Strengthening Trust in the Future Social-Cyber-Physical Infrastructure: An ITU-T Perspective

[1]Tai-Won Um, [2]Gyu Myoung Lee and [3]Jun Kyun Choi
[1]Electronics and Telecommunications Research Institute (ETRI), twum@etri.re.kr
[2]Liverpool John Moores University (LJMU), g.m.lee@ljmu.ac.uk
[3]Korea Advanced Institute of Science & Technology (KAIST), jkchoi59@kaist.edu

Abstract

Evolving towards a knowledge society requires a trusted ICT infrastructure for sharing information and creating knowledge. To advance the efforts to build converged ICT services and reliable information infrastructures, ITU-T has recently started to work on future trusted ICT infrastructures. This article proposes a possible future Social-Cyber-Physical infrastructure which acts as the glue for integrating physical, cyber and social worlds with ICT, and outlines proposals towards an effort to find viable solutions for trust related problems while developing advanced technologies from an ITU-T standards perspective along with the trust conceptual model and the trust architectural framework.

1 Introduction

The widespread availability of feature-rich communications is the result of end-user devices, advanced networks and new services that exploit the developments in Information and Communication Technology (ICT). For evolving towards a knowledge society, 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 [1], various problems exist due to the lack of trust. The large scale collection and analysis of data from sensors and devices in the physical world 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 [2]. If knowledge is exploited for malicious intentions, it could suffer from irreparable damage and uncertain dangers. However, it is difficult to identify and prevent the risks of knowledge sharing in complicated ICT infrastructures.

Smart services using ICT have been required to obtain reliable knowledge from raw data. As an aim of intelligent service provisioning 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 provision of services that comply with users' needs and rights. It is therefore necessary to find a way to minimize the unexpected risks and maximize the survivability of future knowledge society. Within certain reliability and predictability, the ICT infrastructure should be operating in a controlled environment. It should be robust to unexpected conditions and adaptable to system failures.

With the emergence of Internet of Things (IoT) [3] and related technologies, more heterogeneous objects get connected to the Internet. The marriage of IoT and Web transforms smart objects into social entities which are capable of bridging human-to-object interactions. The paradigm of Cyber-Physical-Social Systems (CPSS) [4], [5] has recently gained momentum as an environment that combines knowledge from various smart spaces to form an ecosystem.

Based on the significant efforts made to build converged ICT services and a reliable information infrastructure, ITU-T has recently started to 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 article proposes a possible future Social-Cyber-Physical (SCP) infrastructure which acts as the glue for integrating physical, cyber and social worlds with ICT as a basis for a knowledge society. It then outlines ideas for an effort

to find viable solutions to trust related problems while developing advanced technologies from an ITU-T standards perspective along with the trust conceptual model and the trust architectural framework. The aim is to create a trusted SCP infrastructure for sharing information and creating knowledge, and to stimulate activities for future standardization on trust with related Standards Developing Organizations (SDOs).

2 Trust in the SCP Infrastructure

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 [6]. In computer science, trust has two aspects: "user trust" and "system trust". For a user, trust is based on psychological and sociological considerations because it is "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" [6]. For the IoT, trust relies on the integrity, ability or character of an entity [7], [8]. Trust can be further explained in terms of confidence in the truth or worth of an entity.

The main elements of ICT infrastructures rely mostly on 3Cs (Computation, Communication and Control) to extract knowledge from the information available in the data obtained from various systems, including sensors and actuators. Most importantly, the transition to the SCP infrastructure depends on how useful knowledge is acquired from data and information. Trust is essential in this knowledge acquisition process; also, for awareness and understanding of a specific context, it is of utmost importance to have confidence in decision-making processes. In other words, trust should be an additional consideration with regard to systems that behave intelligently and rationally to sense real-world behaviour, perceive the world using information models, adapt to different environments and changes, learn and build knowledge, and act to control their environments. This is mainly related to the Data, Information, Knowledge, Wisdom (DIKW)[1] hierarchy.

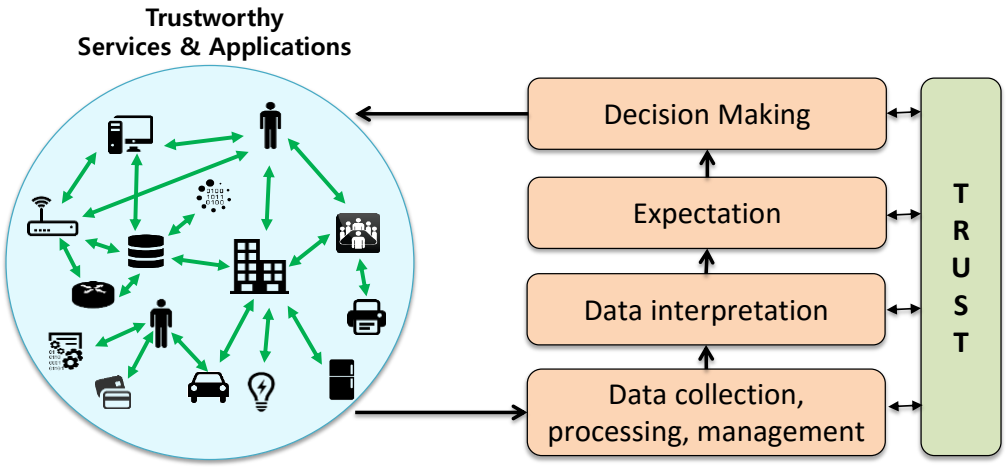

Figure 1: Trust in the whole process from data collection to decision making

The social and economic value of data is mainly reaped at two stages: firstly, when data and information are transformed into knowledge (gaining insights) and secondly, when they are used for decision-making (taking action). The knowledge is accumulated over time by an individual or systems through data analytics. Data processing, management and interpretation for awareness and understanding have been considered as fundamental processes for obtaining knowledge. Furthermore, the expectation process for trust should be additionally considered before decision-making. As shown in Figure 1, trust should be considered throughout the whole process from data collection to decision making for trustworthy services and applications.

[1] DIKW: 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

Figure 2 represents trust in the SCP infrastructure in the shape of a sphere. This infrastructure comprises three domains – the physical domain, the cyber domain and the social domain. The physical domain contains a huge number of objects (i.e., hardware, device) including sensors, actuators and mobile terminals that generate data by sensing physical objects and their behaviours within their environments (e.g., temperature, pressure, etc.). The 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 cooperate for data coding, transmission, fusion, mining and analysis to provide information and knowledge to humans independent of location in fixed/mobile environments. Lastly, the social domain in relation to a trusted technology with an individual and communities is also important. The three different domains need an infrastructure that is more reliable and closely correlated through cross-tier trust management.

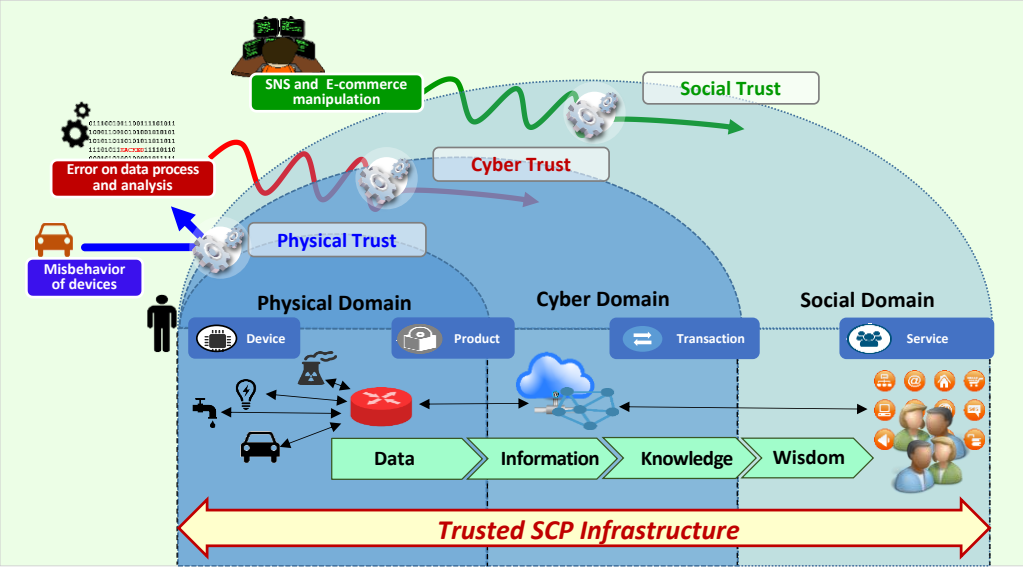

Figure 2: The concept of trust in the SCP infrastructure

To strengthen trust while building a knowledge society, the trusted SCP infrastructure will be a key item for international standardization towards the development of trust technology, while at the same time expanding the functions of the core technology components.

3 Trust Conceptual Model and SCP Trust Threats

3.1 Generic Trust Conceptual Model

The SCP infrastructure comprises objects from the physical domain (physical objects), the cyber domain (virtual (or cyber) objects) and the social domain (humans with attached devices, called social objects). To clarify ICT capabilities for trust provisioning with SCP relationships, the conceptual model is shown in Figure 3. The model comprises different horizontal domains (i.e., social, cyber and physical) and different vertical domains (i.e., humans & objects, networking & environment and data). There are multiple service domains for supporting a multiplicity of applications. The SCP infrastructure is logically sliced so that individual service domains share the infrastructure.

In the proposed model, trust is associated with all vertical and horizontal domains. Thus, similar to security, trust management technology is necessary as a separate common domain which covers all vertical and horizontal domains. Using this model, we intend to illustrate the complex relationships and roles required for trust provisioning between and across domains that are associated with an individual entity of the SCP infrastructure and services.

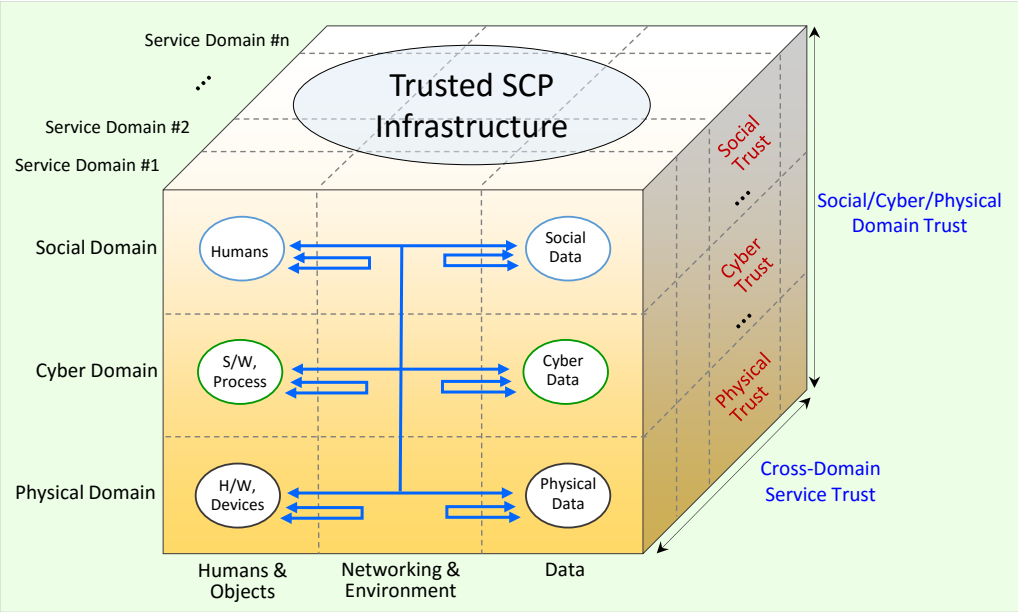

Figure 3: Generic ICT trust model

Physical Trust

In the physical domain, collecting secure and reliable data from physical objects is the first step in providing trustworthy ICT services and applications because the propagation and processing of false data will cause service degradation and waste system resources.

In order to detect trust problems in the physical domain (e.g., injection of obstructive signals), malfunctions of systems, shutdowns or accidents, the operation of the physical objects and its data must be examined. Since much data is created from constrained devices, lightweight security and trust mechanisms are needed for data processing trust (e.g., efficiency, accuracy, reliability, etc.).

Cyber Trust

In order for virtual objects to cooperate safely in the cyber domain, they have to distinguish between malicious and non-malicious objects. One way to resolve this challenge is to evaluate the trust with related indicators (e.g., trust metrics and attributes) to decide with which virtual objects to cooperate. On the other hand, when huge amounts of data are collected in the cyber domain, they should be processed and analysed accurately and transparently.

Data, information and knowledge should also be 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 must be used to support heterogeneous and specific networking contexts.

Social Trust

As social networks are popular for sharing information and knowledge, trust is becoming an important feature among users as well as their service providers. Social trust implies that members of a community act according to the expectation that other members of the community are also trustworthy and expect trust from other community members. It actually depends on the behaviour and interactions of humans in the social networks. If trust is not gained by humans, they may not wish to share their experience and knowledge with others because of the fear that their knowledge and privacy will be misused.

Social/Cyber/Physical Domain Trust

In the SCP infrastructure, there are interactions between objects, as well as data transmission between them. Actually, the objects in the physical/cyber domain interoperate closely with each other and form a system organization around its users in the social domain. Human interactions with virtual/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 between their devices. To define and manage trust between SCP domains, appropriate trust models for the interactions between social, information and communication networks are required while taking into account the severe resource constraints and the dynamics. Trust evaluation and management are especially challenging issues in the SCP cross 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 a cross service trust management that is able to cover SCP trust relationships between different service domains.

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

3.2 Trust issues and threats in the SCP infrastructure

The SCP infrastructure may be unreliable and unpredictable if certain levels of credibility and controllability of objects are not guaranteed. ICT ecosystems based on the SCP infrastructure also would not be trustworthy without guarantee of stability and reliability of objects. Table 1 describes examples of trust issues and threats in the SCP infrastructure based on Figure 3.

Table 1: Trust issues and threats in the SCP infrastructure

	Humans & Objects	Data	Networking & Environment	SCP Domain	Cross-Domain Service
Trust Aspects	Human and object itself	Data generated from objects	Environmental aspects including networking	Cross-social/cyber/physical domains	Cross-heterogeneous services
Social Domain	• How can I believe a correspondent? • Who is an expert in this area? • Who is a proper mediator?	• Is the rumour true? • Timeliness of data • Usability of data	• Is there any personal connection between them? • Is my call secure? • Environment aspects related to humans, location, time	• Are my devices working well? • Who is the owner of that device? • Closeness between humans/objects/services • User interfaces/ experience to use services/devices • Standard compliance of interface between humans/objects/services	• How information/data of a service affect another service? • How reputation and recommendation spread and is calculated among services? • How to exchange knowledge/information/data among services in a secure, reliable manner • How to collect and analyse heterogeneous knowledge/information/data in a standard manner?
Cyber Domain	• Which Web service is better? • Is the cloud service reliable? • Maintainability	• Quality of information • Effectiveness of information presentation • Correctness of data gathering & analysing	• Reliable linking objects • Linking content for recommendation • Linking document • Authentication/authorization		
Physical Domain	• Which one is a proper node to send data? • Correct recognition and identification of objects • Manufacturer of devices	• Standard compliance of data format • Data integrity • Data encryption mechanism	• Communication availability • Communication reliability • Secureness of data channel • Standard compliance of communication protocols		

The social domain relies on people's trustworthiness and reliability as well as on their knowledge and information. The advancement of ICT not only accelerates the spread of knowledge but also makes the interaction between people complicated. False knowledge propagation gives rise to widespread confusion. This false knowledge propagation can occur in social networks through worms, data leaks, botnets, etc.

Virtual objects such as processing/storage/networking resources and software capabilities could be unpredictable or unreliable, since small deviations of expected operations may cause catastrophic failures. It is important to determine whether the virtual objects have operated correctly.

Physical objects such as smart devices are autonomically working and cooperating with each other for executing a certain task assigned from human or virtual objects. A physical object needs to be correctly identified and verified for it to be determined whether the object is a proper correspondent before starting interaction with it. In the physical domain, one of the important trust issues is data integrity, which refers to maintaining and assuring the accuracy and consistency of data. Data integrity failure comes from any unintended changes to data as the results of storage, retrieval, processing operation, including malicious intent, unexpected hardware failure, and human error, etc.

A distinguishing characteristic of the SCP infrastructure is close interactions among objects, which will cause various trust issues across different domains. Furthermore, convergence and mash-up of services could propagate a local error or a fault from within a service domain to other service domains.

4 Trust Architectural Framework

Based on the previous discussion, the trust architectural framework agreed in ITU-T for strengthening trust in the SCP infrastructure is presented in Figure 4 for stakeholders in an ICT ecosystem value chain. It consists of four major parts as follows:

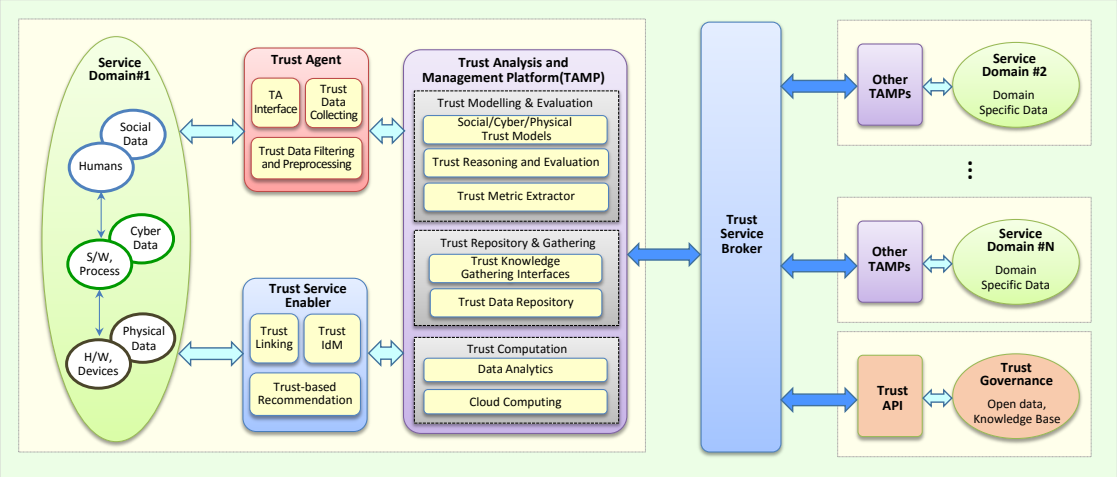

Figure 4: Trust architectural framework

Trust Agent (TA)

TA is used to collect trust-related data from the SCP 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 Preprocessing:** This module is used to refine trust data sets without including other data that can be repetitive, irrelevant or even sensitive for trust evaluation.

Trust Analysis and Management Platform (TAMP)

TAMP is used for modelling, reasoning and managing trust data collected from TAs to check whether 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 domain-specific and service-specific and there are SCP trust models to define a trust model for each domain in the SCP infrastructure. According to its domain and a particular service, a suitable trust model is selected and applied for trust modelling. The trust-related data collected from trust agents can be transformed to structured and annotated formats by using semantic and ontology technologies through this 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 domain and the service, 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 context, a trust reasoning method must handle such dynamics of trust.

- **Trust Metric Extractor:** This module 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 other trust knowledge regarding on object's other trust aspects from related service domains via the Trust Service Broker.

- **Trust Data Repository:** The structured trust data (including operations of objects and the history of interaction 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 has changed or an interaction occurs between objects. To process the large amount of data related to trust evaluation, it can adopt big data technologies for calculation of the trust level of objects and for examining the change of the trust state of objects based on direct observation.

Trust Service Enabler (TSE)

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

- **Trust Linking**: Trust linking is a module capable of creating a link between objects based on trust criteria.

- **Trust IdM:** The identity management (IdM) can be used to manage digital identification/authentication of objects. Trust IdM is able to involve trust knowledge to assure the identity of trustworthy objects and support trust-based services and applications.

- **Trust-based Recommendation**: This module provides recommendations to other objects. A number of individual objects can be interconnected to construct a complex system for providing various services, and many objects with identical capabilities will exist on the Internet. This module aims at providing a recommendation for selecting a suitable object that meets the trust level.

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 via other TAMPs. TSB also provides a brokering service from trust governance information through trust Application Programming Interface (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.

5 Challenges for Standardization on the Trusted SCP Infrastructure

5.1 Current Activities for Standardization on Trust in ITU-T and Related Standardization Bodies

As mentioned in the introduction, ITU-T has recently started ground breaking work on future trusted ICT infrastructures to cope with emerging trends in ICT while also considering social and economic issues. ITU-T Study Group (SG) 13 established the Correspondence Group on Trust (CG-Trust) last year. As a result, the CG-Trust has completed the development of a technical report on trust provisioning of ICT Infrastructures in April 2016.

To date, a number of standards focusing on network security and cybersecurity technologies have been developed in various standardization bodies including the IETF. The scope of these standards needs to be expanded to take into consideration trust issues in the SCP infrastructure. There are a few preliminary activities taking place, for instance in the Online Trust Alliance (OTA) and the Trusted Computing Group (TCG). However, as existing standardization activities are still limited to social trust between humans, trust relationships between humans and objects as well as across domains of SCP and services should also be taken into account. Table 2 summarizes recent activities for standardization on trust in related SDOs.

Table 2: Standardization activities on Trust in the related SDOs

SDO	Key activities
IETF (www.ietf.org)	• Develop standards on trust in routing, access control, Web protocols.
OTA (otalliance.org)	• Develop an IoT framework to identify various requirements for IoT trust covering security and privacy as well as regulatory issues.
TCG (www.trustedcomputinggroup.org)	• Develop use cases and key functionalities (e.g., trusted network connect, self-encrypting device, trusted platform module) for interoperable trusted computing platforms.
W3C (www.w3.org)	• Consider Web of trust as a key design principle to support complex interactions among parties around the globe.
ETSI (www.etsi.org)	• Develop standards to support the European Regulation on electronic identification and trust services for electronic transactions in the internal market.
OASIS (www.oasis-open.org)	• Define trust elevation protocols to promote interoperability among multiple identity providers when authenticating electronic identity credentials.
ISO/IEC JTC1 (www.iso.org/iso/jtc1_home.html)	• Focus on trusted platform concepts, attribute-based credentials for trust, good governance of data to encourage trust.

5.2 Work Items for Future Standardization in ITU-T

From the CG-Trust activity, ITU-T needs to first find various use cases considering user confidence, usability and reliability in ICT ecosystems for new business models which reflect a sharing economy. Then, a framework for trust provisioning including requirements and architectures should be urgently specified in relation to the relevant standards.

More specifically, the following key items should be identified as future work for standardization on trust in the next study period (four years from 2017 to 2020):

- **Overview of trust in ICT**: to provide a clear understanding of trust and identify key differentiations compared to security and privacy as well as to highlight the importance of trust in future SCP infrastructure towards a knowledge society.
- **Service scenarios and capabilities**: to develop service scenarios for trust provisioning and define required capabilities to support trust considering sharing economy.

- **Requirements for trust provisioning**: to specify detailed requirements in terms of different viewpoints, considering various stakeholders.
- **Architectural framework and functional architectures**: to identify core functions for the future trusted SCP infrastructure and develop architectural models including detailed functional architectures.
- **Technical solutions for trust provisioning**: to develop methodologies for specifying trust metrics and measuring trust as well as protocol specifications for trust provisioning and mechanisms for trust-based decision making.
- **Trust provisioning for smart services & applications**: to develop specific technical solutions applicable to newly created vertical services and applications with the connected devices and other technologies (e.g., for healthcare, transportation, etc.).
- **Trust provisioning for cloud computing**: to develop specific technical solutions applicable to the processing and analysis of the large amount of data through cloud computing.

Additionally, ITU-T SG13 needs to incorporate trust issues into related SGs' activities such as the recently established ITU-T SG20 on IoT applications, services and platforms as well as smart cities infrastructure, SG17 on security matters, and SG2 on identification issues. Finally, it is necessary to closely collaborate with other SDOs mentioned in Table 2 and forums, addressing many issues on governance and transparency, while developing trust related standards.

5.3 Open Issues for Bridging the Gap between Research and Standards

Besides the standardization activities, assuring continuous trustworthiness, taking into account such characteristics for the SCP infrastructure with highly interconnected systems, is becoming an essential issue for future research. Therefore, open issues are identified for bridging the gap between research and standards.

SCP Trust Relationships
As all of the objects in the SCP infrastructure have their associated information, trust 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). For SCP trust relationships of individual and community, trust as a cross-domain relationship is needed, taking into consideration coexistence, connectivity, interactivity and spatio-temporal situations between vertical layers.

Holistic Trust for Interconnected Systems
ICT services can be achieved through a chain of interconnected systems and components that share the responsibility for providing stable and robust services. Furthermore, many systems are based on open system architectures and their properties of interconnectivity and autonomics remove system boundaries. 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 also required to apply between heterogeneous systems, service domains and stakeholders, while focusing on the relationships and dependencies between them [9].

Unified Approach to Trust-Security-Privacy
Trustworthiness requires cooperation and co-engineering of trust 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 as trust, security and privacy become tightly coupled [9].

Measurement and Formalization of Trust
Due to the diversity of applications and their inherent differences in nature, trust is hard to formalize in a general setting. However, it is important to quantify a level of trust in ICT. The level of trust can be measured and classified, similar to Quality of Service used in an objective manner (e.g., measured quantitatively) or Quality of Experience used in a subjective manner (e.g., counted qualitatively). A trust metric is used to evaluate a level of trust by which

a human or an object can be judged or decided from trustworthiness. Depending on what levels of trust the users need to know, including those related to sensitivity of information and associated resources, there may be many Trust Level Agreements. In addition, a trust index can be used as 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 stock market index.

Dynamics of Trust

In the SCP infrastructure, the state of objects changes dynamically and the number of entities also fluctuates. Basically, trust is situation-specific and changes over time. Due to the dynamics and complexity of trust, a single trust mechanism cannot perfectly solve all the issues; so it is necessary to combine different trust mechanisms.

Resource Constraints

For small-sized objects with limited computing power, their capabilities as communication objects are lower than those of higher-end processing and computing devices. To cope with these constrained objects, trust solutions with lightweight mechanisms that remove unnecessary loads/messages and minimize energy consumption become a necessity.

6 Conclusion

This article proposed an architectural framework for trust provisioning, and then identified challenges for standardization on the trusted SCP infrastructure based on activities of the ITU-T CG-Trust. With the help of trust standardization, future ICT infrastructures will require more reliable techniques to cope with the risks of knowledge sharing towards a knowledge society. Building and validating trusted relationships will be contingent on trust related information and its processing for supporting trustworthy services and applications. Therefore, global collaboration with related SDOs (e.g., OTA, TCG) is required to further stimulate trust standardization activities in the future, taking into account key technical, policy and governance issues.

Acknowledgement

This research was supported by the ICT R&D program of MSIP/IITP [R0190-15-2027, Development of TII (Trusted Information Infrastructure) S/W Framework for Realizing Trustworthy IoT Eco-system].

References

[1] Ovidiu Vermesan, Peter Friess, “Building the hyperconnected society – IoT research and innovation value chains, ecosystems and markets,” River Publishers, 2015.

[2] Data-driven Innovation for Growth and Well-being – Interim synthesis report, OECD, Oct. 2014. Available: http://www.oecd.org/sti/inno/data-driven-innovation-interim-synthesis.pdf

[3] Gyu Myoung Lee, *et al.*, “Internet of Things,” in a book “Evolution of Telecommunication services,” *LNCS*, vol.7768, pp.257~282, 2013.

[4] Fei-Yue Wang, “The Emergence of Intelligent Enterprises: From CPS to CPSS,” *IEEE Intelligent Systems*, vol.25, issue 4, pp.85~88, Jul. 2010.

[5] Jay Lee, *et al.*, “A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems,” *Manufacturing Letters*, vol.3, pp.18~23, Jan. 2015.

[6] Wanita Sherchan, *et al.*, “A survey of trust in social networks”, *ACM Computing Survey*, vol.45, issue 4, no.47, Aug. 2013.

[7] Zheng Yan, *et al.*, “A survey on trust management for Internet of Things,” *Journal of Network and Computer Applications*, vol.42, pp.120~134, Jun. 2014.

[8] Trust Definition White Paper – “Defining, Understanding, Explaining TRUST within the uTRUSTit Project”, Aug. 2012. Available: http://www.cspforum.eu/uTRUSTit_Trust_Definition_White_Paper.pdf

[9] “Special theme: Trustworthy Systems of Systems Safety & Security Co-engineering,” *ERCIM News*, no.102, Jul. 2015.