International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1033

(04/2016)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Information and network security – Network security

Guidelines on security of individual information services provided by operators

Recommendation ITU-T X.1033

ITU-T

International Telecommunication Union

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	**X.1030–X.1049**
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
PKI related Recommendations	X.1340–X.1349
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

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

Recommendation ITU-T X.1033

Guidelines on security of individual information services provided by operators

Summary

Recommendation ITU-T X.1033 addresses security aspects of the information services provided by telecommunication operators. In the transformation from providing traditional basic telecommunication services to providing comprehensive information services, operators have expanded their services to include content services and information and communication technology (ICT). These new services not only change the operational models but they also add new security issues to be resolved.

This Recommendation provides guidelines on the security of the individual information services provided by telecommunication operators. The scope of this Recommendation covers the classification, security requirements, mechanisms and coordination of individual information services.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1033	2016-04-29	17	11.1002/1000/12849

Keywords

Information service, security.

* 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 X.1033

Guidelines on security of individual information services provided by operators

1 Scope

This Recommendation provides guidelines on the security of individual information services provided by telecommunication operators. It describes the classification of the individual information services provided by telecommunication operators as well as security objectives, requirements, mechanisms and coordination of individual information services.

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.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 bearer service [b-ITU-T I.112]: A type of telecommunication service that provides the capability for the transmission of signals between user-network interfaces.

3.1.2 teleservice [b-ITU-T I.112]: A type of telecommunication service that provides the complete capability, including terminal equipment functions, for communication between users according to protocols established by agreement between Administrations and/or recognized operating agencies (ROAs).

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 basic telecommunication service: A bearer service or teleservice. The terms "bearer service" and "teleservice" are defined in clauses 3.1.1 and 3.1.2, respectively.

3.2.2 individual information service: This is the service process of content searching, indexing, information collection, filtering, ordering and provision of content to specific user(s) or to user groups based on information obtained of users' requirements, privileges, preferences and habitual behaviours, etc.

3.2.3 informationization service: A service that offers solutions to encountered issues or a service that provides assessment, prediction and prevention of possible problems by using information technology and other high-tech means.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CRM Customer Resource Management

ICP Internet Content Provider

ICT Information and Communication Technology

IPTV Internet Protocol TeleVision

ISP Internet Service Provider

IT Information Technology

OA Office Automation

QoS Quality of Service

ROA Recognized Operating Agency

SMS Short Message Service

TV Television

5 Conventions

None.

6 Information services provided by telecommunication operators

Information services provided by telecommunication operators include voice services, data services and information services such as online information providing and data indexing via public networks, e.g., fixed networks, mobile networks, Internet and other telecommunication infrastructures. The informationization service provided to other organizations by operators is also included. To provide information services, telecommunication operators and/or other third parties must collect, analyse and process information and construct a platform to help users to access, share and exchange the information.

Information services provided by telecommunication operators can be classified into three categories (as shown in Figure 1):

– Communication service;

– Content service; and

– Informationization service.

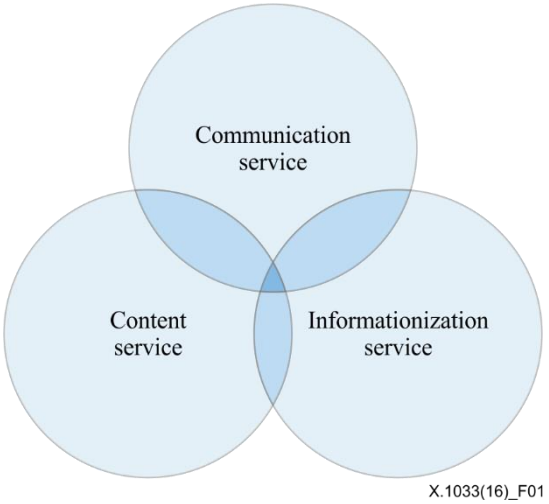

Figure 1 – Composition of information services provided by telecommunication operators

6.1 Communication services

Traditionally, telecommunication operators provide communication services with their network infrastructures including fixed networks, mobile networks, Internet, satellite, etc. These services include voice, video, data and multimedia. Typical communication services include:

– Telephone services;
– Internet broadband service;
– Mobile services;
– Directory service;
– Telegraph service;
– Telematic service;
– Message handling service;
– Videophone.

6.2 Content services

Content services are the extension of communication services. These kinds of services may be provided by operators as well as by third parties, such as Internet service providers (ISPs) and Internet content providers (ICPs). Typical content services include:

– Access portal;
– Web indexing/searching;
– Application store;
– Mobile reading/advertising/newspaper;
– Mobile television (TV)/Internet protocol television (IPTV);
– Location service/mobile navigation;
– Social networking.

Usually, in order to address the application and content services area, operators need to design and develop applications and produce content themselves or simply collect contents from other companies that produce music, television programmes, or financial services such as credit cards, stock trading, etc.

In the transformation from providing traditional basic telecommunication services to providing comprehensive information services, the operators expand their services to include content services and information and communication technology (ICT). Consequently their business value chain changes to include these new businesses, as shown in Figure 2 below.

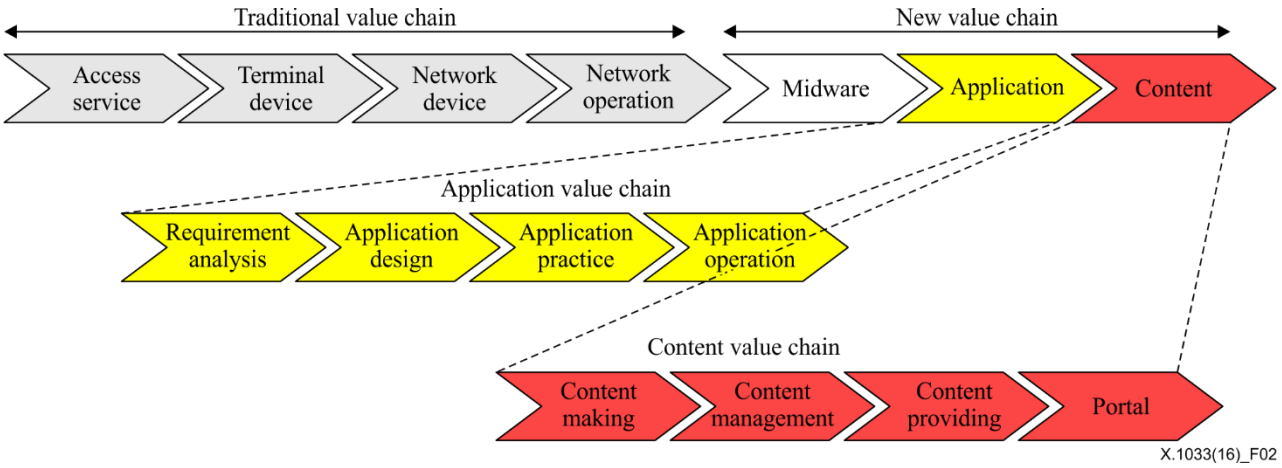

Figure 2 – Content service chain

6.3 Informationization service

Informationization is the goal of an information society. The informationization service is the service that offers solutions to encountered issues or the service that provides assessment, prediction and prevention of possible problems by using information technology and other high-technical means.

Currently operators enter this area with their advantages in information technology (IT) knowledge and network infrastructure. They provide solutions for encountered issues, or provide assessment, prediction and prevention of possible problems, such as consulting, training and information outsourcing, etc. Typical informationization services include:

– E-government (for governments);

– E-commerce, mobile office automation (OA) (for enterprises);

– Digital live, digital entertainment (for homes);

– E-health, e-education (for persons).

6.4 Individual information service

Individual information service is the service process of content searching, indexing, information collection, filtering, ordering and provision of content to specific user(s) or user groups based on the information obtained of users' requirements, privileges, preferences and habitual behaviours, etc.

In this process, the users' requirements, privileges, preferences and habitual behaviours, etc., are (under the user's authorization) perceived by individual information service providers and are used for content searching, indexing, information collection, filtering, sorting and processing, etc. The searching and collecting of user-preferred content information should abide by the users' privileges, while the method, the process and the extent of information provided should comply with the users' preferences and habitual behaviours. The information should be provided to users with user-preferred security and quality of service.

6.5 Classification of roles

As mentioned, stakeholders involved in the information services provided by telecommunication operators can be classified, based on their roles, into regulators, operators, third-party service providers and end users. Under this classification of roles, different stakeholders each have their own security requirements:

– Regulators. Based on service regulations and legislations, regulators need to put forward security requirements for operators and service providers to ensure service availability, fair competition and privacy protection, etc.

– Operators. Operators need security measures to safeguard their infrastructures, service operation and business interests. Operators have obligations to fulfil their duties towards their users and the public at national and international level.
– Service providers. Third-party service providers need to enforce security measures to ensure their services are delivered to end users through operators' networks and to protect their own business information from leaking to malicious users.
– End users/subscribers. When accepting the offered services, the end users/subscribers should ensure data confidentiality (ensure privacy protection as well as service availability).

7 Security objectives

Security objectives are the ultimate security goal for providing information services from telecommunication operators. Here the primary concerns are in which security requirements should be met rather than on how security is enforced. The security objectives for the information services provided by telecommunication operators are:

– Only legitimate users should be able to access the information services provided by the telecommunication operators; on the other hand, users should use the service legitimately and abide by service requirements.
– Operators or third-party service providers should provide privacy protection for subscribers and service users.
– In order to ensure service availability and business continuity, operators should provide protection against unsolicited access and ensure a secure delivery of services.
– Manageability and controllability should be provided to the extent that upon encountering security incidents, either normal state can be restored or damage can be minimized.
– The security measures should not compromise essential quality of service; they should be considered comprehensively including performance, service availability, upgrading and costs.
– Only authorized operators, service providers and users may have access to their prescribed scope of security-related information.

8 Security requirements

Security requirements aim to meet security objectives. They should address the following issues:

– Confidentiality (confidentiality of stored and transferred information);
– Data integrity (protection of stored and transferred information);
– System integrity (protection of the operating platform);
– Accountability (all actions should be documented and should be accounted for by their initiators);
– Availability (all legitimate users should be able to correctly access the services); and
– Recoverability and manageability (any security violations should be handled to ensure that the system or the services can be restored to their normal state).

8.1 Security requirements of traditional telecommunication services

As people's needs change and services evolve, new features and functions are added to traditional telecommunication services. This transformation brings new security issues as well as new security technologies to mitigate them. For example, as the traditional telephone directory service expands to personal and enterprise switchboards, operators are further required to protect the privacy of their users. In order to improve service convenience and quality of service (QoS), etc., new identity

recognition and authentication technologies (such as voice recognition via the phone, etc.) might be used. This example shows that even for the traditional telecommunication services, the expansion and transformation of services brings new security issues as well as new security technologies to mitigate them. Figure 3 shows a schematic model of telecommunication services provision.

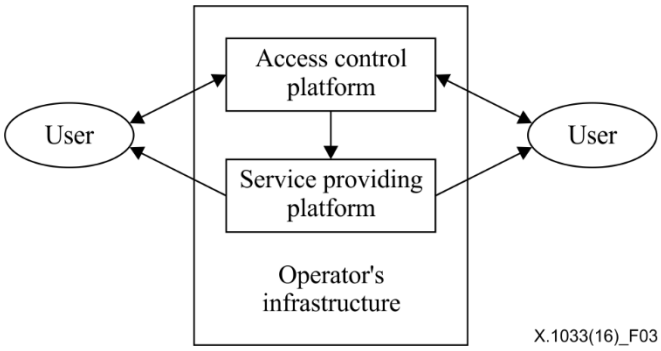

Figure 3 – Schematic model of telecommunication services provision

Under the classification of roles described in clause 6.5, these roles respectively bring forward security requirements for traditional telecommunication services as listed below.

8.1.1 Security requirements given by regulators

Security requirements of traditional telecommunication services given by regulators include:

– Recommend and/or supervise the enforcement of regulations based on the hierarchical importance of the traditional telecommunication services. Recommend and/or supervise the enforcement of security ratings and risk assessment to services and underlying infrastructures.

– The following capabilities should be provided: network security monitoring, network security incident announcement and emergency security coordination.

– Establish the rules to promote fair business competition between operators.

– Set the rules to prevent users from utilizing the traditional telecommunication services for illegal purposes.

8.1.2 Security requirements for operators

Security requirements of traditional telecommunication services for operators include:

– Maintain the infrastructures operating securely and steadily.

– Provide adequate authentication to prevent illegal users from accessing the services.

– Provide measures to prevent users from utilizing the services illegally.

– Ensure service availability and protect the services from malicious attacks.

– Ensure the capability of emergency recovery from disasters, attacks and other unexpected service breakdowns.

– Provide protection against unintended information leakage or intentional attacks.

8.1.3 Security requirements given by users

Security requirements of traditional telecommunication services given by users include:

– Have access to pre-authorized services without obstacles.

– User privacy information is protected from unintended leakage or intentional attacks.

8.2 Security requirements of content services

Content services provided by telecommunication operators are mainly related to the new types of/extended services that originate from the Internet, broadcasting and television, etc. These new types of/extended services include e-commerce, Internet searching, on-demand video and digital television terrestrial broadcasting, etc. that are transmitted via the telecommunication infrastructures. These new types of services/extended services relate to technologies including malicious/detrimental information reports, identity authentication, customer resource management (CRM) and access control, etc., and are also accompanied by new forms/types of security threats and associated new security requirements. Figure 4 shows a schematic model of third-party content service provision.

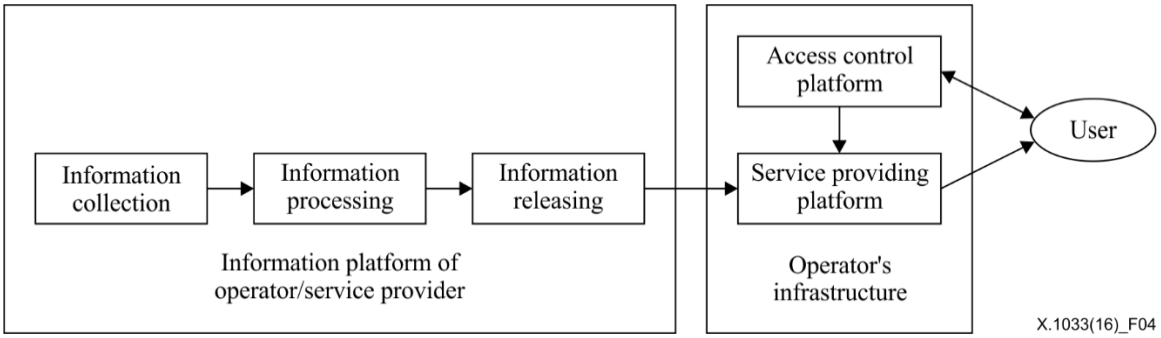

Figure 4 – Schematic model of third-party content service provision

8.2.1 Security requirements for regulators

Security requirements of content services for regulators include:

– Establish the rules to maintain fair business competition for operators and third-party service providers.

– Set the rules for service providers (operators and third-party service providers) to avoid publishing harmful content or services.

– Require providers (operators and third-party service providers) to provide the capability to control, when necessary, the spread of harmful content and/or other harmful behaviour utilizing the content services.

8.2.2 Security requirements for operators

Security requirements of content services for operators include:

– Maintain service availability, especially real-time service operational consistency.

– Ensure that service users are authorized.

– Ensure that users' operations are pre-authorized.

– Ensure that the outsourced third-party content services provided via the operator's systems and networks are authorized, controllable and clean from fake/illegal contents.

– Protect the services from malicious attacks (especially phishing attacks on personal data and properties).

– Have the ability to properly handle service interruptions, provide quick recovery and keep service operational consistency.

– Prevent information leakage either unintentionally or by attackers stealing the information.

8.2.3 Security requirements for third-party service providers

Security requirements of content services for third-party service providers include:

– Ensure that the provided content is delivered to clients correctly and ensure that the normal interactions between service providers and users are conducted according to the established norms.
– Protect information integrity and protect information from being tampered with or lost.
– Protect provided content from being illegally stolen or leaked.

8.2.4 Security requirements given by users

Security requirements of content services given by users include:

– Service availability and privacy are ensured.
– Stable service performance (especially for paid services) is provided.
– Personal information especially bank cards, passwords, home addresses and phone numbers are protected from unauthorized access or leakage.
– In cases of unexpected service breakdown, personal data can be recovered and restored and personal information leakage is prevented.

8.3 Security requirements of informationization services

If the operator provides an enterprise with informationization services such as an e-mail system, a telephone directory, data storage, an office automation system, intranet, information technology (IT) planning and consulting, etc., then the informationization service is, as a result, involved in the business processes of the enterprise as well as trade secrets and technical know-how of its customer(s). For this reason, the informationization services must be provided with security protection.

8.3.1 Security requirements for regulators

Security requirements of informationization services for regulators include:

– Set the rules to protect key information confidentiality, such as business information, technical information and so on.
– Establish the rules to maintain fair business competition among the different operators.

8.3.2 Security requirements for operators

Security requirements of informationization services for operators include:

– Maintain service availability to keep normal work or business activities.
– Ensure that the service users are authorised users; and ensure that the authorized users' operations are pre-authorised.
– Protect the services especially those of the financial sector from malicious attacks.
– Have the ability to properly handle service interruption; provide quick recovery and maintain service operational consistency.
– Prevent information leakage either unintentionally or by an attacker stealing the information.

8.3.3 Security requirements given by users

Security requirements of informationization services given by users include:

– Ensure service availability. Ensure that work or business processes run efficiently and continue to do so as expected.
– Ensure confidentiality. Maintain key information confidentiality such as geolocation, business information and technical information.
– Ensure service stability. Ensure that work or business processes are not disrupted by service breakdown in key process activities, especially for group users.

– Ensure instant service recovery based on the backup system especially for real-time services.
– Protect key information from unauthorized access or leakage.

8.4 Security coordination

The individual user is the basic unit of an individual information service. A group user consists of a number of basic units. Therefore, the security of an individual user information service should be harmonized with that of the group user information service; and the security policies applied for individual users and those applied for group users should be coordinated. The following mechanisms need to be considered:

– The security policies for individual users should be based on the security policies for the group users to which they belong. This means that the individual users should implement the security policies for the group users to which they belong. For example, individual employees are usually required to install the anti-virus software and update the software patches provided by their employing company.
– When the specific security requirements of an individual user are in conflict with the group security policies, a revision of the current situation has to be carried out in order to reach a new security resolution. In addition, all these activities have to be documented.
– When an individual of a group is attacked or has vulnerabilities, the group security administrator needs to be informed. The existing security measures should be adjusted and/or the new security measures should be implemented based on the whole group user environment.
– When a security exception occurs on an individual of a group, the individual needs first be isolated from the group network environment. He or she can then re-access the group network after security assessment and enforcement.
– The security policies should be stored and applied preferably on the server group or on the border of the group network, so that personal terminal loads can be reduced.

9 Security mechanism

In order to reduce the operational costs and enhance competitiveness, operators shall consider various service requirements and security issues comprehensively. For example, operators currently are trying to develop application recognition and user recognition technology; in other words, they are trying to capture the user's preferences and push more applications and services to the user. In this case, the operators have to find a balance between the ability to serve their customers and the protection of their privacy.

The existing security technologies of network and information systems are mainly applied to devices, networks and services to meet security requirements such as access control, confidentiality, availability, data integrity and authentication. From the viewpoint of the information service, the main concern is the users. All users are different and ideally, they should be served differently/individually. The security elements such as encryption, identity authentication, logs, information filtering and privacy protection, should be regrouped and tailored to be a part of the information service. It is necessary to reconsider the mechanisms in accordance with the concrete devices, networks and services.

Table 1 gives some related security mechanisms for the different types of individual information services.

Table 1 – Related security mechanisms for the different types of individual information services

Security mechanism category	Security mechanism	Traditional telecommunication service	Content service	Informationization service
Rules and regulations	Set the rules to promote fair business competition	√	√	√
	Security rating and risk assessment	√	√	√
Data and system backup	History data backup for network crime tracing and digital evidence	User access related information	User behaviour such as financial transactions	
	Backup system (including network device, servers and data) for service recovery	√	√	√
Identity management	Identity authentication including password, digital certificate, short message service (SMS) verification code, biometrics identification (voice recognition, facial recognition, iris recognition, fingerprint identification)	Password, biometrics identification (mainly voice recognition)	Password, digital certificate, short message service (SMS) verification code	Password, biometrics identification (mainly facial recognition, iris recognition, fingerprint identification)
	Role-based access control	√	√	√
Data security management	Data encryption, including database encryption, and transferred data encryption	Identity information encryption	Identity information encryption, service related personal information encryption	Mainly encryption on business information, technical information and government information
	Data integrity check	√	√	√
Malicious attack prevention	Enterprise version of anti-virus software or anti-spam software			√
	Terminal monitoring and control for group users			√
	Client anti-virus software	√	√	√
	Server-based intrusion detection system	√	√	√
	Risk assessment and safety reinforcement	√	√	√

Table 1 – Related security mechanisms for the different types of individual information services

Security mechanism category	Security mechanism	Traditional telecommunication service	Content service	Informationization service
	Operator network based firewall and anti-virus software	√	√	

Bibliography

[b-ITU-T I.112] Recommendation ITU-T I.112 (1993), *Vocabulary of terms for ISDNs*.

[b-ITU-T Q.956.3] Recommendation ITU-T Q.956.3 (1995), *Integrated services digital network (ISDN) – Stage 3 description for charging supplementary services using DSS 1: Clause 3 – Reverse charging*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
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	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
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 and next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2016