International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1550

(03/2017)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cybersecurity information exchange – Exchange of policies

Access control models for incident exchange networks

Recommendation ITU-T X.1550

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

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

Recommendation ITU-T X.1550

Access control models for incident exchange networks

Summary

Recommendation ITU-T X.1550 introduces existing approaches for implementing access control policies for incident exchange networks. This Recommendation introduces a variety of well-established access control models, sharing models as well as criteria for evaluating incident exchange network performance. Standards-based solutions are considered to facilitate implementation of different access control models within different cybersecurity information-sharing models and under diverse trust environments.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1550	2017-03-30	17	11.1002/1000/13198

Keywords

Access control, authorization, CERT, CSIRT, CYBEX, IAM, incident exchange network, incident response.

* 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.1550

Access control models for incident exchange networks

1 Scope

This Recommendation introduces existing approaches for implementing access control policies for computer incident exchange networks. This Recommendation introduces a variety of well-established access control models, sharing models as well as criteria for evaluating incident exchange network performance. Standards-based solutions are considered to facilitate implementation of different access control models within different sharing models and under diverse trust environments.

2 References

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

[ITU-T X.1500] Recommendation ITU-T X.1500 (2011), *Overview of cybersecurity information exchange*.

[ITU-T X.1570] Recommendation ITU-T X.1570 (2011), *Discovery mechanisms in the exchange of cybersecurity information*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 access control [b-ITU-T X.1252]: A procedure used to determine if an entity should be granted access to resources, facilities, services, or information based on pre-established rules and specific rights or authority associated with the requesting party.

3.1.2 authorization [b-ITU-T M.3345]: It presents how, and under what conditions, self-service management actors can use self-service functions and what self-service actions they are permitted to perform.

3.1.3 incidents exchange [ITU-T X.1570]: The transfer of cybersecurity information between two or more cybersecurity entities. This transfer may be uni-directional, bi-directional, or multi-directional, i.e., many-to-many.

NOTE – In this Recommendation, the term "incident exchange" is considered equivalent to "exchange".

3.1.4 trust domain [b-ITU-T M.3410]: A set of information and associated resources consisting of users, networks, data repositories, and applications that manipulate the data in those data repositories. Different trust domains may share the same physical components. Also, a single trust domain may employ various levels of trust, depending on what the users need to know and the sensitivity of the information and associated resources.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 access control policy conflict: It defines the actions of two rules contradicting each other. The entity implementing the policy will not be able to determine which action to perform.

NOTE: This definition is based on the definition given for 'policy conflict' in [b-ITU-T X.1036].

3.2.2 dynamic policy conflict resolution: Conflict resolution strategies applied at runtime.

3.2.3 incidents exchange networks: Generalization of cybersecurity information exchange (CYBEX) operational infrastructure based on centralized or federated management.

3.1.4 incidents information: Subset of cybersecurity information, structured information or knowledge concerning forensics related to incidents or events.

NOTE – This definition is based on the description given for "exchange (cybersecurity information)" in [b-ITU-T X.1570].

3.2.5 static policy conflict resolution: Conflict resolution strategies applied at the design stage.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ABAC	Attribute-Based Access Control
ACL	Access Control List
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
CYBEX	Cybersecurity information Exchange
DAC	Discretionary Access Control
IAM	Identity and Access Management
IODEF	Incident Object Description Exchange Format
IT	Information Technology
MAC	Mandatory Access Control
PBAC	Policy-Based Access Control
PDP	Policy Decision Point
PERMIS	Privilege and Role Management Infrastructure Standards
RAdAC	Risk-Adaptive Access Control
RBAC	Role-Based Access Control
RID	Real-time Inter-network Defense
RIDT	Real-time Inter-network Defense Transport
STIX	Structured Threat Information Expression
TAXII	Trusted Automated Exchange of Indicator Information
TBAC	Task-Based Access Control
TBAM	Task-Based Access Management
XACML	extensible Access Control Markup Language

XML extensible Markup Language

5 Conventions

In the context of this Recommendation, "access control" is considered as a generic mechanism supporting authorization procedures.

6 General overview

Risk mitigation may be required to decrease financial costs of mitigating computer attacks as well as to provide security assurance within an organization/collaboration or a service/system. Incident exchange networks operate to prevent or reduce risks associated with computer attacks. Cybersecurity incident exchange practices introduce a variety of information-sharing models that are implemented in centralized or federated environments. Incident information sharing is based on a level of trust that correlates with associated risks and imposes the need to assure that confidential or sensitive information is not inappropriately shared. This makes some access control models more effective than others in terms of performance, implementation and security assurance.

The overall growth and mutual integration of global information systems has encouraged the development of advanced access control models that underlie authorization processes. Existing access control policy languages facilitate deployment of security policies and introduces challenges specific to different access control models and operating environments.

Mechanisms and approaches presented in this Recommendations may be used as profiles that provide access control policies implementation for underlying cybersecurity information exchange (CYBEX)-formats and transport protocols such as: incident object description exchange format (IODEF) [b-ITU-T X.1541], real-time inter-network defense (RID) [b-ITU-T X.1580] + real-time inter-network defense transport (RIDT) [b-ITU-T X.1581], structured threat information expression (STIX) [b-stix]+ trusted automated exchange of indicator information (TAXII) [b-taxii] and others.

7 Incident exchange network taxonomy

7.1 Operating environments

Incident exchange networks operate in the following environments:

– Single trust domain (centralized management);

– Federated trust domains (decentralized management).

7.2 Incidents information exchange models

Incident information exchange models are represented as follows:

– "Peer-to-peer", uni- or bi-directional exchange of information between two participants.

– "Hub-spokes". This type of model often has a central hub that receives data from the participating members (i.e., spokes). Either the hub can redistribute the incoming data directly to other members, or it can provide value-added services and send the new (and presumably more useful) information to the members. With this approach, the hub acts as a clearinghouse that can facilitate information sharing while protecting the identities of the members. A related challenge is that sharing information in this model requires a high degree of trust in the hub [b-MITRE Models].

– "Post-to-all". This model enables any participant to share with the entire membership roster, rather than going through a central hub. Because members share directly with one another, information dissemination is quick and can be easily scaled to many participants. [b-MITRE Models].

Based on these three models the following service-oriented models may be constructed:

– "Discovery-request-response". This is a two-stage model, where at the first stage (optional) discovery mechanisms [ITU-T X.1570] shall be used to identify centralized or distributed sources of incidents-related information. At the second stage consumers acquire information by querying databases; response decisions are based on access control model.
– "Discovery-subscription-notification". This is a two-stage model, where at the first stage (optional) discovery mechanisms [ITU-T X.1570] shall be used to identify centralized or distributed sources of incidents-related information. At the second stage consumers acquire data by subscribing and receiving information from selected sources in the form of notifications.

7.3 Access control models

Access control models are the basis of security policy. In practice, they are formalized by specific extensible markup language (XML)-dialects (access control policy languages).

As per [b-NIST Models], the following access control models are presented starting from conservative models (considering less granular policies) to adaptive models (considering more granular and environment-dependent policies):

– **ACL/DAC**. The concept of access control lists (ACLs)/discretionary access control (DAC) is one where each resource on a system to which access should be controlled, referred to as an object, has its own associated list of mappings between the set of entities requesting access to the resource and the set of actions that each entity can take on the resource.
– **MAC**. The mandatory access control (MAC) is most often used in systems where priority is placed on data confidentiality. MAC works by assigning a classification label to each file resource. Classifications include a category of information and a sensitivity level, for example: confidential, secret or top secret. Each subject is assigned a similar classification, called a clearance. When a subject tries to access a specific resource, the system checks the subject's privileges to determine whether access will be granted, as well as compares the clearance of the subject against the classification of the resource.
– **RBAC**. In role-based access control (RBAC) access to a resource is determined based on the relationship between the requester and the organization or owner in control of the resource; the requester's role or function will determine whether access will be granted or denied.
– **TBAC/TBAM**. Task-based access control (TBAC)/task-based access management (TBAM) [b-IEEE TBAC] is an extension of RBAC based on defining business tasks which allow finer granularity for access control.
– **ABAC**. The attribute-based access control (ABAC) model employs mechanisms such as ACLs which contain the attributes of those subjects together with the operations allowed on that resource. When an attribute matches the one held in the ACL, the subject is given the privilege to perform on the resource the operations mentioned for that attribute in the ACL.
– **PBAC**. Policy-based access control (PBAC) is a harmonization and standardization of the ABAC model at an enterprise level in support of specific governance objectives. PBAC combines attributes from the resource, the environment, and the requester with information on the particular set of circumstances under which the access request is made, and uses rule sets that specify whether the access is allowed under organizational policy for those attributes under those circumstances.
– **RAdAC**. The risk-adaptive access control (RAdAC) model was devised to bring real-time, adaptable, risk-aware access control. It extends other earlier access control models by introducing environmental conditions and risk levels into the access control decision process. It combines information about a person's (or a machine's) trustworthiness, information about the corporate information technology (IT) infrastructure, and environmental risk factors, and

uses all of this information to create an overall quantifiable risk metric. RAdAC also uses situational factors as input for the decision-making process. These situational inputs could include information on the current threat level an organization faces based on data gathered from other sources, such as computer emergency response teams (CERTs), computer security incident response teams (CSIRTs) or security vendors. (See [b-IEEE ARES], [b-NIST RADAC].)

7.4 Trust level

In order to emphasize the dependence between trust levels and risks, the following quantitative levels of trust in incidents exchange networks are recommended: **low**, **medium**, **high**. It is naturally implied that the higher the level of trust, the simpler the requirements and granularity for access control. That is, the level of trust directly influences the level of complexity for access control mechanisms.

Techniques for evaluating quantitative and qualitative levels of trust are outside the scope of this Recommendation.

The following correlation between trust levels and sharing models is considered:

– "Post-to-all" model usually requires a **high** degree of trust among participants.

– "Hub-spokes" model usually requires a high or medium (since "hub" may filter information) level of trust.

– "Peer-to-peer" model, in general, may not require a high degree of trust since the single communication channel can be controlled by diverse variety of methods.

Higher-level sharing models do not explicitly depend on degree of trust, but for an increasing number of participants and in presence of more complex environments, these models may require more advanced access control models.

Thereby, the following taxonomy, shown in Figure 1, is considered:

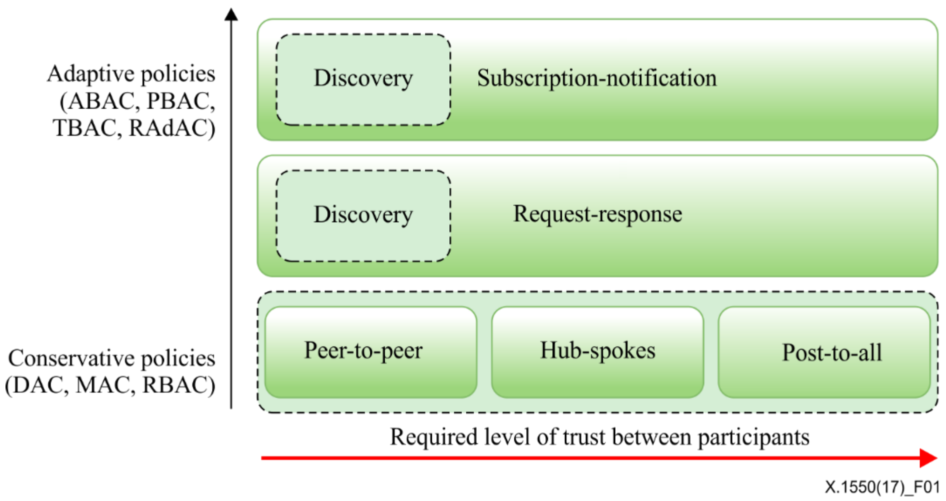

Figure 1 – Access control models, sharing models and trust level taxonomy

8 Facilitation techniques for implementation of access control policies

8.1 Recommendations on evaluating policy expression languages

Among well-established access control languages that are used to facilitate implementation of access control policies in identity and access management (IAM) systems there are:

– Extensible access control markup language (**XACML)**. This standard defines a declarative access control policy language (for ABAC model) implemented in markup language and a processing model describing how to evaluate access requests according to the rules defined in policies.

NOTE 1 – XACML 2.0 has been adopted as [b-ITU-T X.1142].

NOTE 2 – XACML 3.0 has been adopted as [b-ITU-T X.1144].

– Privilege and role management infrastructure standards (**PERMIS)** is a sophisticated policy-based authorization system that implements an enhanced version of RBAC (similar to ABAC). The PERMIS policy is XML-based and provides XACML interface which allows PERMIS and XACML policy decision points (PDPs) to be seamlessly interchanged.

It is recommended to evaluate the applicability of access control models under various environments and to determine minimal requirements for implementing them with policy languages such as [b-ITU-T X.1142], [b-ITU-T X.1144] or [b-UKENT PERMIS].

An example evaluation is provided in Table 1:

Table 1 – Implementation of access control models under various environments in policy definition languages

Model/ environment	ACL/ DAC	MAC	RBAC	ABAC	TBAC/ TBAM	PBAC	RAdAC
Centralized	[b-ITU-T X.1142]; PERMIS	Experimental XACML	[b-ITU-T X.1142]; PERMIS	[b-ITU-T X.1142]; PERMIS*	Experimental	[b-ITU-T X.1142]; PERMIS*	[b-ITU-T X.1142]; PERMIS*
Federated	[b-ITU-T X.1144]; PERMIS	Experimental XACML	[b-ITU-T X.1144]; PERMIS	[b-ITU-T X.1144]; PERMIS*	Experimental	–	[b-ITU-T X.1144]

NOTE 1 – XACMLv2 [b-ITU-T X.1142] and XACMLv3 [b-ITU-T X.1144] are separated since "delegation", required for most federated environments, appeared in XACMLv3.

NOTE 2 – Known MAC implementations require XACML extension.

NOTE 3 – Currently TBAC/TBAM implementations require XACML extension which is considered experimental.

NOTE 4 – PBAC by definition is applicable only in centralized environments, federated environments may require usage of RAdAC.

NOTE 5 – When included with an asterisk, i.e., PERMIS*, some limitations for the PERMIS implementation of ABAC (and PBAC, RAdAC if these considered as an extended ABAC model) are indicated in [b-UKENT PERMIS].

8.2 Considerations on policy conflict resolution

Access control policy conflict results in contradicting actions of two or more policy rules. The basic mechanism for mitigating policy conflicts is unambiguous design of policy rules (*static conflict resolution*). Another approach is based on evaluation of policies in runtime (*dynamic conflict resolution*) [b-UKENT PERMIS].

While static conflict resolution for centralized systems is considered feasible [b-USB CONFLICT], [b-SPIIRAN POLICY] it may be challenging to achieve static resolution in a dynamic federated environment.

Basic static conflict resolution strategies feature:

– Deny-override. Conflicting rules are combined, action "deny" is preferred over "permit".

– Permit-override. Conflicting rules are combined, action "permit" is preferred over "deny".

– First-applicable. The first action among conflicting rules is executed.

Strategies [b-UKENT PERMIS] for dynamic policy conflict resolution feature algorithms for selecting appropriate static strategy with respect to current access request context.

It is recommended to evaluate conflict resolution strategies from the perspective of performance and compatibility with access control models under various environments.

Considering performance evaluation for *static policy* conflict resolution [b-IJCSIT XACML] combined with dynamic access control such as [b-FUSCAT RADAC], it is recommended to minimize the number of policies without breaking the security assurance level or utilize *dynamic policy* conflict resolution strategies.

An example evaluation is provided in Table 2:

Table 2 – Policy conflicts resolution for access control models under various environments

Model/ environment	**ACL/ DAC**	**MAC**	**RBAC**	**ABAC**	**TBAC/ TBAM**	**PBAC** (Note)	**RAdAC**
Centralized	Static	Static	Static	Static	Static	Static	Dynamic
Federated	Dynamic	Dynamic	Dynamic	Dynamic	Dynamic	–	Dynamic
NOTE – PBAC by definition is applicable only in centralized environments.							

8.3 Recommendations on performance evaluation

Although markup languages (such as [b-W3C XML], [b-ECMA JSON]) intend to be human-readable, significant amount of nested and advanced access rules may present a challenging task of profiling and debugging implemented policies.

Complex incidents sharing services in incidents exchange networks may imply the use of advanced access control models. Considering operation in federated environments this may degrade performance of incidents exchange networks, which results in security assurance issues.

For the purpose of assessment of quality/performance/compliance of policies, corresponding metrics may be calculated. Evaluation mechanisms of such metrics for incidents exchange networks are out of scope of this Recommendation. However, a set of criteria and indicators for such evaluation is recommended [b-KIT PERFIAM], [b-NIST METRICS]:

– **Response time**. Response time for IAM infrastructure components, information sharing components enables evaluation of basic performance metrics.

– **Wrong access control decisions**. Evaluating the number of wrong authentication or authorization decisions in tense situations provides information about the robustness of the underlying IAM architecture.

– **Trusted components**. Access control is a sensible task that requires a certain trust level between cooperating entities. Therefore, a metric that lists trusted components for an access control decision is helpful to determine possible data leakage.

– **Policy distribution**. Used to evaluate capabilities and performance of policy distribution in centralized or federated access control systems.

– **Ease of privilege assignments**. Determines the number of steps required to assign/change/remove/inherit a subject's or group's capabilities.

– **Quality of policy expression**. Determines whether access control could be defined via logical and programmable expressions.

– **Delegation capabilities**. Determines whether an access control system is capable of delegating privileges to subjects.

- **Policy combination and resolution**. Determines policy combination strategies that are used to resolve conflicts (if any).
- **Bypass**. Determines whether any components ignore access control policies.
- **Safety**. Determines safety enforcement capabilities, such as constraints for access control rules used to prevent privileges escalation.
- **Granularity**. Determines the level of granularity an access control system can control. This could reflect a set of subject's attributes that are evaluated during the access control process.
- **Authentication integration**. Determines whether an access control system is capable of integrating with authentication systems.

Bibliography

[b-ITU-T M.3345] Recommendation ITU-T M.3345 (2009), *Principles for self-service management*.

[b-ITU-T M.3410] Recommendation ITU-T M.3410 (2008), *Guidelines and requirements for security management systems to support telecommunications management*.

[b-ITU-T X.1036] Recommendation ITU-T X.1036 (2007), *Framework for creation, storage, distribution and enforcement of policies for network security*.

[b-ITU-T X.1142] Recommendation ITU-T X.1142 (2006), *eXtensible Access Control Markup Language (XACML 2.0)*.

[b-ITU-T X.1144] Recommendation ITU-T X.1144 (2013), *eXtensible Access Control Markup Language (XACML 3.0)*.

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.

[b-ITU-T X.1541] Recommendation ITU-T X.1541 (2012), *Incident object description exchange format*.

[b-ITU-T X.1580] Recommendation ITU-T X.1580 (2012), *Real-time inter-network defence*.

[b-ITU-T X.1581] Recommendation ITU-T X.1581 (2012), *Transport of real-time inter-network defence messages*.

[b-IEEE TBAC] IEEE IET Software (2008), *Types for task-based access control in workflow systems*.

[b-IEEE ARES] IEEE (2011), *Sixth International Conference on Availability, Reliability and Security (ARES), An Attribute Based Framework for Risk-Adaptive Access Control Models*.

[b-ECMA JSON] ECMA International (2013), *The JSON Data Interchange Format*.

[b-FUSCAT RADAC] Federal University of Santa Catarina (2014), *A Dynamic Risk-based Access Control Architecture for Cloud Computing*.

[b-IJCSIT XACML] International Journal of Computer Science and Information Technology (IJCSIT) (2010), *Design and evaluation of XACML conflict policies detection mechanism*.

[b-KIT PERFIAM] Karlsruhe Institute of Technology (2009), *Performance Evaluation of Identity and Access Management Systems in Federated Environments*.

[b-MITRE Models] The MITRE Corporation (2012), *Cyber Information-Sharing Models*.

[b-NIST METRICS] NIST Internal Report 7874 (2012), *Guidelines for Access Control System Evaluation Metrics*. [b-NIST Models] NIST Computer Security Division (2009), *A survey of access control models*.

[b-NIST RADAC] NIST Computer Security Division (2009), *Risk-adaptable access control (RAdAC)*.

[b-SPIIRAN POLICY] SPIIRAN (2006), *Conflict Detection and Resolution in Security Policies of Computer Networks*.

[b-stix] OASIS CTI TC (2017), *A structured language for cyber threat intelligence*.
<https://oasis-open.github.io/cti-documentation/>

[b-taxii] OASIS CTI TC (2017), *A transport mechanism for sharing cyber threat intelligence*. <https://oasis-open.github.io/cti-documentation/>

[b-UKENT PERMIS] The University of Kent (2013), *Adding privacy protection to policy based authorisation systems*.

[b-USB CONFLICT] IEEE First AESS European Conference on Satellite Telecommunications (ESTEL) (2012), *Conflict detection in security policies using Semantic Web technology*.

[b-W3C XML] W3C (1997), *Extensible Markup Language (XML)*.

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