International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3057

(12/2021)

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

Future networks

A trust index model for information and communication technology infrastructures and services

Recommendation ITU-T Y.3057

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
Computing power networks	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.3599
BIG DATA	Y.3600–Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800–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.3057

A trust index model for information and communication technology infrastructures and services

Summary

Recommendation ITU-T Y.3057 describes a trust index model for information and communication technology (ICT) infrastructures and services. In order to provide a commonly applicable way for evaluating trust that covers different characteristics, trust index is a key concept for trust provisioning by considering the trust value chain in the ICT environment. A trust index, which can evaluate and quantify trust of stakeholders, is a comprehensive accumulation of trust indicators. This Recommendation identifies trust indicators that represent fundamental criteria for evaluating trust of entities in ICT environments. To represent characteristics of trust, trust indicators are categorized into two parts: objective trust indicators and subjective trust indicators. A list of trust indicators and an application of a trust index are introduced.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3057	2021-12-06	13	11.1002/1000/14769

Keywords

Model, trust index, trust indicator.

* 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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.3057

A trust index model for information and communication technology infrastructures and services

1 Scope

This Recommendation provides a trust index model for information and communication technology (ICT) infrastructures and services. A trust index is a composite and relative value that combines multiple trust indicators for representing trust of an entity quantitatively into one benchmark measure to help decision-making of stakeholders through identifying characteristics of entities in ICT environments. More specifically, this draft Recommendation covers the following:

– The importance of the trust and trust value chain in ICT environment;

– The necessity of a trust index for trust provisioning;

– A list and detailed description of trust indicators for obtaining trust index;

– An application of a trust index.

This Recommendation provides a generic, flexible approach to the evaluation of trust. It does not specify the mechanics for trust index calculation or the underlying decision-making process based on trust. Use of trust, and the supporting trust evaluation, are specific to a particular application or network setting. As a result, detailed trust evaluation algorithms and methods, and the application of those calculations, are out of scope for this Recommendation.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.3052] Recommendation ITU-T Y.3052 (2017), *Overview of trust provisioning in information and communication technology infrastructures and services*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 trust [ITU-T Y.3052]: Trust is the measurable belief and/or confidence which represents accumulated value from history and the expecting value for 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.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 trust provisioning: A process to evaluate trust and provide trust-related information (e.g., trust index) to help decision-making of stakeholders through identifying characteristics of entities.

NOTE – Various trust perspectives can be considered separately for trust evaluation.

3.2.2 trust index: A composite and relative value that combines multiple trust indicators for representing trust of an entity quantitatively into one benchmark measure.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ICT Information and Communication Technology

5 Conventions

None.

6 Overview

The concept of trust infers belief and confidence that the functional entities in ICT infrastructures and services will behave in expected ways. The concept of trust provisioning is to provide "an integral function of physical, cyber and social trust that provides a valuable method of minimizing risks through identifying the trust characteristics of entities" [ITU-T Y.3052]. The considered risks for trust provisioning are described in [ITU-T Y.3052].

Based on the model for trust provisioning in ICT infrastructures and services [ITU-T Y.3052], there are four major stakeholders: humans (including individuals and communities) in the social world, services and control, communication and computing devices in the cyber world, and physical things in physical world. Since each world has different characteristics and criteria for judging trust, trust provisioning is done from various different perspectives (e.g., technical, business, social, ethical) to cover various cases. In addition, it is important to find commonly applicable criteria for trust provisioning that cover different characteristics to set up the same measurable condition. Based on trust provisioning, an individual player can utilize trust information to interact with other players. Figure 1 shows trust provisioning from various perspectives.

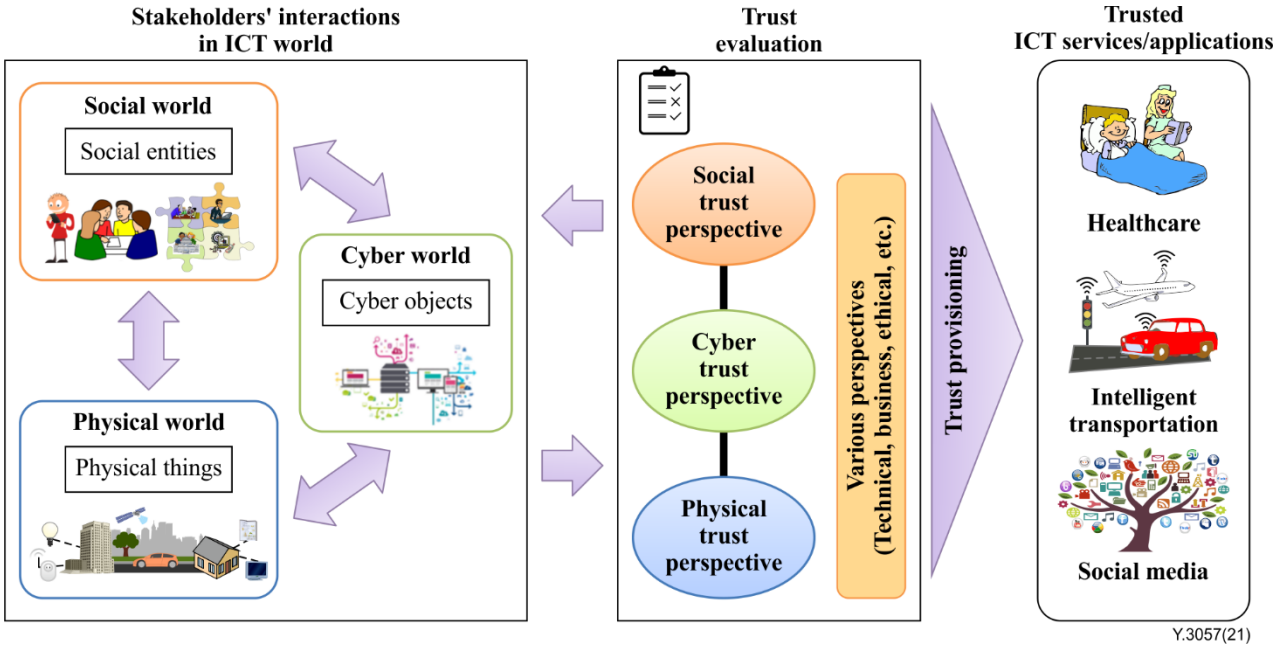

Figure 1 – Trust provisioning in ICT environments from various perspectives

NOTE – Three trust perspectives (social, cyber and physical trust) in Figure 1 are aligned with [ITU-T Y.3052]. For trust evaluation, according to applications, each trust perspective can be selectively

considered. The detailed evaluation methods of each trust perspective are out of scope for this Recommendation.

Information flow is a process of dividing various activities among stakeholders in the ICT world which consists of interactions, for examples, among creators, intermediate providers and consumers. The information flow is tightly related to human life and business activities. Each activity in an information flow is identified to analyse trust assessment. For multiple information flows, one activity in a single flow may have some effects on all the corresponding flows. Trust from a single information flow can give some information to evaluate trust in all the related value chains. The classification of the information value chain for trust evaluation is as follows.

– **Primary activities of information flow**: Information flows based on stakeholder activities are related at the direct interface between stakeholders (e.g., creator and consumer, provider and consumer, provider and distributor). Direct information flows between stakeholders can be associated with corresponding or cascading information flows from a single value chain. All activities of a single value chain are analysed and accumulated by the trust index. The trust in a single information flow can be used to maintain success flows (e.g., for advertising, promotion, sales, marketing and further analysis).

– **Secondary activities of information flow**: Secondary and supporting activities are not directly related to primary activities of the original information flow. Some activities in the primary information flow can invoke other activities in other flows. In an integrated environment of multiple information flows, the activities of a single flow can lead to corresponding activities in other flows. Some activities in a single flow can trigger appropriate activities in other information flows. Secondary activities from different information flows, on the other hand, can give important information about the original flow while calculating trust.

As described above, to provide successful interactions among stakeholders, one of the critical factors is trust. If trust is high, the collaborative relationship through information flows can be improved. Trust is a kind of tool to maintain honesty, fairness, openness and competence among stakeholders, and it can also reduce costs for security provisioning and risks of privacy violation. Therefore, it is important to identify the trust value chain among stakeholders. Even if stakeholders have multiple types of interactions between or among them, a relationship between stakeholders can be described as "A trustor trusts a trustee".

One stakeholder can be either trustor or trustee depending on the context of the relationship. For example, when a mobile device installs an application, the device may evaluate the trust of the application with the context of deciding whether it installs the application or not. In this case, the device becomes the trustor, and the application becomes the trustee. On the other hand, when the device runs the application, the application may evaluate the trust of the device with the context of evaluating the usage behaviour of the device. In this case, the application becomes the trustor, and the device becomes the trustee.

The trust value chain is described as follows (Figure 2):

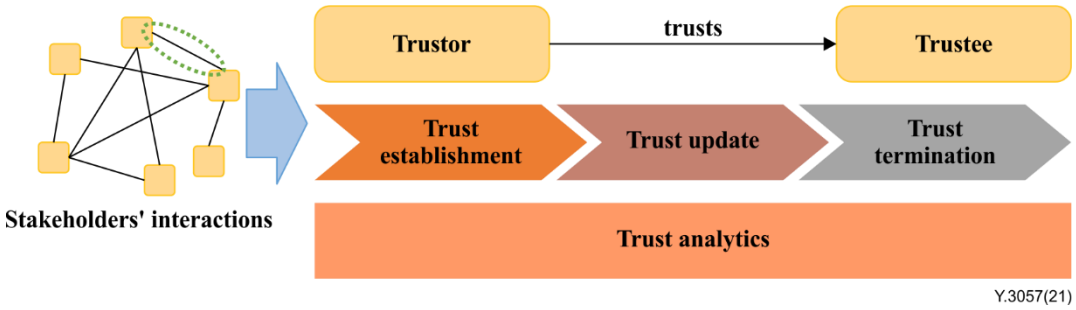

Figure 2 – Trust value chain

– **Trust establishment**: The stakeholder establishes a certain level of trust of other stakeholders based on the result of trust analytics. The stakeholder has a chance to make interactions with trust if other stakeholders' level of trust satisfies its requirement.

– **Trust update**: As time goes on, the measured value of the criteria for trust have changed depending on context, environment, and behaviour of other stakeholders, etc. Therefore, the stakeholder periodically updates the trust of other stakeholders.

– **Trust termination**: Based on the results of the trust update, the stakeholder decides to terminate the trust evaluation of other stakeholders. The stakeholder may end its interaction with stakeholders who have a lower level of trust than its requirement.

– **Trust analytics**: A stakeholder analyses and evaluates the trust of other stakeholders in whom the stakeholder has interests. The stakeholder analyses and decides specific criteria for measuring trust.

Since trust provisioning is a process to evaluate trust and provide trust-related information (e.g., trust index) to help decision-making of stakeholders through identifying characteristics of entities, it can be applied to trust analytics in a trust value chain by providing useful information when the stakeholder needs to decide the trust of other stakeholders.

For trust provisioning, a commonly applicable trust assessment method is needed. The concept of the trust index is introduced in [ITU-T Y.3052] for representing the trust of entities in ICT infrastructures and services as a numerical value. The detailed trust evaluation model is shown in Figure 3. A trust evaluation model is based on a set of trust indicators to evaluate trust between a trustor and a trustee, and a trust indicator is a composite of various trust attributes that represent characteristics of the trustee.

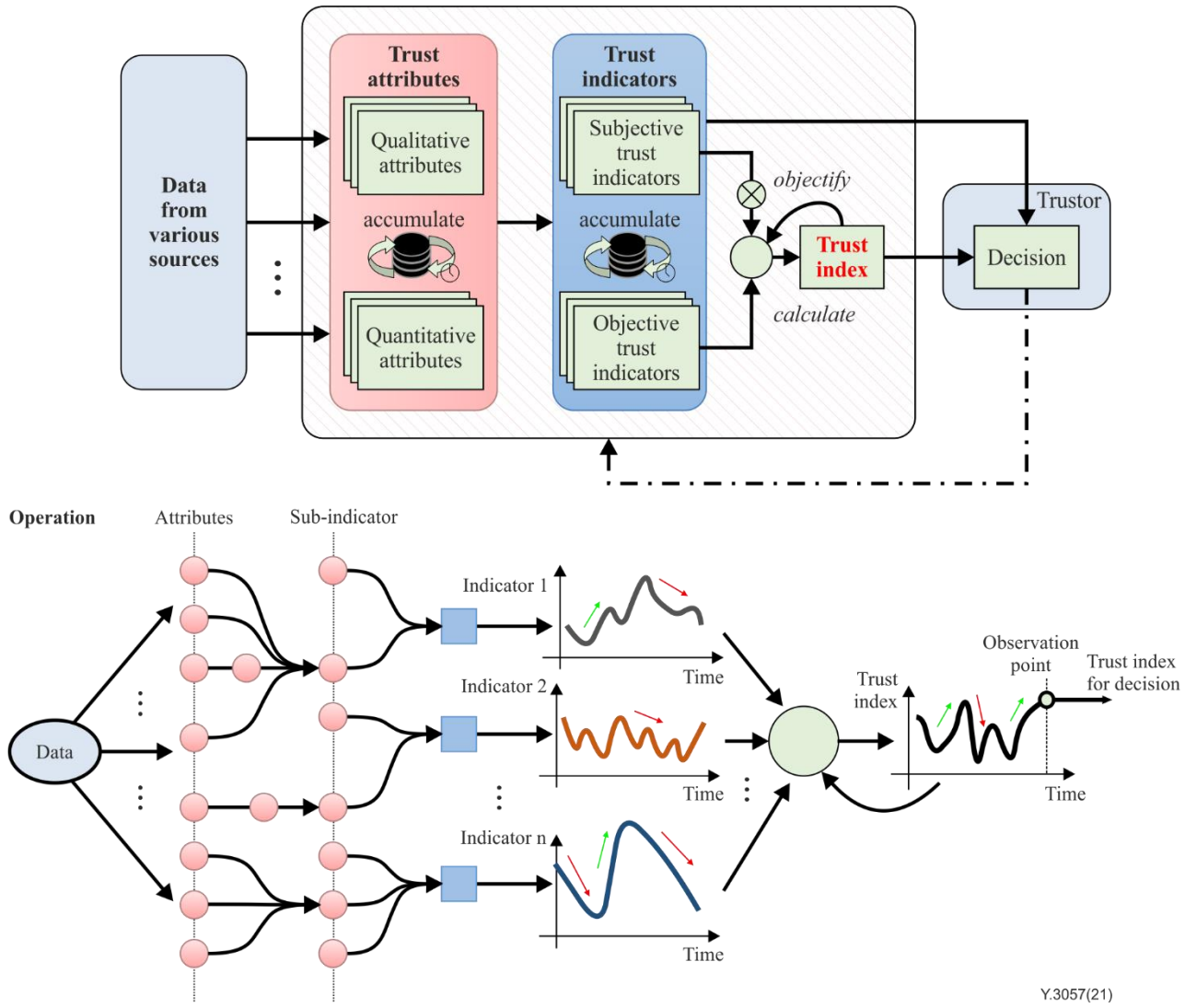

Figure 3 – Trust evaluation model [ITU-T Y.3052]

– **Trust attribute**: Trust attributes represent characteristics of an entity (including direct and indirect trust), which consist of qualitative and quantitative attributes. Trust attributes refer to properties and features of an entity that can be trusted. Qualitative attributes need the quantization process to accumulate with 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 the trustworthiness of an entity quantitatively. In addition to objective trust indicators, subjective trust indicators can be optionally considered to reflect subjective or personal attributes of trust entities. The trust indicators are calculated at the measurement instance of their trustworthiness since their values are changing 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 the ICT development index or stock market index. A trust index is a comprehensive accumulation of the objective trust indicators and the subjective trust indicators objectified for calculation. A trust index evaluates and quantifies the trustworthiness of a trustee.

NOTE – The detailed trust provisioning process is described in [ITU-T Y.3052].

7 Trust indicators for measuring a trust index

Trust includes both trustworthiness and trust propensity, so it may be influenced not only by entities' characteristics but also by entities' expectations and context. In addition, trust also includes context-dependent characteristics. Hence, in principle, trust can be considered subjectively by the entities and may differ from one entity to another. However, it is often estimated using objective measurements (including objectified methods) as shown in Figure 3.

Trust indicators for measuring a trust index can be categorized into two different types: objective and subjective.

– **Objective trust indicators** are appraised only with unbiased factors without the intervention of the opinions, views, attitudes or experiences of the evaluator. Objective trust indicators are sets of common features that can be directly quantified through various methods. For example, technical aspects, ability, integrity and benevolence can be categorized as objective trust indicators.

– **Subjective trust indicators** are determined by entities based on the intrinsic perspectives and propensities of the evaluator, including their opinions, cultural perspectives and intent. Accordingly, subjective trust indicators will reflect personal opinions, perspectives and attitudes as well as non-technical aspects (such as social, political, economic or cultural context) that are subject to dynamic parameters. Such subjective aspects cannot be directly measured and, therefore, the manner by which subjective trust indicators are identified, measured and used is outside the scope of this Recommendation. For example, experience, reputation and inclination can be categorized as subjective trust indicators.

Figure 4 shows examples of trust indicators for ICT infrastructures and services. This Recommendation describes only commonly applicable trust indicators in ICT infrastructures and services. The detailed trust indicators are listed below. This list is not exhaustive.

Examples of objective trust indicators

– **Ability** represents characteristics that enable an entity to have influence within some specific contexts. The indicator 'ability' indicates the characteristics related to competency and ability in handling ICT infrastructures and services.

– **Integrity** represents the quality of being honest and fair in the social world, the state of being complete in cyber and physical worlds, or intactness and consistency of information in terms of information. The indicator 'integrity' indicates the characteristics of the trustee's adherence to principles related to ICT infrastructures and services.

– **Benevolence** represents to the desire to do well to others and the willingness to work or act together for common purposes or benefits. The indicator 'benevolence' indicates the characteristics of the trustee's attitude to work or acts with ICT infrastructures and services.

Examples of subjective trust indicators

– **Experience** may represent the observation about the interactions between the evaluator and the subject of the evaluation, which is achieved by accumulating the state of interactions among entities over time. The indicator 'experience' may indicate the accumulated interactions between the evaluator and the subject of the evaluation.

– **Reputation** may represent the accumulated experience of the evaluator about the subject of the evaluation with respect to its prior behaviour. The indicator 'reputation' may indicate the appraisals of the trustee's previous behaviour.

– **Inclination** may represent the subjective preferences of evaluators toward the subjects of the evaluation, which is accumulated from experience and reputation. The indicator 'inclination' may imply the importance of the other trust indicators. For example, it may express the weights of the indicators in the trust index calculation.

NOTE 1 – Detailed interpretation, measurement and application of each trust indicator are dependent upon contexts. For example, an appendix of [b-ITU-T Y.3055] describes a use case for applying trust indicators and a trust index in the personal data management context.

NOTE 2 – Various approaches can be applied to quantify each trust indicator. The details are out of scope for this Recommendation.

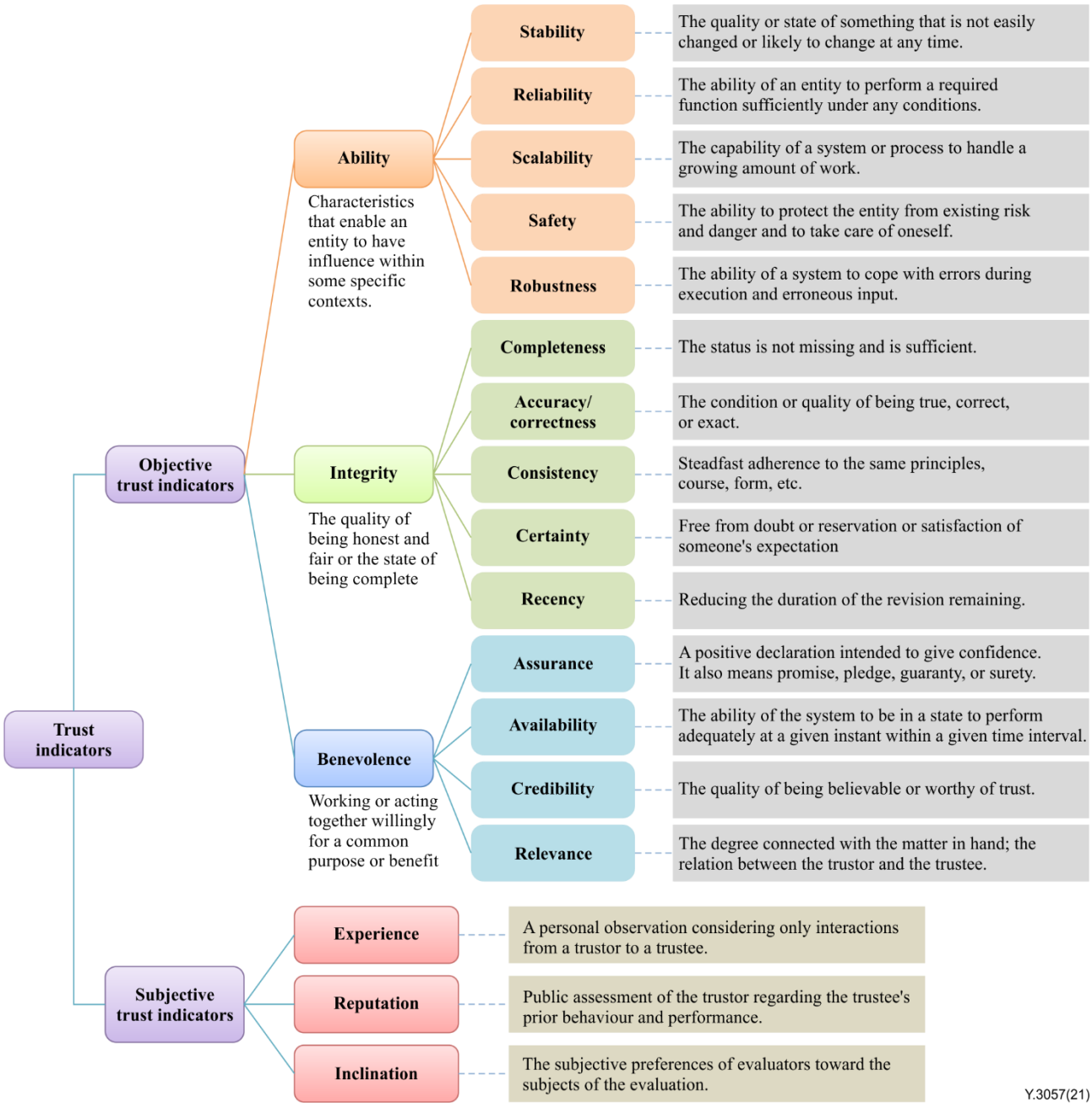

Figure 4 – An example of trust indicators for ICT infrastructures and services

8 Application of trust index

As described in Figure 3, the trust evaluation model measures the quantified value of trust indicators and performs a trust index calculation by using the measured trust indicators. Since the trust index represents the trust of an entity quantitatively into one benchmark measure, it can be used as one piece of useful information. Various approaches (e.g., from simple weighted sum to complex artificial intelligence) can be applied to obtain a trust index.

Figure 5 shows an application of a trust index aligned with a general decision-making process. During the decision-making process, a trust index can be utilized as one of the decision criteria. Particularly when a decision maker (i.e., trustor) needs a trust index, a trust evaluation model performs a trust provisioning process for evaluating a trust index (in this case, the decision maker itself or any trustworthy entity perform a trust provisioning process). Then the decision maker can utilize the trust index (including trust indicators if necessary) to choose the best alternatives for the decision-making process.

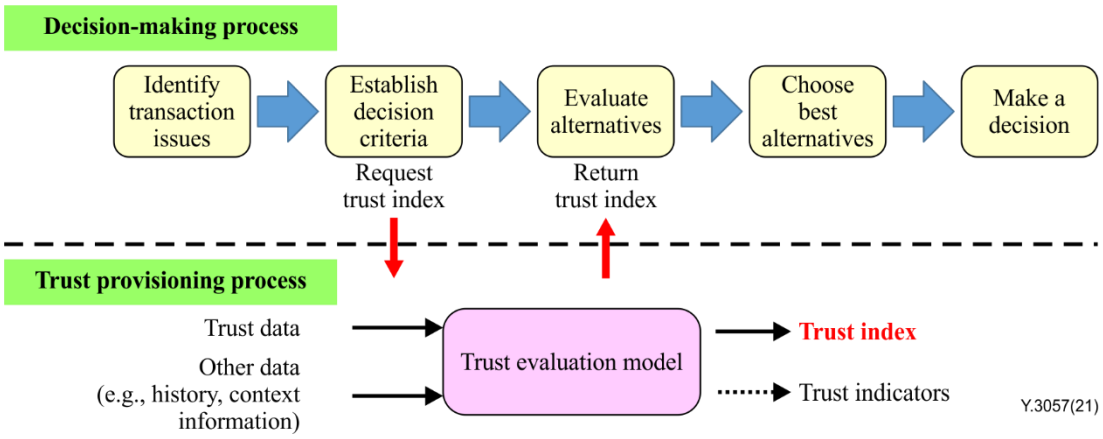

Figure 5 – An application of trust index obtained by trust provisioning process

The trust evaluation model can be deployed by multiple stakeholders and applications. Since each stakeholder may have different requirements, the resulting trust indicators can be different from stakeholder to stakeholder. It is possible to identify common criteria for applying trust indices across multiple stakeholders or applications. What is required is transparency of the trust evaluation model. With a trust model fully documented, each stakeholder or application can decide if the generated trust index is useful in their application. Any interoperability of a common trust index relies on the transparency of the full trust model, its indicators and the calculations of the trust index.

To find common criteria for applying a trust index among different stakeholders, each stakeholder could check detailed trust indicators of other stakeholders' trust index evaluation models. This will allow the stakeholders to decide whether they can accept the provided trust index based on the trust index evaluation model or not. For those stakeholders that choose to utilize a commonly applicable trust index, they may exchange their trust indicators and methods for measuring them.

By applying a trust index model with trust indicators for ICT environments, various risks and limitations need to be carefully considered. For combining detailed criteria (e.g., trust indicators and trust attributes) to measure a certain value, a trust evaluation model keeps in mind that unpredictable situations can occur. For example, measured values can result in unpredictable biases influencing the entities of trust. Therefore, it is important to consider transparent, explainable and auditable approaches. Moreover, since a trust index model may consider both objective and subjective trust indicators for calculation, it may not be possible to obtain a value in real-time due to the characteristics of trust such as context and time dependency.

On the other hand, each trust indicator has a different importance to each stakeholder who actually wants to use it. Therefore, even stakeholders who use the same measurement method for obtaining trust indicators may find that the result of trust index calculation may differ due to differences in the weights assigned to different factors. Therefore, stakeholders' priority factors should be shared among stakeholders to establish common criteria for providing a common understanding of trust index applications. This is an essential part of making the trust index model transparent, explainable and auditable to stakeholders and other interested parties.

9 Security considerations

Any activities, including data collection, analysis and management, for measuring trust indicators and calculating a trust index should follow technical and/or regulatory guidelines for security and privacy such as [b-ITU-T X.1058], [b-ISO/IEC 27701], [b-ISO/IEC 29100], etc. Details of security and privacy related technologies for trust index evaluation are out of scope for this Recommendation.

Bibliography

[b-ITU-T Y.3055] Recommendation ITU-T Y.3055 (2020), *Framework for trust-based personal data management*.

[b-ITU-T X.1058] Recommendation ITU-T X.1058 (2017), *Information technology – Security techniques – Code of practice for personally identifiable information protection.*

[b-ISO/IEC 27701] ISO/IEC 27701:2019, *Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines.*

[b-ISO/IEC 29100] ISO/IEC 29100:2011, *Information technology – Security techniques – Privacy framework.*

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, 2022