International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1145

(05/2017)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services – Web security

Security framework and requirements for open capabilities of telecommunication services

Recommendation ITU-T X.1145

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
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1379
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.1145

Security framework and requirements for open capabilities of telecommunication services

Summary

Recommendation ITU-T X.1145 focuses on an analysis of the security requirements of open capabilities of telecommunication services and provides a security framework.

Currently, due to the boom in over-the-top (OTT) services in the information communication technology (ICT) domain, operators need to explore innovative ways to cooperate with third-party service providers and especially with information technology (IT) service providers in order to avoid the traffic growth associated with such services without the commensurate income increases. Open capabilities of telecommunication services can bridge the operators' telecommunication services capabilities and the third-party service providers' customized service requirements, thus becoming a win-win cooperation paradigm.

As the core asset for operators, capabilities of telecommunication services should be opened in a secure way and be fully protected, as both operators' business security and users' information security are implicated. Without a comprehensive security mechanism, an unsecure/spiteful application/service from a third-party service provider using the capabilities of telecommunication services may harm the operators' transmission network, business system and even users' personally identifiable information (PII). Consequently, to offer secure telecommunication service capabilities to cooperative service providers, the security requirements for open capabilities of telecommunication services need to be analysed exhaustively and an overall security framework needs to be established.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T X.1145	2017-05-14	17	11.1002/1000/13260

Keywords

Open capability, security framework, telecommunication service.

[*] 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.1145

Security framework and requirements for open capabilities of telecommunication services

1 Scope

This Recommendation provides a security framework and requirements for open capabilities of telecommunication services. This Recommendation analyses the challenges brought forward by open capabilities of telecommunication services and identifies hence the specific security requirements for the operators. These security requirements specified together form a security framework for operators to manage the security of open capabilities of their telecommunication services. The purpose of this Recommendation is to safeguard operators' capabilities of telecommunication services and the business paradigm of open capabilities of telecommunication services, to protect operators' telecommunication systems and to enhance user experience.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 access control [b-ITU-T X.800]: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

3.1.2 authentication information [b-ITU-T X.800]: Information used to establish the validity of a claimed identity.

3.1.3 authentication exchange [b-ITU-T X.800]: A mechanism intended to ensure the identity of an entity by means of information exchange.

3.1.4 authorization [b-ITU-T X.800]: The granting of rights, which includes the granting of access based on access rights.

3.1.5 availability [b-ITU-T X.800]: The property of being accessible and useable upon demand by an authorized entity.

3.1.6 cryptography [b-ITU-T X.800]: The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use.

NOTE – Cryptography determines the methods used in encipherment and decipherment. An attack on a cryptographic principle, means, or method is cryptanalysis.

3.1.7 encipherment [b-ITU-T X.800]: The cryptographic transformation of data (see cryptography) to produce ciphertext.

NOTE – Encipherment may be irreversible, in which case the corresponding decipherment process cannot feasibly be performed.

3.1.8 key [b-ITU-T X.800]: A sequence of symbols that controls the operations of encipherment and decipherment.

3.1.9 personally identifiable information (PII) [b-ITU-T X.1252]: Any information a) that identifies or can be used to identify, contact, or locate the person to whom such information pertains; b) from which identification or contact information of an individual person can be derived; or c) that is or can be linked to a natural person directly or indirectly.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 authentication: A short form of the term 'authentication exchange' defined as in clause 3.1.3 above.

3.2.2 capability: An ability that a system or an equipment provides for offering a service.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DDoS	Distributed Denial-of-Service
DoS	Denial of Service
ICT	Information Communication Technology
IT	Information Technology
OCTS	Open Capabilities of Telecommunication Services
OSI	Open Systems Interconnection
OTT	Over-The-Top
PII	Personally Identifiable Information

5 Conventions

None.

6 Overview

Due to network evolution and communication technology development, applications and services in the telecommunication domain increasingly contain more and more diverse technologies. Along with the enhancing of communication device capabilities and the boom in applications and services, users' usage requirements are becoming more varied.

To respond to this over-the-top (OTT) services boom in the domain of information communication technology (ICT) and to satisfy users' requirements, operators are exploring the open capabilities of telecommunication services as an innovative business paradigm. Moreover, telecommunication operators own and provide competitive resources and service capabilities for the over-the-top services which can be categorized as follows:

- network capability: enables operators to assign and dynamically adjust specific network resources based on users' requirements;
- business capability: enables operators to assign specific business resources;
- cooperation capability: enables operators to offer platforms or interfaces to business partners to create innovation businesses.

6.1 General model of open capabilities of telecommunication services

The general model of open capabilities of telecommunication services (OCTS) is shown in Figure 1.

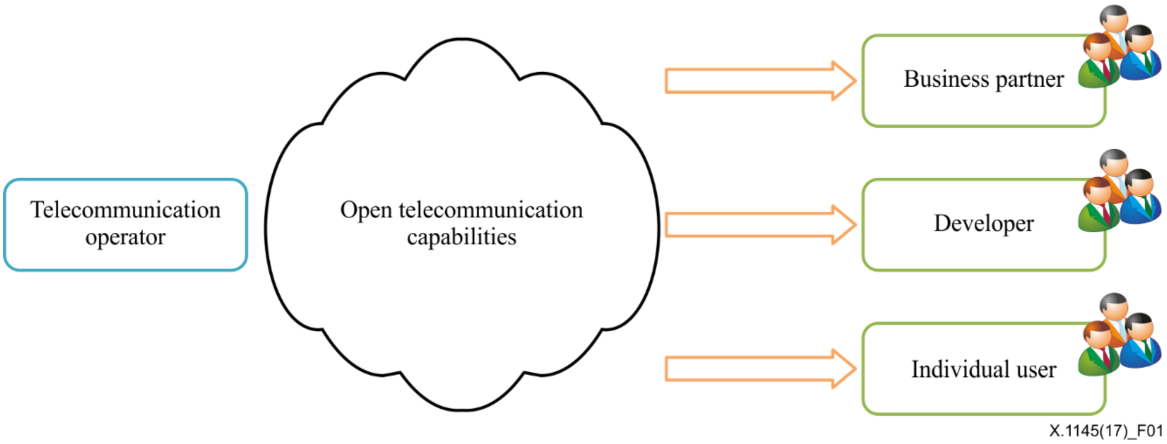
Telecommunication operator
Open telecommunication capabilities
Business partner
Developer
Individual user
X.1145(17)_F01

Figure 1 – General model of OCTS

There are four entities in the OCTS model: 1) the telecommunication operator, 2) the business partner, 3) the developer, and 4) the individual user.

The telecommunication operator offers open capabilities to the business partner, the developer and the individual user.

The business partner generally has its own business rather than an offered telecommunication service, such as an electronic payment service or online education service. The business partner cooperates with the telecommunication operator that uses the open telecommunication capabilities to enhance its customized services. For example, an electronic payment service provider uses the open short message capability that sends a real-time message to remind a customer about the details of an online payment.

The developer generally uses the open capabilities through the open platform or interfaces that are offered by the operator to develop new applications.

The individual user generally uses the open network capability to get personalized services, such as obtaining high network bandwidth during off-work time for their personal mobile devices compared to lower network bandwidth during work time.

6.2 Open capabilities categorization

Open capabilities of telecommunication services can be abstracted into the three categories: network capability, business capability, and cooperation capability. An overview of open capabilities is shown in Figure 2.

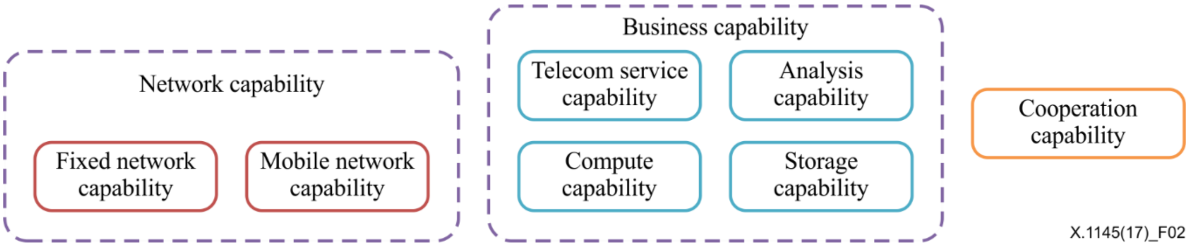

Figure 2 – Overview of open capabilities

Network capability is composed of the fixed network capability that offers Internet access/line telephone services and the mobile network capability that offers mobile telecommunication services.

Business capability implies the specific business capabilities based on an operator's network and information assets, such as computation capability, storage capability, analysis capability and telecommunication service capability. For example, the operator usually has its own data centre which is composed of large scale servers, storage devices and so on. The operator can offer computation capability and storage capability to third-party service providers by using its servers and information technology (IT) devices in the data centre. The operator can offer analysis on the network traffic information through its analysis capability and can then provide the analysis result to the Internet service providers to enhance their quality of service. In addition, the operator can offer a telecommunication service capability, e.g., short message service, to an e-business service provider to remind customers about their online order status.

Cooperation capability is based on the network capability and business capability. The operator cooperates with a third-party service provider to create new paradigm services. For example, an operator cooperates with a business bank to innovate online payment services.

7 Security threats to open capabilities of telecommunication service

7.1 Disclosure of personally identifiable information

During open telecommunication capability usage, attackers may impersonate a legal entity that has an opportunity to get personally identifiable information (PII) from an operator's assets.

7.2 Modification of capability usage

This occurs when an unauthorized entity inserts, changes or deletes a capability usage privilege. The unauthorized entity could be a person, a program or a device. These attacks occur when an attacker adds data to an existing connection with the open capability usage for the purpose of hijacking the connection or maliciously sending configuration data. This can result in a denial of service (DoS) attack and/or avoidance of charges for using open capabilities.

7.3 Relationship of security threats to OCTS model

Security threats appear in particular places of the open capabilities of telecommunication services model. The relationship of security threats and functional entities in models is shown in Table 1.

In Table 1, the letter "Y" (Yes) in each cell indicates that the entity is related to a particular security threat.

Table 1 – Relationship of security threats to OCTS model

Threats / Entities	Unauthorized access	Modification of capability usage	Trojan/virus	Disclosure of personally identifiable information (PII)
Telecommunication operator	Y	Y	Y	Y
Business partner			Y	
The developer			Y	
Individual user			Y	Y
Entity between telecommunication operator and the business partner	Y	Y	Y	Y
Entity between telecommunication operator and the developer	Y	Y	Y	Y
Entity between telecommunication operator and the individual user	Y	Y	Y	Y

7.4 Trojan and virus attacks

An attack occurs when a malicious developer or attacker impersonates a legal developer and injects Trojans or viruses into the new application or service. These threats may be implemented by using application software bugs or operating system bugs to achieve the attack.

7.5 Unauthorized access

An unauthorized access threat occurs when an illegal entity, such as a business partner or developer, gains access to open telecommunication resources or services by masquerading as an authorized entity.

8 Security requirements for open capabilities of telecommunication services

As the core asset of the operators, telecommunication service capability should be opened through a secure way. Without a comprehensive security mechanism, an unsecure and spiteful application/service from a business partner or developer using telecommunication service capability may harm the operator's transmission network, business system and even users' information.

This clause and its subclauses analyse the security requirements for open capabilities of telecommunication services with consideration of their characteristics.

8.1 Access control

Access control is required to ensure that only authorized users or business partners are allowed to access appropriate open telecommunication resources or services.

8.2 Authentication

Authentication is required to confirm the identities of the entities. Authentication ensures the validity of the claimed identities of the entities participating in an open capability of a telecommunication service and provides assurance that an entity is not attempting to masquerade as an authorized entity. Authentication techniques may be required as part of access control.

8.3 Business isolation

Business isolation is required to isolate the open capability of a telecommunication service from other telecommunication resources. Business isolation ensures that non-open telecommunication capabilities will not be disclosed to the operator's subscribers or business partners. Data mirror technology may be required as a part of business isolation.

8.4 Emergency response for virus/DDoS

Emergency response for virus/distributed denial-of-service (DDoS) is required to pre-deploy security mechanisms in response to and to deal with a virus or DDoS attack in time.

8.5 Innovation business security test before online usage

Innovation business security test before online usage is required to test the security of an innovation business/application before its commercial online usage. It tests the vulnerability and malicious code for innovation business, to prevent the application of potentially insecure innovation business.

8.6 Personally identifiable information protection

As the telecommunication service capability is open, mechanisms should be deployed to protect users' PII and to prevent un-authorized access and disclosure of PII.

8.7 Physical network capability security

Physical network capability security is required to ensure physical network capability and resource availability and integrity.

8.8 Secure audit

Secure audit is required to audit the user's behaviour when using an open capability of a telecommunication resource or service. Secure audit collects and makes available necessary evidential information related to the operation and use of any telecommunication service with open capability.

8.9 Virtual network capability security

Virtual network capability security is required to ensure virtual network capability and resource availability and integrity.

8.10 Relationship between security requirements and security threats

Each security requirement is a countermeasure against certain security threats. The relationship between security requirements and security threats is shown in Table 2.

In Table 2, the letter "Y" (Yes) in each cell indicates that the security requirement is related to a particular security threat.

Table 2 – Relationship between security requirements and security threats

Threats Requirements	Unauthorized access	Modification of capability usage	Trojan/virus	Disclosure of personally identifiable information
Business isolation	Y		Y	Y
Access control	Y	Y		
Authentication	Y			Y
Secure audit	Y	Y	Y	Y
Emergency response for virus/DDoS			Y	
Innovation business security test before online	Y	Y	Y	Y
Physical network capability security	Y		Y	
Virtual network capability security	Y		Y	
Personally identifiable information protection	Y			Y

9 Security functions for open capabilities of telecommunication services

This clause describes some of the security functions that may be used to meet security requirements for an open telecommunication service capability, as follows:

– access control;

– authentication;

– digital signature;

– encipherment;

– event detection;

– key exchange;

– security audit trail; and

– security recovery.

9.1 Access control

The access control function may use the authenticated identity of a user or information about the user (such as membership within a known set of users) or the capabilities of the user, to determine and enforce the access rights of the same. If the user attempts to use an unauthorized resource or an authorized resource with an improper type of access, then the access control function will reject the attempt and may additionally report the incident for the purposes of generating an alarm or recording it as part of a security audit trail.

The access control function may be based on the use of the following items:

- access control information bases, where the access rights of peer entities are maintained in a database;
- authentication information, such as passwords, the possession and subsequent presentation of which is evidence of the accessing user's authorization;
- capabilities, the possession and subsequent presentation of which is evidence of the right to access the user or resource defined by the capability;
- security labels, which, when associated with a user, may be used to grant or deny access, usually according to a security policy;
- time of attempted access;
- route of attempted access;
- duration of access; and
- physical location of attempted access.

The access control function may be applied to the individual user, the developer and the business partner.

9.2 Authentication

Some security technologies that may be applied include:

- the use of authentication information, such as passwords supplied by a sending user and checked by the receiving user;
- cryptographic technologies; and
- the use of characteristics or possessions of the user.

The authentication function may be incorporated to provide communicating user authentication. If the function does not succeed in authenticating the user, this will result in rejection or termination of the connection and may cause a user to show up on the security audit trail and/or a report to a security management centre.

When cryptographic techniques are used, they may be combined with "handshaking" protocols to protect against replay (i.e., to ensure liveness).

The choices of security technologies, which are used to realize authentication, will depend upon the circumstances in which they need to be used, alongside:

- timestamping and synchronized clocks;
- two- and three-way handshakes (for unilateral and mutual authentication respectively); and
- non-repudiation functions achieved by digital signature or notarization mechanisms.

9.3 Digital signature

The digital signature function defines two processes:

1) signing data; and
2) verifying the signed data.

The first process uses information that is private (i.e., unique and confidential) to the signatory. The second process uses procedures and information which are publicly available, but from which the signatory's private information cannot be deduced.

The signing process involves either an encipherment of the data or the production of a cryptographic check value of the data, using the signatory's private information as a private key.

The verification process involves the use of public procedures and information to determine whether the signature was produced correctly with the signatory's private information.

The essential characteristic of the signature function is the fact that the signature can only be produced using the signatory's private information. Thus, when the signature is verified, it can subsequently be proven to a third-party (e.g., a judge or arbitrator) at any time that only the unique holder of the private information could have produced the signature.

Due to the diversity of the applications and the services explored over OCTS, the digital signature algorithms may be different when this function is implemented.

9.4 Encipherment

The encipherment function can ensure the confidentiality of either communication data or stored data. Encipherment algorithms may be reversible or irreversible. There are two general classifications of reversible encipherment algorithms:

1) symmetric (i.e., secret key) encipherment, in which knowledge of the encipherment key implies knowledge of the decipherment key and vice versa; and

2) asymmetric (e.g., public key) encipherment, in which knowledge of the encipherment key does not imply knowledge of the decipherment key, or vice versa. The two keys of such a system are sometimes referred to as the "public key" and the "private key".

Irreversible encipherment algorithms may or may not use a key. When they use a key, this key may be public or secret. In the OCTS scenarios, the entities that use the open capabilities are various, therefore the choice of encipherment algorithms may be flexible.

9.5 Event detection

Security-relevant event detection includes the detection of apparent violations of security and may also include detection of "normal" events, such as a successful access (or log on). Security-relevant events may be detected by entities within open systems interconnection (OSI) including security mechanisms. The specification of what constitutes an event is maintained by event handling management. Detection of various security-relevant events may, for example, cause one or more of the following actions:

- local reporting of the event;
- remote reporting the event;
- logging the event; and
- recovery action.

Examples of such security-relevant events are:

- a specific security violation;
- a specific selected event; and
- an overflow on a count of a number of occurrences.

Standardization in this field will take into consideration the transmission of relevant information for event reporting and event logging and the syntactic and semantic definition to be used for the transmission of event reporting and event logging.

In the OCTS scenarios, the event detection function could help to detect the security violations of the open capability usage among the individual user, the developer and the business partner.

9.6 Key exchange

The key exchange function allows for key sharing in encipherment implementations, especially that of the symmetric encipherment algorithm.

9.7 Security audit trail

Security audit trails provide a valuable security mechanism as potentially they permit detection and investigation of breaches of security by permitting a subsequent security audit. A security audit is an independent review and examination of system records and activities to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to aid in damage assessment and to recommend any indicated changes in controls, policy and procedures. A security audit requires the recording of security-relevant information in a security audit trail and the analysis and reporting of information from the security audit trail. The logging or recording is considered to be a security mechanism and so is described in this clause. The analysis and report generation is considered a security management function.

Collection of security audit trail information may be adapted to various requirements by specifying the kind of security-relevant events to be recorded (e.g., apparent security violations or completion of successful operations).

The known existence of a security audit trail may serve as a deterrent to some potential sources of security attacks.

OSI security audit trail considerations take into account what information shall optionally be logged, under what conditions that information shall be logged and the syntactic and semantic definition to be used for the interchange of the security audit trail information.

This function could be used to audit the behaviour of the individual user, the developer and the business partner when using an open capability of telecommunication resources and services.

9.8 Security recovery

Security recovery deals with requests from mechanisms such as event handling and management functions and takes recovery actions as the result of applying a set of rules. These recovery actions may be of three kinds:

1) immediate: the system should be recovered as soon as possible, commonly within one day;
2) temporary: the system needs to be recovered within a few days, such as a week;
3) long-term: it would take a relatively longer time to recover the system, such as a month.

This function could be used for recovery of the operators' assets such as system, software, hardware, and business capability, when they are attacked by an attacker or malicious user.

9.9 Relationship between security functions and security requirements

The security functions listed and described in clause 9 are used to satisfy some of the security requirements. The mapping of security functions to security requirements is shown in Table 3.

In Table 3, the symbol "√" in each cell indicates that the security requirement is related to a particular security function. More precisely, the marked security requirement should be supported by the implementation of the marked function.

Table 3 – Relationship between security requirements and security functions

Functions Requirements	Encipher ment	Key exchange	Digital signature	Access control	Authen-tication exchanges	Event detection	Security audit trail	Security recovery
Business isolation	√	√		√				
Access control				√	√			
Authentication	√	√	√		√			
Secure audit							√	
Emergency response for virus/DDoS						√		√
Innovation business security test before online						√		
Physical network capability security				√			√	√
Virtual network capability security				√			√	√
Personally identifiable information protection	√	√	√	√	√			

Bibliography

[b-ITU-T X.800]	Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.
[b-ITU-T X.1033]	Recommendation ITU-T X.1033 (2016), *Guidelines on security of individual information services provided by operators*.
[b-ITU-T X.1252]	Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.
[b-ITU-T X-Sup.2]	Recommendation ITU-T X.800-X.849 series (2007), *Supplement on security baseline for network operators*.

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