Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N13949
Date:	2009-05-18
Replaces:	
Document Type:	Liaison Organization Contribution
Document Title:	Liaison statement from ITU-T SG 17 to JTC 1/SC 6 on the report of ITU-T Study Group 17 meeting, February 2009
Document Source:	ITU-T SG 17 Liaison Officer
Project Number:	
Document Status:	For report at the SC 6 Tokyo meeting.
Action ID:	FYI
Due Date:	
No. of Pages:	25

ISO/IEC JTC1/SC6 Secretariat Ms. Jooran Lee, KSA (on behalf of KATS)

Korea Technology Center #701-7 Yeoksam-dong, Gangnam-gu, Seoul, 135-513, Republic of Korea ;

Telephone: +82 2 6009 4808 ; Facsimile: +82 2 6009 4819 ; Email : jooran@kisi.or.kr

Source: ITU-T SG 17 Liaison Officer to JTC 1/SC 6 (Olivier Dubuisson)
Title: Report of February 2009 ITU-T Study Group 17 meeting

1. World Telecommunication Standardization Assembly

The World Telecommunication Standardization Assembly meets every four years. It is the highest decision making organ of ITU's Standardization Sector. It performs a strategic review of the sector, and renews its structure and management.

The last meeting was held in October 2008 in Johannesburg, South Africa.

WTSA08 revised (with slight modifications) Resolution 7 "*Collaboration with the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)*" (http://www.itu.int/publ/T-RES-T.7-2008/en).

3. Telecommunication Standardization Advisory Group

In view of the fact that the update to the guide for ITU-T and ISO/IEC JTC 1 cooperation (Annex A to Recommendation ITU-T A.23 | previously annex K of the JTC 1 directives) is planned for approval at the November 2010 meeting of JTC 1, the Telecommunication Standardization Advisory Group (TSAG) determined the revised text of ITU-T A.23 at its April 2009. The text is now under TAP (Traditional Approval Process) consultation among ITU Member States and is planned for approval at the February or March 2010 meeting of TSAG.

The draft revised text retains all the basic principles in the current guide while updating the text to take into account changes in both organizations since late 2001. The most significant changes are closer alignment of the JTC 1 procedures to those in common between ISO and IEC, reference to the revised procedures in the ITU-T and consideration of the common patent policy for ITU-T/ITU-R/ISO/IEC adopted in 2006.

3. Work achieved at the last meeting of SG 17

The first meeting of Study Group 17 in the current 2009-2012 ITU-T study period was held 11-20 February 2009 in Geneva, Switzerland.

The primary goals of this meeting were to:

- implement the decisions made at WTSA08;
- agree on a new structure for the study group; and
- progress and/or achieve work on the Recommendations assigned to Study Group 17.

During the SG 17 meeting, collaborative meetings with SC 6 were held as follows:

- Question 6/17 met collaboratively with SC 6/WG 7 to progress work on USN security;
- Question 11/17 met collaboratively with SC 6/WG 8 to progress work on Directory
- Question 12/17 met collaboratively with SC 6/WG 9 to progress work on ASN.1 and registration authorities.

It is worth noting that former Question 1/17 collaborative with SC 6/WG 7 on Multicast was transferred to Study Group 11.

4. Liaison officers from SG 17 to SC 6

This table provides the names and responsibilities for SG 17 Liaison officers to ISO/IEC JTC 1/SC 6 at agreed at the February 2009 meeting:

Entity	Position	Name
ISO/IEC JTC 1/SC 6 (Telecommunications and Information exchange between systems)	SG 17 Liaison officer SG 17 Liaison officer for USN security	Olivier Dubuisson (France Telecom Orange, France, Heung Youl Youm (SCH Univ., Korea)

It may be of interest to SC 6 to note that the Joint Coordination Activity on Identity Management (JCA-IdM) is continuing for the 2009-2012 study period. SC 6 is represented to this coordination activity by Byung-ho Ahn and John Larmouth.

5. Next meetings of SG 17

The provisional plans for the next meetings of Study Group 17 in 2009 and 2010 are:

- 16 – 25 September 2009 in Geneva;
- 7 – 16 April 2010 in Geneva;
- 27 October – 5 November 2010 in Geneva.

6. Annexes

Annex 1 gives the new ITU-T Study Group 17 structure;

Annex 2 gives the complete list of actions taken on Recommendations and Supplements at the closing plenary of SG 17.

Annex 3 gives the list of draft Recommendations (and their summary) that SG 17 is currently working on for approval in the 2009-2012 study period.

ANNEX 1

Study Group 17 structure for the 2009-2012 study period

WP 1/17, Network and information security:

Q.1/17	**Telecommunications systems security project**
Q.2/17	**Security architecture and framework**
Q.3/17	**Telecommunications information security management**
Q.4/17	**Cybersecurity**
Q.5/17	**Countering spam by technical means**

WP 2/17, Application security:

Q.6/17	**Security aspects of ubiquitous telecommunication services**
Q.7/17	**Secure application services**
Q.8/17	**Service oriented architecture security**
Q.9/17	**Telebiometrics**

WP 3/17, Identity management and languages:

Q.10/17	**Identity management architecture and mechanisms**
Q.11/17	**Directory services, Directory systems, and public-key/attribute certificates**
Q.12/17	**Abstract Syntax Notation One (ASN.1), Object Identifiers (OIDs) and associated registration**
Q.13/17	**Formal languages and telecommunication software**
Q.14/17	**Testing languages, methodologies and framework**
Q.15/17	**Open Systems Interconnection (OSI)**

ANNEX 2

Actions taken on Recommendations and Supplements at the 20 February 2009 SG 17 plenary

Recommendations approved (TAP – Resolution 1)

Q.	Recommendation	
	No.	**Title**
5	X.1242 (X.ssf)	Short message service (SMS) spam filtering system based on user-specified rules
6	X.1171 (X.nidsec-1)	Threats and requirements for protection of personally identifiable information in applications using tag-based identification
6	X.1191 (X.iptvsec-1)	Functional requirements and architecture for IPTV security aspects

Recommendations determined (TAP – Resolution 1)

Q.	Recommendation	
	No.	**Title**
10	X.1250 (X.idmreq)	Baseline capabilities for enhanced global identity management trust and interoperability
10	X.1251 (X.idif)	A framework for user control of digital identity

Supplements approved

Q.	Supplement	
	No.	**Title**
5	X.Sup6	Supplement 6 to X-series Recommendations - ITU-T X.1240 series: Supplement on countering spam and associated threats
10	X.Sup7	Supplement 7 to X-series Recommendations - ITU-T X.1250 series: Supplement on overview of identity management in the context of cybersecurity

ANNEX 3

Summaries for work items under development in Study Group 17

Q.	Acronym	Title	Equivalent e.g., ISO/IEC	Timing
2	X.1034 (revised)	Framework for extensible authentication protocol (EAP)-based authentication and key management in a data communication network		2010-04
2	X.gsiiso	Guidelines on security of the individual information service for operators		TBD
2	X.interfaces	Architecture of external interrelations for a telecommunication network security system		2009-09
3	X.isgf*	Information security governance framework	ISO/IEC 27014	2010-04
3	X.ismf	Information security management framework		2010-10
4	X.abnot*	Abnormal traffic detection and control guideline for telecommunication network		2011
4	X.bots*	Frameworks for botnet detection and response		2011
4	X.dexf*	Digital evidence exchange file format		2011
4	X.gopw*	Guideline on preventing malicious code spreading in a data communication network		2010
4	X.gpn*	Mechanism and procedure for distributing policies for network security		2011
4	X.sips*	Framework for countering cyber attacks in SIP-based services		2011
4	X.sisfreq*	Requirements for security information sharing framework		2010-10
4	X.tb-ucc*	Traceback use cases and capabilities		2010
5	X.fcsip*	Framework for countering IP multimedia spam		2009-09
5	X.ics*	Functions and interfaces for countering email spam sent by botnet		2010-10
5	X.tcs*	Technical means for countering spam		TBD
5	X.tcs-1*	Interactive countering spam gateway system		2009-09
5	X.tcs-2*	Technical means for countering VoIP spam		2010-10
6	X.iptvsec-2	Functional requirements and mechanisms for secure transcodable scheme of IPTV		2010-10
6	X.iptvsec-3	Key management framework for secure IPTV services		2010-10
6	X.iptvsec-4	Algorithm selection scheme for service and content protection (SCP) descrambling		2010-10
6	X.iptvsec-5	Service and content protection (SCP) interoperability scheme		2010-10
6	X.mcsec-1	Security requirement and framework for multicast communication		2010-10
6	X.msec-5	Security aspects of mobile multi-homed communications		2010-10

6	X.usnsec-1	Security framework for ubiquitous sensor network	ISO/IEC 29180	2011-1Q
6	X.usnsec-2	Ubiquitous sensor network (USN) middleware security guidelines		2010-10
6	X.usnsec-3	Secure routing mechanisms for wireless sensor network		2010-10
7	X.1141, Amd.1	Security Assertion Markup Language (SAML 2.0) - Amendment 1: Errata	OASIS SAML 2.0 errata	2009-09
7	X.1142, Amd.1	eXtensible Access Control Markup Language (XACML 2.0) - Amendment 1: Errata	OASIS XACML 2.0 errata	2009-09
7	X.p2p-3	Security requirements and mechanisms of peer-to-peer-based telecommunication network		2010-10
7	X.sap-3	Management framework for one time password based authentication service		2010-10
7	X.websec-4	Security framework for enhanced web based telecommunication services		2010-10
9	X.1081, Amd.1	The telebiometric multimodal model – A framework for the specification of security and safety aspects of telebiometrics - Amendment 1: Object identifier assignments under the Telebiometrics arc		2009-09
9	X.1081, Amd.2	The telebiometric multimodal model – A framework for the specification of security and safety aspects of telebiometrics - Amendment 2: Appendix V on information on hierarchies		2009-09
9	X.1082, Amd.1	Telebiometrics related to human physiology – Amendment 1: Object identifier assignments under the Telebiometrics arc	IEC 80000-14, Amd.1	2009-09
9	X.ott	Authentication framework with one-time telebiometric template		2011-3Q
9	X.th1	Telehealth and world-wide telemedicines – Generic telecommunications protocol		2010-04
9	X.th2*	Telebiometrics related to physics	ISO 80003-2	2010-04
9	X.th3*	Telebiometrics related to chemistry	ISO 80003-3	2010-04
9	X.th4*	Telebiometrics related to biology	IEC 80003-4	2010-04
9	X.th5*	Telebiometrics related to culturology	IEC 80003-5	2010-04
9	X.th6*	Telebiometrics related to psychology	IEC 80003-6	2010-04
9	X.tif	Integrated framework for telebiometric data protection in telehealth and worldwide telemedicines		2012-3Q
9	X.tpp-2	Telebiometrics protection procedures – Part 2: A guideline for data protection in multibiometric systems		2009-09
9	X.tsm-2	Telebiometrics system mechanism – Part 2: Protection profile for client terminals		2009-09
10	X.1250	Baseline capabilities for enhanced global identity management trust and interoperability		In TAP
10	X.1251	A framework for user control of digital identity		In TAP
10	X.eaa*	Information technology – Security techniques – Entity authentication assurance	ISO/IEC 29115	2010
10	X.EVcert*	Extended validation certificate	CA/Browser Forum EVcert specification	TBD

10	X.idmdef*	Baseline identity management terms and definitions		2009-09
10	X.idm-dm*	Common identity data model		2010
10	X.idm-ifa*	Framework architecture for interoperable identity management systems		2011
10	X.idmsg*	Security guidelines for identity management systems		2011
10	X.priva*	Criteria for assessing the level of protection for personally identifiable information in identity management		2011
10	X.rfpg*	Guideline on protection for personally identifiable information in RFID applications		2009-09
11	E.115, Amd.1	Computerized directory assistance, Amendment 1 – Support of E.115 capabilities		TBD
11	X.500-series, Amd.1	Information technology – The Directory – Amendment 1 – Communication support enhancement	ISO/IEC 9594-All Parts, Amd.1	TBD
11	X.500-series, Amd.2	Information technology – The Directory – Amendment 2 – Password policy support	ISO/IEC 9594-All Parts, Amd.2	TBD
12	X.oid-res	Object identifier resolution system	ISO/IEC 29168	TBD
13	X.901 (revised)	Information technology – Open distributed processing – Reference model: Overview	ISO/IEC 10746-1	TBD
13	X.902 (revised)	Information technology – Open distributed processing – Reference model: Foundations	ISO/IEC 10746-2	2009-09
13	X.903 (revised)	Information technology – Open distributed processing – Reference model: Architecture	ISO/IEC 10746-3	2009-09
13	X.904 (revised)	Information technology – Open distributed processing – Reference model: Architectural semantics	ISO/IEC 10746-4	TBD
13	X.906, Cor.1	Information technology – Open distributed processing - Use of UML for ODP system specification – Technical Corrigendum 1	ISO/IEC 19783-6, Cor.1	2009-09
13	X.uml-asn1	UML profile for ASN.1		TBD
13	Z.100 (revised)	Specification and description language: Overview of SDL-2008		2009-09
13	Z.101	Specification and description language: Basic SDL-2008		2009-09
13	Z.102	Specification and description language: Comprehensive SDL-2008		2009-09
13	Z.103	Specification and description language: Shorthand notation and annotation in SDL-2008		2009-09
13	Z.104 (revised)	Specification and description language: Data and action language in SDL-2008		2009-09
13	Z.105 (revised)	Specification and description language: SDL-2008 combined with ASN.1 modules		2009-09
13	Z.106 (revised)	Specification and description language: Common interchange format (CIF) for SDL-2008		2009-09
13	Z.109 (revised)	Specification and description language: SDL-2008 combined with UML		2009-09
13	Z.120 (revised)	Message sequence chart (MSC)		TBD
13	Z.120, Amd.1 (revised)	Message sequence chart (MSC) – Amendment 1: Appendix I, Application of MSCs		2009-09

13	Z.150 (revised)	User requirements notation (URN) – Language requirements and framework		TBD
13	Z.151 (revised)	User requirements notation (URN) – Language definition		TBD
13	Z.Imp100 (revised)	Specification and description language Implementers' Guide – Version 2.0.0		2009-09
13	Z.Sup1** (revised)	Supplement 1 to Z-series Recommendations – ITU-T Z.100-series – Supplement on methodology on the use of description techniques		TBD
13	Z.uml-msc	UML profile for MSC		TBD
13	Z.uml-ttcn	UML profile for TTCN		TBD
13	Z.uml-urn	UML profile for URN		TBD
13	Z.urn-ma	URN - Methodological approach		TBD
14	Z.161 (revised)	Testing and Test Control Notation version 3: TTCN-3 core language	ETSI ES 201 873-1	2009-09
14	Z.164 (revised)	Testing and Test Control Notation version 3: TTCN-3 operational semantics	ETSI ES 201 873-4	2009-09
14	Z.165 (revised)	Testing and Test Control Notation version 3: TTCN-3 runtime interface (TRI)	ETSI ES 201 873-5	2009-09
14	Z.166 (revised)	Testing and Test Control Notation version 3: TTCN-3 control interface (TCI)	ETSI ES 201 873-6	2009-09
14	Z.167 (revised)	Testing and Test Control Notation version 3: TTCN-3 mapping from ASN.1	ETSI ES 201 873-7	2009-09
14	Z.169 (revised)	Testing and Test Control Notation version 3: TTCN-3 mapping from XML data definition	ETSI ES 201 873-9	2009-09

* Marked draft Recommendations are for determination; all unmarked Recommendations are for consent

** For approval

*** Target date for consent or determination of Recommendations or for approval of Appendices, Supplements or Implementers' Guides

WORKING PARTY 1/17 - NETWORK AND INFORMATION SECURITY

Question 2/17 – Security architecture and framework

X.1034 (revised), Framework for extensible authentication protocol (EAP)-based authentication and key management in a data communication network
The extensible authentication protocol (EAP) is an authentication framework that supports multiple authentication mechanisms between a supplicant and an authentication server in a data communication network. EAP can be used as a basic tool for enabling user authentication and distribution of session keys in a data communication network. Since there are several EAP methods, the application designer should select the optimal EAP method among them.
This revision describes a framework for EAP-based authentication and key management for securing the lower layer in a communication network. It provides guidance on the selection of EAP methods and describes the mechanism for key management for the lower layer of a data communication network. The framework described in this Recommendation can be applied to protect data communication networks with either wireless access network or wired access network with a shared medium.

X.gsiiso, Guidelines on security of the individual information service for operators
This Recommendation addresses the aspects of security of the information service provided by telecommunication operators. In the transforming from traditional basic network operator to comprehensive information service provider, the operators expand their services to content service and ICT. The new services not only change the operational models, and they also bring new security issues to be resolved.
This Recommendation provides the guideline on security of the individual information service for operators. The scope covers the classification of individual information service, the security requirement, the mechanism, and the coordination.

X.interfaces, Architecture of external interrelations for a telecommunication network security system
This Recommendation provides four models that make possible a review of interrelations for telecommunication network security system (TNSS) with various groups of external objects. Each object is considered as per its main functions and probable effect of this object on TNSS construction and functioning principles. This Recommendation serves as a foundation for developing the detailed recommendations for network security with regard to external objects effect.

Question 3/17 – Telecommunications information security management

X.isgf, Information security governance framework
The purpose of the Recommendation | International Standard is to promote effective, efficient, and acceptable use of information security activities in organizations by:

- assuring stakeholders that, if the Recommendation is followed, they can have confidence in the organization’s corporate governance of information security;
- informing and guiding directors in governing the use of information security activities in their organization; and
- providing a basis for objective evaluation of the corporate governance of information

security.
This Recommendation | International Standard provides a framework of information security governance and suggests some best practices of information security governance implementation. The framework consists of objectives, principles, and processes of information security governance. It also shows how the information security governance is related with information security management system (ISMS). It also includes the best practices to successfully implement the information security governance.

X.ismf, Information security management framework
This Recommendation provides an information security management framework (ISMF). ISMF maps the controls defined by ITU-T X.1051 to the practical implementation methodologies by defining a set of management areas, such as asset management, incident management, risk management, policy management, etc. The Recommendation gives an overview of the framework and analyzes the relationships between these areas.
The specific guidelines of each area defined in this Recommendation will be provided in a series of other ITU-T Recommendations.

Question 4/17 - Cybersecurity

X.abnot, Abnormal traffic detection and control guideline for telecommunication network
This Recommendation analyzes the requirement of deploying abnormal traffic detection and control means, summarizes the characteristics of typical abnormal traffic, packet, and network behaviour in telecommunication environments, and develops detailed abnormal traffic detection mechanism and control solution for the telecommunication networks.

X.bots, Frameworks for botnet detection and response
This Recommendation provides frameworks for botnet detection and response. The Recommendation provides a definition, organization characteristics and behavior models of botnet. Also, it specifies various types of attack threat caused by botnet. And, the Recommendation provides considerations required for botnet detection and response, defines functions and interfaces used in framework for botnet detection and response.

X.dexf, Digital evidence exchange file format
This Recommendation specifies extensible capabilities, structures and data elements for digital evidence exchange file formats, including both ASN.1 and XML modules and schema. The specification includes network transportation security capabilities. The primary purpose is to support trusted and interoperability of digital forensic systems.

X.gopw, Guideline on preventing malicious code spreading in a data communication network
This Recommendation provides guidelines on preventing malicious code spreading. The Recommendation provides technical guideline such as a definition, a classification, infection route and symptoms of malicious code. Also, it specifies countermeasures to prevent malicious code from spreading. This Recommendation can be used as a guideline to end users and system managers for preventing malicious code spreading.

X.gpn, Mechanism and procedure for distributing policies for network security
Based on the network security information policy model and network security policy framework defined in ITU-T X.1036, this Recommendation further defines the detailed distribution

mechanism and distribution procedure of security policy, so that the security policies can be negotiated and distributed between different devices and between the device and the policy center.

X.sips, Framework for countering cyber attacks in SIP-based services
This Recommendation provides a framework for countering cyber attacks in SIP-based services. The Recommendation provides analysis of SIP-based attacks and characteristics of detection and response in SIP-based services. Also, it provides requirements for information sharing between service providers.

X.sisfreq, Requirements for security information sharing framework
This Recommendation provides requirements for a framework for the sharing of security information regarding the identification of threats, attacks, intrusions and other malicious behavior. This framework will allow previously independent acting entities to participate in various coordinated efforts such as the prevention or halting of targeted behavior or the coordination of analysis and determination efforts.

X.tb-ucc, Traceback use cases and capabilities
This Recommendation describes capabilities derived from example traceback use cases. The use cases include traceback scenarios which occur in a single ISP, a single region/domain and across multiple regions/domains. These traceback capabilities should help to find ingress point, path, partial path or source of a network event. Traceback systems architectures, functional components, internal and external interfaces, protocols, and message format are not within the scope of this Recommendation.

Question 5/17 – Countering spam by technical means

X.fcsip, Framework for countering IP multimedia spam
This Recommendation specifies the general architecture of countering spam system on IP multimedia applications such as IP telephony, instant messaging, multimedia conference, etc. It provides functional blocks of necessary network entities to counter spam and their functionalities, and describes interfaces among the entities. To build secure session against spam attack, user terminals and edge service entities such as proxy server or application servers are extended to have spam control functions. Shown are interfaces between these extended peer entities, and interfaces with other network entities which can play a role in countering spam.

X.ics, Functions and interfaces for countering email spam sent by botnet
This Recommendation suggests the functions and interfaces for countering email spam sent by botnet. The email spam countering functions using botnet information and interfaces between botnet databases are defined. And it gives the reference model that the functions and interfaces applied to the countering spam gateway defined in ITU-T X.tcs-1.

X.tcs, Technical means for countering spam
Communication network is evolving, more services are emerging, and capability of spammers is stronger. Moreover, no single technical means has perfect performances on countering spam currently. It may be necessary to propose new technical countermeasures.

X.tcs-1, Interactive countering spam gateway system
This Recommendation specifies interactive countering spam gateway system as a technical mean for countering various types of spam. The gateway system enables spam notification from receiver’s gateway to sender’s gateway, prevents spam traffic from going across the network.

This Recommendation defines architecture for the countering spam gateway system, describes basic entities, protocols and functions, provided mechanisms for spam detection, countering spam information sharing, and countering spam actions of the gateway systems.

X.tcs-2, Technical means for countering VoIP spam
VoIP is an IP multimedia application and it is easy to become vehicle of spam, just as e-mail is. This Recommendation describes the technical means for countering VoIP spam. It is in succession to ITU-T X.1244 and ITU-T X.fcsip. It defines the functional architecture and blocks. Also, it describes the protocol procedures associated with functional blocks.

WORKING PARTY 2/17 - APPLICATION SECURITY

Question 6/17 - Security aspects of ubiquitous telecommunication services

X.iptvsec-2, Functional requirements and mechanisms for secure transcodable scheme of IPTV
This Recommendation defines the functional requirements, architectures and mechanisms for secure transcoding scheme of IPTV content. For the secure transcoding, this involves the threats on the IPTV network infrastructure, the framework, the functionalities, and interfaces between components in the architectures for secure transcoding. The objective of this Recommendation is to serve as a foundation for developing detailed architecture and scheme for secure transcoding.

X.iptvsec-3, Key management framework for secure IPTV services
This Recommendation develops a complete set of requirements for key management of unicast, multicast, and group services in IPTV context. This includes a general framework, key hierarchy, protocols, and message format/relevant parameters for key management.

X.iptvsec-4, Algorithm selection scheme for service and content protection (SCP) descrambling
This Recommendation develops a set of function of algorithm selection scheme from existing algorithms for contents descrambling. This includes algorithm selection scheme, service and content protection (SCP) function, resource abstraction layer (RAL) function, interoperability support function and message format.

X.iptvsec-5, Service and content protection (SCP) interoperability scheme
This Recommendation develops a complete set of requirements for the interoperable service and content protection (SCP) to support interoperability between multiple SCP mechanisms. This includes interoperable SCP scenarios, interoperable SCP architecture and interoperable SCP process.

X.mcsec-1, Security requirements and framework for multicast communication
This Recommendation investigates threat analysis for multicast communication services and describes security requirements and framework for secure multicast communication services. In addition, this Recommendation develops secure multicast services including group management, reliable multicast data transmission, and so forth.

X.msec-5, Security aspects of mobile multi-homed communications
This Recommendation discusses the security requirements, architecture, and mechanisms dealing with the security and protection aspects of mobile multi-homed communications, terminal

devices, and users.

X.usnsec-1, Security framework for ubiquitous sensor network
This Recommendation | International Standard describes security threats and security requirements to the ubiquitous sensor network. In addition, it categorizes security technologies by security functions that satisfy above security requirements and by the place to which the security technologies are applied in the security model of the ubiquitous sensor network. Finally, the security function requirements for each entity in the network and possible implementation layer for security function are presented.

X.usnsec-2, Ubiquitous sensor network (USN) middleware security guidelines
This Recommendation analyzes security threats on ubiquitous sensor network (USN) middleware, defines the functional requirements, and develops the guidelines for USN middleware security.

X.usnsec-3, Secure routing mechanisms for wireless sensor network
This Recommendation provides secure routing mechanisms for wireless sensor network in ubiquitous sensor network. It introduces general network topologies and routing protocols in ubiquitous sensor network. It describes security threats of wireless sensor network and provides countermeasures for secure routing in wireless sensor network.

Question 7/17 - Secure application services

X.1141, Amd.1, Security Assertion Markup Language (SAML 2.0) - Amendment 1: Errata
The Amendment amends ITU-T X.1141 to reflect the official errata that have been approved by OASIS regarding the OASIS SAML 2.0 version.

X.1142, Amd.1, eXtensible Access Control Markup Language (XACML 2.0) – Amendment 1: Errata
The Amendment amends ITU-T X.1142 to reflect the official errata that have been approved by OASIS regarding the OASIS XACML 2.0 version.

X.p2p-3, Security requirements and mechanisms of peer-to-peer-based telecommunication network
This Recommendation analyzes the special security requirements in the peer-to-peer (P2P)-based telecommunication environment, designs the security technical framework for the new P2P-based telecom network architecture and service scenarios, and defines the security solutions and detailed mechanisms to assure the network and services security.

X.sap-3, Management framework for one time password based authentication service
This Recommendation provides the management framework of the one-time password (OTP)-based authentication service to provide strong authentication in the telecommunication network. This Recommendation includes the requirements and architecture for the provision of a security framework providing OTP-based authentication services.

X.websec-4, Security framework for enhanced web based telecommunication services
This Recommendation provides security framework for enhanced web based telecommunication services. This Recommendation describes security threats and security requirements of the enhanced web based telecommunication services, and it also describes security functions and technologies that satisfy the security requirements.

Question 9/17 - Telebiometrics

X.1081, Amd.1, The telebiometric multimodal model - A framework for the specification of security and safety aspects of telebiometrics - Amendment 1: Objet Identifier assignments under the Telebiometrics arc
This Amendment allocates arcs under the object identifier **{joint-iso-itu-t(2) telebiometrics(42)}** allocated for the work on telebiometrics, with top level OID-IRI value **"/Telebiometrics"**. Eight arcs are defined for ITU-T X.1081, ITU-T X.1082 and the six parts of ITU-T X.th. Under the arc allocated to ITU-T X.1081, new arcs are allocated to layers (scientific, sensory, metric), fields of study (physics, chemistry, biology, culturology, psychology) and modalities (video, audio, tango, chemo, radio).

X.1081, Amd.2, The telebiometric multimodal model - A framework for the specification of security and safety aspects of telebiometrics - Amendment 2: Appendix V on information on hierarchies
This Amendment updates the current edition (2002) with clarification on hierarchy theory and provides a bibliography.

X.1082, Amd.1, Telebiometrics related to human physiology - Amendment 1: Object Identifier assignments under the Telebiometrics arc
This Amendment allocates arcs under the object identifier **{joint-iso-itu-t(2) telebiometrics(42) human-physiology(2)}** allocated in ITU-T X.1081 Amendment 1, for the work on human-physiology, with OID-IRI value **"/Telebiometrics/Human_Physiology"**. The new arcs are related to symbols (14 arcs) and symbol combinations (4095 arcs).

X.ott, Authentication framework with one-time telebiometric template
This Recommendation describes a user-authentication framework with biometric one-time templates. The framework provides generation and transmission method on one-time biometric template transmitted over open networks for providing multi-factor authentication and for preventing replay attacks on biometric template. This Recommendation also describes the security requirements associated with biometric one-time templates.

X.th1, Telehealth and world-wide telemedicines – Generic telecommunications protocol
This Recommendation is designed to provide wide-area communication in support of health-related activities, where the communication can usefully be undertaken as structured messages. It aims to remove the need for medical staff and patients to be co-located, and supports both multi-party (for audit and training purposes) as well as one-to-one interactions. It recognises that in many cases interactions between medical staff and patients need to be supplemented by unstructured voice and/or video communication, which may need synchronization with the structured message flows.
There are many standards development groups involved in health-care, including standardization of various aspects of medical and dental and DNA records. This Recommendation recognizes and identifies their defined data formats and interactions using ASN.1 object identifiers (OIDs). It aims to support "world-wide medicines" (plural). This is intended to include not only Western medicine and drugs, but also alternative therapies, including herbal remedies and interventions such as acupuncture. This Recommendation specifies complete protocols (including a service discovery protocol) using TCP/IP and SOAP/HTTP, with bindings similar to those specified in ITU-T X.1083 | ISO/IEC 24708. Security features are provided using ITU-T X.509 | ISO/IEC 9594-8 and its derivatives.

The communications require the identification of a variety of objects ranging from medical practitioners, medical and dental record formats, to drugs and surgical intervention procedures. It also requires identification of physiological quantities and units. This Recommendation specifies ASN.1 Information Object Classes for the identification of these objects, and other parts of this series of Recommendations provide the Internationalized Object Identifiers to identify objects in these classes. The other five parts (covering the fields of physics, chemistry, biology, culturology and psychology) provide the associated Information Object definitions and assign OIDs for both quantities and units and other objects associated with the fields of study.

X.th2, Telebiometrics related to physics
This Recommendation specifies two aspects of telebiometrics related to safety, security, privacy and anonymity. One is the set of messages, with authentication and integrity and privacy (specified using ASN.1) that provide the telebiometric communications between an operator and a remote telemedicine device. The other is the tables of physiological quantities and units and their thresholds that define the thresholds for safety of a human being when various sensors or actions are being applied to the human body. This Recommendation uses the framework defined in ITU-T X.1081 for optimal safety and security in telebiometrics.
It is applicable to both physics and biometrics (the measurement of physiological, biological, and behavioral characteristics limited to the field of physics). A taxonomy of wetware and hardware/software interactions is defined. Thresholds are specified using the set of International System of Quantities (ISQ) and the related International System of Units (SI).

X.th3, Telebiometrics related to chemistry
This Recommendation specifies two aspects of telebiometrics related to safety, security, privacy and anonymity. One is the set of messages, with authentication and integrity and privacy (specified using ASN.1) that provide the telebiometric communications between an operator and a remote telemedicine device. The other is the tables of physiological quantities and units and their thresholds that define the thresholds for safety of a human being when various sensors or actions are being applied to the human body. This Recommendation uses the framework defined in ITU-T X.1081 for optimal safety and security in telebiometrics.
It is applicable to both chemistry and biometrics (the measurement of physiological, biological, and behavioral characteristics to the field of chemistry). A taxonomy of wetware and hardware/software interactions is defined. Thresholds are specified using the set of International System of Quantities (ISQ) and the related International System of Units (SI).

X.th4, Telebiometrics related to biology
This Recommendation specifies two aspects of telebiometrics related to safety, security, privacy and anonymity. One is the set of messages, with authentication and integrity and privacy (specified using ASN.1) that provide the telebiometric communications between an operator and a remote telemedicine device. The other is the tables of physiological quantities and units and their thresholds that define the thresholds for safety of a human being when various sensors or actions are being applied to the human body. This Recommendation uses the framework defined in ITU-T X.1081 for optimal safety and security in telebiometrics.
It is applicable to both biology and biometrics (the measurement of physiological, biological, and behavioral characteristics to the field of biology). A taxonomy of wetware and hardware/software interactions is defined. Thresholds are specified using the set of International System of Quantities (ISQ) and the related International System of Units (SI).

X.th5, Telebiometrics related to culturology
This Recommendation specifies two aspects of telebiometrics related to safety, security, privacy and anonymity. One is the set of messages, with authentication and integrity and privacy (specified using ASN.1) that provide the telebiometric communications between an operator and a remote telemedicine device. The other is the tables of physiological quantities and units and their thresholds that define the thresholds for safety of a human being when various sensors or actions are being applied to the human body. This Recommendation uses the framework defined in ITU-T X.1081 for optimal safety and security in telebiometrics.
It is applicable to both culturology and biometrics (the measurement of physiological, biological, and behavioral characteristics to the field of culturology). A taxonomy of wetware and hardware/software interactions is defined. Thresholds are specified using the set of International System of Quantities (ISQ) and the related International System of Units (SI).

X.th6, Telebiometrics related to psychology
This Recommendation specifies two aspects of telebiometrics related to safety, security, privacy and anonymity. One is the set of messages, with authentication and integrity and privacy (specified using ASN.1) that provide the telebiometric communications between an operator and a remote telemedicine device. The other is the tables of physiological quantities and units and their thresholds that define the thresholds for safety of a human being when various sensors or actions are being applied to the human body. This Recommendation uses the framework defined in ITU-T X.1081 for optimal safety and security in telebiometrics.
It is applicable to both psychology and biometrics (the measurement of physiological, biological, and behavioral characteristics to the field of psychology). A taxonomy of wetware and hardware/software interactions is defined. Thresholds are specified using the set of International System of Quantities (ISQ) and the related International System of Units (SI).

X.tif, Integrated framework for telebiometric data protection in telehealth and worldwide telemedicines
This Recommendation provides an integrated framework for biometric data and private information protection in telehealth and worldwide telemedicines. It defines a model of health services using telebiometrics for user identification and authentication. It identifies the threats in transmitting various sensory data related to human health and provides their countermeasures for secure transmission when applying the integrated framework.

X.tpp-2, Telebiometrics protection procedures - Part 2: A guideline for data protection in multibiometric systems
This Recommendation provides the procedures and methods for the security of the telemultibiometric system. It adopts the general concepts of multibiometrics in ISO/IEC 24722, mainly regarding four kinds of multibiometrics fusion schemes such as sample-level fusion, feature-level fusion, score-level fusion, and decision-level fusion. This Recommendation defines vulnerable points in all kinds of multibiometrics, and the threats on them. Then, it provides countermeasures against the threats on newly introduced vulnerable points. Also, user-customized data transmission, which is one countermeasure for multibiometric data protection, is provided for some indispensable applications where not all biometric measurements are available.

X.tsm-2, Telebiometrics system mechanism - Protection profile for client terminals
This Recommendation defines the requirements on client terminals for biometric authentication over open networks, based on the models defined in ITU-T X.1084. System mechanisms and

security profile of the client side are specified based on Common Criteria: ISO/IEC 15408, *Evaluation criteria for IT security* such as protection profile.

WORKING PARTY 3/17 - IDENTITY MANAGEMENT AND LANGUAGES

Question 10 - Identity management architecture and mechanisms

X.1250 (X.idmreq), Baseline capabilities for enhanced global identity management trust and interoperability
This Recommendation describes baseline capabilities for global identity management (IdM) trust and interoperability (i.e., to enhance exchange and trust in the identities used by entities in telecommunication/ICT networks and services). The definitions and need for identity management trust are highly context dependent and often subject to very different policies and practices in different countries. The trust capabilities include the protection and control of personally identifiable information.

X.1251 (X.idif), A framework for user of digital identity
This Recommendation defines a framework to enhance user control and exchange of their digital identity related information. The Recommendation also defines user and functional requirements of the digital identity information exchange. The work includes providing the user with the ability to control the release of personally identifiable information.

X.eaa, Information technology – Security techniques – Entity authentication assurance
This Recommendation | International Standard concerns entity authentication assurance. It provides a life cycle framework for the assurance of an entity's identities in given contexts. The framework includes:

- processes and procedures for enrolment, proofing, vetting, issuance, credentialing, management, usage, auditing, and revocation of an identity;
- guidelines for the evaluation of the strength of the authentication of an identity;
- a set of identity authentication assurance measures that are general and applicable to the entire entity's identity life cycle.

X.EVcert, Extended validation certificate
This Recommendation adopts the CA Browser Forum specification to support very high assurance trust and security mechanisms for transactions between end users and organizations that provide high value or critical services or code. Based on ITU-T's X.509 digital certificate, it adds an array of identity proofing, technologies, and protocols to significantly enhance trust. This includes the creation of an encrypted transport layer path with the trusted party. Browser providers, and increasingly other client-based software vendors now support the capability on an estimated 60 percent of computers worldwide.

X.idm-dm, Common identity data model
This Recommendation develops a common data model for identity data that can be used to express identity related information among identity management (IdM) systems.

X.idm-ifa, Framework architecture for interoperable identity management systems
This Recommendation proposes a blueprint for a modular framework architecture for identity management systems. The architecture is expected to serve as a reference while discussing, designing and developing future interoperable identity management (IdM) systems. The

architecture is intended to be generic in order to satisfy versatile requirements of user-centric, network-centric and service-centric IdM systems.
In addition, an informative mapping of the architecture on to next generation networks is included.

X.idmdef, Baseline identity management terms and definitions
This Recommendation provides a collection of terms and definitions used in identity management (IdM). They are drawn from many sources; all are believed to be in common use in IdM. These definitions are to be used as a baseline for IdM Recommendations throughout ITU-T; they may be expanded if necessary to provide greater clarity for a specific context. This will ensure the main features of IdM are consistent, aligned and understood.

X.idmsg, Security guidelines for identity management systems
This Recommendation defines security guidelines for identity management (IdM) systems. The security guidelines provide how an IdM system should be deployed and operated for secure identity services in NGN (next generation networks) or cyberspace environment. The security guidelines focus on providing advice on how to employ various security mechanisms to protect a general IdM system and also study proper security procedures required when two IdM systems are interoperated.

X.priva, Criteria for assessing the level of protection for personally identifiable information in identity management
This Recommendation defines the criteria for assessing the level of protection for personally identifiable information (PII) of the identity provider and the relying party concerned in identity service, depending on the protection for personally identifiable information requested by them to the requesting/asserting party, and the type and use purpose of PII and maintain period of PII, as well as the technical and administrative measures for protection for PII.

X.rfpg, Guideline on protection for personally identifiable information in RFID application
This Recommendation recognizes that as RFID greatly facilitates the access and dispersion of information pertaining specifically to the merchandise that individuals wear and/or carry, it also creates an opportunity for the same information to be abused for tracking an individual's location or invading their privacy in a malfeasant manner. For this reason the Recommendation provides guidelines and best practices regarding RFID procedures that can be used by service providers to gain the benefits of RFID while attempting to protect personally identifiable information.

Question 11/17 – Directory services, Directory systems, and public-key/attribute certificates

E.115, Amd.1, Computerized directory assistance, Amendment 1 – Support of E.115 capabilities
This Amendment provides important additions to ITU-T E.115 to allow directory assistance service provider to exchange information about databases supported and the functionalities that are available.

X.500-series, Amd.1, Information technology – The Directory – Amendment 1 – Communication support enhancement
Communications enhancements to ITU-T X.500-series include extended communications capabilities for X.500 itself and provide communications support for other specifications. Communications enhancements include extended interworking with LDAP and extended support for tag-based applications.

X.500-series, Amd.2, Information technology – The Directory – Amendment 2 –Password policy support
Password policy is a set of rules that controls how passwords are used and administered in the Directory. It improves the security of the Directory and makes it difficult for password cracking programs to break into the Directory. These rules ensure that users change their passwords periodically, that passwords meet quality requirements that re-use of old passwords is restricted, and that users are locked out after a certain number of failed attempts.

Question 12/17 - Abstract Syntax Notation One (ASN.1), Object Identifiers (OIDs) and associated registration

X.oid-res, Object identifier resolution system
This Recommendation | International Standard provides the necessary text for the development of an infrastructure to support access to information associated with nodes in the International Object Identifier tree (see ITU-T X.660 | ISO/IEC 9834-1) using DNS.

Question 13/17 - Formal languages and telecommunication software

X.901 (revised), Information technology – Open distributed processing – Reference model: Overview
This Recommendation | International Standard is an integral part of the open distributed processing (ODP) reference model. It contains a motivational overview of ODP, giving scoping, justification and explanation of key concepts, and an outline of the ODP architecture. It contains explanatory material on how this reference model is to be interpreted and applied by its users, who may include standards writers and architects of ODP systems. It also contains a categorization of required areas of standardization expressed in terms of the reference points for conformance identified in ITU-T X.903 | ISO/IEC10746-3.

X.902 (revised), Information technology – Open distributed processing – Reference model: Foundation
This Recommendation | International Standard contains the definition of the concepts and analytical framework for normalized description of (arbitrary) distributed processing systems. It introduces the principles of conformance to open distributed processing (ODP) standards and the way in which they are applied. This is only to a level of detail sufficient to support ITU-T X.903 | ISO/IEC 10746-3 and to establish requirements for new specification techniques.
The Recommendation | International Standard revises descriptions of role, action, policy, component, and additional definitions such as refinement of interaction, relationship between specification and instantiation, and human-system interaction. Additionally, multi-provider business, services and causalities are revisited.

X.903 (revised), Information technology – Open distributed processing – Reference model: Architecture
This Recommendation | International Standard contains the specification of the required characteristics that qualify distributed processing systems as open. These are the constraints to which open distributed processing (ODP) standards must comply. It uses the descriptive techniques from ITU-T X.902 | ISO/IEC 10746-2.
The Recommendation | International Standard revises descriptions of community, channel rules, and provide alignments with ITU-T X.902 | ISO/IEC 10746-2 on the number of parameters, flows and use of signals, relationship between the computational and engineering viewpoints, the

nature of the technology viewpoint, and infrastructure. Additionally, interaction rules and signatures of action templates are revisited.

X.904 (revised), Information technology – Open distributed processing – Reference model: Architecture semantics
This Recommendation | International Standard is an integral part of the open distributed processing (ODP) reference model. It contains a formalization of the ODP modelling concepts defined in ITU-T X.902 | ISO/IEC 10746-2, clauses 8 and 9. The formalization is achieved by interpreting each concept in terms of the constructs of the different standardized formal description techniques.

X.905, Cor 1, Information technology – Open distributed processing – Use of UML for ODP system specification – Technical Corrigendum 1
This Technical Corrigendum changes the use of UML comments to the use of UML constraints. A UML constraint is a packageable element (and therefore has a name, and can be traced and managed, since it can be directly owned by a package), which declares some of the semantics of one or more elements. UML superstructure 2.1.1, section 7.3.10 justifies the representation of rules with constraints, and using constraints leaves room to specify such rules using more powerful languages, such as those specific for policies and rules. (The UML specs explicitly mentions that "A user-defined constraint is described using a specified language, whose syntax and interpretation is a tool responsibility. One predefined language for writing constraints is OCL. In some situations, a programming language such as Java may be appropriate for expressing a constraint. In other situations natural language may be used.") A constraint is associated with an ordered set of elements to which the constraint applies. In this way we can trace these elements.

X.uml-asn1, ASN.1 combined with UML2.0
This Recommendation defines a Unified Modelling Language (UML) profile that maps UML2.0 data descriptions to ASN.1 so that UML can be used in combination with ASN.1.

Z.100 (revised), Specification and description language: Overview of SDL-2008
This Recommendation is a part of the set of *Specification and description language* Recommendations for SDL-2008. It provides an overview and common material (such as conventions and tool compliance). It gives concepts for behaviour, data description and (particularly for larger systems) structuring. The basis of behaviour description is extended finite state machines communicating by messages. Data description is based on data types for values and objects. The basis for structuring is hierarchical decomposition and type hierarchies. A distinctive feature is the graphical representation. SDL-2008 is backwards compatible with previous versions of SDL while adding significant new features.
This Recommendation is revised as part of the restructuring of the ITU-T Z.100 series for SDL-2008.

Z.101, Specification and description language: Basic SDL-2008
This Recommendation is part of the set of *Specification and description language* Recommendations for SDL-2008. It covers core features such as agent (block, process) type diagrams, agent diagrams for structures with channels, diagrams for extended finite state machines and the associated semantics for these basic features.

Z.102, Specification and description language: Comprehensive SDL-2008
This Recommendation is part of the set of *Specification and description language* Recommendations for SDL-2008. It extends the semantics and syntax of the Basic language to cover full abstract grammar and the corresponding canonical concrete notation. This includes features such as continuous signals, enabling conditions, type inheritance, and composite states.

Z.103, Specification and description language: Shorthand notation and annotation in SDL-2008
This Recommendation is part of the set of *Specification and description language* Recommendations for SDL-2008. It adds notation shorthand (such as asterisk state) that make the language easier to use and more concise, and various annotations that make models easier to understand (such as comments or create lines), but does not add to the formal semantics of the models. The shorthand notations are transformed from the concrete syntax of ITU-T Z.103 to concrete syntax that is allowed by ITU-T Z.102 or ITU-T Z.101.

Z.104 (revised), Specification and description language: Data and action language in SDL-2008
This Recommendation is part of the set of *Specification and description language* Recommendations for SDL-2008. It adds the data and action language used to define data types and expressions. In SDL-2008 it is allowed to use different concrete data notations, such as the SDL-2000 data notation or C with bindings to the abstract grammar and the predefined data package.
This Recommendation is revised to be consistent with the rest of the Z.100 series for SDL-2008. It replaces the data part of ITU-T Z.100 for SDL-2000 and previous ITU-T Z.104 on encoding of data.

Z.105 (revised), Specification and description language: SDL-2008 combined with ASN.1 modules
This Recommendation is part of the set of *Specification and description language* Recommendations for SDL-2008. It defines how Abstract Syntax Notation One (ASN.1) modules can be used in combination with SDL-2008. The combined use of SDL and ASN.1 permits a coherent way to specify the structure and behaviour of telecommunication systems, together with data, messages and encoding of messages that these systems use.
This Recommendation is revised to be consistent with the rest of the ITU-T Z.100 series for SDL-2008, because it references the syntax and semantics of the language in other Recommendations in the series. There are some refinements of this Recommendation based on its use and usefulness, and changes to ASN.1/

Z.106 (revised), Specification and description language: Common interchange format (CIF) for SDL-2008
This Recommendation is part of the set of *Specification and description language* Recommendations for SDL-2008. The common interchange format (CIF) is intended for the interchange of graphical SDL specifications (SDL-GR) made on different tools that do not use the same storage format.
This Recommendation is revised to be consistent with the rest of the ITU-T Z.100 series for SDL-2008.

Z.109 (revised), Specification and description language: SDL-2008 combined with UML
This Recommendation is part of the set of *Specification and description language* Recommendations for SDL-2008. It defines a UML profile that maps to SDL-2008 semantics so that UML can be used in combination with SDL. The combined use of SDL-2000 and UML permits a coherent way to specify the structure and behaviour of telecommunication systems, together with data.
This Recommendation is revised to be consistent with the rest of the ITU-T Z.100 series for SDL-2008, because it references the abstract grammar of the language and paragraphs for transformation models in other Recommendations in the series.

Z.120 (revised), Message sequence chart (MSC)
The purpose of recommending MSC (message sequence chart) is to provide a trace language for the specification and description of the communication behaviour of system components and their environment by means of message interchange. Since in MSCs the communication behaviour is presented in a very intuitive and transparent manner, particularly in the graphical representation, the MSC language is easy to learn, use and interpret. In connection with other languages it can be used to support methodologies for system specification, design, simulation, testing, and documentation.
This Recommendation is revised to reflect the experience and changes in use of the language since the last major revision of the language (to MSC-2000) in 1999 and the last update in 2004.

Z.120, Amd.1 (revised), Message sequence chart (MSC), Amendment 1: Appendix I, Application of MSCs
This Appendix to ITU-T Z.120 is revised to put the figures and paragraphs in an adequate order. Other improvements will be considered at the same time.

Z.150 (revised), User requirements notation (URN) - Language requirements and framework
This Recommendation with other Recommendations in the ITU-T Z.150 series defines URN (user requirements notation) for describing user requirement as goals and scenarios in a formal way without any reference to implementation mechanisms and with optional dependency on component specification. Such a notation is needed to capture user requirements prior to any design.

This Recommendation is revised to reflect the experience and use of the notation, since the initial release of the standard for the notation in 2008 (ITU-T Z.151).

Z.151 (revised), User requirements notation (URN) – Language definition
This Recommendation defines the user requirements notation (URN) intended for the elicitation, analysis, specification, and validation of requirements. URN combines modelling concepts and notations for goals (mainly for non-functional requirements and quality attributes) and scenarios (mainly for operational requirements, functional requirements, and performance and architectural reasoning). The goal sub-notation is called goal-oriented requirements language (GRL) and the scenario sub notation is called use case map (UCM).
This Recommendation is revised to reflect the experience and use of the notation, since the initial release of the standard for the notation in 2008 (ITU-T Z.151).

Z.uml-msc, Unified Modeling Language (UML) profile for MSC
This Recommendation defines a Unified Modelling Language (UML) profile that maps UML2.0 to message sequence chart (ITU-T Z.120) semantics so that UML can be used in combination with MSC. This combined use permits a coherent way to describe message-oriented scenarios for telecommunication systems. This work enables one to use UML2.0 tools and construct models (e.g. interaction diagrams) that will have the semantics of MSC.

Z. uml-ttcn, Unified Modeling Language (UML) profile for TTCN
This Recommendation defines a Unified Modelling Language (UML) profile that maps UML2.0 data descriptions to Testing and Test Control Notation (TTCN) so that UML can be used in combination with TTCN.
This Recommendation presents a definition of the UML2.0-to-TTCN mapping for use in the combination of TTCN and UML.

Z. uml-urn, Unified Modeling Language (UML) profile for URN
This Recommendation defines a Unified Modelling Language (UML) profile that maps UML2.0 to User Requirements Notation (URN) semantics (i.e., GRL combined with UCM) so that UML can be used in combination with Goal-oriented Requirements Language (GRL) and/or Use Case Maps (UCM). This combined use permits a coherent way to describe goal models and causal scenarios for telecommunication systems, complemented with other UML concepts and diagrams. This work enables one to use UML2.0 tools and construct UML models that will have the semantics of URN.

Z.urn-ma, User requirements notation (URN): Methodological approach
This Recommendation describes how best to combine goal-oriented requirements language (GRL) and use case map (UCM) for modeling and analyzing requirements. It also considers links to other ITU-T languages (MSC, SDL, TTCN-3, and UML), especially in the form of transformations. This work provides basic building blocks enabling requirements-driven design and validation based on user requirements notation (URN) models.

Z.Sup1 (revised), Supplement 1 to Z-series Recommendations – ITU-T Z.100-series – Supplement on methodology on the use of description techniques
This Supplement replaces ITU-T Z.100 Supplement 1 (10/96) and includes a tutorial on the use of UML with ITU-T languages. It is intended to be incorporated by the users in their overall methodologies, and tailored for their application systems and specific needs. In particular, this Supplement does not cover the issues of derivation of an implementation from the specification or the testing of systems in detail. In the case of testing, it is expected that this should be partially covered by a separate document dealing with the generation of tests for standards or products.

Z.Imp100 (revised), Specification and description language Implementers' Guide - Version 2.0.0
This Implementers' Guide is principally a compilation of reported defects and their resolutions to the *Specification and description language* ITU-T Recommendations for SDL-2008:
- Z.100, Z.101, Z.102, Z.103, Z.104, Z.105, Z.106, Z.109, Z.111 and Z.119.

It also contains some historical information of the previous set of Z.100-series Recommendations.

Question 14/17 - Testing languages, methodologies and framework

Z.161 (revised), Testing and Test Control Notation version 3: TTCN-3 core language
This Recommendation defines TTCN-3 (Testing and Test Control Notation 3) intended for specification of test suites that are independent of platforms, test methods, protocol layers and protocols. TTCN-3 can be used for specification of all types of reactive system tests over a variety of communication ports. Typical areas of application are protocol testing (including mobile and Internet protocols), service testing (including supplementary services), module testing, testing of CORBA-based platforms and APIs. The specification of test suites for physical layer protocols is outside the scope of this Recommendation.

Z.164 (revised), Testing and Test Control Notation version 3: TTCN-3 operational semantics
This Recommendation defines the operational semantics of TTCN-3 (Testing and Test Control Notation 3). The Recommendation is based on the TTCN-3 core language defined in ITU-T Z.161.

Z.165 (revised), Testing and Test Control Notation version 3: TTCN-3 runtime interface (TRI)
This Recommendation provides the specification of the runtime interface for TTCN-3 (Testing and Test Control Notation 3) test system implementations. The TTCN-3 Runtime Interface provides the recommended adaptation for timing and communication of a test system to a particular processing platform and the system under test, respectively. This Recommendation defines the interface as a set of operations independent of target language.

Z.166 (revised), Testing and Test Control Notation version 3: TTCN-3 control interface (TCI)
This Recommendation specifies the control interfaces for TTCN-3 (Testing and Test Control Notation 3) test system implementations. The TTCN-3 Control Interfaces provides the recommended adaptation for management, test component handling and encoding/decoding of a test system to a particular test platform. This Recommendation defines the interfaces as a set of operations independent of a target language.

Z.167 (revised), Testing and Test Control Notation version 3: TTCN-3 mapping from ASN.1
This Recommendation defines a normative way of using ASN.1 as defined in Recommendations ITU-T X.680, X.681, X.682 and X.683 with TTCN-3. The harmonization of other languages with TTCN-3 is not covered by this Recommendation.

Z.169 (revised), Testing and Test Control Notation version 3: TTCN-3 mapping from XML data definition
The Recommendation defines the mapping rules for W3C Schema to enable testing of XML-based systems, interfaces and protocols.
