Symmetries	Email, personal cloud	Universal platform	Personal cloud as SaaS, Cloud as IaaS, Security as SaaS, LBS as SaaS, M2M B2B

1) Information symmetries

- Targeted product and service
  - Reputation related services: provide privacy and reputation management for private individuals, their families and their businesses.
- Targeted customer and market
  - Messaging services: provides ephemeral messaging service (i.e., messages are deleted and disappeared after recipients read them).
- Business model process
  - Identity management as Software as a Service: provides simplified identification (or authentication) methods using various technologies (simple PIN code, one time password, etc.).

2) Solution symmetries

- Targeted product and service
  - Simple IoT device with integrity and interoperability
- Targeted customer
  - IoT based service applications allowing market efficiency and transaction costs by building two- or multi-sided market.
- Business model process
  - IoT platforms as Platform as a Service: provides the possibility to analyse and visualize the Internet of Things. It can be used to interconnect different devices

over the Internet and can store a history of measured values and can display it with graphs, etc.

- IoT server security as Platform as a Service: provides secure IoT device management servers, which are connected with many IoT devices, for maintenance and support operations.
- Commonality can be achieved through shared software and network platform like big data analytics and cloud computing rather than application service area.

3) Control symmetries

- Targeted product and service
  - Email services: provides security and privacy email exchange methods using cryptographic technologies.
  - Personal cloud (e.g., cloud storage services): provides additional security mechanisms for authentication to help ensure users are protected against data or credential breaches.
- Targeted customer and market
  - Universal platform
- Business model process
  - Personal cloud as Software as a Service: provides personal cloud as SaaS to other companies for developing a solution to synchronize any data with any connected devices.
  - Cloud as Infrastructure as a Service: provides trusted cloud as IaaS to other companies which develop various applications on cloud.
  - Security as Software as a Service
  - LBS (Location Based Service) as Software as a Service: provides location based service to other companies as SaaS.
  - M2M B2B (Business-to-Business): provides the supply of connectivity for embedding in an enterprise's processes/service/products, even if the product ends up in the hands of a consumer.

Appendix IV
Use cases of trust provisioning for ICT infrastructures and services

This appendix describes the use cases of trust provisioning for ICT infrastructure, which can be shown in wide range of the trust domains. In this appendix, use cases on smart home, smart office, document sharing, device selection for data transmission, car sharing, and used car transaction services are introduced. Each use case describes following items:

– Description: describes its background including high level description and illustration;
– Actors: play a role in each use case;
– Detailed service flow: describes a service flow for a use case;
– Trust matrix: represents trust relationship between actors;
– Analysis: explains details about trust relationship in trust matrix.

1 Smart home service

1.1 Description

This use case is to manage connected devices at home. Trust-based smart home service is to enable users to monitor, control, and manage the home appliances and the devices remotely and safely at anywhere and anytime. For this service, it is important for users that trusted data collection, process, analysis, decision-making on the appliances and communication. Since the data, collected and generated at home contains personal life cycle information, trustworthiness is the key factor for users to adopt the service. The use case focuses on a trust provisioning at the home gateway that collects information from the electrical home network and communicates it to a system for aggregating and processing the data on the smart home service management platform. Services can then be developed from the collected data.

The home gateway performs an initial treatment of the data received from various sources (sensors, context) as follows:

– Aggregating and processing the collected data;
– Sending data to the remote service platform.

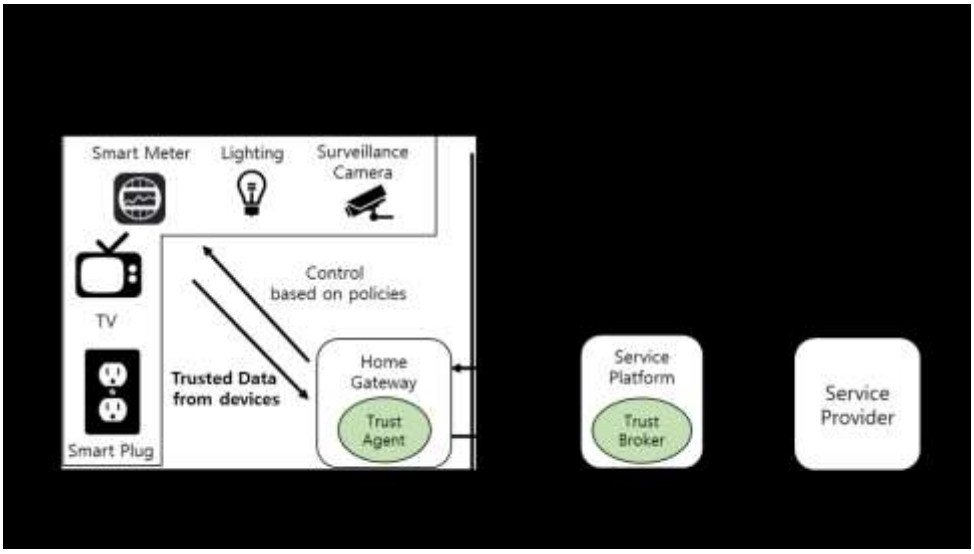

Figure IV-1: Smart home service high level illustration

1.2 Actors

– User: user who are able to control home appliance with terminal devices (e.g., laptop, smartphone, etc.).

– Home Appliance: various appliances from multiple vendors.

– Home Gateway: a device installed in the user's home and receives remote control commands from the management server.

– Service Platform: a service platform is in charge of providing services/common functionalities for applications to user.

1.3 Detailed service flow

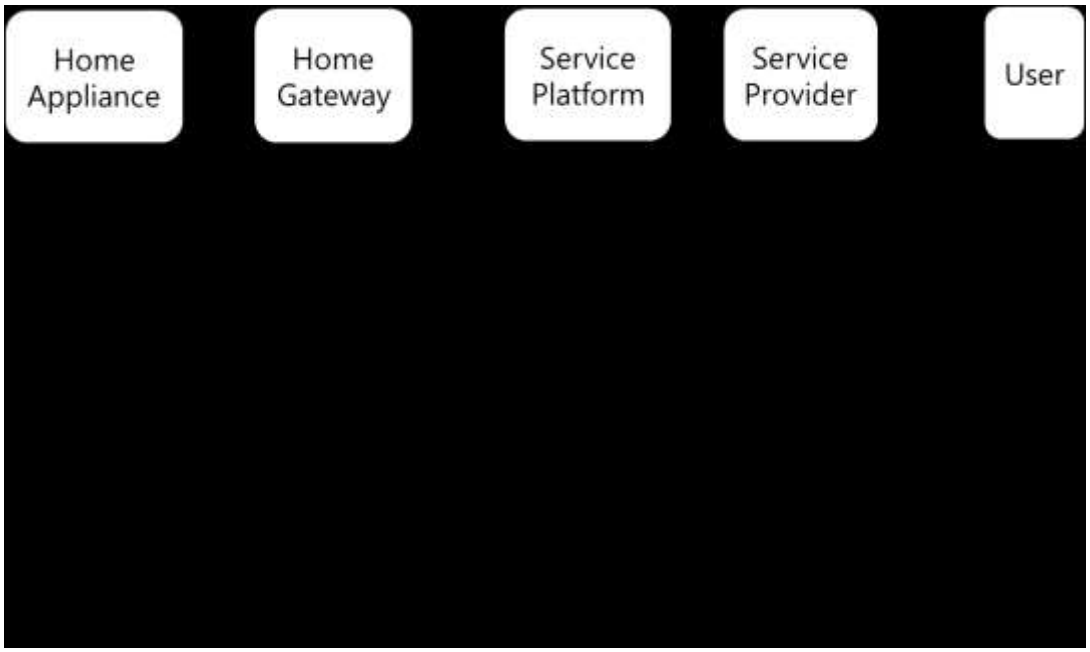

Figure IV-2: Smart home service flow

– Detailed Flow Description

1) A user subscribes to a smart home service.

2) Data from multiple devices such as home appliances (smart meters, electric lightening, fridge, washing machine etc.) is collected. Data may include status of door lock, temperature, level of energy consumption and others.

3) Collected data is stored in the service platform and may be processed at home gateway. Based on polices, the home gateway sends control messages to devices.

4) Collected data may also be sent to service provider which contains the service platform for storage via communication network.

5) Notified information is available for processing. A service provider can process the information before sending to a user depending on subscription profile.

6) A user reacts to the shared /collected information and can send control message (e.g., to switch a home device such as light /appliance or washing machine).

7) Control is propagated back through different operator to appropriate home appliances(s).

1.4 Trust matrix

Trust matrix presents trust relationship among actors in this use case.

Table IV-1: Trust matrix for smart home service

From \ To	Home Appliance	Home Gateway	Service Platform	Service Provider	User
Home Appliance	-	Trusted data collection and aggregation	-	-	-
Home Gateway	Trusted data collection and aggregation	-	Trusted data collection and aggregation Trusted data process and analysis	-	-
Service Platform	-	Trusted data process and analysis	-	Trustworthy application	-
Service Provider	-	-	Trustworthy application	-	Privacy
User	-	-	-	Privacy	-

1.5 Analysis

– Trusted data collection and aggregation

Transmitted data should be trustworthy from devices (home appliances) to home gateway and gateway to service platform. In flow #2, data from devices is collected in a gateway and service platform. When data is produced and transmitted to other entities, trustworthiness of data is required.

– Trusted data process and analysis

Information which is processed by home gateway and service platform should be trustworthy. In flow #3, collected data is processed and analysed in a gateway to decide extra actions depending on policies stored in the gateway. Also, the gateway can put additional data (e.g., location, time, etc.) to collected data in order for a service platform to get accurate conditions of each device at home. In flow #4, a service platform also can process and analyse data from the gateway to produce useful information to a user. Since the gateway and the service platform manipulate collected data, the trustworthiness of information (i.e., processed and analysed data) is required to be maintained in each process.

– Trustworthy application

In flow #5, application (service provider) notifies processed information to user depending on their subscription profile. The trustworthiness of application is recommended to be maintained in each process.

– Privacy

In flow #5, when smart home management system notifies some information to user, providing displayable event or control information to the end-user/consumer terminals (e.g., PC, mobile phone, TV screen, etc.) may be unintentionally exposed. Application (or service provider) utilizes user's data for big data process, and this may cause user privacy issue.

2 Smart office service

2.1 Description

In a trust-based smart office service, usage rights on various office facilities depend on each users' trust level. For example, it is assumed there are three kinds of user trust level - high, middle and low. For a user who has a high level of trust, he or she can read and write the cloud storage. However, a user who has middle level of trust can only read the documents in cloud storage. A user who has low level of trust has no right to access. Figure IV-3 shows an example of smart office service with different priority of users and different permission to office facilities. For the trust management, various properties like social/business relationship and membership can be considered to analyse user's trust level.

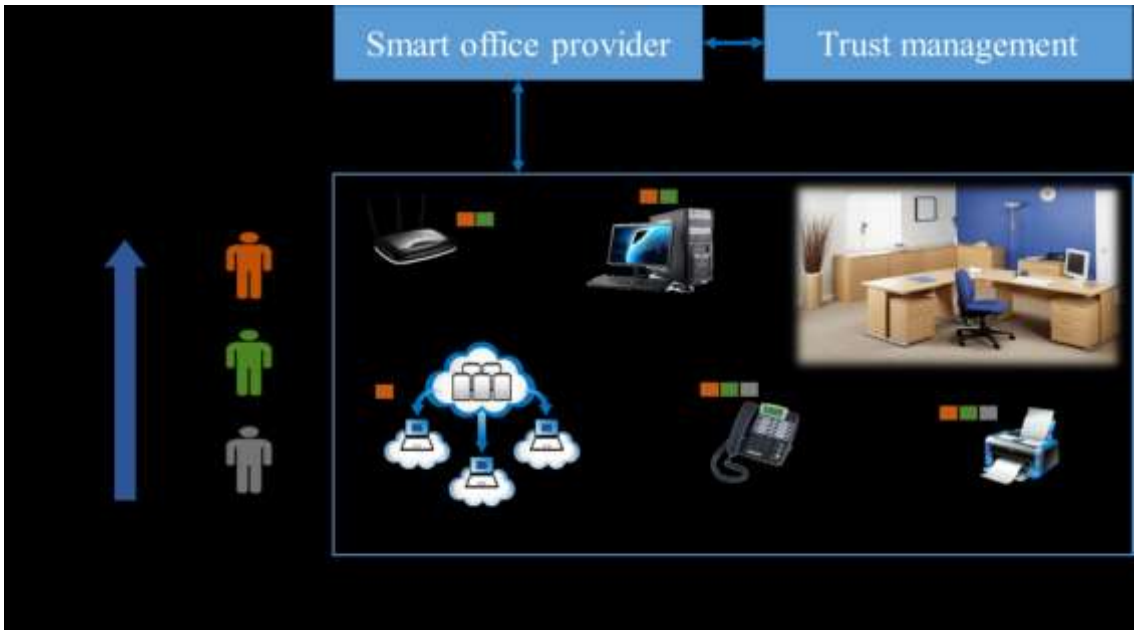

Figure IV-3: Smart office service high level illustration

2.2 Actors

– User: users are able to control and access smart office devices and facilities by using their own devices or office devices (e.g., employer, employee, etc.).

– Smart office devices and facilities: connected devices and facilities in office (e.g., Wi-Fi access point, personal computer, telephone, printer, meeting room, canteen, etc.).

– Smart office provider: a smart office provider is in charge of providing common functionalities for smart office services. It is collecting the status of smart office devices and facilities. Based on user's trust level provided by trust management service, it permits appropriate usage right of them to users (e.g., building management service provider, service providers, etc.).

– Trust management service provider: a trust management service provider responses trust level and information request from smart office providers or service brokers.

2.3 Detailed service flow

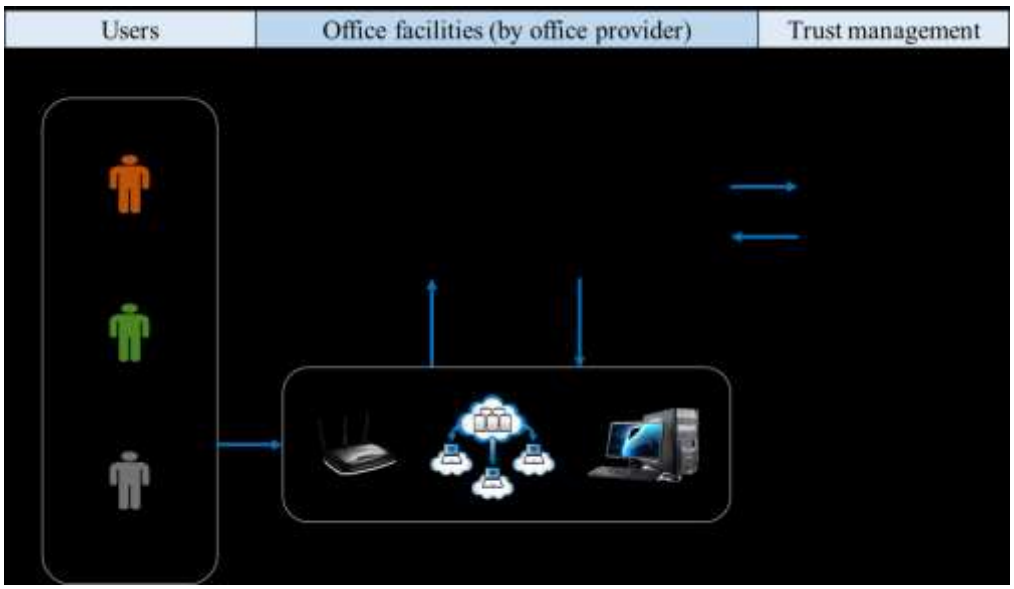

Figure IV-4: Smart office service flow

– Detailed Flow Description

1) Users request to use office facilities.
2) Office facilities request the validation of users and user's trust information.
3) Facility management requests user's information including trust level.
4) A trust management evaluates user's trust level after analysing user data gathered in physical and cyber ICT domain.
5) Based on the user's trust level, facility management decides the usage right on each facilities and functions for a user.

2.4 Trust matrix

Trust matrix presents trust relationship among actors of this use case based on flow of data.

Table IV-2: Trust matrix for smart office service

From \ To	Office Devices & Facilities	Smart Office Service Provider	Trust Management Service Provider	User
Office Devices & Facilities	-	Trusted data collection and aggregation	-	-
Smart Office Service Provider	Trustworthy application	-	Trustworthy application	-
Trust Management Service Provider	-	Trusted data process and analysis	-	Privacy
User	-	-	Privacy	-

2.5 Analysis

– Trusted data collection and aggregation

Data should be trustworthy from smart office devices and facilities to smart office service provider and from trust management service provider to smart office service provider. In flow #2, smart office devices and facilities produce data, and smart office provider collects data from devices and facilities. When data is produced and transmitted to other entities, trustworthiness of data is required to be maintained.

– Trusted data process and analysis

Information which is processed by trust management service provider should be trustworthy. In flow #4, collected data is processed and analysed in a trust management service provider to decide the trustworthiness of user, devices and facilities.

– Trustworthy application

In flow #3 and #5, an office service provider provides smart office application to not only devices and facilities but also trust management service provider. Smart office application should be trustworthy.

– Privacy

When a trust management service provider collects and analyses data and information for deciding trustworthiness of user, the trust management service provider may access user privacy information and it may cause user privacy issues.

3 Document sharing service

3.1 Description

This use case considers a social IoT [b-Atzori] environment with no centralized trusted authority. In the social IoT, each device has the subjective value based on the owner's social relationship as well as the Community of Interest (CoI) [b-Bao] of each device. This use case focuses on using the social trust when sharing the document between co-workers. Without the social IoT trust, a document owner takes the document from own storage, sends the document to receiver and notifies a guest account to receiver. However, the document owner does not need to do anything with the social IoT trust. A trust management platform calculates the trust value using the collected social data from intermediate entity (e.g., smartphone) of co-workers and then, these trust value will be used to judge whether a receiver has enough authorization to get the document or not.

3.2 Actors

– User: A user who takes the ownership of the things (e.g., wireless portable hard drive, smartphone, etc.) and wants to share the documents in the wireless portable hard drive.

– Smartphone: A device which is an intermediate entity and is available to send its owner’s social relationship information and its CoI information to wireless portable hard drive.

– Trust management platform: A trust management platform is mainly in charge of collecting the social relationship and calculating the subjective trust value.

– Wireless portable hard drive: A device, which is mainly in charge of judging authorization to share the document.

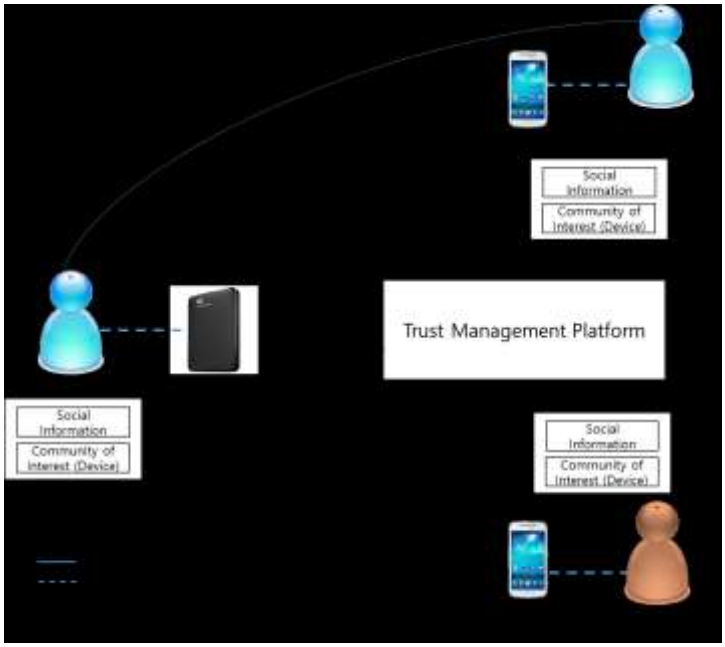

Figure IV-5: Document sharing service high level illustration

3.3 Detailed service flow

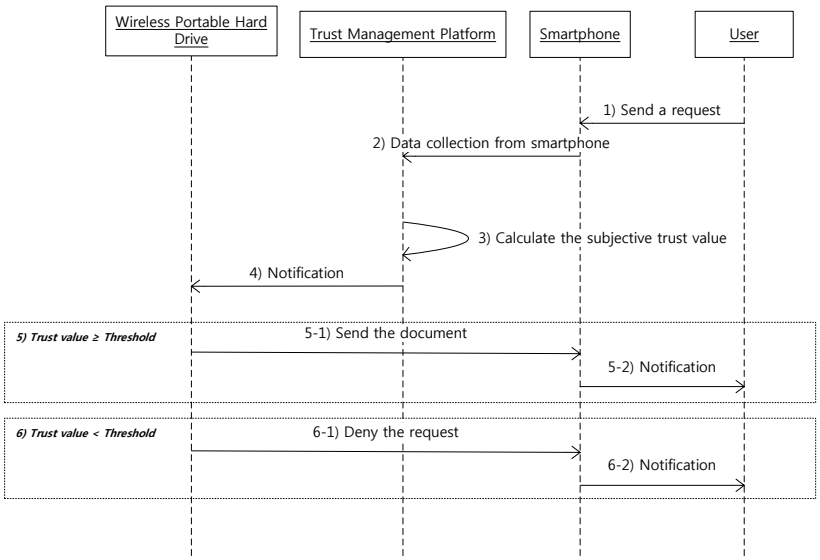

Figure IV-6: Document sharing service flow

– Detailed flow description

1) When User B requests the document to User A's wireless portable hard drive (WPH) by using B's own smartphone.

2) User B's smartphone as a gateway sends User B's social information CoI value to trust management platform.

3) From User A's perspective, trust management platform calculates the subjective trust value (Ta,b) of User B toward User A by using given information of User A and B.

4) The trust management platform notifies the subjective trust value to WPH. After that, WPH judges whether User B has enough authorization to get the document.

5) If the subjective trust value exceeds the threshold value,

1-1) WPH sends the document to User B's smartphone.

1-2) Then, the smartphone notifies User B of results.

6) If the subjective trust value is lower than the threshold value,

1-3) WPH notifies that the request was denied.

1-4) Then, the smartphone notifies User B of results.

3.4 Trust matrix

Trust matrix presents trust relationship among actors in this use case.

Table IV-3: Trust matrix for document sharing service

From \ To	Smartphone / Wireless portable hard drive	Trust Management Platform	User
Smartphone / Wireless portable hard drive	-	Trusted data collection and aggregation Trusted data process and analysis	Ownership
Trust Management Platform	Trusted data collection and aggregation Trusted data process and analysis	-	-
User	Ownership	-	-

3.5 Analysis

– Trusted data collection and aggregation
  - Social relationship information: This trust property represents whether or not the trustee is socially cooperative with the trustor. We use the social friendship relationship among device owners to characterize the cooperativeness.
  - CoI information: This trust property represents whether or not the trustor and trustee are in the same social communities of interest (e.g., co-location, co-work, or parental object relationship).

– Trusted data process and analysis
  - A trust management platform processes and analyses data from other devices to produce useful information (e.g., subjective trust value) to a user.

– Ownership: This trust property represents whether or not the objects (smartphones) used by the device owner.

4 Device selection for data transmission

4.1 Description

This use case also focuses on using the social trust when selecting the device for data transmission in multi-hop D2D (Device-to-Device) environment. Reliable transmission is possible by using social information in the process of D2D communication. Trust management platform calculates the trust value by using the collected social data from intermediate entity (e.g., smartphone) of users and then, this trust value will be used to judge whether that device has enough authorization to send information

or not. The social IoT trust also can be used in the device selection process for the reliable exchange of information. To complement the objective trust, the subjective trust is required in addition.

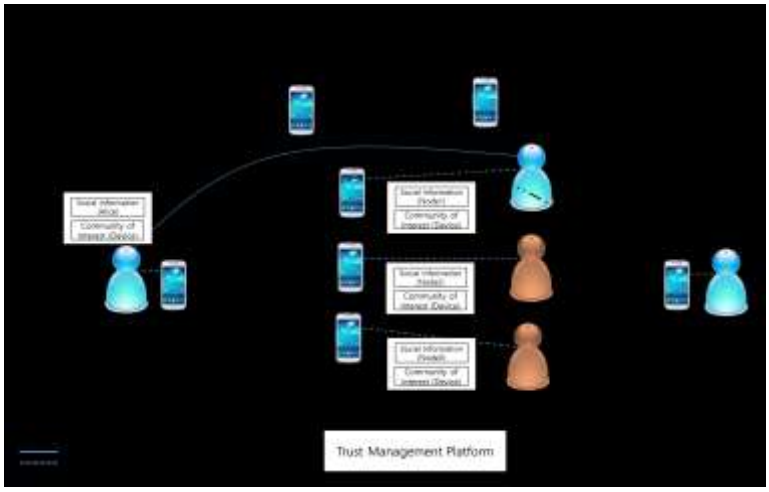

Figure IV-7: Device selection for data transmission

4.2 Actors

– User: A user who takes the ownership of the things (e.g., smartphone, laptop, etc.) and wants to exchange information with another peer via other users.

– Device (Smartphone): A device, which is an intermediate entity, is available to send its owner's social relationship information and its CoI information to other devices. Also, it is in charge of judging authorization to send information.

– Trust management platform: A trust management platform is mainly in charge of collecting the social information and calculating the subjective trust value.

4.3 Detailed service flow

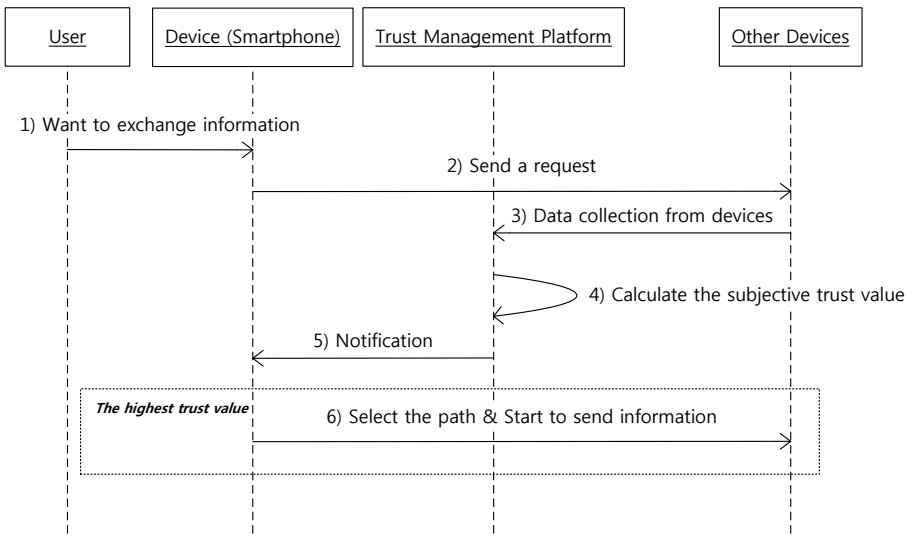

Figure IV-8: Device selection for data transmission service flow

– Detailed flow description

1) User A wants to exchange information with another peer in multi-hop D2D environment.
2) User A's smartphone requests the social information of other devices (e.g., Node 1, Node2, Node 3) and its CoI value.
3) The trust management platform collects relevant information from other devices.
4) Then, the trust management platform calculates subjective trust values (e.g., $T_{a,n1}$, $T_{a,n2}$, $T_{a,n3}$) of other devices from the perspective of User A.
5) The trust management platform notifies the subjective trust value to User A's smartphone. After that, User A's smartphone judges which Nodes have enough authorization to send information.
6) If Node 1's subjective trust value ($T_{a,n1}$) is the highest value, User A's smartphone judges Node 1 has enough authorization to send information and select the transmission path with Node 1. Then, it starts to send information.

4.4 Trust matrix

Trust matrix presents trust relationship among actors of this use case.

Table IV-4: Trust matrix for device selection as data transmission service

To / From	Device (Smartphone)	Trust Management Platform	User
Device (Smartphone)	-	Trust data collection and aggregation Trusted data process and analysis	Ownership
Trust Management Platform	Trust data collection and aggregation Trusted data process and analysis	-	-
User	Ownership	-	-

4.5 Analysis

– Trusted data collection and aggregation
  - Social relationship information: This trust property represents whether or not the trustee is socially cooperative with the trustor. We use the social friendship relationship among device owners to characterize the cooperativeness.
  - CoI information: This trust property represents whether or not the trustor and trustee are in the same social communities of interest (e.g., co-location, co-work, or parental object relationship).

– Trusted data process and analysis
  - A trust management platform process and analysis data from other devices to produce useful information (e.g., subjective trust value) to a user.

– Ownership: This trust property represents whether or not the objects (smartphones) used by the device owner.

5 Car sharing service

5.1 Description

Car Sharing aims at offering a new service for automobile transportation. Simply, car sharing is a self-service, on-demand alternative to car ownership; a service that is offered to urban residents (B2C) and businesses (B2B).

This service is particularly designed for two user groups – first of all, people who live in cities but do not drive a car every day and secondly tourists who live in cities but do not own a car. Thus, people who need a car at short period can take this alternative to car ownership.

The brief procedure of this service is 1) joining the membership, 2) unlocking the car door, 3) driving away, 4) parking to any reserved spot provided by the service provider and/or public, and 5) paying as you drive (including gas, insurance, and etc.).

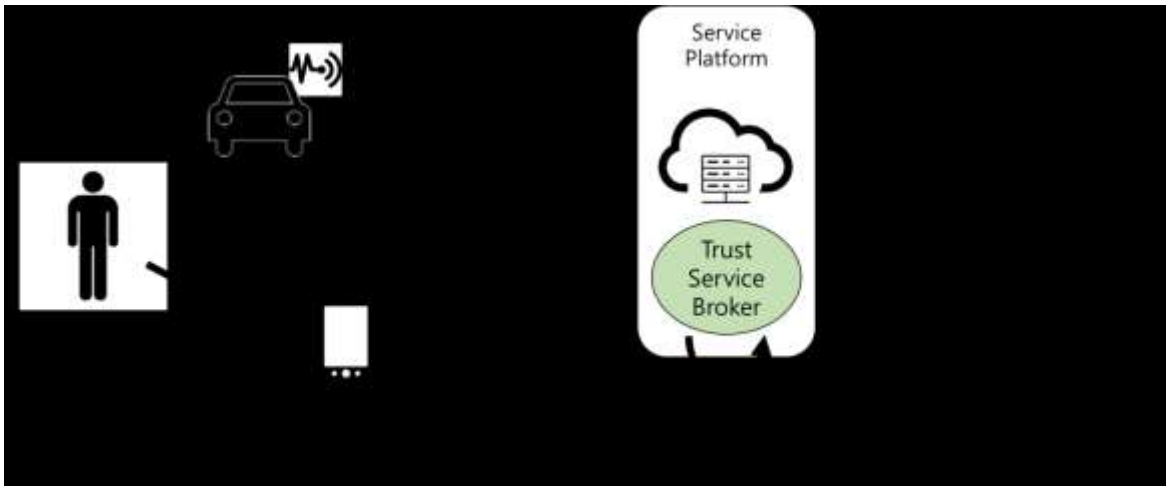

Figure IV-9: Car sharing service high level illustration

5.2 Actors

– Users: A user who takes the ownership of the shared things which are car. Users would connect to the service with their smartphone which have not only capability of communicate with sensor devices, but also applications that used by car sharing services.

– Sensors (or Sensor Devices): Sensor Devices can be various based on its usage, and do not have any direct communication interfaces to the service platform.

– Service Platform: In charge of providing common functionalities for the services. It is mainly in charge of collecting the status and configuration information of sensors and controlling them via the smartphone and/or gateway.

– Service Providers: Companies which provide its own services for the user through the service platform. The service providers can be various according to the types of services.

5.3 Detailed service flow

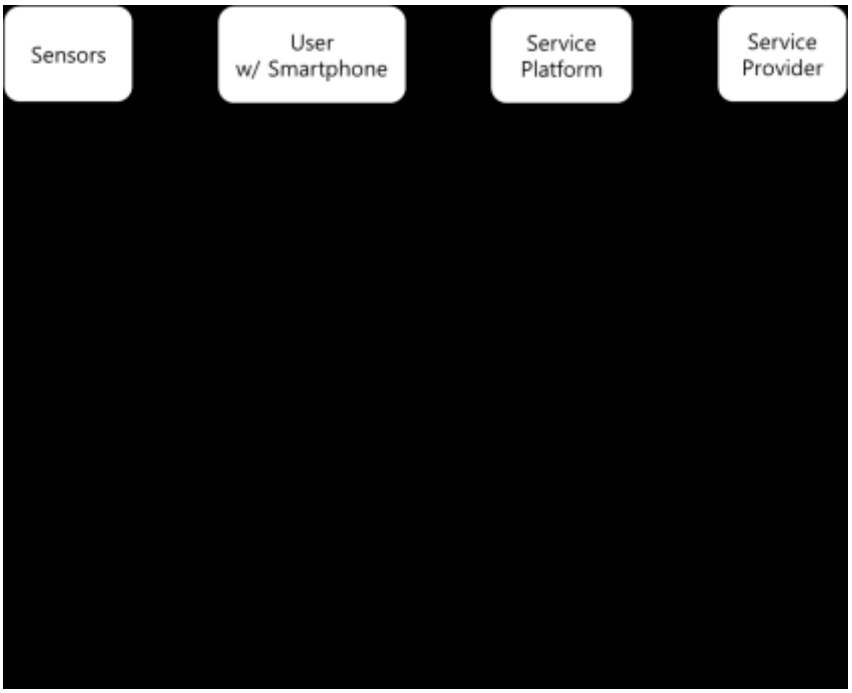

Figure IV-10: Car sharing service flow

– Detailed flow description

1) The applications of each service provider in the service domain register and subscribe to changes of resources (or information) about the car sharing service in the service platform.
2) As the user finds a shared car, opens the car door and turns on the ignition using interfaces of the Smartphone such as Bluetooth or Near Field Communication (NFC), if the user is authorized.
3) The sensors report the changed status to the service platform via the smartphone as a gateway when the specific condition of "Car is just got used" is triggered.
4) The service platform notifies the car sharing service provider of the changed status.
5) The sensors report the changed status to the service platform. It is occurred periodically that are location reporting and car health check for maintenance reasons.
6) The service platform notifies the car sharing service provider of the changed status.
7) The sensors report the changed status of "low fuel" to the service platform.
8) The service platform immediately notifies the car sharing service provider of the changed status.
9) The car sharing service provider finds out the nearest gas station according to the received location information and a service agreement between the car sharing service provider and the gas station, and the provider sends the route information to service platform.
10) The service platform notifies the smartphone of the route information.
11) After filling gas, the sensors report the changed status of "enough amount of fuel" to the service platform.
12) The service platform reports the change of car status.

13) As the user arrives at the destination, and turns off the ignition, the sensors report the accumulated information, normal event subscription information, to the service platform via smartphone.

14) The service platform notifies the car sharing provider of the usage of the shared car.

5.4 Trust matrix

Trust matrix presents trust relationship among actors of this use case based on flow of data.

Table IV-5: Trust matrix for car sharing service

From \ To	Sensors	Smart Phone (User)	Service Platform	Service Provider
Sensors	-	-	Trusted data collection and aggregation	-
Smart Phone (User)	Trusted data collection and aggregation	-	Privacy	Privacy
Service Platform	Trusted data collection and aggregation	Privacy	-	Trusted data process and analysis
Service Provider	-	Privacy	Trusted data process and analysis	Trustworthy application

5.5 Analysis

– Trusted data collection and aggregation

Data should be trustworthy from devices (sensors) to gateway (smartphone) service platform. In flow #3 and #5, devices produce data, and data is collected in a service platform. And, in flow #11, data is transmitted from service platform to devices. In flow #7 and #11, devices report their status to the service platform via gateway. When data is produced and transmitted to other entity, trustworthiness of data is required to be maintained.

– Trusted data process and analysis

Information which is processed by service platform and application should be trustworthy. In flow #1, applications send registration information with proper access right of the resources and grant that request to service platform. In flow #4, #6, #8 and #12, service platform detects changed status by processing collected data from devices and notifies to applications. Since the gateway and service platform manipulate collected data, the trustworthiness of information (i.e., processed and analysed data) is required to be maintained in each process.

– Trustworthy application

This use case can contain multiple service providers (applications), so trustworthy application and interactions between applications are important. In flow #7 and #13, two applications exchange data and information (e.g., location information, transaction information, etc.) to provide proper services. Since applications handle many data and information, the trustworthiness of application is required to be maintained in each process.

– Privacy

In flow #2, user profile information is used to figure out authorized user. User profile and payment information contains many user privacy data (e.g., location, amount of payment, credit card information etc.) Thus, privacy preserving is required to consider OS.

6 Used car transaction service

6.1 Description

While the used car market has been growing consistently in worldwide, there exists inevitable distrust in used car transactions. Comparing to purchasing a new car, buying a used car involves high level of uncertainty and risk. The market for used car is called as "the market for the lemons", which is produced by asymmetric information, in which a buyer can not accurately assess the exact condition of the car through examination before sale is made while a seller can more accurately assess the condition of the car prior to sale. Specifically, owners of good cars will not sell their cars while only owners of defective cars will sell their cars. When a seller is going to sell their used vehicle, he or she has a weak motivation of disclosing the problems in the car. As a result, consumers are hardly satisfied with the used cars because of unexpected car trouble. General transaction model and each entity's information level of a used car are depicted in Figure IV-11.

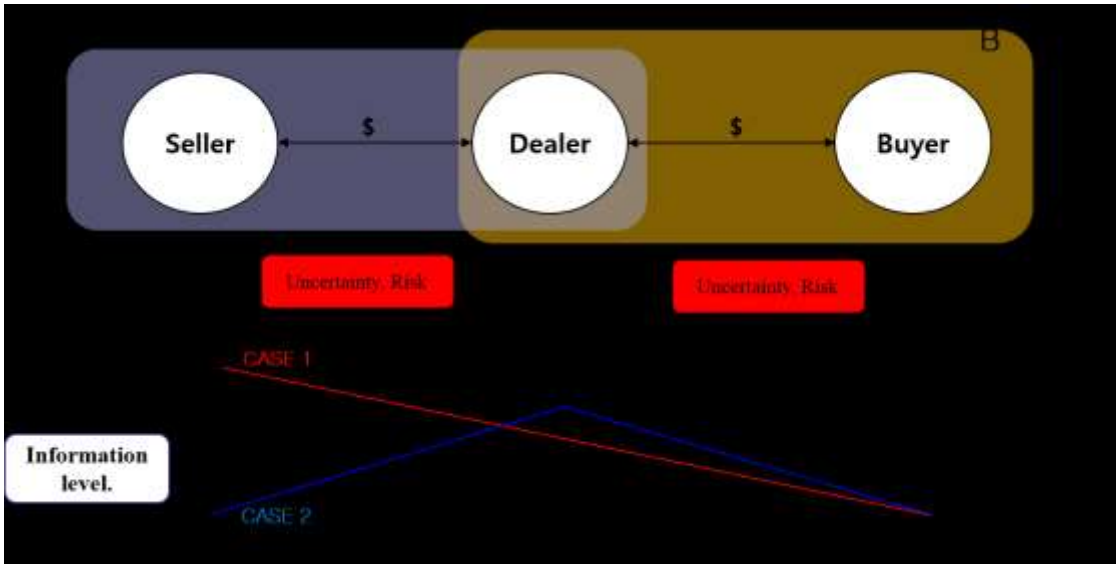

Figure IV-11: Risk, uncertainty and motivation in used car transactions

Transaction *A* describes a situation that a dealer purchases a used vehicle from a seller. In this transaction a dealer is a risk taker. A dealer should investigate the car carefully to assess the condition of the car and evaluate the price because a dealer cannot confirm a seller's explanation about the car. Specifically, a seller does not have a strong motivation of disclosing all information about the car because this information directly influences the price (Case 1). It is also plausible to assume that a seller is not aware of the exact condition of the car because symptoms of trouble has not yet clearly shown (Case 2). Thus, a deal should investigate the car. However, this cross-sectional investigation is not enough to understand the real condition of the car. Thus, intense disputes commonly occurs after a transaction.

Transaction *B* describes the situation of that a buyer purchases a dealer the used car. In this transaction, a buyer is a risk taker. Similar to transaction *A*, a buyer cannot trust in a dealer (seller) because a dealer has a strong motivation of hiding the exact information about current condition of the car (Case 1). Although a dealer detects the critical problems of the used vehicle after transaction *A* finished, a

dealer will not intend to unveil the detected the problems (Case 2) because this transaction accounts for dealer's income. As a result, a dealer – a risk taker in transaction *A* – sells defective used cars deliberately partly with intention, partly by accident.

As a result, each entity participating in these transactions have conflicting motivations of unveiling information on the condition of a used vehicle, so motivations cannot be aligned without an external intervention. Because of this confliction, "trust" cannot be guaranteed in used vehicle transaction. Although a seller and buyer need a mediating entity – a dealer – to reduce transaction cost, the problem is that a dealer is a buyer in transaction *A* and also a seller in transaction *B*. Here, transaction cost refers to a cost incurred in making an economic exchange. In addition, a dealer always tries to make used car transactions for his or her revenue.

As a result, asymmetric information causes inevitable distrust in economic transaction for used car through conflicting motivation. A buyer cannot trust in sellers' word about the condition of the vehicle. While consumers need a careful investigation in order to avoid purchasing defective vehicle, they are not accustomed to investigate the car. Consequently, asymmetric information makes them fail to trust in sellers and used cars, so level of satisfaction is always threatened. A great number of articles have shown that trust is strongly related to satisfaction of various goods.

In summary, as seen in Figure IV-12, the current used car transaction involves following inevitable problems; (1) asymmetric information, (2) conflicting motivation of disclosing the condition of used car due to (1), and (3) distrust among entities due to (2). Thus, an appropriate intervention is needed for avoiding dispute among entities and activating the used car market.

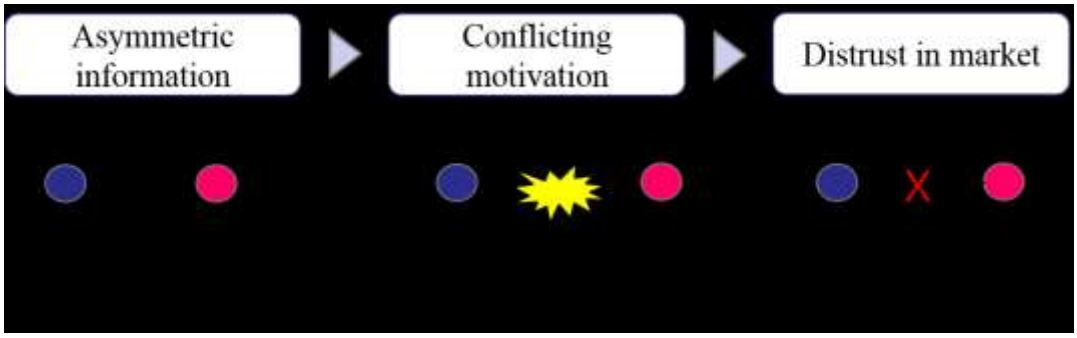

Figure IV-12: Problems of the current used car transaction service

In order to overcome sequential problems discussed, it is direct remedy to make participants share information. Trust management platform can play an important role in mediating entities who participate in used vehicle market and sharing trustful data and information (Figure IV-13).

When a buyer request selling his/her car, a dealer registers that vehicle in an online market place liked to trust service broker. Then, trust management platform automatically collects data from various sources such as insurance company, public organization, social network services, and vehicle itself. If a vehicle owner attaches On-Board Diagnostics 2 (OBD2) scanner, this IoT device records and accumulates wide ranges of vehicle-oriented information such as driving distance, recorded fuel efficiency, accident, driving habits, and maintenance and repair history.

In the next step, by transforming these fragmented data into single information, trust management platform identifies and evaluate the level of trust of an owner of used car, a registered vehicle, and a dealer. Based on this refined and trustful information, a buyer can assure the condition of the used vehicle prior to purchasing and make a purchase decision with comparably low level of uncertainty and risk.

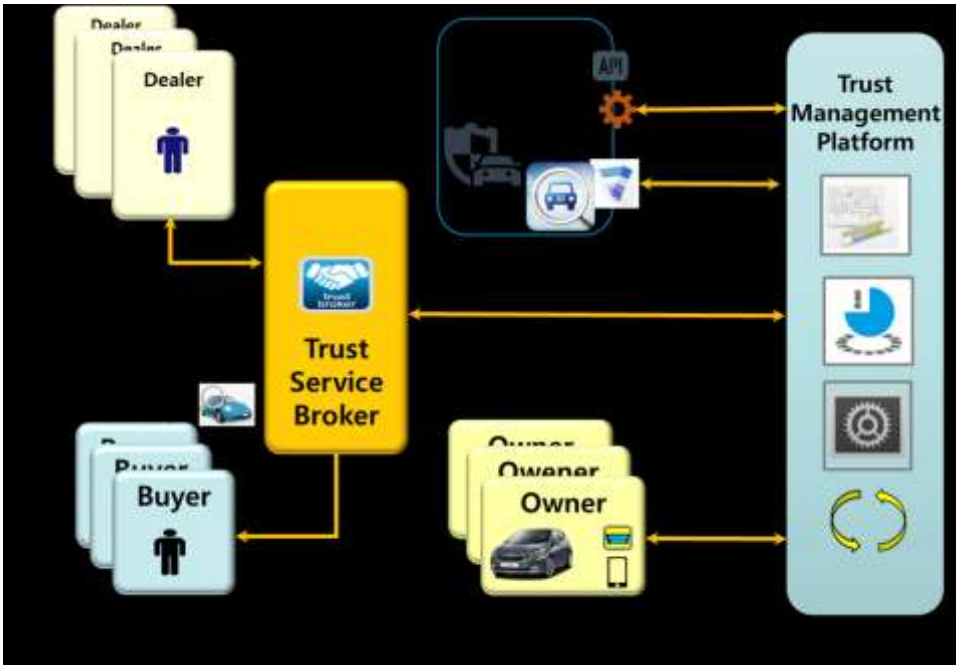

Figure IV-13: Used car transaction service high level illustration

6.2 Actors

As the participants in the used car transaction process depicted in Figure IV-13 have different goals, each actor plays a distinctive role and conducts different function.

- Dealer
  - The major role of a dealer is mediating buyer and seller (owner) to gain economic profit.
  - A dealer can sell the possessed cars, which were already purchased, or can mediate the transaction between sellers and buyers.
- Buyer
  - A buyer is someone who wants to purchase a used car from a dealer or seller.
  - When a buyer wants to purchase a used car, a buyer can search the car in a market place or on the web provided by service broker.
  - When a buyer requests dealers and brokers for purchasing the car, he or she generally describe the specific constraints such as vehicle age, accumulated mileage, brand, model, budget, and so on.
  - Based on identified information about the condition of the car, he or she can make a purchase decision under relatively low uncertainty and risk.
  - The more provided information is trustful and abundant, the more they can reduce risk and uncertainty.
- Owner (Seller)
  - An owner (seller) is someone who wants to sell his or her car to others including a dealer and individual buyer.
  - When an owner tries to sell the car, he or she simply sell a dealer or an individual the car at a negotiated price. Otherwise, he or she can ask a dealer transaction brokering.
- (Trust) Service Broker

- Trust service broker is a broker mediating an interaction among buyers, sellers, and dealers through the information transferred by trust management platform.
- Based on the information, trust service broker can inform the identified level of trust of owner, registered vehicle, and seller.

• Trust Management Platform
- Trust management platform responses various requests from a service broker and others.
- Trust management platform analyses the level of trust by tracing the accumulated data from various sources including social network, insurance company, vehicle repair shop, public, and the car itself.

6.3 Detailed service flow

Figure IV-14: Used car transaction service flow

– Detailed flow description

1) A dealer registers the used car in trust service brokers as an owner makes a request to a dealer for selling the used car.
2) Trust management platform complies with a service broker's request of transferring trustworthy data related to the car.
3) Trust management platform gathers the relevant data from not only the external data sources such as insurance company, public organization, social network services, but also an internal data source such as OBD scanner, which transfers historical data from car to the platform. If car owner attaches OBD scanner in the car, he can confirm the condition of the car and identify problems via applications on a smartphone.
4) A dealer registers the car with explanatory data about the car in the marketplaces connecting with a number of service brokers. At this time, the car is ready for sales.

5) A buyer can search number of used cars in order to purchase the car.

6) When a buyer is interested in a specific car, he or she can ask the service brokers relevant data and information. Then, trust management platform replies service broker's requests by providing processed trustful data including the level of trust of owner, registered car, and seller (or dealer).

7) In order to help a buyer's purchase decision, a service broker visualizes the analysis results.

8) A buyer can make a purchase decision with relatively low risk and uncertainty.

9) The used car transaction occurs among parties.

10) After completing the transaction, transaction commission can be transferred. The commission rate and recipient depends on business model and pre-determined rules.

6.4 Trust matrix

In order to achieve valuable analysis results, the proposed system needs data from various sources. The data source includes social network service, insurance company, an organ of credit, car repair shop, bank, and OBD2 scanner attached in the car. An example for possible trust matrix structure is shown in Table IV-6.

Table IV-6: Trust matrix for used car transaction

From \ To	Owner	Used car	Trust Management Platform	Buyer
Owner	-	Ownership	Trusted data collection and aggregation Trusted data process and analysis	-
Used car	Ownership	-	Trusted data collection and aggregation Trusted data process and analysis	Risk, uncertainty
Trust Management Platform	Trusted data collection and aggregation Trusted data process and analysis	Trusted data collection and aggregation Trusted data process and analysis	-	Trustworthy application
Buyer	-	Risk, uncertainty	Trustworthy application	-

6.5 Analysis

– Participants' advantage of adopting used car transaction through trust management platform.

This clause describes how trust can be achieved in used car transaction by trust management platform, which plays an important role in reducing the information gap among entities, refining data from various data sources, and mediating entities through trust service broker. By adopting this platform, each entity participating in used car ecosystem can take following advantage. Details are explained in following Table IV-7.

Table IV-7: Advantages of actors from trust based used car transaction service

	Main advantages	Side advantages
Seller	- Providing trustful data which influence on selling price	- Reasonable vehicle maintenance based on trustful data transmitted by vehicle itself - Reducing insurance cost by a vehicle specific data
Dealer	- Reducing investigation effort - Decreasing dispute	- Restoring confidence in used car transaction
Buyer	- Reducing uncertainty and risk from purchasing used goods	- Succession to well-maintained vehicle - Purchasing relatively low retail price in P2P market
Insurance Corp.	- Realizing usage-based insurance by absorbing deadweight loss	
Government	- Reducing dispute - Revitalizing market - Promoting international vehicle transaction	- Improving road infrastructure and traffic flows
Vehicle Manufacturer	- Detecting defective vehicle model in early stage	- Gathering real data for improving vehicle performance
OBD2 Scanner manufacturer	- Creating new revenue stream	- Taking opportunity of analysing vehicles' historical data

– Cost structure of adopting used car transaction through trust management platform

In order to adopt the used car truncation based on trust, it is required to discuss who has a responsibility for deploying the trust platform, which is composed of trust service broker, trust management platform, and other entities. Although the adoption of this platform needs investment, the responsibility for deployment depends on business model and government policy.

For example, buyers can compensate for the investment since they are regarded as the one who takes the most advantage of adopting trust platform. Otherwise, the government can invest on building and operating trust management platform instead of consumers. Simply, government will invest on this platform if the platform can increase both consumer and producer surplus. If dealers can take the most advantage, dealers should be responsible for deploying trust platform. However, it needs further studies because a careful investigation is required to figure out who is taking the greatest advantage.

As we discussed, there exists other issues such as business models, ecosystem, and policies. Careful investigation about these issues can lead to figure out the cost structure and responsibilities. When each entity's motivations are clearly aligned, the problem of cost structure can be resolved. Thus, relevant studies on business models and ecosystem, and economic analysis for this platform are fundamentally required.

Bibliography

[b-ITU-T X.1601] Recommendation ITU-T X.1601 (2014), Security framework for cloud computing

[b-ITU-T Y.2060] Recommendation ITU-T Y.2060 (2012), Overview of the Internet of things

[b-Afuah] Afuah, Allan and Tucci, Christopher L. (2001), Internet Business Models and Strategies, McGraw-Hill Irwin.

[b-UN] Understanding Knowledge Societies: In twenty questions and answers with the Index of Knowledge societies, UN. 2005.

[b-UNESCO] Towards Knowledge Societies, UNESCO Publishing, ©UNESCO 2005, ISBN 92-3-204000-X

[b-Alcalde] Alcalde, B., Dubois, E., Mauw, S., Mayer, N. and Radomirović, S. (2009), Towards a Decision Model based on Trust and Security Risk Management, 7th Australasian Conference on Information Society, Vol. 98, pp. 61-70.

[b-Josang] Josang, A., Ismail, R. and Boyd, C. (2007), *A Survey of Trust and Reputation System for Online Service Provision*, Decision Support System, Vol. 43, No.2, March, pp. 681-644.

[b-McKnight] McKnight, D.H., Carter, M., Thatcher, J.B. and Clay, P.F. (2011), *Trust in a specific technology: An investigation of its components and measures*, ACM Transactions on Management Information Systems (TMIS), Vol. 2, No. 2, June, pp. 12-36

[b-uTRUSTit] Trust Definition White Paper (2012), *Defining, Understanding, Explaining TRUST within the uTRUSTit Project*, August.

[b-Chang-2005] Chang, E., Hussain, F.K. and Dillon T.S. (2005), *Fuzzy nature of trust and dynamic trust modelling in service oriented environments*, Proceedings of the 2005 workshop on Secure web services (SWS '05). ACM, New York, NY, USA, November, pp. 75-83.

[b-Chang-2006] Chang, E., Dillon, T. and Hussain, F.K. (2006), *Trust and Reputation for Service-Oriented Environments: Technologies for Building Business Intelligence and Consumer Confidence*. West Sussex, England: John Wiley & Sons Ltd.

[b-Bertino] Bertino, E. (2012), *Trusted Identities in Cyberspace*, IEEE Internet Computing, Vol. 16, No. 1, February, pp. 3-6.

[b-Wahab] Wahab, O.A., Bentahar, J., Otrok, H. and Mourad, A. (2015), *A survey on trust and reputation models for Web services: Single, composite, and communities*, Decision Support Systems, Vol. 74, June, pp. 121-134.

[b-Grandison] Grandison, T. and Sloman, M. (2000), *A Survey of Trust in Internet Applications*, Communications Surveys & Tutorials, IEEE, Vol. 3, No. 4, September, pp. 2-16.

[b-Blaze] Blaze, M., Kannan, S., Lee, I, Sokolsky, O., Smith, J.M., Keromytis, A.D. and Lee, W. (2009), *Dynamic Trust Management*, IEEE Computer, Vol. 42, No. 2, February, pp. 44-52.

[b-Yan] Yan, Z., Zhang, P. and Vasilakos, A.V. (2014), *A survey on trust management for Internet of Things*, Journal of Network and Computer Applications, Vol. 42, March, pp. 120-134.

[b-Govindan] Govindan, K. and Mohapatra, P. (2012), *Trust computations and trust dynamics in mobile adhoc networks: A survey*, Communications Surveys & Tutorials, IEEE, Vol. 14, No. 2, May, pp. 279-298.

[b-Yu] Yu, H., Shen, Z., Leung, C., Miao, C. and Lesser, V.R. (2013), "*A survey of Multi-Agent Trust Management systems*," IEEE Access, Vol. 1, May, pp. 35-50.

[b-Ahmed] Ahmed, A., Bakar, K.A., Channa, M.I., Haseeb, K. and Khan, A.W. (2015), *A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks*, Frontiers of Computer Science, Vol. 9, No. 2, April, pp. 280-296.

[b-Sherchan] Sherchan, W., Nepal, S. and Paris, C. (2013), *A Survey of trust in social networks*, ACM Computing Surveys, Vol. 45, No. 4, August, pp. 47-79.

[b-EU-Safeharbor] EU Safe Harbor, http://www.export.gov/safeharbor/eu/eg_main_018476.asp

[b-Yoo-2012] Yoo, Y., Boland, R.J., Lyytinen, K. and Majchrzak, A. (2012), *Organizing for Innovation in the Digitized World*, Organization Science, Vol.23, No.5, October, pp. 1398-1408.

[b-Yoo-2010] Yoo, Y., Henfridsson, O. and Lyytinen, K. (2010). *Research commentary: The new organizing logic of digital innovation: an agenda for information systems research*, Information Systems Research, Vol.21, No. 4, June, pp. 724-735.

[b-Eisenmann] Eisenmann, T., Parker, G., and Van Alstyne, M. W. (2006). *Strategies for two-sided markets*. Harvard business review, Vol.84, No.10, October, pp. 92-104.

[b-Gawer] Gawer, A. (Eds.) (2009). *Platforms, markets and innovation,* Cheltenham, UK: Edward Elgar Publishing.

[b-Sandberg] Sandberg, J., Holmstrom, J. and Lyytinen, K. (2013). *Platform change: theorizing the evolution of hybrid product platforms in process automation*, In Platform Strategy Research Symposium. Boston University, Boston, MA.

[b-Mayer] Mayer, R. C., Davis, J. H. and Schoorman, F. D. (1995). *An integrative model of organizational trust*, Academy of management review, Vol.20, No. 3, July, pp. 709-734.

[b-Gilson] Internet of Things Lacks Safety Today, Opening Door to Major Threats Tomorrow, Warns OTA. Online Trust Alliance. Retrieved from https://otalliance.org/news-events/press-releases/internet-things-lacks-safety-today-opening-door-major-threats-tomorrow

[b-OTA] OTA IoT Trust Framework – Pre-Release Draft. Retrieved from https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework_lastcall.pdf

[b-TCG 2013] TCG Published. (2013, October). Architect's Guide: Cybersecurity. TCG Published. Retrieved from http://www.trustedcomputinggroup.org/files/resource_files/CA36D107-1A4B-B294-D08829372D5796E1/Architects Guide Cybersecurity.pdfLeigh Ann Gilson. (2015). Internet of Things Lacks Safety Today, Opening Door to

Major Threats Tomorrow, Warns OTA. Online Trust Alliance. Retrieved from https://otalliance.org/news-events/press-releases/internet-things-lacks-safety-today-opening-door-major-threats-tomorrow

[b-TCG 2015] TCG Published. (2015, September 14). Guidance for Securing IoT Using TCG Technology. 1.1. TCG Published. Retrieved from https://www.trustedcomputinggroup.org/files/resource_files/CD35B517-1A4B-B294-D0A08D30868AB3D1/TCG_Guidance_for_Securing_IoT_1_0r21.pdf

[b-Christensen] Christensen, Clayton M. (2014). Disruptive Innovation. In: Soegaard, Mads and Dam, Rikke Friis (eds.). The Encyclopedia of Human-Computer Interaction, 2nd Ed. Aarhus, Denmark: The Interaction Design Foundation.

[b-McKnight 2002] McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. Information systems research, 13(3), 334-359.

[b-Tilson] Tilson, D., K. Lyytinen, et al. (2010). Research Commentary – Digital Infrastructures: The Missing IS Research Agenda. Information Systems Research.

[b-Atzori] L Atzori, et al., "The social internet of things (SIoT)–when social networks meet the internet of things: Concept, architecture and network characterization", Computer Networks 56 (16), 3594-3608, 2012

[b-Bao] F. Bao, I. R. Chen, and J. Guo, “Scalable, Adaptive and Survivable Trust Management for Community of Interest Based Internet of Things Systems,” 11th International Symposium on Autonomous Decentralized System, Mexico City, Mexico, 2013.