International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3052

(03/2017)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Future networks

Overview of trust provisioning in information and communication technology infrastructures and services

Recommendation ITU-T Y.3052

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	**Y.3000–Y.3499**
CLOUD COMPUTING	Y.3500–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.3052

Overview of trust provisioning in information and communication technology infrastructures and services

Summary

Recommendation ITU-T Y.3052 provides an overview of trust provisioning in information and communication technology (ICT) infrastructures and services. Recommendation ITU-T Y.3052 introduces necessity of trust to cope with potential risks due to lack of trust. The concept of trust provisioning is explained in the context of trusted ICT infrastructures and services. From the general concept of trust, the key characteristics of trust are described. In addition, a trust relationship model and trust evaluation based on the conceptual model of trust provisioning are introduced. Recommendation ITU-T Y.3052 then describes trust-provisioning processes in ICT infrastructures and services.

Details of potential risks and trustworthiness attributes, and use cases of trust provisioning are also provided in appendices.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3052	2017-03-29	13	11.1002/1000/13252

Keywords

Trust, trust provisioning, trust index, trusted ICT infrastructure

---

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.3052

Overview of trust provisioning in information and comunication technology infrastructures and services

1 Scope

This Recommendation provides an overview of trust provisioning in information and communication technology (ICT) infrastructures and services. More specifically, this Recommendation covers the following:

- potential risks and necessity of trust;
- trusted ICT infrastructures and services;
- the concept of trust and characteristics of trust;
- a trust relationship model and trust evaluation based on the conceptual model of trust provisioning;
- trust-provisioning processes.

NOTE – Detailed potential risks are provided in Appendix I, trustworthiness attributes are described in Appendix II, and use cases of trust provisioning are provided in Appendix III.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 Trust: The measurable belief and/or confidence which represents accumulated value from history and the expecting value for the future.

NOTE – Trust is quantitatively and/or qualitatively calculated and measured. Trust is used to evaluate values of entities, value-chains among multiple stakeholders and human behaviours, including decision making.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CPS Cyber-Physical System

DIKW Data, Information, Knowledge and Wisdom

ICT Information and Communication Technology

IoT Internet of Things

5 Conventions

None.

6 Introduction

Digital technologies, information and communication technology (ICT) infrastructures and services are increasingly evolving toward a future knowledge society. ICT infrastructure not only improves the transmission speed at which users send and receive multimedia data, but also allows individual users to enjoy previously inconceivable tools that improve life and business.

The world can be divided into physical, cyber and social worlds. The physical world is composed of physical things that connect to other physical things, controlled by humans and devices. Physical things can have sensing and actuating capabilities that can gather raw data for analysis and actuate the corresponding physical things autonomously.

In the cyber world, ICT infrastructures and services provide computing, communication as well as human-to-human and human-to-machine control platforms. Big data analytics and cloud computing technologies are becoming important to drive value creation, as well as fostering new products, processes and markets. Moreover, it may be possible to invent a new ecosystem by extracting accumulated knowledge from the raw data gathered by things in the physical world.

The social world contains social entities, such as individual human beings and social organization. ICT infrastructures and services enable social entities to connect to the cyber world. With the advent of online social network services, people can share their opinions and experiences in the cyber world. On the other hand, human-centric computing technologies make it easier for humans to interact with the physical and cyber worlds by using human interfaces (i.e., using the five human senses). Moreover, the knowledge extracted by big data analytics can give wisdom to human beings [b-Chen, J.]. ICT technologies also provide convergence services for various industrial areas to offer a common service platform. ICT infrastructures and services act as the glue for integrating physical, cyber and social worlds.

6.1 Potential risks and necessity of trust

While ICT infrastructures and service have grown in size and complexity, the ICT world has risks, threats and vulnerabilities at component, device, system, service and human levels. There are many potential risks in the world as follows.

- **Risks in nature**. Any scientific progress and technology development may incur potential risks. The development of new technologies may sometimes be undesirable if 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. The new technological revolution may provide great advantages for utilizing networking resources; however, it confronts unidentified risk beforehand.
- **Risks in the physical world**. Devices and sensors have become more and more integrated into ICT infrastructures, a fact which is sometimes unrecognized by humans. Physical components are usually resource constrained and computation limited, resulting in poor implementation of security mechanisms. Thus, they are vulnerable to both external and internal attack.
- **Risks in the cyber world**. The number of vulnerabilities, threats and cyber-attacks increases in cyberspace. Cyber security and privacy mechanisms should protect both networks and services from unauthorized access. However, large-scale data collection and data analytics can pose critical privacy, security and trust issues. The risks of unanticipated uses of consumer data (such as human life and business behaviours) may increase.

- **Risks in the social world**. Social networking services have given rise to numerous online communities and people use them as communication media. Also, social networking services try to connect as many people as possible. Since many people share their private activities on social networks, their private information is propagated to others outside their community. Furthermore, artificial intelligence or the social Internet of things, which try to mimic human behaviour, also give rise to unexpected risks.

- **Risks due to the integration of the physical, cyber and social worlds**. In ICT infrastructures and services, entities in the physical, cyber and social worlds are integrated. A cyber-physical system (CPS) cannot be fully operational if the physical and cyber worlds have some mismatch. If the malfunction of a physical system is not notified to the responsible entities in the cyber world, there is some risk of deteriorating safety in the physical world. Moreover, without recognizing a set of rules and external conditions of a CPS, both humans and devices may understand or perceive CPS operations incorrectly, which may result in risks or failures of the integrated environment. Unintentional or intentional errors, as well as mismatch of the integrated environment, may be primary causes of or contributing factors to risks and accidents.

- **Risks due to data, information, knowledge and wisdom processes**. ICT infrastructures and services provide data, information, knowledge and wisdom (DIKW)[1] processes. As numerous data are generated, the number of erroneous data also increases. Malfunctions in a DIKW process, which may be caused by malicious inputs, misbehaviour of the process itself or unintended or intended manipulation, etc., create false or biased results. There are also unidentified risks due to entities that produce and utilize DIKW processes.

NOTE – Detailed potential risks are explained in Appendix I.

ICT has an important role in the increasing interconnectivity in physical, cyber and social worlds. However, the lack of trust has provoked various problems, as previously mentioned. Large-scale data acquisition from sensors and devices in the physical world imposes many issues, ranging from risks of unanticipated uses of consumer data offered by stakeholders to undesirable discrimination enabled by data analytics. If all the entities in ICT infrastructures and services are exploited for malicious intentions, irreparable damage and uncertain dangers may occur. Therefore, it is important to build a trusted ICT infrastructure to minimize unexpected risks and to maximize the survivability of physical, cyber and social worlds.

The concept of trust implies belief and confidence that the functional entities in ICT infrastructures and services will behave in expected ways. As ICT-based applications and services underpin other industrial domains and involve multiple stakeholders, trust evaluation of the corresponding value chains of business, as well as of the system and component levels, in a holistic manner can enable users to have confidence in their services and applications. Consequently, trust provisioning is one of the most important functional capabilities in ICT infrastructures and services.

6.2 Trust provisioning in ICT infrastructures and services

Trust provisioning is an integral function of physical, cyber and social trust that provides a valuable method of minimizing risks through identifying the trust characteristics of entities. Using trust provisioning, it is possible to develop trusted ICT infrastructures and services that cooperate with ICT applications in order to support these applications and services for better quality of services and experience by mitigating inherent and extraneous risks.

---

[1] This term was coined in [b-Rowley] and refers loosely to a class of models for representing purported structural 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."

Figure 1 shows the concept of trusted ICT infrastructures and services. Three types of trust provisioning are classified into: physical trust for physical things (including sensors, actuators and devices); cyber trust for communication, computing and control; and social trust for stakeholders, which are mapped with trust in the physical, cyber and social worlds, respectively. In the trusted ICT world, trust entities may assume DIKW processes to minimize potential risks and to maximize the value of assets.

NOTE – Detailed explanations of physical, cyber, and social trust are given in clause 7.3.

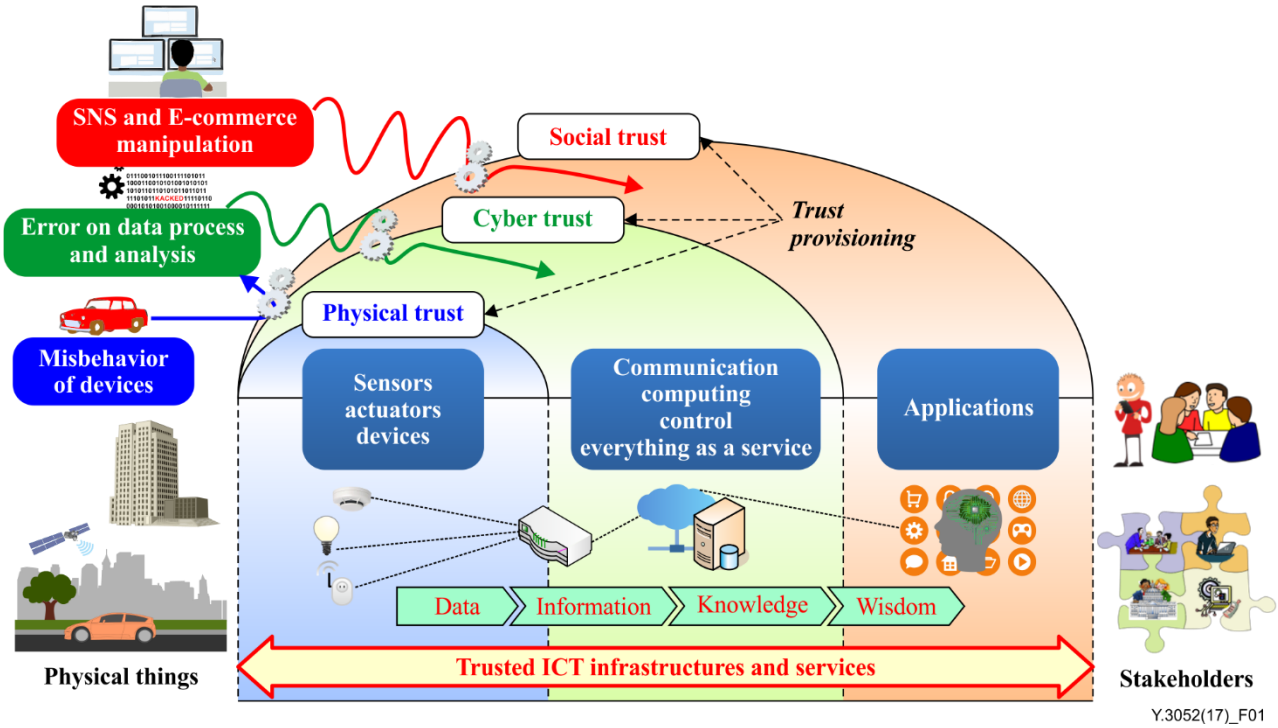

Figure 1 – The concept of trusted ICT infrastructures and services

7 Overview of trust and trust provisioning

7.1 Concept of trust

The trust concept itself is a complicated notion with different meanings depending on both participators (i.e., a trustor is one entity that trusts another entity, known as a trustee) and situations, as well as being influenced by both measurable and non-measurable factors. From a sociological point of view, trust is defined as the trusting behaviour that is impaired when one person suspects another in a situation where an ambiguous path exists. In such situation, trust is used to mitigate risks of business dealings with others. Trust is also interpreted as the capacity and belief of an entity that the other entity will meet its expectations.

The term trust in the contexts of the physical and cyber worlds differs from that of the social world. Trust in the social world can be viewed as a subjective expectation that a social entity predicts about another social entity's future behaviour. On the other hand, trust in physical and cyber worlds can be viewed as the expectation that a physical thing or a cyber object will accomplish a given task in an expected manner to fulfil its intended purpose.

In ICT environments, trust affects the preference of an entity to consume a particular service offered by another entity. It also affects the decision making process of an entity to transact with another entity. Trust evaluation is especially significant in ICT environments where a huge number of entities mutually interact with each other to provide and consume information or resources.

From the perspectives of standardization, trust should be quantitatively or qualitatively calculated and measured, and then used to evaluate values of physical components, value-chains among multiple stakeholders and human behaviours including decision making. Trust is an important factor in the decision-making process not only by humans, but also by applications and service transactions in ICT environments. Therefore, trust has been highlighted to evaluate the functional capabilities of ICT resources, as well as ICT services and applications.

When a trustor and a trustee create trust relationships, both parties have their own characteristics, so-called trust propensity and trustworthiness, respectively [b-Mayer]. Trust propensity (i.e., the characteristic of the trustor) is a trait that leads to a generalized expectation about the trustworthiness of others. Trustworthiness (i.e., the characteristic of the trustee) refers to a property that can be trusted and relied upon by the trustee.

In general, a trustor considers three main sources of information when seeking trust, namely its own understanding about a trustee (as knowledge), personal expertise about the situation and the context (as experience), and public evidence about the trustee (i.e., reputation). Knowledge can be characterized as a direct trustworthiness attribute. It is measured from the primary data that are available to the trustor at first hand even before any meaningful communication has happened. On the other hand, experience and reputation information can be demonstrated to be indirect trustworthiness attributes that are estimated basically from secondary data, often available after at least one interaction between the parties.

7.1.1 Direct trust

Figure 2 shows various trustworthiness attributes that are categorized into three major factors: ability, integrity and benevolence [b-Mayer], [b-Colquitt]. Many attributes can represent trustworthiness, which can be applied to ICT infrastructures and services.

– **Ability (or capability)**. Ability means characteristics that enable an entity to have influence in some specific contexts. The ability is specific because the trustee may be highly competent in some technical area, meaning that a person is trusted on tasks related to that specific area. The attributes related to ability include robustness, safety, stability, scalability and reliability.

– **Integrity (or honesty**). Integrity means the quality of being honest and fair in the social world or means the state of being complete in cyber and physical worlds. In terms of information, integrity means that information about an object is prevented from being modified; in other words, information shows consistency by ensuring that it will not be accidentally or maliciously altered or destroyed. The attributes related to integrity include completeness, consistency, accuracy, certainty and recency.

– **Benevolence (or cooperation)**. Benevolence means the desire to do well to others, in other words, working or acting together willingly for a common purpose or benefit when a trustor has an interaction with a trustee. Benevolence is also the extent to which a trustee is believed to do good to the trustor, aside from an egocentric profit motive. The attributes related to benevolence include availability, assurance, relevance and credibility.

NOTE – Appendix II provides detailed information about trustworthiness attributes.

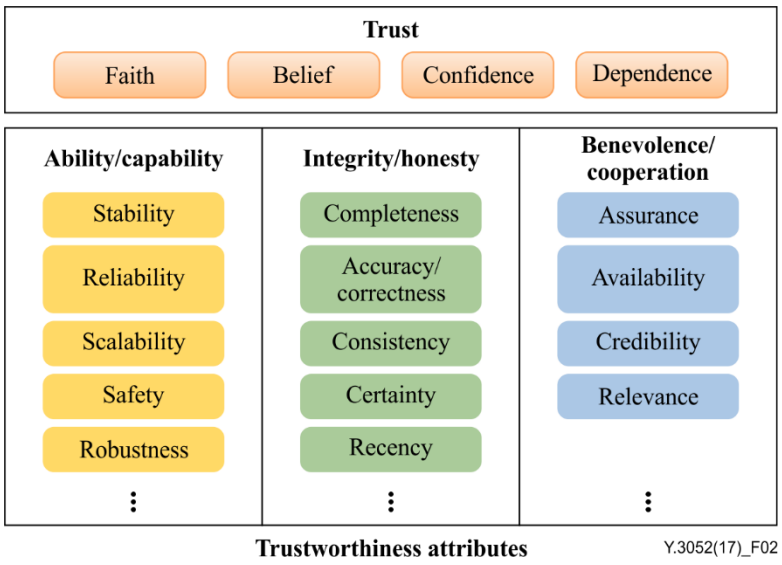

Figure 2 – Attributes related to trustworthiness

7.1.2 Indirect trust

Indirect trust is formed by self-judgement about the situation and third party reputations. Unlike direct trust, indirect trust is derived by the experience gained through previous conversations with the trustee and the reputation gained through global views of the trustee, respectively. This is particularly important in circumstances where information to estimate trustworthiness attributes is not available at first hand.

– **Experience**

  Experience represents a personal observation only about interactions between a trustor and a trustee. Experience is achieved by accumulating the state of interactions among entities over time. The left-hand side of Figure 3 illustrates how trust based on experience is formed between trustor and trustee using previous interactions between the two.

– **Reputation**

  Reputation is a public assessment of the trustor with respect to the prior behaviour of a trustee and performance. Reputation can be evaluated based on the accumulated experience of trustors about the trustee as shown in the right-hand side of Figure 3. To acquire trust information based on the reputation of a trustee, two kinds of information require examination: a) previous trust transactions from all entities to the trustee; b) the relationship between a trustor and the trustee.

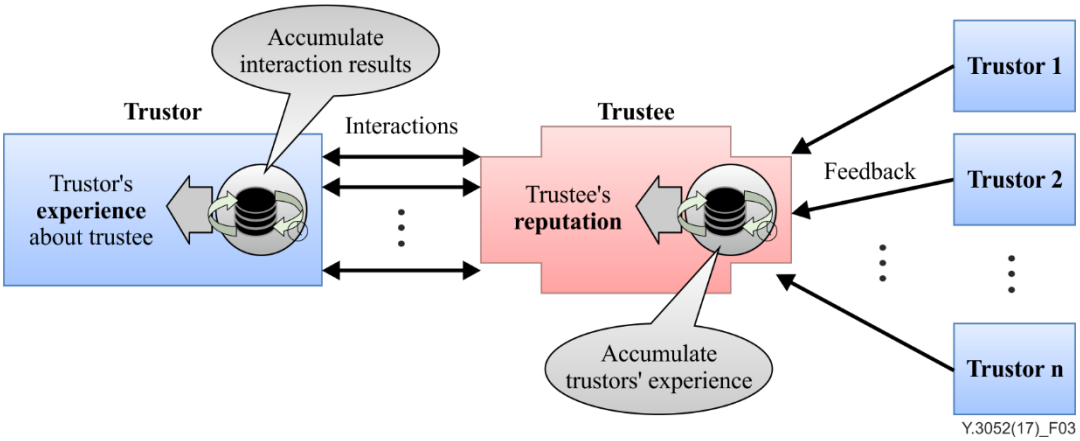

Figure 3 – Indirect trust (experience and reputation)

7.2 Fundamental characteristics of trust

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

– **Trust is dynamic**. Trust applies only in a given time period and may change as time goes on.

NOTE 1 – For the past year, Alice highly trusts Bob. However, today Alice found out that Bob has lied to her; consequently, Alice no longer trusts Bob.

– **Trust is context-dependent**. Trust applies only in a given context. The degree of trust in different contexts is significantly different.

NOTE 2 – Alice may trust Bob to provide financial, but not medical, advice. Also, the articulation of the trust context in two entities may differ based on opposing perspectives. For example, Alice trusts Bob in the context of "buying" a book; however, the context from Bob to Alice concerns "selling" a book.

– **Trust is not transitive in nature, but maybe transitive within a given context**. When entity A trusts entity B and entity B trusts entity C, entity A may or may not trust entity C. Entity A may trust any entity and entity B trusts entity C in a given context although this derived trust may be explicit and hard to quantify. Also, the duration of trusting relationships may be defined differently between the entities.

NOTE 3 – Alice has trusted Bob for 3 years; however, it is possible that Bob thinks that the trust relationship has only lasted for 1 year.

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

– **Trust is subjective**. trust is influenced by or based on personal feelings. Also, the degree of seriousness in trust relationships may differ between the entities.

NOTE 4 – Bob gives an opinion about music. If Alice thinks that Bob's music recommendation is good, she will trust Bob's review. However, it is possible that John thinks differently about Bob's opinions and may not trust his review.

7.3 Model for trust provisioning

From the perspective of trust provisioning, there are physical, cyber and social worlds. To build an ICT ecosystem, raw data from physical things in the physical world are produced by physical interfaces like sensors and actuators. In the cyber world, there are physical objects and logical objects. Physical objects are those mapping to hardware devices and equipment that have capabilities of data processing, data storage and communication, etc. Logical objects are algorithms, functions and software that work on computing, storage and networking components. In the social world, entities like humans, stakeholders and software agents, which are computer programs that act for a user, produce and consume various data and applications through user interfaces. Physical things, cyber objects and social entities interact to perform trusted ICT applications taking into consideration physical, cyber and social trust, respectively. Figure 4 shows the role of trust provisioning in the ICT world in realizing various trusted ICT applications.

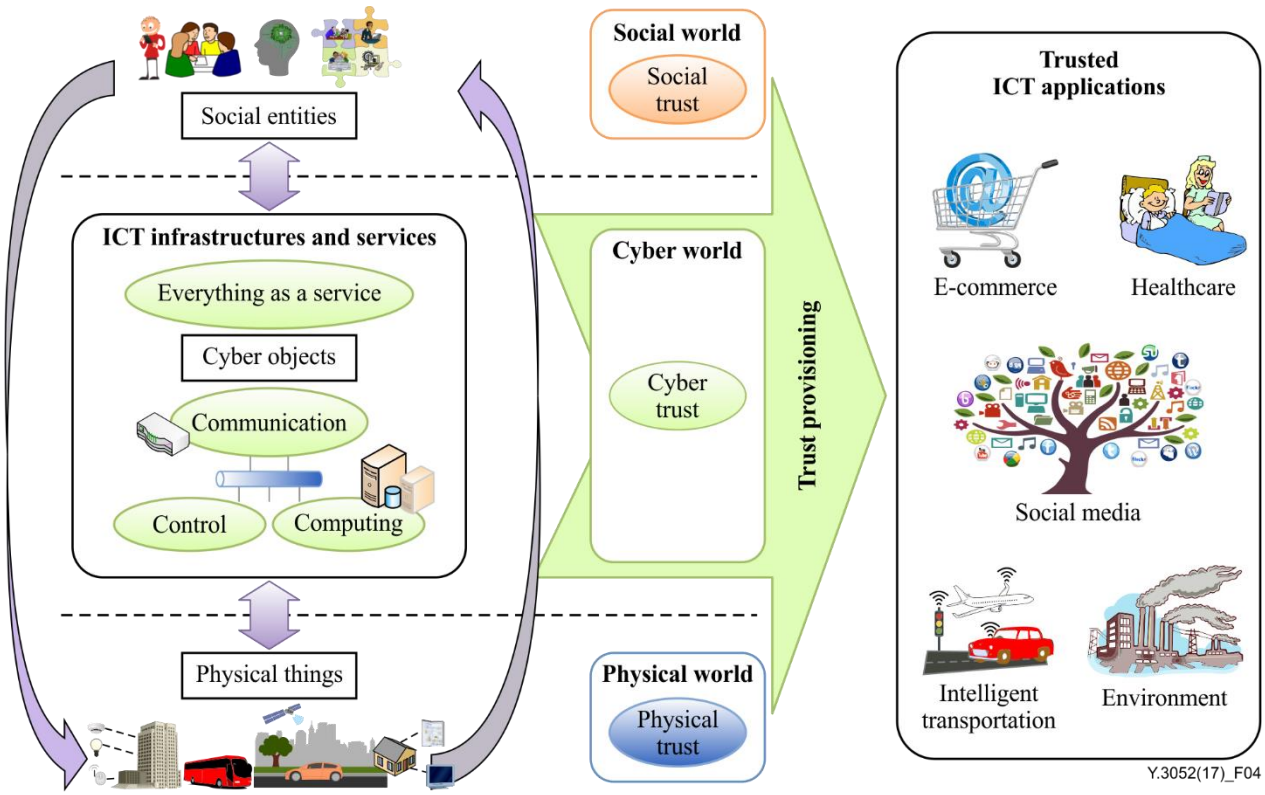

Figure 4 – Trust provisioning in the ICT world for trusted ICT applications

– **Physical trust**. Physical trust reflects various trust aspects of physical things, which can be measured by counting on theirs trustworthiness in terms of capability, integrity and cooperation. Its capability means the ability of the physical thing to perform its task with correct functionality. Its integrity means the state of the physical thing, being stable without trouble or breakdown. Its cooperation means that the physical thing works together with other physical things for their common purposes. Physical trust reflects trust propensity that is affected by risks related to the physical world.

– **Cyber trust**. Cyber trust reflects various trust aspects of cyber objects, which can be measured by counting on their trustworthiness in terms of capability, integrity and cooperation. Its capability means that the ability of a cyber object is correct and certain to execute control, computing and communication. Its integrity means that data handled or provided by cyber objects are not accidentally or maliciously altered or destroyed during control, computing and communication. Its cooperation means how well the cyber object works together with other objects. Cyber trust reflects trust propensity that is affected by risks related to the cyber world.

– **Social trust**. Social trust reflects various trust aspects of social entities. Social trust can be measured by considering its trustworthiness in terms of ability, honesty and benevolence. Its ability means human competence in the individual's activity. Its honesty implies that the social entity treats others honestly. Its benevolence means how nicely the social entity behaves to other social entities or how much the social entity interacts with other entities for their kindness. Social trust reflects trust propensity that is affected by risks in the social world.

In a trust relationship model, cyber and virtual objects are linked with physical things and social entities as shown in Figure 5. A virtual physical object is the virtualized model of a physical thing through physical interfaces, such as sensors and actuators. Cyber objects are modelled as physical and logical objects. Physical objects are models of hardware devices and equipment and logical objects are models of the corresponding software. A virtual social object is the virtual model of a social entity derived through applications and user interfaces. Virtual physical objects, cyber objects

and virtual social objects can be seen as trust components for physical trust, cyber trust and social trust, respectively.

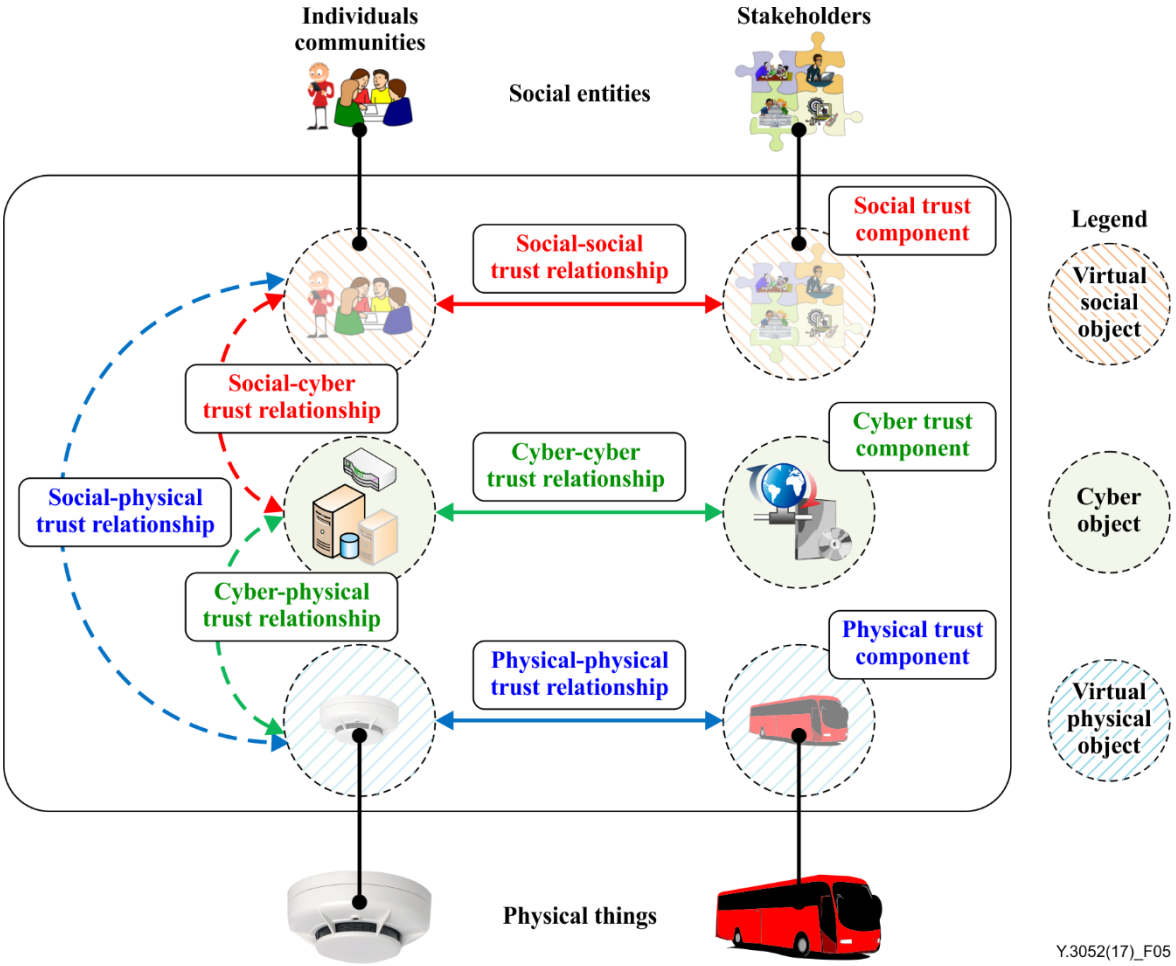

Figure 5 – Trust relationship model

Based on the model of physical, cyber and social trust components, in ICT infrastructures and services horizontally, there are various trust relationships: social-social; cyber-cyber; and physical-physical. Trust relationships between trust components are also established vertically among different types of trust components, and are of the types: social-cyber; cyber-physical; and social-physical. When one trust component establishes trust relationships with others, that component receives trust information from others.

7.4 Trust evaluation for trust provisioning

To compare the degree of trust between different entities, a method is needed to measure, quantify and assess trust. From input data of various sources, trust evaluation is the way of calculating trust for target services or objects. Three types of trust information are defined as follows.

– **Trust attribute**. Trust attributes represent characteristics of an entity (including direct and indirect trust) and are of qualitative and quantitative types. Trust attributes refer to properties and features of an entity that can be trusted. Qualitative attributes need a quantization process to accumulate quantitative attributes.

– **Trust indicator**. Trust indicators are used to calculate a trust index by combining qualitative and quantitative attributes of trust. Objective trust indicators stand for features that represent trustworthiness of an entity quantitatively. Subjective trust indicators reflect subjective or personal attributes of trust entities. Trust indicators are calculated as the measurement instance of their trustworthiness, since their values change as time goes on.

– **Trust index**. A trust index is a composite and relative value that combines multiple trust indicators into one benchmark measure for representing the trustworthiness of an entity, which is similar to an ICT development index or stock market index. A trust index is a comprehensive accumulation of the objective trust indicators and the subjective trust indicators that are objectified for calculation. A trust index evaluates and quantifies the trustworthiness of a trustee.

For a trust evaluation as shown in Figure 6, data require collection from various sources. Collected data are categorized into two trust attribute types, namely, qualitative and quantitative. Trust attributes are self-accumulated from inputs of various sources. Trust attributes are used to calculate trust indicators. Trust indicators also have self-accumulated properties from subjective or objectives attributes. Note that the time-varying behaviour of trust indicators also becomes apparent by accumulation of every new instance. A trust index is calculated in a self-accumulated manner by combination of objective and subjective trust indicators. The trustor finally makes a decision with a certain trust value. A trust value represents a numerical quantity that determines an entity's trust in a trustor's perspective. Based on the trust indicators and trust index of the entity, the trustor obtains a trust value of the entity on which to make a decision.

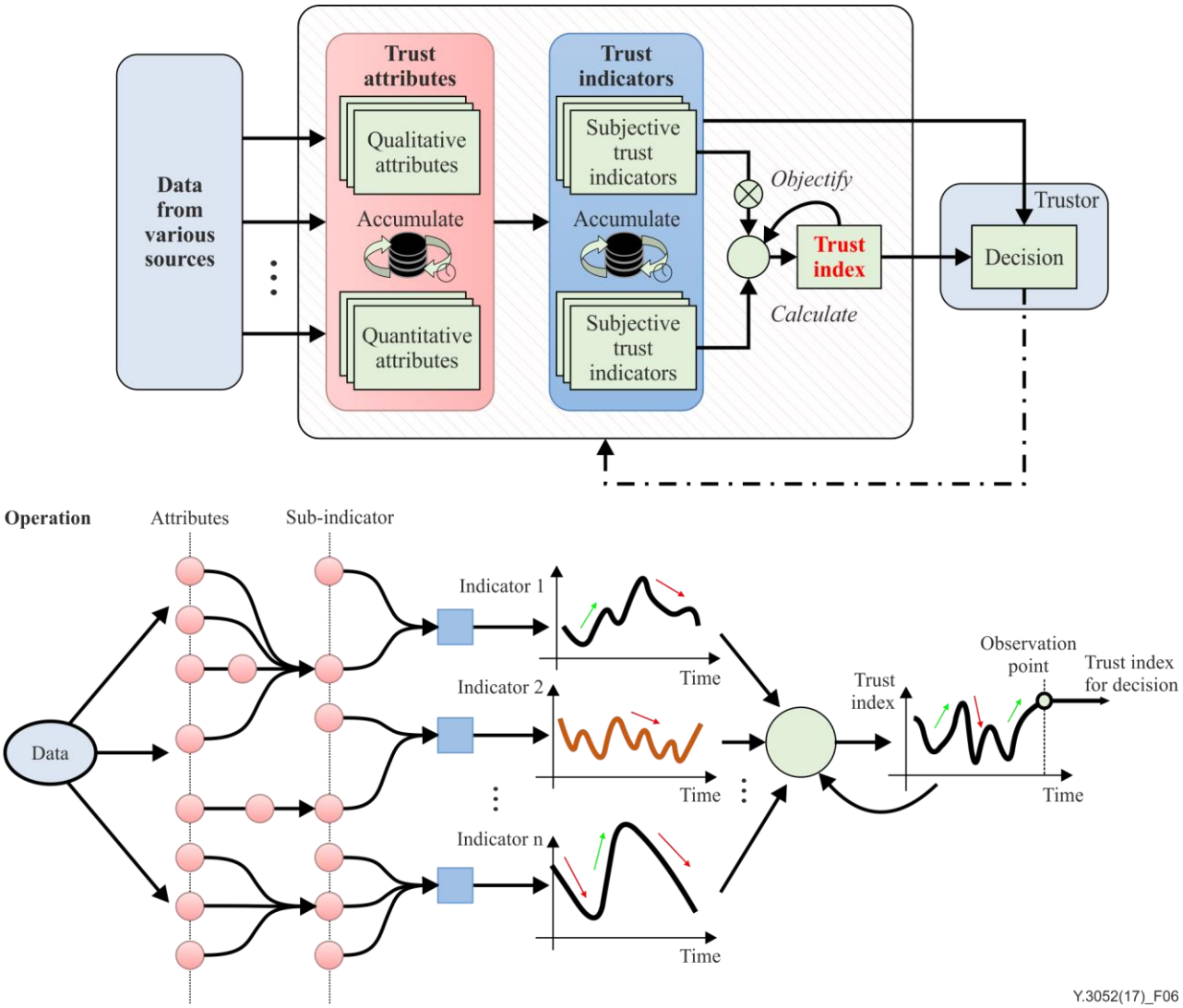

Figure 6 − Trust evaluation for trust provisioning

8 Trust-provisioning processes

Trust provisioning in ICT infrastructures and services consists of a set of processes that include gathering data from entities, producing and distributing trust information by evaluating all aspects of trust to support the decision making of entities when establishing trust relationships with other entities. This clause describes trust-provisioning processes as follows: i) data collection; ii) data management; iii) trust information analysis; iv) dissemination of trust information; and v) trust information lifecycle management.

8.1 Data collection

The data collection process gathers raw data on trust information. Data collection should focus on which and how many data should be collected. Data collection is closely related to the purpose of trust provisioning. Data should be collected at acceptable expense to extract relevant trust information, because excessive data collection may cause privacy problems.

8.2 Data management

In this process, collected data are used to generate trust information. Data are carefully handled with respect to trustworthiness. As the number of data sources and types have dramatically increased, the trustworthiness of data itself is significant. Because false data will lead to degradation of the accuracy of trust information and increase waste of resources, it is important to detect corrupt or polluted data. From the perspective of data management, data should be protected to extract the correct trust information.

8.3 Trust information analysis

The trust information analysis process extracts meaningful trust information from data. Because trust can be measured by consideration of the complicated relationship between the trustor and the trustee, trust information explicitly reflects the trust relationship, both objectively and subjectively.

As ICT environments continue to emerge, building trust is becoming much more challenging. Since trust is difficult to quantify, the exact trustworthiness value of an entity can have different interpretations. Trust attributes should be defined as mutually independent characteristics of entities and may reflect the dynamic characteristics of trust.

A trust model is a method of specifying, building, evaluating and ensuring trust relationships among entities. The trust model is used to obtain trust information and is designed to understand trust characteristics and account for trust factors. Since a trust model is domain-specific, there exist numerous ways to define a trust model according to application domains. In order to calculate a trust index for specific applications, common indicators should be developed to identify trust characteristics of an entity and to compare them with trust indices of different entities.

8.4 Dissemination of trust information

Dissemination of trust information is a way of distributing trust information to others. There are various ways of disseminating trust information in different domains (e.g., binary data transmission in the physical world, service or product recommendations in the cyber world, and information visualization taking into consideration human perceptions in the social world). Efficient, effective and appropriate dissemination methods should be developed so that a trustor can determine the trust of the trustee according to subjective criteria of trust information.

8.5 Trust information lifecycle management

Because of the dynamic characteristics of trust, trust information is created, updated and destroyed as time goes on. Trust information is replaced due to changes in a trust component. Feedback from a trustor who receives trust information about a trustee can also be used to recalculate trust values

during the update phase. During the update phase, the trust index is updated and trust value is re-evaluated.

NOTE – Appendix III provides trust provisioning use cases.

9 Security considerations

Trust is a concept that can cover security and privacy. Security is considered to be the technological aspects, while privacy is considered to be the user aspects. By utilizing security and privacy mechanisms, trust can be realized in ICT infrastructures and services.

Appendix I

Detailed potential risks in ICT infrastructures and services

(This appendix does not form an integral part of this Recommendation.)

This appendix provides details of potential risks in ICT infrastructures and services with respect to physical, cyber and social worlds.

I.1 Risks in the physical world

a) **Natural threats** [b-Brauch]

Natural threats, e.g., earthquakes, hurricanes, floods and fire, can cause severe damage to physical components and computer systems. It is hard to predict and prevent natural disasters in advance, and few safeguards can be implemented against them.

b) **Physical threats**

Outbreaks caused by physical threats can interfere with hardware components and device protocols, e.g., insertion of positive reputation and recommendation values into a untrustworthy device, installing and booting fraudulent or modified software, and environmental or side-channel manipulation, both before and after deployment of a device.

Trust and privacy are also issues in the physical world due to the broadcast nature of communication media. Confidential information communication is vulnerable over a network in the presence of eavesdroppers who can intercept the information exchange between legitimate terminals and disrupt the desired behaviour of legitimate users and devices.

In addition, inadequate and unreliable information or physically unstable devices themselves can give rise to potential risks in the proper behaviour of a system. Furthermore, due to interdependencies, the system structure (e.g., cascade or parallel) and compatibility issues among systems can do more harm than anticipated.

I.2 Risks in the cyber world

a) **Cyber or information security threats** [b-Wilson]

1) Threats on the core network, e.g., delivery of fake trust information, impersonation of devices, traffic tunnelling between impersonated devices and misconfiguration of the firewall in network equipment, can result in several kinds of hazard.
2) Configuration vulnerabilities, e.g., fraudulent software update or configuration changes, misconfiguration by software agents, subscribers, users or the owner, and misconfiguration or compromise of access control lists, can occur.
3) Compromise of credentials comprising brute force attacks on authentication tokens and algorithms, physical intrusion or side-channel attacks and malicious cloning of authentication tokens, are also risks.
4) User data and identity privacy attacks, including eavesdropping on other user or device data sent over the system; masquerading as another user or subscriber device; user network identifier or other confidential data revealed to unauthorized third parties, present threats.
5) Access vulnerabilities, resulting in unauthorized persons gaining access to networks or devices to which they have no right, are of two different types: the first is physical access, whereby the intruder can gain access to a physical device; the second is remote access, where access is gained to Internet-connected devices.

b) **Privacy threats** [b-Weber]

Privacy protection, especially in Internet of things (IoT) environments, has become increasingly challenging due to large volumes of information easily available through remote access mechanisms.

1) **Lack of control and information asymmetry**: interaction between objects that communicate automatically and by default, between objects and individuals' devices, between individuals and other objects, and between objects and back-end systems, will result in the generation of data flows that are difficult to manage by the traditional tools used to ensure adequate protection of data subjects' interests and rights.
2) **Quality of the user's consent**: the possibility of rejecting certain services is not a real alternative in IoT environments and classic mechanisms used to obtain consent are scarcely applicable. Therefore, new ways of obtaining the valid consent of a user should be considered, including implementing consent mechanisms through the devices themselves as privacy proxies and "sticky" policies (conditions and constraints attached to data that describe how it should be treated).
3) **Inferences derived from data and repurposing of original processing**: secondary uses of data, inferences from raw information and sensor fusion, require that at each level IoT stakeholders ensure that the data are used for purposes that are compatible with the original processing purposes and that those purposes are known by the user.
4) **Intrusive identification of behaviour patterns and profiling**: generating knowledge from trivial or even anonymous data will be made easy by the proliferation of sensors and that might enable very detailed and comprehensive life and behaviour patterns.
5) **Security risks**: weak points can occur not only at the device level, but also in communication links, storage infrastructure and other inputs of this ecosystem.

c) **Cyber-crime**

The Internet and smart objects are used to exploit users and data for material gain, such as intellectual property theft (violation of patent, trade secret or copyright laws), identity theft, brand theft and fraud. In addition, cybercrime also includes attacks against computers to deliberately disrupt processing or may include espionage to make unauthorized copies of classified data.

Botnets are becoming a major tool for cybercrime, partly because they can be designed to very effectively disrupt targeted computer systems in different ways, and because a malicious user, without possessing strong technical skills, can initiate these disruptive effects in cyberspace by simply renting botnet services from a cybercriminal.

Malicious codes, such as computer viruses, are used to infect a computer to make it available for takeover and remote control. Malicious code can infect a computer when the user opens an email attachment or clicks an innocent-looking link on a website.

I.3 Risks in the social world

a) **Risk of lacking trust in interactions**

1) **Human-to-human interactions**: If there is no trust among people, their interactions (e.g., exchanging data and information) become meaningless due to lack of confidence in each other. If people are not trustworthy, personal interactions do not invoke any response. Unclear decision making or unrealistic situations can occur due to low or impaired trust in human relationships.
2) **Human-to-machine interactions**: When a human cannot trust a machine (e.g., resulting from imprecise data delivery from a machine to a human), human-to-machine interactions cannot be established and potential benefits to system performance are lost. Human-machine systems have always proved unpredictable and fallible, whereas the

nature of the system is to function normally. It relies on technology, which accentuates risks.

b) **Threats in the social world** [b-Chen, I.-R.]

A malicious entity is dishonest and socially uncooperative in nature and can break the basic functionality of ICT infrastructures and services. The entity can perform the following attacks.

1) **Self-promoting attacks**: a malicious user can intentionally promote its importance (by providing good recommendations for itself) in order to be selected as service provider, but then delivers malfunctioning service.
2) **Whitewashing attacks**: a malicious entity can disappear and rejoin the application to wash away its bad reputation.
3) **Discriminatory attacks**: a malicious entity can discriminatively attack non-friends or entities without strong social ties (i.e., without many friends in common) because of human nature or propensity towards friends in social networks.
4) **Bad-mouthing attacks**: a malicious entity can ruin the reputation of another well-behaved entity by providing bad recommendations so as to decrease the chance of this good entity being selected as a service provider. This is a form of collusion attack, i.e., it can collaborate with other bad entities to ruin the reputation of a good entity.
5) **Ballot-stuffing attacks**: a malicious entity can boost the reputation of another bad entity by providing good recommendations for it so as to increase the chance of this bad entity being selected as a service provider. This is also a form of collusion attack, i.e., it can collaborate with other bad entities to mutually boost reputations.

c) **Threats in social networks**

Social networking tools have changed the way people interact in their personal lives and business. Increasingly, these tools play a significant role in how business gets done; however, they also have risks as follows.

1) **Phishing bait**: Many users of social networking services have had their accounts compromised. Although numbers represent only a tiny fraction of a percentage point, they are still significant, considering that widespread social networking services have several million users. To their credit, social networking services have acted quickly, working to blacklist guilty domains, but many copycat efforts have ensued.
2) **Data leaks**: Social networks are all about sharing. Unfortunately, many users share too much sensitive information about their organizations, e.g., projects, products, financial data, organizational changes or scandals.
3) **Botnets**: Recently, the accounts of a social networking service have been used as the command and control channel for a few botnets. The service concerned is shutting these accounts down, given the ease of access to infected machines via the social networking service.
4) **Advanced persistent threats**: One of the key elements of advanced persistent threats is the gathering of intelligence of persons of interest, for which social networks are a data source. Perpetrators use this information to further their threats by placing more intelligence gathering (e.g., malware, Trojans), and then gaining access to sensitive systems.
5) **Cross-site request forgery**: This attacks exploit the trust that a social networking application has in a logged-in user's browser. Consequently, as long as the social network application does not check the referrer header, it is easy for an attack to share an image in a user's event stream that other users might click on to catch and spread the attacks.

6) **Impersonation**: The social network accounts of several prominent individuals with thousands of followers have been hacked. Furthermore, several impersonators have gathered hundreds and thousands of followers.

I.4 Risks arising from the integration of physical, cyber and social worlds

a) A large number of ICT resources

Risks threaten ICT infrastructures and services when they try to cope with the complexity of the interactions and mechanisms of the entities. Access to ICT infrastructures and services by a large number of ICT resources causes irreparable damage and creates unpredictable dangers. It is essential to make trustworthy ICT resources accessible to all people, but there are unknown dangers.

b) Complexity of network operation

There are many algorithms for network resource optimization, including efficient routing, congestion avoidance, and guaranteeing quality of service and quality of experience. When unpredictable situations occur in a network, the possibility of the network going out of service increases. Intentional attacks from outside (e.g., distributed denial-of-service attacks) are also among the risks. While network control functions can arrange bypass or detour routes to cope with overflow traffic, unexpected side effects, e.g., traffic fluctuation and domino effects, can bring additional risks. To increase network survivability during network operation, networking protocols and operations, administrations, maintenance and provisioning functions should be redesigned to be trustworthy. Moreover, when a network infrastructure includes a cloud platform with a large volume of storage and processing capabilities, network instability does not comes from traffic congestion alone. The operation of a cloud platform and high-level applications are additional harmful sources that increase network risks. The existing security functions, including firewall and deep packet inspection, could be replaced to provide a certain level of trust through the implementation of a trust gateway system and trust-guaranteed network operation, administration and maintenance functions.

Appendix II

Trustworthiness attributes

(This appendix does not form an integral part of this Recommendation.)

This appendix provides some descriptions about trustworthiness attributes. Table II.1 lists general descriptions of trustworthiness attributes that are introduced in clause 7.1.1.

Table II.1 – Trustworthiness attributes

Trust-worthiness	Attributes	Description
Ability/ capability	Stability	The quality or state of something that is not easily changed or likely to change at any time.
		Stability means that a physical thing performs its own operation consistently. That is, with a given input, the physical thing always gives the same output. Users may consider cyber objects to be stable if they perform communication, control and computing functions that work continuously. In other words, stability might imply that a stakeholder continuously performs its role.
	Reliability	The ability of an entity to perform a required function sufficiently under any conditions.
		Reliability means that a physical thing works properly by following user requests under any conditions. The reliability of a cyber object might imply that the cyber object fulfils the required quality of service. The reliability can be measured as the probability that an entity correctly performs a required job in a specified period of time under stated conditions.
	Scalability	The ability of something to adapt to increased demands. The capability of a system or process to handle a growing amount of work or its potential to be enlarged in order to accommodate that growth.
		Cyber-physical systems that can manage numerous sensors and their measured data might be judged scalable. Cyber objects that can process huge numbers of queries and requests might also be considered as scalable.
	Safety	The ability to protect the entity from existing risk and danger; the ability to take care of itself and not be a danger to itself. The ability to operate without risk of injury or harm to users and the system environment.
		A service that adopts a cyber security system might be thought safe from existing internal and external cyber-attack. On the other hand, the device itself might be safe when the device satisfies relevant safety certification.
	Robustness	Strong and effective in all or most situations and conditions. The ability of a system to cope with errors during execution and erroneous input. The capability of the service to behave in an acceptable way in anomalous or unexpected situations or when the context changes.
		Users might consider a system with backup to be process and fault tolerant robust. For example, a communication system might be established with robustness by installing duplicate paths to each destination. The robustness might also take into consideration the financial status of the stakeholder, because it explains whether the stakeholder has an ability to endure a financial crisis.

Table II.1 – Trustworthiness attributes

Trust-worthiness	Attributes	Description
Integrity/ honesty	Accuracy/ correctness	The condition or quality of being true, correct or exact. Freedom from error or defect. Set or make true, accurate, or right. Remove the errors or faults.
		Accuracy means the degree of difference between the true and measured value. This trust attribute does not imply the ability to measure the environment correctly or the ability to correct the error, but implies the willingness to measure the truth. A physical thing with appropriate sensors and a cyber object not infected by any viruses might have accuracy and thus be able to exchange correct data.
	Consistency	Steadfast adherence to the same principles, course, form, etc.
		Data consistency refers to the usability of data. Data must be consistent within the confines of many different transaction streams from one or more applications. Once a person makes a decision, takes a stand, or performs an action, he or she strives to make all future behaviour match this past behaviour.
	Certainty	Free from doubt or reservation or satisfaction of someone's expectation.
		Certainty means that the entity works exactly following someone's expectation. It is possible to consider the entity has certainty when a physical thing and a cyber object perform their own function without any exception.
	Recency	Reducing the duration left from the revision of the data.
		Trust is dynamic, so the measurement of data needs to be conducted as soon as possible for the accuracy of the data.
Benevolence/ cooperation	Assurance	A positive declaration intended to give confidence. It also means promise, pledge; guarantee or surety.
		The degree of confidence that the process or deliverable meets defined characteristics or objectives. That is, assurance implies the guaranteed value of how much the trustee can cooperate with the trustor.
	Credibility	The quality of being believable or worthy of trust.
		Credibility indicates the degree to which the trustor believes that trustee will participate in the collaboration. A trustee might provide an assurance to the trustor to guarantee the degree of participation in the cooperation; however, the trustor might determine the trust of the trustee by analysing not only the assurance, but also credibility. Credibility of information, which is observed to be conflicting, incomplete, etc., might be measured based on the level of uncertainty. Credibility in social media might be measured by statistical methods.
	Relevance	The degree connected with the matter in hand; the relation between the trustor and the trustee.
		Relevance of entities might be measured by similarity, e.g., the number of interactions among entities, etc. Similarity represents how many common criteria, attributes or behaviour patterns exist between entities.
	Availability	The ability of the system to be in a state to perform adequately at a given instant of time within a given time interval.
		Availability might be measured with the amount of capacity of the trustee to cooperate or help the trustor. The limit of the cooperation or benevolence might be restricted by the availability of the trustee.
	Cooperation	Working or acting together willingly for a common purpose or benefit.
		The number of interactions between entities that have been held in a positive manner. For example, in communication networks, packet dropping or

Table II.1 – Trustworthiness attributes

Trust-worthiness	Attributes	Description
		forwarding behaviour is used to estimate cooperative behaviour of a node. In information networks, whether sharing information would reflect an aspect of cooperative behaviours. In social networks, prompt or frequent email replies can be regarded as cooperative behaviour.

Appendix III

Trust provisioning use cases

(This appendix does not form an integral part of this Recommendation.)

This appendix provides trust provisioning use cases in ICT infrastructures and services. In this appendix, five use cases are introduced: peer-to-peer accommodation, smart office sharing, document-sharing service, intermediate device selection for device-to-device environment, and used car sharing service. Each use case describes following items:

- description: describes the background to each case including high-level description and illustration;
- actors: those who play a role in each use case;
- service flow: describes a detailed service flow for each use case.

III.1 Trustworthy peer-to-peer accommodation service

III.1.1 Description

This use case is a scenario in which a peer-to-peer accommodation service provider connects hosts (vendors of rooms or accommodation) and travellers. Hosts make their rooms available through the service provider, and travellers choose rooms based on price, grade of facilities, review scores, etc. When a traveller chooses a room, a host decides whether to accept the traveller. During this transaction, there are three trust entities: i) trust of the accommodation; ii) trust of the host; and iii) trust of the traveller. A trust information provider collects data that can be utilized to calculate a trust index that is provided to all entities. Figure III.1 is a high-level illustration of a peer-to-peer accommodation scenario. This use case example illustrates how trust information (including a trust index) is applied to a service provider, users (host and traveller) and accommodation facilities by showing how a trust index for each actor is accumulated and managed during a transaction.

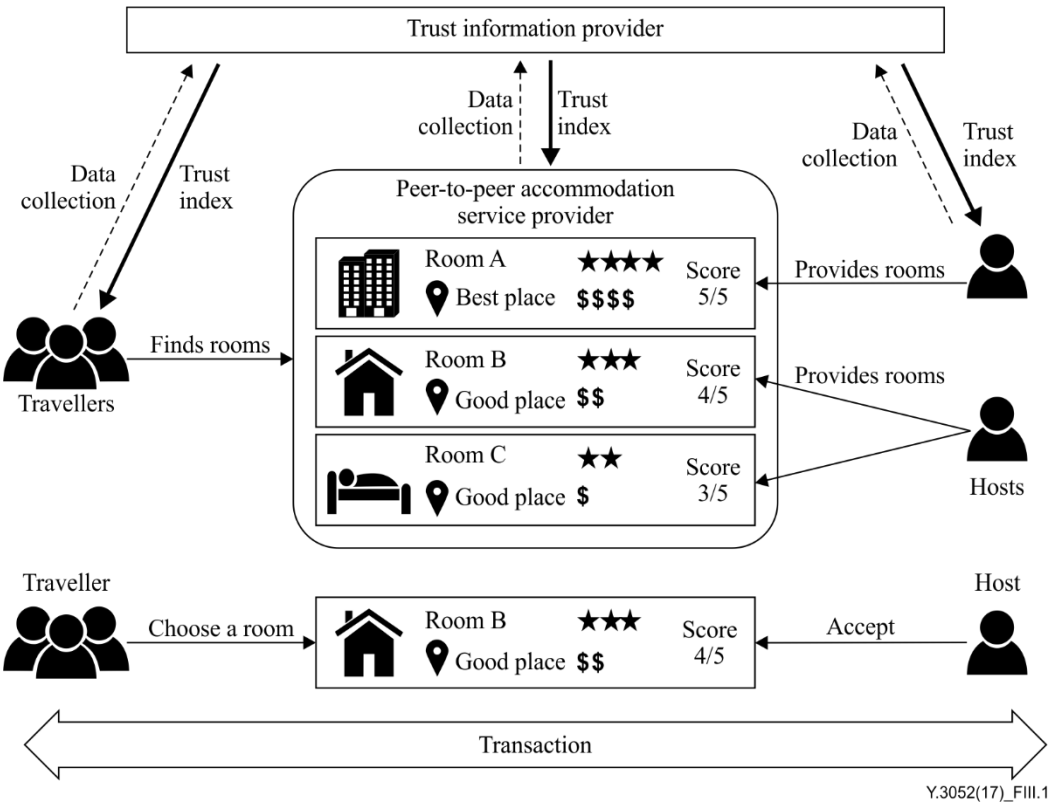

Figure III.1 – High-level illustration for a peer-to-peer accommodation scenario

III.1.2 Actors

This use case involves interactions among the following entities.

– Host: provides available accommodation.

– Traveller: uses accommodation from host.

– Accommodation: facilities provided by host.

– Peer-to-peer accommodation service provider: provides services that connect hosts and travellers for their transactions.

– Trust information provider: provides trust index for each entity based on collected information.

III.1.3 Service flow

Detailed flow description (see Figure III.2).

1) A host registers his/her available accommodation on the service provider (the service provider checks the host's trust index).

2) A traveller finds accommodation through the service provider and chooses one for reservation based on the accommodation trust index (the traveller checks the accommodation trust index, and the host checks the traveller trust index).

3) The host receives the traveller's reservation request and accepts it based on the traveller trust index.

4) The traveller stays in the accommodation for the duration of the reservation. During this period, resource usage is recorded by the host for further evaluation.

5) After the traveller checks out, both the host and the traveller review the experience. Review results are transferred to the trust information provider to adjust the actors' trust index.

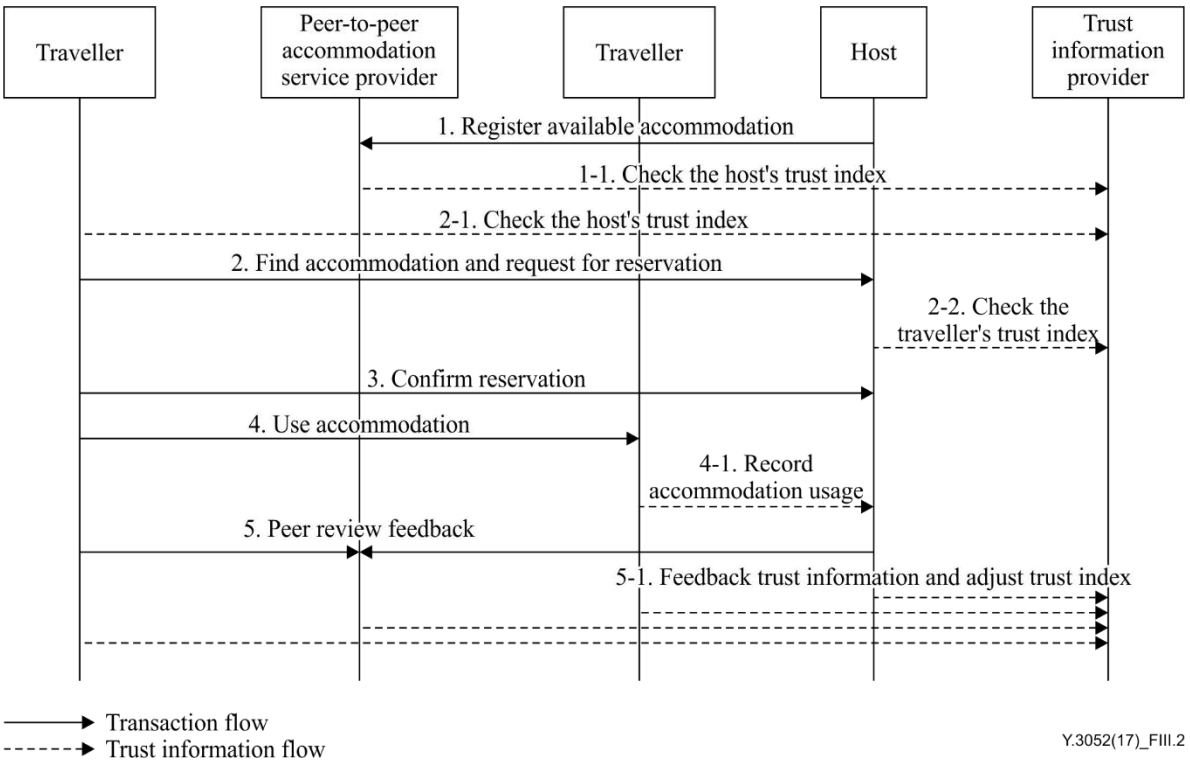

Figure III.2 – Peer-to-peer accommodation service flow

III.2 Smart office sharing

III.2.1 Description

In a trust-based smart office service, usage rights to various office facilities depend on each users' trust level, which is derived from the trust index of each user. For example, it is assumed there are two kinds of user trust level (high and low) with a certain trust index threshold. For a user who has a high level of trust, he/she can read off and write to cloud storage. However, a user who has a middle level of trust can only read documents in cloud storage. A user who has low level of trust has no right to access. Figure III.3 is a high-level illustration of a smart office service with different priorities of users and different permissions to office facilities. For the trust information provider, various properties like social or business relationship and membership can be considered to analyse the user trust level.

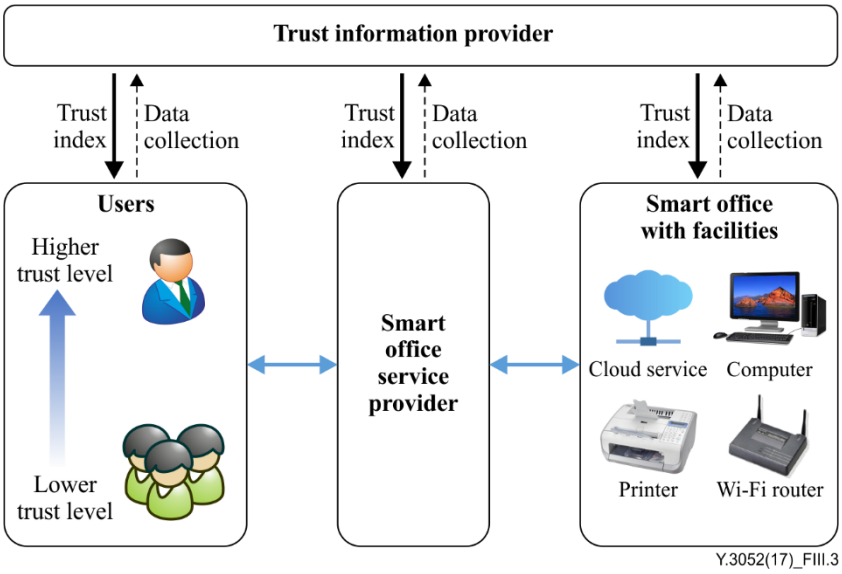

Figure III.3 – High-level illustration for smart office service

III.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 or employee).

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

– Smart office provider: in charge of providing common functionalities for smart office services. It collects the status of smart office devices and facilities. Based on the user trust level provided by the trust management service, it assigns appropriate usage rights to users (e.g., building management service provider and service providers).

– Trust information provider: provides responses about trust indexes and information requests from smart office providers or service brokers.

III.2.3 Service flow

Detailed flow description (see Figure III.4).

1) Users request to use office facilities.

2) Office facilities request the validation of users and user trust information.

3) Facility management requests user information including trust index.

4) A trust information provider evaluates the user trust index after analysing user data gathered.

5) Based on the user trust index, facility management decides the user trust level and the usage rights on each facility and function for a user.

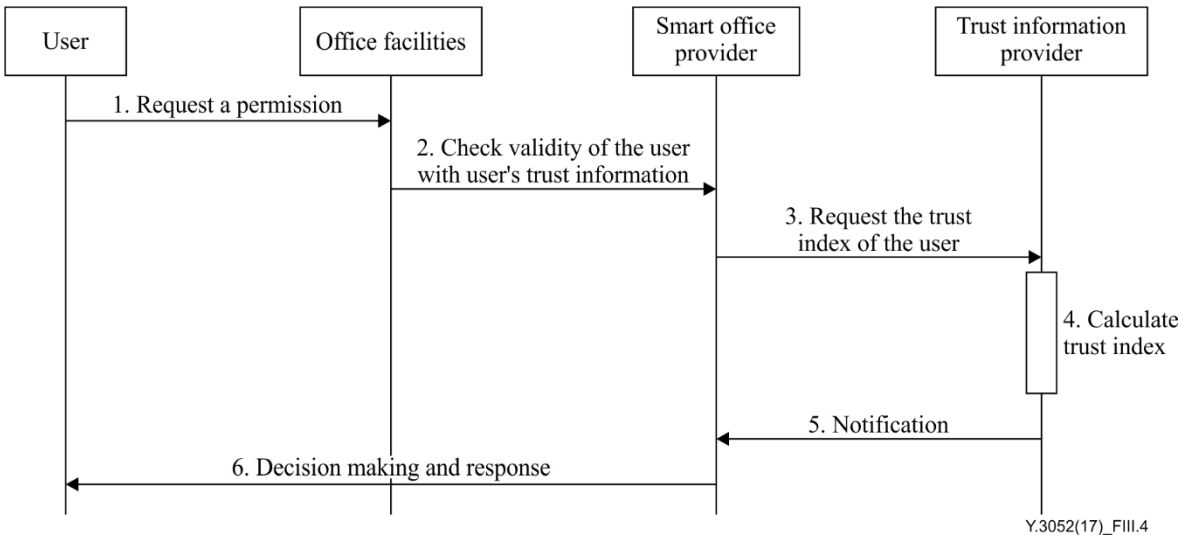

Figure III.4 – Smart office service flow

III.3 Document-sharing service

III.3.1 Description

This use case considers a social IoT environment with no centralized trusted authority. In the social IoT, each device has a subjective value based on the owner's social relationship as well as the community of interest [b-Bao] of each device. This use case focuses on using the social trust when sharing a document between co-workers. Without the social IoT trust, a document owner takes the document from his/her own storage, sends the document to the receiver and notifies a guest account to the receiver. However, the document owner does not need to do anything with the social IoT trust. A trust management platform calculates a trust value using the collected social data from an intermediate entity (e.g., a smartphone) of co-workers and this trust value is then used to judge whether a receiver has enough authorization to get the document. Figure III.5 is a high-level illustration of a document-sharing service.

III.3.2 Actors

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

– Smartphone: a device that is an intermediate entity and is available to send social relationship information and community of interest information of its owner to the wireless portable hard drive.

– Trust information provider: mainly in charge of collecting the social relationship and calculating the trust index.

– Wireless portable hard drive: a device that is mainly in charge of judging authorization to share the document.

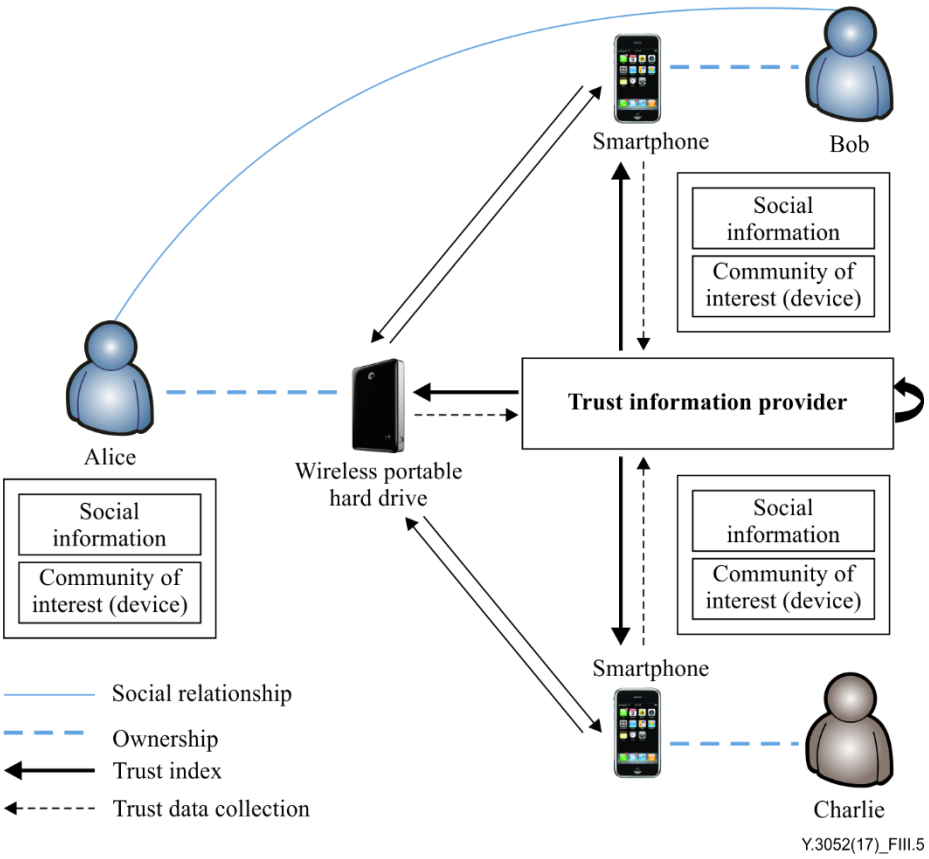

Figure III.5 – High-level illustration for document-sharing service

III.3.3 Service flow

Detailed flow description (see Figure III.6).

1) User B requests a document from user A's wireless portable hard drive by using B's own smartphone.
2) User B's smartphone as a gateway sends user B's social information community of interest value to the trust information provider.
3) From user A's perspective, the trust information provider calculates a trust index of user B by using information supplied by users A and B.
4) The trust information provider notifies the trust index to the wireless portable hard drive. It then judges whether user B has enough authorization to get the document.
5) If the trust index exceeds the threshold value,
   - 5-1) the hard drive sends the document to user B's smartphone.
   - 5-2) the smartphone notifies the result to user B.
6) If the trust index is lower than the threshold value,
   - 6-1) the hard drive notifies that the request was denied.
   - 6-1) the smartphone notifies the result to user B.

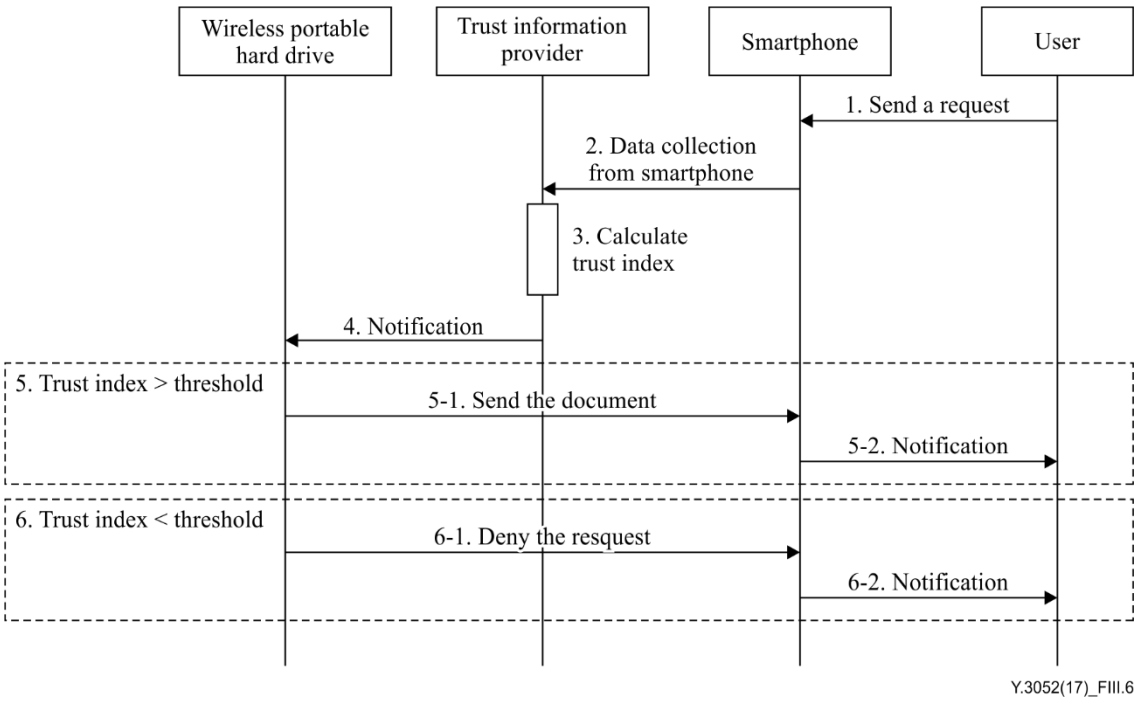

Figure III.6 – Document-sharing service flow

III.4 Intermediate device selection in device-to-device environment

III.4.1 Description

This use case focuses on using social trust when selecting a device for data transmission in a multi-hop device-to-device environment. Reliable transmission is possible by using social information in the process of device-to-device communication. The trust information provider calculates the trust index by using the collected social data from intermediate entities (e.g., a smartphone) of users and this trust index is then used to judge whether that device has enough authorization to send information. The social IoT trust can also be used in the device selection process for the reliable exchange of information. Figure III.7 is a high-level illustration for an intermediate device selection scenario in a device-to-device environment.

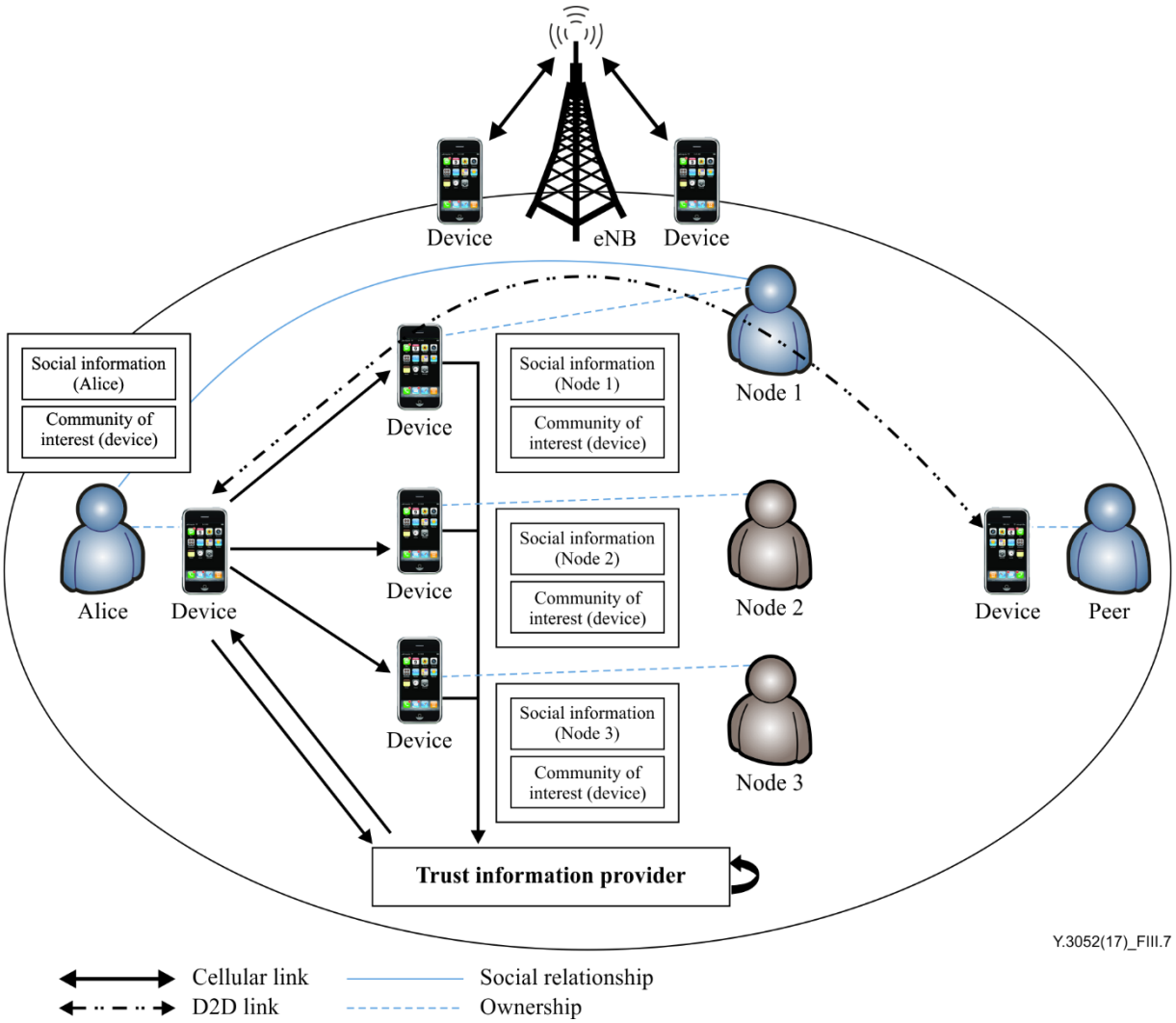

Figure III.7 – High-level illustration for intermediate device selection

III.4.2 Actors

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

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

– Trust information provider: this is mainly in charge of collecting social information and calculating the trust index.

III.4.3 Service flow

Detailed flow description (see Figure III.8).

1) A user wants to exchange information with another peer in a multi-hop device-to-device environment.

2) The user's smartphone requests the social information of other devices (e.g., node 1 and node 2) and its community of interest value.

3) The trust information provider collects relevant information from other devices.

4) The trust information provider then calculates trust indices of the devices.

5) The trust information provider notifies the trust index to the user's smartphone. After that, it judges which nodes have enough authorization to send information.

6) If node 1's trust index is the highest value, the user's smartphone decides that node 1 has enough authorization to send information and select the transmission path with node 1. It then starts to send information.

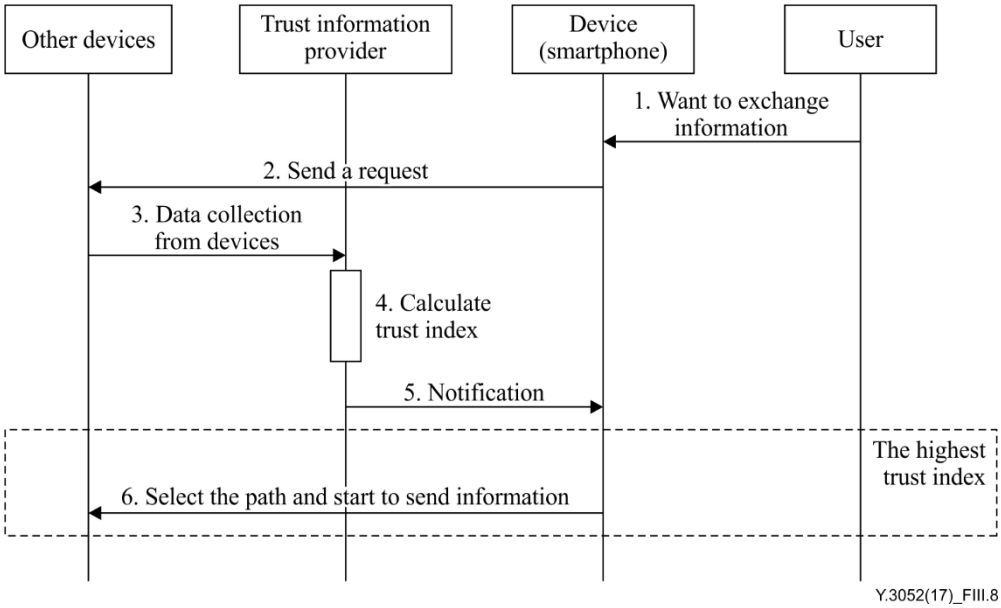

Figure III.8 – Intermediate device selection service flow

III.5 Used car transaction service

III.5.1 Description

While the used car market has been growing consistently worldwide, there exists inevitable distrust in used car transactions. Compared to purchasing a new car, buying a used car involves a high level of uncertainty and risk. The market for used cars is called "the market for the lemons", due to asymmetric information, in which a buyer cannot accurately assess the exact condition of the car through examination before sale, while a seller can more accurately assess the condition of the car prior to sale. Specifically, owners of good cars will not sell them, while owners of defective ones will. When a seller is going to dispose of their used vehicle, he/she has weak motivation to disclose the problems in the car. As a result, consumer satisfaction with used cars can be impaired because of unexpected car trouble. A general transaction model and each entity's information level of a used car are depicted in Figure III.9.

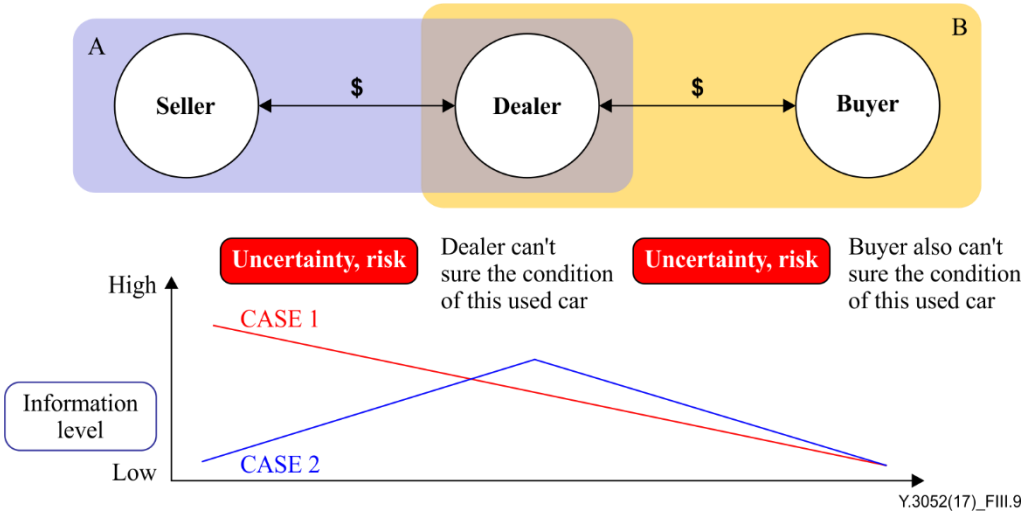

Figure III.9 – Risk, uncertainty and motivation in used car transactions

Transaction A is the purchase by a dealer of a used vehicle from a seller. In this transaction, the dealer is a risk taker. A dealer should investigate carefully to assess the condition of the car and evaluate the price, because a dealer cannot accept a seller's description of a car without verification. Specifically, a seller does not have a strong motivation to disclose 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 have not yet clearly shown (Case 2). Hence, a dealer should investigate the car. However, this cross-sectional investigation is not enough to understand the real condition of the car. Thus, intense disputes commonly occur after a transaction.

Transaction B is the purchase by a buyer of a used car from a dealer. In this transaction, the buyer is a risk taker. Similarly to transaction A, the buyer cannot implicitly trust in the dealer (seller), because a dealer has a strong motivation to hide the exact information about the current condition of the car (Case 1). Although a dealer might detect critical problems with the used vehicle after transaction A finished, a dealer will not intend to reveal the detected problems (Case 2) because this transaction contributes to the dealer's income. As a result, a dealer – a risk taker in transaction A – sells defective used cars partly with intention, partly by accident.

As a result, each entity participating in these transactions has a conflicting motivation for revealing information about the condition of a used vehicle; such motivations cannot be aligned without an external intervention. Because of this conflict, "trust" cannot be guaranteed in used vehicle transactions. Although a seller and buyer need a mediating entity – a dealer – to reduce transaction costs, 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 sum incurred in making an economic exchange. In addition, a dealer always tries to make used car transactions contribute to his/her revenue.

As a result, asymmetric information causes inevitable distrust in used car transactions due to conflicting motivations. A buyer cannot trust a seller’s 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 investigating 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 III.10, the current used car transaction involves the following inevitable problems: 1) asymmetric information; 2) conflicting motivation of disclosing the condition of used car due to item 1); and 3) distrust among entities due to item 2). Thus, an appropriate intervention is needed to avoid disputes among entities and to activate the used car market.

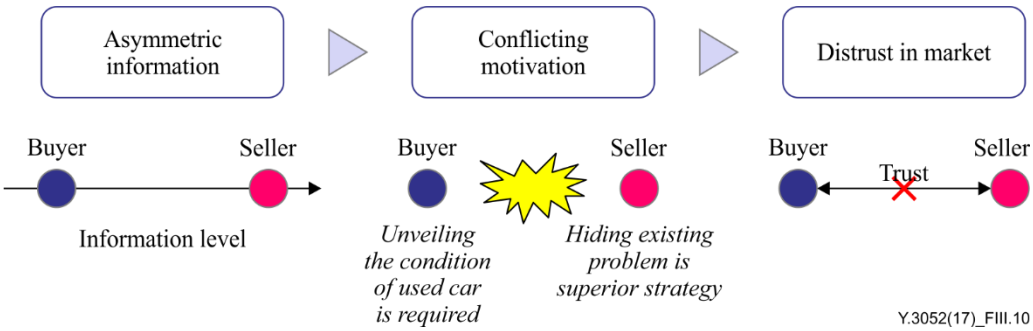

Figure III.10 – Problems of the current used car transaction service

In order to overcome the sequential problems discussed, making participants share information is a direct remedy. A trust information provider can play an important role in mediating entities who participate in the used vehicle market by sharing trustworthy data and information, as shown in Figure III.11.

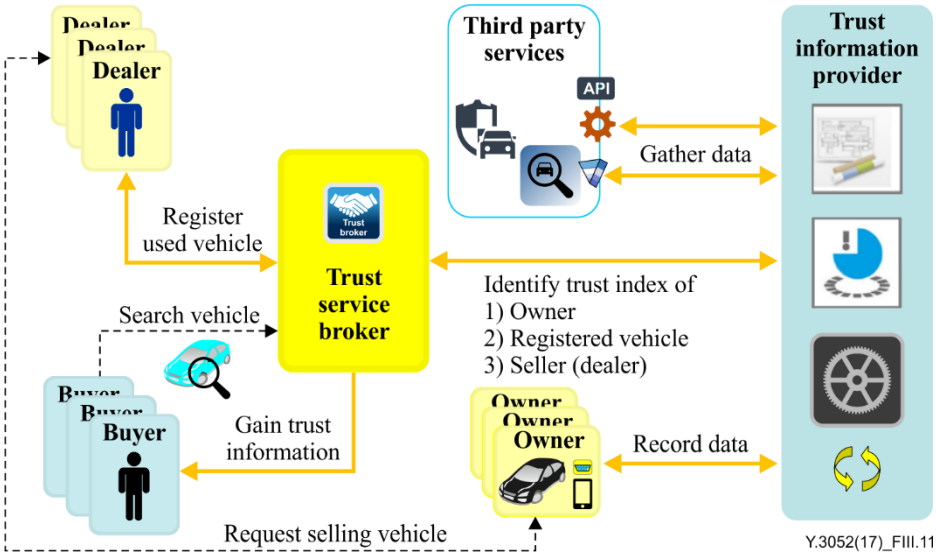

Figure III.11 – High-level illustration for used car transaction service

When selling a car, a dealer registers that vehicle in an online market place linked to a trust service broker. Then, the trust management platform automatically collects data from various sources, e.g., insurance company, public organization, social network services and the vehicle itself. If a vehicle owner attaches an on-board diagnostics scanner, this device records and accumulates a wide range of vehicle-oriented information, e.g., driving distance, recorded fuel efficiency, accident record, driving habits, and maintenance and repair history.

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

III.5.2 Actors

As the participants in the used car transaction process depicted in Figure III.11 have different goals, each actor plays a distinctive role and functions differently.

– Dealer: The major role of a dealer is to mediate between buyer and seller (owner) to gain economic profit. A dealer can sell already purchased cars or can mediate the transaction between seller and buyer.

– 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 for one in the market place or on the web provided by service broker. When a buyer makes a request to dealers and brokers to purchase a car, he/she generally describes specific constraints, e.g., vehicle age, accumulated mileage, brand, model and budget. Based on the responses about the condition of the car, he/she can make a purchase decision with low uncertainty and risk. The more trustful and abundant information is provided, the greater the likelihood of reducing risk and uncertainty.

– Owner (Seller): An owner (seller) is someone who wants to sell his/her car to others, including dealers and individual buyers. When an owner tries to sell the car, he/she simply sells the car at a negotiated price to the dealer or individual. Otherwise, he/she can ask a dealer to broker a transaction.

– Service Broker: A service broker mediates an interaction among buyers, sellers and dealers through the information transferred by a trust information provider. Based on this information, a trust service broker can communicate the identified levels of trust of the owner, registered vehicle and seller.

– Trust information provider: A trust information provider responds to various requests from service brokers and others. A trust information provider analyses the level of trust by tracing the accumulated data from various sources, including social network, insurance company, vehicle repair shop, the public and the car itself.

III.5.3 Service flow

Detailed flow description (see Figure III.12).

1) A dealer registers a used car with a trust service broker after an owner has made a request to the dealer to sell the used car.

2) A trust information provider complies with a service broker's request to transfer trustworthy data related to the car.

3) The trust information provider gathers the relevant data from not only external data sources, e.g., insurance company, public organization and social network services, but also internal data sources, e.g., an on-board diagnostic scanner, which transfers historical data from the car to the platform. If a car owner installs on-board diagnostic scanner in the car, he/she can confirm the condition of the car and identify problems via applications on a smartphone.

4) The dealer registers the car with explanatory data about the car in marketplaces connected to a number of service brokers. At this time, the car is ready for sale.

5) A buyer can search a number of used cars in order to make a purchase.

6) When a buyer is interested in a specific car, he/she can ask the service broker for relevant data and information. Then, the trust information provider replies to the service broker's requests by providing processed trustful data, including the trust index of the 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 low risk and uncertainty.

9) The used car transaction then occurs among the parties.

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

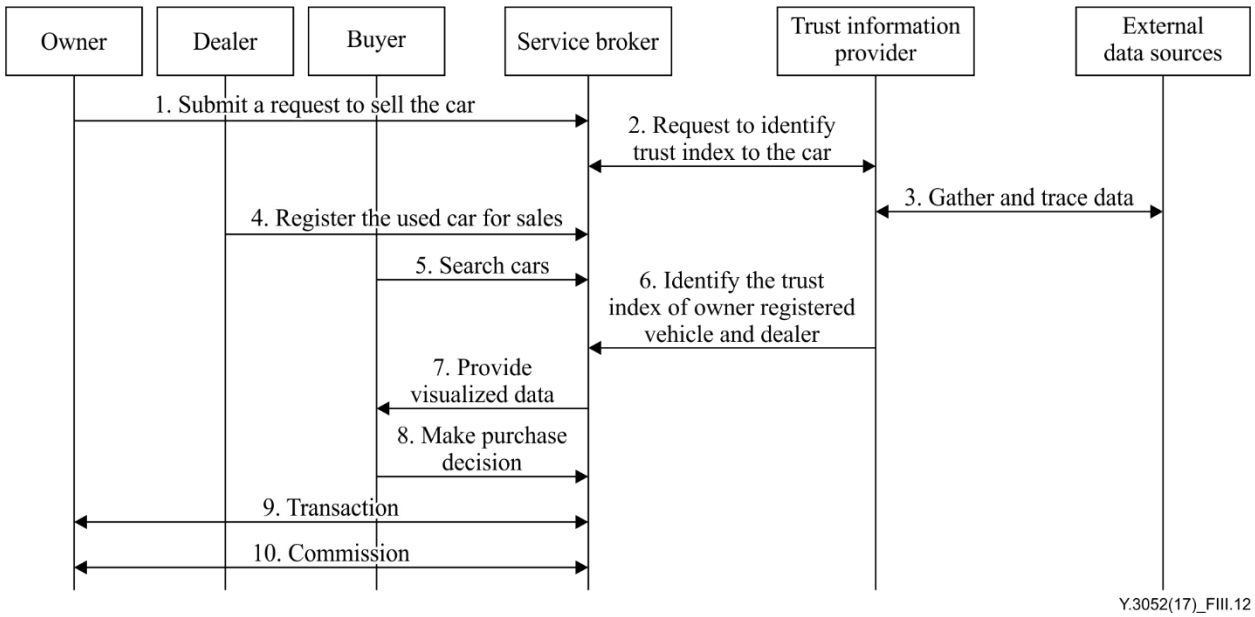

Figure III.12 – Used car transaction service flow

.

Bibliography

[b-Bao] Bao, F., Chen, I.-R., Guo, J. (2013). Scalable, adaptive and survivable trust management for community of interest based Internet of things systems. In: *Proc. IEEE 11th International Symposium on Autonomous Decentralized Systems*, Mexico City, Mexico, pp. 1–7.

[b-Brauch] Brauch, H.G. (2011). Concepts of security threats, challenges, vulnerabilities and risks, In: Brauch, H.G., *et al*., eds. *Coping with global environmental change, disasters and security*, *Hexagon Series on Human and Environmental Security and Peace*, vol. 5, pp. 61–106. Berlin: Springer.

[b-Chen, I.-R.] Chen, I.-R., Bao, F., Gou, J. (2016). Trust-based service management for social Internet of things systems. *IEEE Transactions on Dependable and Secure Computing*. **13**, pp. 684–696.

[b-Chen, J.] Chen, J., Ma, J., Zhong, N., *et al*., (2014). Waas: Wisdom as a service. *IEEE Intelligent Systems*, **29**(6), pp. 40–47.

[b-Colquitt] Colquitt, J.A., Scott, B.A., LePine, J.A. (2007). Trust, trustworthiness, and trust propensity: A meta-analytic test of their unique relationships with risk taking and job performance. *Journal of Applied Psychology*, **92**, pp. 909–927.

[b-Mayer] Mayer, R.C., Davis, J.H., Schoorman, F.D. (1995). An integrated model of organizational trust. *Academy of Management Review*, **20**, pp. 709–734.

[b-Rowley] Rowley, J. (2007). The wisdom hierarchy: Representations of the DIKW hierarchy. *Journal of Information Science*, **33**(2), pp. 163–180.

[b-Weber] Weber, R.H. (2010). Internet of things – New security and privacy challenges. *Computer Law & Security Review*, **26**(1), pp. 23–30.

[b-Wilson] Wilson, C. (2008). *CRS Report for Congress: Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for Congress*. Washington DC: Congressional Research Service. 43 pp.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2017