International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3051

(03/2017)

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

Future networks

Basic principles of trusted environment in information and communication technology infrastructure

Recommendation ITU-T Y.3051

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.3051

Basic principles of trusted environment in information and communication technology infrastructure

Summary

Recommendation ITU-T Y.3051 specifies basic principles for creating a trusted environment in information and communication technology (ICT) infrastructure that provides information and communication services. The Recommendation provides the definition, common requirements and the basic principles of creating a trusted environment.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3051	2017-03-29	13	11.1002/1000/13251

Keywords

Trusted environment, information communication technology (ICT).

---

* 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.3051

Basic principles of trusted environment in information and communication technology infrastructure

1 Scope

This Recommendation specifies basic principles for creating a trusted environment in information and communication technology (ICT) infrastructure that provides information and communication services. This issue has become extremely important in the modern knowledge society that has seen a significant growth rate in information technology usage. This Recommendation contains a rationale for the necessity for a trusted environment in ICT infrastructure. This Recommendation is relevant for service developers as well as network designers and should be considered as a set of fundamental principles for creating a convenient and secure environment. While the basic principles outlined in this Recommendation aim at creating a trusted environment for the provision of services using ICT, they may be applied in a broader interpretation of the concept of a trusted environment.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 trust [b-ITU-T Y.3052]: Trust is the measureable 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, which 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 term:

3.2.1 trusted environment (in ICT infrastructure): An information and communication technology-enabled environment providing a set of technical and regulatory conditions sufficient for establishing trust between interacting entities.

NOTE – From a broader perspective, the trusted environment can be perceived as a multidimensional concept with technological and societal implications.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviation and acronym:

ICT Information and Communication Technology

5 Conventions

In this Recommendation:

The keywords "is required to" indicate a requirement which must be followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "can optionally" and "may" indicate an optional requirement which is permissible, without implying any sense of being recommended. These terms are not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Necessity of trusted environment in ICT infrastructure

Due to the development of information technology and future networks, the number of entities and their interactions (e.g., human to human, human to machine, machine to machine) is increasing significantly. In any uncertain circumstance, people need to be able to predict the results of these interactions especially with the entities that they cannot control remotely. To provide the desired level of confidence and protection, it is necessary to conduct a complex of special technical and organizational measures. One possible way is to create a trusted environment in ICT infrastructure.

Globalization and the wide spread of information technologies lead to the displacement of the context of trust by special technological means. Therefore, ICT infrastructure needs to play a role in building a trusted environment with interoperability and information security. In addition, ICT infrastructure needs trust between interacting parties at a high level of responsibility in a resource-limited environment (e.g., to save human lives in emergencies).

A trusted environment in ICT infrastructure is necessary for social, critical and life-protecting services (e.g., e-government, e-commerce and e-health). For such services, establishment of trust between service providers and consumers can solve problems of fraud and increase the availability of services.

In summary, creating a trusted environment in the ICT infrastructure allows entities to predict the results of their interactions and minimizes risks caused by the growing number of interactions and the loss of their context, while providing interoperability and information security.

7 Requirements for a trusted environment in the ICT infrastructure

A Trusted environment in the ICT infrastructure must meet the requirements specified in clauses 7.1 to 7.4.

7.1 Predictability

- All participants within a trusted environment are required to be equipped with the capability to predict the outcome of their interactions in order to reduce the risks of negative consequences caused by the inappropriate behaviour of any participant(s).
- For this, the ICT infrastructure used for a trusted environment is required to meet a certain level of quality.
- Provision of handy user interfaces and systems of access to a trusted environment is recommended for participants to improve predictability, by using comfortable and familiar methods of interaction each time.

7.2 Information security

- It is required to provide confidentiality, integrity and the availability of information, as well as the absence of misinformation (spam, etc.), for all participants interacting within a trusted environment.
- Each participant is required to be verified for compliance with the common minimal security requirements.

- Minimal security requirements for a trusted environment in an ICT infrastructure are required to be developed for all security dimensions [b-ITU-T X.805] with the goal of providing electronic exchange of information in a trusted environment at the same level of trust as in a non-electronic interaction.

7.3 Interoperability

- It is required to enable all participants interacting within a trusted environment to exchange information with any other entity within a trusted environment in an ICT infrastructure.
- A trusted environment in an ICT infrastructure is required to support internetwork connections to provide unified interaction capabilities to each participant, independent of technical infrastructure (core networks) used.
- All predictability, information security and availability of administration services requirements are required to be supported for internetwork connections.

7.4 Availability of administration services

- Provision of continuous customer support is required for all interacting participants within a trusted environment in an ICT infrastructure, as well as prompt compensation if service provision fails.
- A trusted environment in an ICT and its technical infrastructures are required to maintain the capacity to enrol new participants enabling them to rapidly integrate and start operating within the trusted environment in the ICT.

8 The basic principles of for a trusted environment in an ICT

The need to create a trusted environment is associated with the increased convergence of ICT, general mobility and the increasing number of interactions between humans and machines. The task of creating a trusted environment is especially actual for ICT used in socially and economically significant interactions between machines, humans, organizations and other entities. Examples of such interactions are e-commerce, e-government and emergency rescue guidance. The last is related to a direct threat to human life and also represents a high importance interaction within a trusted environment.

On the global scale, a trusted environment is not possible in the absence of ICT interoperability. The field of interoperability of ICT can be characterized by statements 1 to 3.

1. Presence of a large number of information systems operating within governmental institutions and companies. These systems typically use their own hardware and software, and most of them cannot exchange information directly in "machine-to-machine" mode.
2. The presence of many competing standards that only hinder information exchange, despite the excellent work carried out by numerous standardization bodies (at national, regional and international levels).
3. The majority of developed economies are not ready to abandon the already established and well-functioning information systems for the benefit of future non-prescribed systems.

The basic principles for creation of a trusted environment in ICT are:

1. The principle of **non-discrimination** – the electronic interaction in a trusted environment is not exempt from legal consequences, validity or enforceability solely on the ground that it is provided in electronic form. This involves adoption of legal regulations, but the first step is to provide appropriate technological capabilities in an ICT infrastructure to ensure the same level of security for electronic transactions as for signatures on paper. E-signature and certification authorities can serve as examples of such technologies.

2. The principle of **technological neutrality** of ICT in a trusted environment, which involves creating a trusted environment that is ICT neutral with regard to the technology used. Given the rapid pace of technological progress, neutral regulations are intended to allow the use of any future development without further legislation.
3. The principle of **functional equivalence**, which sets the criteria by which electronic interactions (e.g., electronic documents) can be recognized as the equivalent of live interactions (e.g., paper documents). This provision involves the adoption of legal regulations, but the first step is to provide appropriate technological capabilities in an ICT infrastructure to ensure the integrity of transported information (electronic documents).
4. The principle of **unification**. ICT used in a trusted environment is required to have unified forms of information, while maintaining its unique content. Due to the possible wide range of entities involved in information interaction within the trusted environment, it is especially important to use unified interfaces of information interaction within the entire trusted environment.
5. The principle of **scalability**. Organizational and technical infrastructures of a trusted environment in ICT are required to have the capacity to enrol new participants, enabling them to start operating within a trusted environment. These infrastructures are also required to enable their users to choose a set of services matching the user's needs.
6. The principle of **equal reliability** of infrastructure of a trusted environment, which applies common minimal security requirements to all participants, regardless of their own parameters. This is important to prevent the occurrence of vulnerabilities in a trusted environment in ICT, which can be used to attack the whole trusted environment.
7. The principle of **legalization** of electronic documents in a trusted environment, ensuring that issued e-documents are equally recognized by respective jurisdictions (e-apostille). It is important to ensure safety and integrity of information flows during transportation through networks that combine numerous ICTs and standards.
8. The principle of **client-oriented** architecture that includes simple, clear and handy user interfaces, in addition to a unified system of accessors to the services in a trusted environment in ICT. It also includes provision of the capabilities of a trusted environment in ICT within widely used general purpose networks, e.g. the Internet.
9. The principle of **systematization**, which includes three main components:
   - consistency of organizational, legal and technical arrangements;
   - consistency in reliability structures and infrastructure systems;
   - moving from bilateral interoperability arrangements towards multi-vectored ones, where appropriate.

This principle concerns not only the technological, but also mainly the legal and organizational fields.

1. The principle of **finiteness** of a trusted environment, which suggests that a trusted environment can be organized within the scope of a specific information interaction space, and continuously maintained and improved within this space. If the trusted environment covers the whole existing ICT infrastructure, its maintenance (including administration) becomes extremely complex. Therefore it is reasonable to establish a trusted environment only within the specific part of the ICT infrastructure, where maintenance is possible.

It is important for ICT infrastructure to support implementation of all these principles to be compatible with a trusted environment.

Appendix I

The first steps for creating a trusted environment for cross-border e-commerce

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

Cross-border e-commerce is an example of informational interaction of entities that are residents of different economies, and therefore subject to different regulations and laws. Each economy has its own rules of information handling and this fact gives rise to an important issue with e-commerce. Cross-border e-commerce should support the rules of each interacting economy in order to establish trust between interacting entities. Therefore, the cross-border e-commerce system should be implemented within a trusted environment with such characteristics as interoperability and information security.

The following first steps can be used to implement the above mentioned principles to:

1) Initiate a dialogue at the global level on cross-border regulatory exchange of information and to start collecting information on existing practices in this area.
2) Exchange national experiences on co-regulatory initiatives in the private sector, in consultation with regulators.
3) Establish a cross-sector group on cross-border e-commerce.
4) Initiate the development of a legal framework for interoperability at the global level.
5) Provide not direct interoperability ICT, but to ensure recognition of certificates of authenticity of information transmitted across borders. This can be achieved through the following steps: a) creation of national systems of certification authorities and national regulators of these systems; b) conclusion of an international agreement on mutual recognition and the conditions of mutual recognition of certificates of authenticity for information transmitted across borders.
6) Ensure cross-border transparency and accessibility requirements. The development of a standardized process to ensure the integration and exchange of data with the legal significance, both within and between economies, is required.
7) Overcome linguistic barriers. The problems of incompatibility of existing standards, standard classifications, reference books (national, international, industry, etc.) used in the Internet economy require resolution and electronic transactions and linguistic algorithms for information systems of e-commerce require development.

Appendix II

Use case of creating a trusted environment for rescue systems

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

This appendix describes an example of forming a trusted environment related to ensuring the safety of people in emergency situations.

Nowadays, it is not easy for a person to navigate in technological environment. This problem becomes critical in an emergency, when the wrong action or delay could lead to human casualties. The use of modern ICT to create a different kind of warning and safety system to assist such processes as evacuation can improve the safety of people in an emergency.

Moreover, safety systems services (e.g., notification, evacuation management) should be provided in a trusted environment to minimize direct threats to human life or activity that occurs as an unwanted effect from an interaction or security breach in the environment.

The basic properties of a trusted environment can be implemented in safety systems as follows:

Predictability: Users require information about the possible operation scenarios of the system, the types of information provided by this system (audio, video, text or tactile messages) and its mission. Alarm messages require predefinition and users require an introduction to the verity of possible alarm messages. The system is required to use only evacuation plans that are familiar to users to minimize the perception time of information and avoid any delay that could lead to human casualties.

Information security: Integrity and availability of warning signals, information about the evacuation process and other vital information in an emergency are required to be guaranteed for all users of the system.

Interoperability: All users of the system are required to be able to receive alarm messages and other information via any of the established public communication channels (cellular network, radio and television broadcasting, Internet, etc.) and with any of available devices (mobile phone, smart phone, TV, etc.). Alarm messages and other emergency information are required to be provided for both residents (employees) and non-residents (visitors) in the appropriate language.

Availability of administration services: Continuous customer support is required to be provided for all users of the system (residents, workers, visitors, etc.) in terms of assistance with safety-related issues. All actions and instructions of the system are required to be recorded in a special vault (black box) in order to further establish their eligibility.

The basic principles of safety systems in a trusted environment can be described as follows:

The principle of **non-discrimination** – in security systems based on ICT, electronic alerts and evacuation instructions in case of emergency are required to have the same legal force and the same level of responsibility as the direct commands of rescue services.

The principle of **technological neutrality** – information from the security system is required to be provided using all available user technologies (see Interoperability).

The principle of **functional equivalence** – in security systems based on ICT, electronic alerts and evacuation instructions in case of emergency are required to be equivalent to the direct commands of rescue services.

The principle of **unification** – a substantial part of the information from a security system is required to be independent of the transmission technology used in the communication channel.

The principle of **scalability** – the security system is required to support the connection of new users and groups, and ensure their interaction with the system immediately after connection. For example,

if people enter a building in which there is an emergency, they should be immediately informed about the emergency situation and their further actions should be corrected by the security system.

The principle of **equal reliability** – individual user characteristics (limits of hearing, vision, motor functions, etc.) are required not to affect the timeliness of information provision or the eligibility notification and control process in an emergency evacuation.

The principle of **legalization** – information from one security system is required to have full legal force in another trusted environment. For example, the alarms from external security systems (federal, regional, municipal) should be relevant in the object security system (in the buildings) in the case of natural disasters. The object system is required to organize the evacuation process and other actions of people in the building in accordance with the external instructions to minimize the risk to human life.

The principle of **client-orientation** – personalization of messages and signals from the security system to the user is recommended. For example, the object security system may support individualized management of the evacuation process and provide personal messages to mobile user terminals.

The principle of **systematization** – the development of uniform standards for security systems in a trusted environment as well as a uniform set of instructions in case of emergency are required.

The principle of **finiteness** – the security system should be implemented within a limited space (of the object, state, federation), in which the system will be maintained and improved: updating of manuals, instructions, the set of supporting events, types of emergencies, types of natural and man-made disasters, technical characteristics of sensors, etc. is required.

Bibliography

[b-ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.

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

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