Summaries for work items under development in Study Group 17 (updated 6 November 2009)

Q.	Acronym	Title	Editor	Location of Text	Equivalent e.g., ISO/IEC	Timing ***
2	X.1034 (revised)	Guideline on extensible authentication protocol-based authentication and key management in a data communication network	Heung Ryong Oh, Heung Youl Youm	TD 0495		2010-12
2	X.gsiiso	Guidelines on security of the individual information service for operators	Yuanfei Huang, Lijun Liu, Ziqin Sang, Huirong Tian	TD 0551		2010-12
2	X.interfaces*	Architecture of external interrelations for a telecommunication network security system	Nikolaï Etroukhin	TD 0515		2010-04
3	X.amg	Information asset maintenance guidelines in telecommunication organizations	Sangseo Jang, Taein Jung, Kyuman Ko, Jintae Lee	TD 0635		2011
3	X.isgf*	Information technology – Security techniques – Information security governance framework	Jungduk Kim (K. Harada) (Ch. Provencher)	TD 0313 Attach. 2	ISO/IEC 27014	2012
3	X.ismf	Information security management framework	Xin Chen, Jiwei Wei, Zhi Zhou	TD 0486		2010-12
3	X.sgsm	Information security management guidelines for small and medium telecommunication organizations	Hangbae Chang, Chungyun Chung, Sangsoo Jang	TD 0636		2011
4	X.abnot*	Abnormal traffic detection and control guideline for telecommunication network	Xu Chen, Shen He, Lijun Liu	TD 0526		2011
4	X.bots*	Frameworks for botnet detection and response	Chaetae Im, Hyung Cheol Jeong, Mi Joo Kim, Joo Hyung Oh, Yoo Jae Won	TD 0596		2011

Q.	Acronym	Title	Editor	Location of Text	Equivalent e.g., ISO/IEC	Timing ***
4	X.capec*	Common attack pattern enumeration and classification	Bob Martin	TD 0503 Rev.1		2010-12
4	X.cce*	Common configuration enumeration	Bob Martin	TD 0503 Rev.1		2010-12
4	X.cee*	Common event expression	Bob Martin	TD 0503 Rev.1		2010-12
4	X.chirp*	Cybersecurity heuristics and information request protocol	Anthony Rutkowski	TD 0503 Rev.1		2010-12
4	X.cpe*	Common platform enumeration	Bob Martin	TD 0503 Rev.1		2010-12
4	X.crf*	Common result format	Bob Martin	TD 0503 Rev.1		2010-12
4	X.cve*	Common vulnerabilities and exposures	Bob Martin	TD 0405		2010-04
4	X.cvss*	Common vulnerability scoring system	Damir Rajnovic, Gavin Reid, Craig Schultz	TD 0412 Rev.1		2010-04
4	X.cwe*	Common weakness enumeration	Bob Martin	TD 0503 Rev.1		2010-12
4	X.cwss*	Common weakness scoring system	Bob Martin	TD 0503 Rev.1		2010-12
4	X.cybex*	Cybersecurity information exchange framework	Inette Furey, Youki Kadobayashi, Bob Martin, Angela McKay, Damir Rajnovic, Gavin Reid, Anthony Rutkowski, Gregg Schudel, Craig Schultz	TD 0503 Rev.1		2010-04
4	X.cybex.1*	An OID arc for cybersecurity information exchange	Olivier Dubuisson, Anthony Rutkowski	TD 0369 Rev.1		2010-12
4	X.cybex.2*	Use of XML namespace in the cybersecurity information exchange framework	Youki Kadobayashi, Craig Schultz	TD 0556 Rev.1		2010-12
4	X.cybex-beep*	Definition of blocks extensible exchange protocol (BEEP) profile for cybersecurity information exchange framework	Youki Kadobayashi, Craig Schultz	TD 0555 Rev.1		2010-12
4	X.cybex-disc*	Discovery mechanisms in the exchange of cybersecurity information	Youki Kadobayashi, Craig Schultz	TD 0501 Rev.1		2010-12
4	X.cybex-tp*	Transport protocols supporting cybersecurity information exchange	Youki Kadobayashi, Damir Rajnovic, Craig Schultz	TD 0502 Rev.1		2010-12
4	X.dexf*	Digital forensics exchange file format	Youn-Hee Gil	TD 0599 Rev.1		2011

Q.	Acronym	Title	Editor	Location of Text	Equivalent e.g., ISO/IEC	Timing ***
4	X.dpi*	Deep packet inspection exchange format	Anthony Rutkowski	TD 0503 Rev.1		2010-12
4	X.eipwa*	Exchange of information for preventing web-based attacks	Wei Xie, Heung Youl Youm	TD 0575		2011
4	X.gopw*	Guideline on preventing malicious code spreading in a data communication network	Mijoo Kim, Angela McKay, Heung Youl Youm	TD 0579 Rev.1		2010-12
4	X.gpn*	Mechanism and procedure for distributing policies for network security	Lijun Liu, Zhimeng Teng, Zhengqing Yan	TD 0549		2011
4	X.gridf*	SmartGrid incident exchange format	Anthony Rutkowski	TD 0503 Rev.1		2010-12
4	X.iodef*	Incident object description exchange format	Bob Martin	TD 0503 Rev.1		2010-12
4	X.oval*	Open vulnerability and assessment language	Bob Martin	TD 0503 Rev.1		2010-12
4	X.pfoc*	Phishing, fraud, and other crimeware exchange format	Anthony Rutkowski	TD 0503 Rev.1		2010-12
4	X.scap*	Security content automation protocol	Bob Martin	TD 0503 Rev.1		2010-12
4	X.sips*	Framework for countering cyber attacks in session initiation protocol (SIP)-based services	Hwan Kuk Kim, Kyoung Hee Ko	C 122		2011
4	X.sisfreq*	Use cases and capabilities for cybersecurity information sharing and exchange	Il-Ahn Cheong, Craig Schultz	TD 0509 Rev.2		2010-04
4	X.tb-ucc*	Traceback use cases and capabilities	Youki Kadobayashi, Huirong Tian, Heung Youl Youm	TD 0550		2010-12
4	X.teef*	Cyber attack tracing event exchange format	Geon-Lyang Kim, Jong-Hyun Kim, Hyung-Woo Lee, Jung-Chan Na	TD 0487		2010-12
4	X.trm*	Traceback mechanisms	Youki Kadobayashi, Anthony Rutkowski, Huirong Tian, Heung Youl Youm	TD 0572 Rev.1		2011
4	X.xccdf*	Extensible configuration checklist description format	Bob Martin	TD 0503 Rev.1		2010-12
5	X.fcsip*	Framework for countering spam in IP-based multimedia applications	So-Young Park, Seokung Yoon	TD 0577 Rev.1		2010-04

Q.	Acronym	Title	Editor	Location of Text	Equivalent e.g., ISO/IEC	Timing ***
5	X.ics*	Functions and interfaces for countering email spam sent by botnet	Chaetae Im, Hyung Cheol Jeong, Joo Hyung Oh, Yong Geun Won, Yoo Jae Won	TD 0595 Rev.1		2010-12
5	X.tcs*	Technical means for countering spam				TBD
5	X.tcs-1*	Interactive gateway system for countering spam	Xu Chen, Jiang Hua, Zhimeng Teng	TD 0546		2010-04
5	X.tcs-2*	Technical means for countering VoIP spam	Seokung Yoon	TD 0533		2010-12
6	X.iptvsec-2	Functional requirements and mechanisms for secure transcodable scheme of IPTV	Jae Hoon Nah	TD 0581		2010-12
6	X.iptvsec-3	Key management framework for secure IPTV services	Heung Youl Youm	TD 0586		2010-12
6	X.iptvsec-4	Algorithm selection scheme for service and content protection (SCP) descrambling	Nhut Nguyen Jongyoul Park	TD 0570, and TD 0571		2010-12
6	X.iptvsec-5	Service and content protection (SCP) interoperability scheme	Yeonjeong Jeong, Hogab Kang, Taehyun Kim, Dowon Nam, Kisong Yoon	TD 0553		2010-12
6	X.mcsec-1	Security requirement and framework for multicast communication	Miyeon Yoon, Heung Youl Youm	TD 0580		2010-04
6	X.msec-5	Security requirements and mechanism for reconfiguration of mobile device with multiple communication interfaces	Gaeil Ahn, Guntae Bae Kiyoung Kim	TD 0470 Rev.2		2010-12
6	X.msec-6	Security aspects of mobile phones	Wei Li, Lijun Liu, Hongwei Luo, Qi Yuan	TD 0645 Rev.2		2011-4Q
6	X.usnsec-1	Information technology – Security framework for ubiquitous sensor network	Eunyoung Choi Heung Youl Youm	TD 0534 Rev.1	ISO/IEC 29180	2011-1Q
6	X.usnsec-2	Ubiquitous sensor network (USN) middleware security guidelines	Mi Joo Kim, Nam Jae Park Miyeon Yoon	TD 0578		2010-12

Q.	Acronym	Title	Editor	Location of Text	Equivalent e.g., ISO/IEC	Timing ***
6	X.usnsec-3	Secure routing mechanisms for wireless sensor network	Eunyoung Choi, Hyuncheol Jung, Howon Kim, Hyangjin Lee	TD 0630		2010-12
7	X.1141, Amd.1	Security Assertion Markup Language (SAML 2.0) - Amendment 1: Errata	Abbie Barbir		OASIS SAML 2.0 errata	2010-04
7	X.1142, Amd.1	eXtensible Access Control Markup Language (XACML 2.0) - Amendment 1: Errata	Abbie Barbir		OASIS XACML 2.0 errata	2010-04
7	X.p2p-3	Security requirements and mechanisms of peer-to-peer-based telecommunication network	Lijun Liu, Hongwei Luo, Zhenqing Yan, Hongru Zhu	TD 0460		2010-12
7	X.sap-3	Management framework for one time password based authentication service	Hyungjin Lim, Heewoon Shim	TD 0347		2010-12
7 (10)	X.sap-4*	The general framework of strong authentication on multiple authentication authorities environment	Tadashi Kaji, Hyungjin Lim	TD 0628		2011-4Q
7	X.sap-5	A guideline on anonymous authentication for e-commerce service	Sokjoon Lee	TD 0642		2011-4Q
7	X.websec-4	Security framework for enhanced web based telecommunication services	Jae Seung Lee, Heang Suk Oh	TD 0159		2010-12
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	John Larmouth	LC text		In AAP
9	X.1081, Amd.3	The telebiometric multimodal model – A framework for the specification of security and safety aspects of telebiometrics – Amendment 3: Enhancement to support ISO/IEC 80000-series	John Larmouth, Jean-Paul Lemaire	TD 0602 Rev.1		2010-04
9	X.1082, Amd.1	Telebiometrics related to human physiology – Amendment 1: Object identifier assignments under the Telebiometrics arc	John Larmouth	LC text	IEC 80000-14, Amd.1	In AAP
9	X.1082, Amd.2	Telebiometrics related to human physiology – Amendment 2: Enhancement to support ISO/IEC 80000-series	John Larmouth Jean-Paul Lemaire	TD 0601 Rev.1	IEC 8000-14, Amd.2	2010-04
9	X.gep	A guideline for evaluating telebiometric template protection techniques	Yoshiaki Isobe Tetsushi Ohki	TD 0603		2012-3Q

Q.	Acronym	Title	Editor	Location of Text	Equivalent e.g., ISO/IEC	Timing ***
9	X.ott	Authentication framework with one-time telebiometric template	Yunsu Chung, Hyung-Woo Lee, Yongjin Lee, Kiyoung Moon	TD 0585		2011-3Q
9	X.th1	Telehealth and world-wide telemedicines – Generic telecommunication protocol	Jean-Paul Lemaire	TD 0211		2010-12
9	X.th2*	Telebiometrics related to physics	Jean-Paul Lemaire	TD 0088	ISO 80003-2	2010-12
9	X.th3*	Telebiometrics related to chemistry	Jean-Paul Lemaire	TD 0089	ISO 80003-3	2010-12
9	X.th4*	Telebiometrics related to biology	Jean-Paul Lemaire	TD 0090	IEC 80003-4	2010-12
9	X.th5*	Telebiometrics related to culturology	Jean-Paul Lemaire	TD 0091	IEC 80003-5	2010-12
9	X.th6*	Telebiometrics related to psychology	Jean-Paul Lemaire	TD 0092	IEC 80003-6	2010-12
9	X.tif	Integrated framework for telebiometric data protection in telehealth and worldwide telemedicines	Byoung-Jin Han, Hakil Kim, Yongjun Lee, Yong Nyuo Shin	TD 0582		2012-3Q
9	X.tpp-2	Telebiometrics protection procedures – Part 2: A guideline for secure transmission of multibiometric data	Yun-Su Chung, Youn-Hee Gil, Inja Jun, Ki-Young Moon	TD 0583		2010-12
10	X.1252*	Baseline identity management terms and definitions	Mike Harrop, Michael Hird	COM 17-R 11		In TAP
10	X.1275*	Guidelines on protection of personally identifiable information in the application of RFID technology	Hyangjin Lee	COM 17-R 12		In TAP
10	X.authi*	Authentication integration in identity management	Jianyong Chen, Lijun Liu, Hongwei Luo	TD 0548		2011
10	X.eaa*	Information technology – Security techniques – Entity authentication assurance	Richard Brackney	TD 0359 Rev.2	ISO/IEC 29115	2010-12
10	X.EVcert*	Extended validation certificate framework	Anthony Rutkowski	TD 0411	CA/Browser Forum EVcert specification	TBD
10	X.giim*	Generic identity management interoperability mechanisms	Jing Wu	TD 0542 Rev.1		2011

Q.	Acronym	Title	Editor	Location of Text	Equivalent e.g., ISO/IEC	Timing ***
10	X.idm-dm*	Common identity data model	Paul Knight, Anthony Nadalin	TD 4112 [2005-2008]		2010-12
10	X.idm-ifa*	Framework architecture for interoperable identity management systems	Marcin Dąbrowski, Piotr Pacyna	TD 0631 Rev.2		2011
10	X.idmgen*	Generic identity management framework	Richard Brackney, Zhaoji Lin	TD 0658		2011
10	X.idmsg*	Security guidelines for identity management systems	Sangrae Cho, Seung-Hun Jin	TD 0547		2011
10	X.priva*	Criteria for assessing the level of protection for personally identifiable information in identity management	Inkyoung Jeun, Hyangjin Lee	TD 0640		2011
11	E.115 (revised)	Computerized directory assistance	Erik Andersen	TD 0510[1]		2010-04
11	X.500 (revised)	Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services	Erik Andersen, Jean-Paul Lemaire	TD 0588[2], and TD 0589[3]	ISO/IEC 9594-1	2012
11	X.501 (revised)	Information technology – Open Systems Interconnection – The Directory: Models	Erik Andersen, Jean-Paul Lemaire	TD 0588[2], and TD 0589[3]	ISO/IEC 9594-2	2012
11	X.509 (revised)	Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks	Erik Andersen, Jean-Paul Lemaire	TD 0588[2], and TD 0589[3]	ISO/IEC 9594-8	2012
11	X.511 (revised)	Information technology – Open Systems Interconnection – The Directory: Abstract service definition	Erik Andersen, Jean-Paul Lemaire	TD 0588[2], and TD 0589[3]	ISO/IEC 9594-3	2012
11	X.518 (revised)	Information technology – Open Systems Interconnection – The Directory: Procedures for distributed operation	Erik Andersen, Jean-Paul Lemaire	TD 0588[2], and TD 0589[3]	ISO/IEC 9594-4	2012
11	X.519 (revised)	Information technology – Open Systems Interconnection – The Directory: Protocol specifications	Erik Andersen, Jean-Paul Lemaire	TD 0588[2], and TD 0589[3]	ISO/IEC 9594-5	2012
11	X.520 (revised)	Information technology – Open Systems Interconnection – The Directory: Selected attribute types	Erik Andersen, Jean-Paul Lemaire	TD 0588[2], and TD 0589[3]	ISO/IEC 9594-6	2012

[1] This is currently drafted as Amendment 1, *Support of E.115 capabilities*

[2] Relates currently to Amendment 1 to X.500-series, *Communication support enhancement* to be integrated in revised edition of the X.500-series

[3] Relates currently to Amendment 2 to X.500-series, *Password policy support* to be integrated in revised edition of the X.500-series

Q.	Acronym	Title	Editor	Location of Text	Equivalent e.g., ISO/IEC	Timing ***
11	X.521 (revised)	Information technology – Open Systems Interconnection – The Directory: Selected object classes	Erik Andersen, Jean-Paul Lemaire	TD 0588[2], and TD 0589[3]	ISO/IEC 9594-7	2012
11	X.525 (revised)	Information technology – Open Systems Interconnection – The Directory: Replication	Erik Andersen, Jean-Paul Lemaire	TD 0588[2], and TD 0589[3]	ISO/IEC 9594-9	2012
11	X.530 (revised)	Information technology – Open Systems Interconnection – The Directory: Use of systems management for administration of the Directory	Erik Andersen, Jean-Paul Lemaire	TD 0588[2], and TD 0589[3]	ISO/IEC 9594-10	2012
11	e-X.Imp500	Directory Implementers' Guide	Erik Andersen	online www.x500standard.com		
12 (4)	X.alerting	Procedures for the registration of arcs under the alerting object identifier arc	John Larmouth, Anthony Rutkowski	TD 0671 Rev.1		2010-12
12	X.oid-exp[4]	Object identifier repository export format			ISO 13582	2012
12	X.oid-res	Information technology – Object identifier resolution system	Jun Seob Lee	TD 0325	ISO/IEC 29168	2010-04
13	X.902 (revised)	Information technology – Open distributed processing – Reference model: Foundations	Arve Meisingset	LC text	ISO/IEC 10746-2	In AAP
13	X.903 (revised)	Information technology – Open distributed processing – Reference model: Architecture	Arve Meisingset	LC text	ISO/IEC 10746-3	In AAP
13	X.906, Cor.1	Information technology – Open distributed processing – Use of UML for ODP system specification – Technical Corrigendum 1	Arve Meisingset	LC text	ISO/IEC 19793, Cor.1	In AAP
13	Z.100 (revised)	Specification and description language: Overview of SDL-2010	Rick Reed	TD 0473		2010-04
13	Z.101	Specification and description language: Basic SDL-2010	Rick Reed	TD 0472		2010-04
13	Z.102	Specification and description language: Comprehensive SDL-2010	Rick Reed	TD 0471		2010-04
13	Z.103	Specification and description language: Shorthand notation and annotation in SDL-2010	Rick Reed	TD 0474		2010-04

[4] Subject to agreement with ISO TC 215 on collaborative work

Q.	Acronym	Title	Editor	Location of Text	Equivalent e.g., ISO/IEC	Timing ***
13	Z.104 (revised)	Specification and description language: Data and action language in SDL-2010	Rick Reed	TD 0477		2010-04
13	Z.105 (revised)	Specification and description language: SDL-2010 combined with ASN.1 modules	Rick Reed	TD 0475		2010-04
13	Z.106 (revised)	Specification and description language: Common interchange format (CIF) for SDL-2010	Rick Reed	TD 0476		2010-04
13	Z.109 (revised)	Specification and description language: SDL-2010 combined with UML	Thomas Weigert	TD 0516		2010-12
13	Z.120 (revised)	Message sequence chart (MSC)	Loïc Hélouët			TBD
13	Z.150 (revised)	User requirements notation (URN) – Language requirements and framework	Daniel Amyot			2010-12
13	Z.151 (revised)	User requirements notation (URN) – Language definition	Daniel Amyot			TBD
13	Z.Sup1** (revised)	Supplement 1 to Z-series Recommendations – ITU-T Z.100-series – Supplement on methodology on the use of description techniques	Thomas Weigert			2010-12
13	Z.Imp100** (revised)	Specification and description language Implementers' Guide – Version 2.0.0	Rick Reed	TD 0462		2010-04
13	Z.urn-ma	User requirements notation (URN): Methodological approach	Daniel Amyot			2010-12
13	Z.uml-msc	Unified modeling language (UML) profile for MSC	Thomas Weigert	TD 0444, TD 3308 [2005-2008]		TBD
13	Z.uml-urn	Unified modeling language (UML) profile for URN	Thomas Weigert			2010-12
14	Z.161 (revised)	Testing and Test Control Notation version 3: TTCN-3 core language	Dieter Hogrefe		ETSI ES 201 873-1	2010-04
14	Z.164 (revised)	Testing and Test Control Notation version 3: TTCN-3 operational semantics	Dieter Hogrefe		ETSI ES 201 873-4	2010-04
14	Z.165 (revised)	Testing and Test Control Notation version 3: TTCN-3 runtime interface (TRI)	Dieter Hogrefe		ETSI ES 201 873-5	2010-04
14	Z.166 (revised)	Testing and Test Control Notation version 3: TTCN-3 control interface (TCI)	Dieter Hogrefe		ETSI ES 201 873-6	2010-04
14	Z.167 (revised)	Testing and Test Control Notation version 3: TTCN-3 mapping from ASN.1	Dieter Hogrefe		ETSI ES 201 873-7	2010-04

Q.	Acronym	Title	Editor	Location of Text	Equivalent e.g., ISO/IEC	Timing ***
14	Z.168 (revised)	Testing and Test Control Notation version 3: TTCN-3 mapping from CORBA IDL	Dieter Hogrefe		ETSI ES 201 873-8	2010-04
14	Z.169 (revised)	Testing and Test Control Notation version 3: TTCN-3 mapping from XML data definition	Dieter Hogrefe		ETSI ES 201 873-9	2010-04

* Marked draft Recommendations are under TAP or for determination; all unmarked Recommendations are for consent
** Texts for approval
*** Target date for consent or determination of Recommendations or for approval of Appendices, Supplements or Implementers' Guides

ANNEX I

Summaries for work items under development in Study Group 17

WORKING PARTY 1/17 - NETWORK AND INFORMATION SECURITY

Question 2/17 – Security architecture and framework

X.1034 (revised), Guideline on extensible authentication protocol-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 Recommendation 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 the telecommunication operators. In the transforming from traditional basic network operators to comprehensive information service providers, the operators expand their services to telecommunication service, namely, communication service, content service and information service. The new services not only bring new users and new incomes to the operators, but also bring new security issues to the users as well as the operators themselves.

This Recommendation provides guidelines on security of the telecommunication information service for operators. The scope covers classification of telecommunication information service, security objective, requirement, mechanism, and 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.amg, Information asset maintenance guidelines in telecommunication organizations

This Recommendation provides an overview of procedures and methods that need to be addressed in place to identify, classify, and maintain the information assets which telecommunication

organizations have and manage. This also suggests the profile template as a method for maintaining information asset.

X.isgf, Information technology – Security techniques – Information security governance framework

This Recommendation | International Standard provides a framework of information security governance (ISG). Corporate governance requirements place increasing demands on organizations to demonstrate that they have effective internal control arrangements in place. One significant development is the inclusion of information security as part of operational risk in the wider corporate governance definition. Therefore, boards and executive management are increasingly looking for an ISG framework, which will help to achieve the objectives of the organization and meet corporate governance requirements.

The purpose of this Recommendation | International Standard is to promote effective, efficient, and acceptable use of information security activities in organizations by:

- assuring stakeholders that, if the Recommendation | International Standard 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.

The use of this Recommendation | International Standard will provide board of directors and management with the methodology to monitor and control (govern) the information security management system (ISMS) activities in order to meet the internal and external security requirements. Since many organizations need to establish and demonstrate the appropriate information security readiness to the various stakeholders, the governance concepts and implementation models proposed in this Recommendation | International Standard can support the process of directing and controlling the existing ISMS processes and controls.

The framework consists of objectives, principles, focus areas and implementation models of ISG and it shows how the ISG is related with ISMS. The framework needs to be supported by a successful ISMS.

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 | ISO/IEC 27011 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.

X.sgsm, Information security management guidelines for small and medium telecommunication organizations

This Recommendation provides guidelines for establishing and operating information security management for small and medium telecommunication organizations (SMTOs) in the telecommunication industry.

It covers some of necessary security controls from ITU-T X.1051 | ISO/IEC 27011 for information security management in the considering context of small and medium telecommunication organizations without huge cost and human resources to implement its information security

management system.

Question 4/17 - Cybersecurity

X.abnot, Abnormal traffic detection and control guideline for telecommunication network

This Recommendation defines the abnormal traffic protection scenarios, detection technologies, controlling measures and products deployment solutions for a telecommunication network. The aim is to provide a comprehensive guideline to monitor and control the abnormal traffic for telecommunication operators.

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.capec, Common attack pattern enumeration and classification

This Recommendation provides an open means to specify the identification, description, and enumeration of attack patterns. Attack patterns are a powerful mechanism to capture and communicate the attacker's perspective. They are descriptions of common methods for exploiting software. They derive from the concept of design patterns applied in a destructive rather than constructive context and are generated from in-depth analysis of specific real-world exploit examples.

X.cce, Common configuration enumeration

This Recommendation provides unique identifiers to system configuration issues in order to facilitate fast and accurate correlation of configuration data across multiple information sources and tools. For example, common configuration enumeration (CCE) identifiers can be used to associate checks in configuration assessment tools with statements in configuration best-practice documents.

X.cee, Common event expression

This Recommendation standardizes the way computer events are described, logged, and exchanged. By using common event expression's (CEE) common language and syntax, enterprise-wide log management, correlation, aggregation, auditing, and incident handling can be performed more efficiently and produce better results.

X.chirp, Cybersecurity heuristics and information request protocol

This Recommendation defines a flexible data representation that provides a framework for requesting information commonly exchanged by computer incident response teams (CIRTs) about computer security incidents.

X.cpe, Common platform enumeration

This Recommendation is a structured naming scheme for information technology systems, platforms, and packages. Based upon the generic syntax for uniform resource identifiers (URI), common platform enumeration (CPE) includes a formal name format, a language for describing complex platforms, a method for checking names against a system, and a description format for binding text and tests to a name.

X.crf, Common result format

This Recommendation is a standardized IT asset assessment result format that facilitates the exchange of assessment results among systems to increase tool interoperability and allow for the

aggregation of those results across large enterprises that utilize diverse technologies to detect patch levels, policy compliance, vulnerability, asset inventory, and other tasks. Common result format (CRF) leverages standards for common names and naming schemes to report the findings for assets.

X.cve, Common vulnerabilities and exposures

This Recommendation is a structured means to exchange information security vulnerabilities and exposures that aims to provide common names for publicly known problems. The goal of common vulnerabilities and exposures (CVE) is to make it easier to share data across separate vulnerability capabilities (tools, repositories, and services) with this "common enumeration." CVE is designed to allow vulnerability databases and other capabilities to be linked together, and to facilitate the comparison of security tools and services. As such, CVE does not contain information such as risk, impact, fix information, or detailed technical information. CVE only contains the standard identifier number with status indicator, a brief description, and references to related vulnerability reports and advisories.

X.cvss, Common vulnerability scoring system

This Recommendation provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. The goal of common vulnerability scoring system (CVSS) is to enable IT managers, vulnerability bulletin providers, security vendors, application vendors and researchers to speak from a common language of scoring IT vulnerabilities.

X.cwe, Common weakness enumeration

This Recommendation provides an open framework for exchanging unified, measurable sets of software weaknesses that enable more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems as well as better understanding and management of software weaknesses related to architecture and design.

X.cwss, Common weakness scoring system

This Recommendation provides for an open framework for communicating the characteristics and impacts of software weakness.

X.cybex, Cybersecurity information exchange framework

This Recommendation addresses an essential cybersecurity capability – a common framework for providers and cybersecurity centers to exchange cybersecurity related information in a structured and trusted way. This exchange may occur locally or globally among all kinds of communities and entities. This approach enables coherent, comprehensive, global, timely and trusted exchange of cybersecurity information using identified specifications and providing for their global use and information interoperability.

X.cybex.1, An OID arc for cybersecurity information exchange

This Recommendation specifies the allocation and use of an OID arc for the purposes of providing unique global identifiers for cybersecurity information exchange. This approach allows cybersecurity communities and organizations to maintain their autonomy in managing their own identifiers, including legacy uses, and achieving globalization.

X.cybex.2, Use of XML namespace in the cybersecurity information exchange framework

This Recommendation specifies the use of XML namespace for synergetic harmonization of structured data format standards in the cybersecurity information exchange framework.

X.cybex-beep, Definition of blocks extensible exchange protocol (BEEP) profile for cybersecurity information exchange framework

This Recommendation specifies the blocks extensible exchange protocol (BEEP) profile for use within cybersecurity information exchange framework.

X.cybex-disc, Discovery mechanisms in the exchange of cybersecurity information

This Recommendation provides methods and mechanisms which can be used to identify and locate sources of cybersecurity information, types of cybersecurity information, specific instances of cybersecurity information, methods available for access of cybersecurity information as well as policies which may apply to the access of cybersecurity information.

X.cybex-tp, Transport protocols supporting cybersecurity information exchange

This Recommendation provides an overview of exchange protocols which have been adopted and or adapted for use within the cybersecurity information exchange framework.

X.dexf, Digital evidence exchange file format

This Recommendation specifies extensible capabilities, structures and data elements for digital evidence exchange file formats, including both abstract syntax notation one (ASN.1) and extensible markup language (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.dpi, Deep packet inspection exchange format

This Recommendation defines a data representation that provides a framework for sharing information commonly exchanged by computer incident response teams (CIRTs) about the attributes of packet payloads associated with computer security incidents.

X.eipwa, Exchange of information for preventing web-based attacks

This Recommendation describes the framework for preventing the web-based attacks. It describes the use cases for distributing malwares through web, the functional capabilities, and the functional architecture for preventing web-based attacks.

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.gridf, SmartGrid incident exchange format

This Recommendation defines a data representation that provides a framework for sharing information commonly exchanged by computer incident response teams (CIRTs) about the attributes of SmartGrid security incidents.

X.iodef, Incident object description exchange format

This Recommendation defines a data representation that provides a framework for sharing information commonly exchanged by computer incident response teams (CIRTs) about computer security incidents.

X.oval, Open vulnerability and assessment language

This Recommendation provides an open framework for sharing publicly available security content, and standardizes the transfer of this information across the entire spectrum of security tools and services. Open vulnerability and assessment language (OVAL) includes a language used to encode system details, and an assortment of content repositories held throughout the cybersecurity community.

X.pfoc, Phishing, fraud, and other crimeware exchange format

This Recommendation extends the incident object description exchange format (IODEF) to support the reporting of phishing, fraud, and other types of electronic crime. The extensions also support the exchange on information about widespread spam incidents. These extensions are flexible enough to support information gleaned from activities throughout the entire electronic fraud or spam cycle.

X.scap, Security content automation protocol

This Recommendation provides an open framework for organizing and expressing security-related information in standardized ways, as well as related reference data such as unique identifiers for vulnerabilities. This Recommendation describes the requirements and conventions that are to be employed to ensure the consistent and accurate exchange of security content automation protocol (SCAP) content and the ability of the content to reliably operate on SCAP validated tools.

X.sips, Framework for countering cyber attacks in session initiation protocol (SIP)-based services

This Recommendation provides a framework for countering cyber attacks in session initiation protocol (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, Use cases and capabilities for security information sharing and exchange

This Recommendation describes high level use cases and capabilities of cybersecurity information sharing and exchange. This Recommendation provides use cases and capabilities important for supporting interoperability between applications for the sharing and exchange of cybersecurity information regarding the identification of threats, attacks, intrusions and other malicious behavior. The goal of the capabilities listed and described is to support more efficient and effective security operations by supporting the interoperable sharing and exchange of information between trusted parties working together to monitor, maintain and generally manage the security of systems and networks.

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 internet service provider (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.

X.teef, Cyber attack tracing event exchange format

This Recommendation defines a data model and an extensible markup language (XML) schema for cyber attack tracing event exchange format in order to determining attack paths and source of cyber attacks through networks. It also provides interoperability in tracing event transmission to simplify collaboration and data information exchange for traceback systems.

X.trm, Traceback mechanisms

This Recommendation describes various types of traceback mechanisms.

X.xccdf, Exensible configuration checklist description format

This Recommendation provides an open specification language for writing security checklists, benchmarks, and related kinds of documents. An extensible configuration checklist description format (XCCDF) document represents a structured collection of security configuration rules for some set of target systems. The specification is designed to support information interchange, document generation, organizational and situational tailoring, automated compliance testing, and compliance scoring.

Question 5/17 – Countering spam by technical means

X.fcsip, Framework for countering spam in IP-based multimedia applications

This Recommendation provides approaches and general framework for countering spam on IP-based multimedia applications such as IP telephony, instant messaging, multimedia conference, etc. It defines anti-spam functional units including *core anti-spam unit* (C-ASU), *recipient-side anti-spam unit* (R-ASU), and *sender-side anti-spam unit* (S-ASU) and specifies their functionalities in the anti-spam framework. It also describes interfaces among the functional entities and security considerations for countering IP multimedia spam.

X.ics, Functions and interfaces for countering email spam sent by botnet

This Recommendation specifies the functions and interfaces for countering email spam sent by botnet. In order for countering email spam sent by botnet, the functions and interfaces are defined in this Recommendation. And the reference model is described that the functions and interfaces are applied to the interactive gateway for countering spam defined in ITU-T X.tcs-1.

X.tcs, Technical means for countering spam

The 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 gateway system for countering spam

This Recommendation specifies interactive gateway system for countering spam as a technical mean for countering inter-domain spam. The gateway system enables spam notification among different domains, prevents spam traffic from one domain to the others. In addition, this Recommendation defines the architecture of the gateway system, describes basic entities, protocols and functions of the gateway system, and provides mechanisms for spam detection, information sharing and specific actions in the gateway system for countering spam.

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 requirements and architecture for key management including key hierarchy for the unicast and the multicast IPTV services in IPTV context. This Recommendation also develops a key management for downloadable service content protection (SCP), if downloadable SCP is deployed.

X.iptvsec-4, Algorithm selection scheme for service and content protection (SCP) descrambling

This Recommendation develops a set of algorithm selection functions from existing descrambling algorithms to share terminal devices between service providers and security providers. This includes algorithm selection scheme, signalling for the selection and interoperability issues.

X.iptvsec-5, Service and content protection (SCP) interoperability scheme

This Recommendation develops an interoperable service and content protection (SCP) architecture 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 defines network and service models for multicast telecommunication. It shows security threats and the requirements as countermeasures. The threats are defined on general and mobility-oriented and multicast specific aspects. Especially, the multicast-specific threats are analyzed in detail. Security requirements, framework and technologies are defined and explained as a main focus.

X.msec-5, Security requirements and mechanism for reconfiguration of mobile device with multiple communication interfaces

This Recommendation describes security requirements and mechanism for reconfiguration of mobile device with multiple communication interfaces. The security aspects of the mobile users, terminal devices, communication services and mobile networks with multiple communication interfaces are investigated. The Recommendation identifies security threats, followed by the description of security requirements. And it provides appropriate countermeasures including security reconfiguration mechanism.

X.msec-6, Security aspects of mobile phones

This Recommendation describes the security threats to mobile phones and specifies the security requirements for mobile phones.

X.usnsec-1, Information technology – Security framework for ubiquitous sensor network

This Recommendation | International Standard describes security threats and security requirements to the ubiquitous sensor network. In addition, this Recommendation 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 requirements and security technologies are presented for the ubiquitous sensor network.

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

Because of the obvious merits of peer-to-peer (P2P) network (such as the lower cost, the scalability and fault tolerance, etc.), some operators begin to consider the possibility to construct the next generation kernel network based on P2P. In order to implement an operable and manageable P2P-based telecommunication network, security solution must be a critical part to be studied.

This Recommendation provides a security guideline for a telecommunication network based on P2P technology. The characteristics of the network are briefly introduced, the security requirements of the network and services are analyzed in detail, and security solutions to fulfil these requirements are then specified.

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. This Recommendation includes management frameworks for both the basic model and the interoperable model, plus management requirements for providing OTP authentication service in a secure telecommunication network.

X.sap-4, The general framework of strong authentication on multiple authentication authorities environment

This Recommendation provides the general framework of strong authentication on multiple authentication authorities (AAs) environment for service provider to achieve strong authentication

like multi-factor authentication. The framework in this Recommendation describes models, basic operations and security requirements against each model components and each messages between model components to keep the total assurance of authentication in case of the combination of multiple AAs. In addition, the framework also describes models, basic operations and security requirements to support the authentication service that manages combination of multiple AAs.

X.sap-5, A guideline on anonymous authentication for e-commerce service

This Recommendation develops an anonymous authentication guideline and reference model for e-commerce because anonymous authentication can be used for providing privacy-preserving technology. This Recommendation describes privacy threats and security requirements for privacy enhanced e-commerce service. It also describes security functions that satisfy the security requirements and anonymous authentication reference models for e-commerce.

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. 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.3, The telebiometric multimodal model – A framework for the specification of security and safety aspects of telebiometrics – Amendment 3: Enhancement to support ISO/IEC 80000-series

This Amendment changes references to ISO 31 and IEC 60027 by references to ISO 80000 and IEC 80000 series which supersedes these two previous standards.

This Amendment also replaces a term “biosphere” by “1m radius biosphere”, per request by ISO/IEC/JTC 1/SC 37/WG 1, as “biosphere” is classically a bigger object, around planet Earth (Sol-3).

This Amendment also adds a sixth modality: “CALOR”.

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 arc **{joint-iso-itu-t(2) telebiometrics(42)}** allocated for the work on telebiometrics, with top level OID-IRI value **"/Telebiometrics".** This is primarily intended to provide Object Identifier support for an emerging protocol for telehealth). To support that work, Object Identifier values are needed for significant concepts in ITU-T X.1081 and ITU-T X.1082.

X.1082, Amd.2, Telebiometrics related to human physiology – Amendment 2: Enhancement to support ISO/IEC 80000-series

This Amendment updates the Recommendation to allow for further development.

This Amendment adds a sixth modality: “CALOR”.

X.gep, A guideline for evaluating telebiometric template protection techniques

This Recommendation describes a general guideline for testing the performance of biometric template protection techniques based on biometric cryptosystem and cancelable biometrics. This guideline clarifies targets of two biometric template protection techniques in telebiometrics system for evaluation reference models. Then, it defines the protection performance metrics for each biometric template protection technique and specifies requirements and procedures of evaluating methods.

X.ott, Authentication framework with one-time telebiometric template

This Recommendation describes a user-authentication framework with biometric one-time templates. The framework provides secure user-authentication and protection mechanisms for biometric templates transmitted over open networks. It prevents replay attacks and protects original biometric templates by generating a new disposable template for each authentication. This Recommendation also addresses the security requirements associated with the framework for biometric one-time templates

X.th1, Telehealth and world-wide telemedicines – Generic telecommunication 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 recognizes 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". 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 secure transmission of multibiometric data

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.

WORKING PARTY 3/17 - IDENTITY MANAGEMENT AND LANGUAGES

Question 10 - Identity management architecture and mechanisms

X.1252, 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.1275, Guidelines on protection of personally identifiable information in the application of RFID technology

This Recommendation recognizes that RFID technology renders information pertaining specifically to the merchandise worn or carried by individuals open to abuse even as it greatly facilitates access to and distribution of such information for useful purpose. The abuse can be manifest as tracking the location of the individual or invasion of his or her privacy in another malfeasant manner. For

this reason this Recommendation provides guidelines regarding the RFID procedures that can be used to enjoy the benefits of RFID while attempting to protect personally identifiable information.

X.authi, Authentication integration in identity management

This Recommendation provides a guideline for the telecom operators to implement the authentication integration of the network layer and the service layer, so that a user need not to be re-authenticated again in the service layer if (s)he has been strictly authenticated when access the operator's network. This Recommendation analyzes the scenarios in which the authentication integration can be implemented well. It also provides the technical frameworks and solutions for the authentication integration in these scenarios.

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 framework

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.giim, Generic identity management interoperability mechanisms

This Recommendation defines mechanisms to support interoperability across different identity management (IdM) services. Considering current IdM approaches, this recommendation describes the similarity and commonality of the different models while interoperating across domain boundaries.

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.idmgen, Generic identity management framework

This Recommendation provides a generic framework for identity management (IdM) that is independent of network types, technology or vendor specific products used to provide solutions, and operating environment. In addition, this Recommendation is independent of any service or scenarios specific model (e.g., web services, third party or federated models), assumptions or solution specifications. The primary purpose of this framework is to describe a structured approach for designing, defining, and implementing IdM solutions and facilitate interoperability in heterogeneous environments.

This framework is intended to be used as a foundation to develop and specify specific aspects of IdM such as detailed requirements, mechanisms and procedures as needed to facilitate interoperability between different federations, service providers or enterprises (e.g., government or private corporations) using different IdM systems and solutions based on different specifications or technology, and operating under different regulatory rules, policies and conditions.

There are no restrictions imposed on the applicability of this Recommendation. Since the described framework is generic it could be applied or used as appropriate to any specific IdM solution or networking environment such as private or public enterprises (e.g., government or private corporations), next generation network (NGN), managed IP networks.

X.idmsg, Security guidelines for identity management systems

This Recommendation proposes 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 network) or cyberspace environment. The security guidelines will focus on providing official advice how to employ various security mechanisms to protect a general IdM system and it will 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.

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

E.115 (revised), Computerized directory assistance

This Recommendation specifies the protocol, called the directory assistance protocol, to be used for directory assistance information exchange among service providers. This supports assistance/inquiry as part of the international telephone operator service. This Recommendation also gives a description of the principles and procedures to be followed in interconnecting different national computerized directory assistance services. It specifies two versions of the protocol. Version 1 specifies basic functions, while version 2 of the protocol provides enhancements and uses HTTP as the underlying service.

This revision provides important additions to allow directory assistance service providers to exchange information about databases supported and the functionalities that are available.

X.500 (revised), Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and service

This Recommendation | International Standard introduces the concepts of the Directory and the DIB (Directory Information Base) and overviews the services and capabilities which they provide.

This revision includes extended interworking with LDAP, extended support for tag-based applications, and a set of rules that controls how passwords are used and administered in the Directory.

X.501 (revised), Information technology – Open Systems Interconnection – The Directory: Models

This Recommendation | International Standard provides a number of different models for the Directory as a framework for the other Directory Recommendations | International Standards. The models are the overall (functional) model, the administrative authority model, generic Directory Information models providing Directory User and Administrative User views on Directory information, generic Directory System Agent (DSA) and DSA information models and operational framework and a security model.

This revision includes extended interworking with LDAP, extended support for tag-based applications, and a set of rules that controls how passwords are used and administered in the Directory.

X.509 (revised), Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks

This Recommendation | International Standard defines a framework for public-key certificates and attribute certificates. These frameworks may be used by other standards bodies to profile their application to Public Key Infrastructures (PKI) and Privilege Management Infrastructures (PMI). Also, this Recommendation | International Standard defines a framework for the provision of authentication services by Directory to its users. It describes two levels of authentication: simple authentication, using a password as a verification of claimed identity; and strong authentication, involving credentials formed using cryptographic techniques. While simple authentication offers some limited protection against unauthorized access, only strong authentication should be used as the basis for providing secure services

This revision includes extended interworking with LDAP, extended support for tag-based applications, and a set of rules that controls how passwords are used and administered in the Directory.

X.511 (revised), Information technology – Open Systems Interconnection – The Directory: Abstract service definition

This Recommendation | International Standard defines in an abstract way the externally visible service provided by the Directory, including bind and unbind operations, read operations, search operations, modify operations and errors.

This revision includes extended interworking with LDAP, extended support for tag-based applications, and a set of rules that controls how passwords are used and administered in the Directory.

X.518 (revised), Information technology – Open Systems Interconnection – The Directory: Procedures for distributed operation

This Recommendation | International Standard specifies the procedures by which the distributed components of the Directory interwork in order to provide a consistent service to its users.

This revision includes extended interworking with LDAP, extended support for tag-based applications, and a set of rules that controls how passwords are used and administered in the Directory.

X.519 (revised), Information technology – Open Systems Interconnection – The Directory: Protocol specifications

This Recommendation | International Standard specifies the Directory Access Protocol, the Directory System Protocol, the Directory Information Shadowing Protocol and the Directory Operational Binding Management Protocol fulfilling the abstract services specified in ITU-T X.501 | ISO/IEC 9594-2, ITU-T X.511 | ISO/IEC 9594-3, ITU-T X.518 | ISO/IEC 9594-4 and ITU-T X.525 | ISO/IEC 9594-9. It includes specifications for supporting underlying protocols to reduce the dependency on external specifications.

This revision includes extended interworking with LDAP, extended support for tag-based applications, and a set of rules that controls how passwords are used and administered in the Directory.

X.520 (revised), Information technology – Open Systems Interconnection – The Directory: Selected attribute types

This Recommendation | International Standard defines a number of attribute types and matching rules which may be found useful across a range of applications of the Directory. One particular use for many of the attributes defined is in the formation of names, particularly for the classes of object defined in ITU-T X.521 | ISO/IEC 9594-7.

This revision includes extended interworking with LDAP, extended support for tag-based applications, and a set of rules that controls how passwords are used and administered in the Directory.

X.521 (revised), Information technology – Open Systems Interconnection – The Directory: Selected object classes

This Recommendation | International Standard defines a number of selected object classes and name forms which may be found useful across a range of applications of the Directory. An object class definition specifies the attribute types which are relevant to the objects of that class. A name form definition specifies the attributes to be used in forming names for the objects of a given class.

This revision includes extended interworking with LDAP, extended support for tag-based applications, and a set of rules that controls how passwords are used and administered in the Directory.

X.525 (revised), Information technology – Open Systems Interconnection – The Directory: Replication

This Recommendation | International Standard specifies a shadow service which Directory system agents (DSAs) may use to replicate Directory information. The service allows Directory information to be replicated among DSAs to improve service to Directory users, and provides for the automatic updating of this information.

This revision includes extended interworking with LDAP, extended support for tag-based applications, and a set of rules that controls how passwords are used and administered in the Directory.

X.530 (revised), Information technology – Open Systems Interconnection – The Directory: Use of systems management for administration of the Directory

This Recommendation | International Standard describes the requirements for Directory management, and analyses these requirements to identify those that may be realized by OSI systems management services (and protocols), those that are realized by Directory services (and protocols), and those that are realized by local means.

This revision includes extended interworking with LDAP, extended support for tag-based applications, and a set of rules that controls how passwords are used and administered in the Directory.

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

X.alerting, Procedures for the registration of arcs under the alerting object identifier arc

This Recommendation describes the procedures for the registration and implementation of arcs under the alerting object identifier arc. These provisions include: responsibilities of registration authorities, criteria for acceptance, operation of the registration authority, registration application, registration announcement, time-scale for processing applications and publication, notice of rejection, change of registration information, fees, appeals process, and re-appointment of the registration authority.

X.oid-exp, Object identifier repository export format

This Recommendation | International Standard specifies both an XML and a binary export format for object identifier repositories, including additional requirements for e-health repositories.

X.oid-res, Information technology – 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.902 (revised), Information technology – Open distributed processing – Reference model: Foundations

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.

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.

X.906, Cor 1, Information technology – Open distributed processing – Use of UML for ODP system specification – Technical Corrigendum 1

This corrigendum corrects the following three defects:

1) The standard currently proposes attaching a UML comment to a piece of behaviour to express that it requires, creates or fulfils an obligation, permission, prohibition or authorization i.e. to

express deontic rules. Concerns have been expressed about the traceability and management of UML comments, particularly in the specifications of very large-scale systems.

2) The standard currently uses the UML construct "note" where it should use "comment"

3) The standard has a typographical error in the cardinalities of figure 9.

Z.100 (revised), Specification and description language: Overview of SDL-2010

This Recommendation is a part of the set of *Specification and description language* Recommendations for SDL-2010. 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-2010 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-2010.

Z.101, Specification and description language: Basic SDL-2010

This Recommendation is part of the set of *Specification and description language* Recommendations for SDL-2010. 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-2010

This Recommendation is part of the set of *Specification and description language* Recommendations for SDL-2010. 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-2010

This Recommendation is part of the set of *Specification and description language* Recommendations for SDL-2010. 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-2010

This Recommendation is part of the set of *Specification and description language* Recommendations for SDL-2010. It adds the data and action language used to define data types and expressions. In SDL-2010 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-2010. 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-2010 combined with ASN.1 modules

This Recommendation is part of the set of *Specification and description language* Recommendations for SDL-2010. It defines how Abstract Syntax Notation One (ASN.1) modules can be used in combination with SDL-2010. 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-2010, 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-2010

This Recommendation is part of the set of *Specification and description language* Recommendations for SDL-2010. 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-2010.

Z.109 (revised), Specification and description language: SDL-2010 combined with UML

This Recommendation is part of the set of *Specification and description language* Recommendations for SDL-2010. It defines a unified modeling language (UML) profile that maps to SDL-2010 semantics so that UML can be used in combination with SDL. The combined use of SDL-2010 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-2010, 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.150 (revised), User requirements notation (URN) - Language requirements and framework

This Recommendation with other Recommendations in the ITU-T Z.150 series defines user requirements notation (URN) 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 modeling 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.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 unified modeling language (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-2010:

- 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.

Z.uml-msc, Unified modeling language (UML) profile for MSC

This Recommendation defines a unified modeling 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-urn, Unified modeling language (UML) profile for URN

This Recommendation defines a unified modeling 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-2010, 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.

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.

The core language of TTCN-3 can be expressed in a variety of presentation formats. While this Recommendation defines the core language, ITU-T Z.162 defines the tabular format for TTCN (TFT) and ITU-T Z.163 defines the graphical format for TTCN (GFT). The specification of these formats is outside the scope of this Recommendation. The core language serves three purposes:

1) as a generalized text-based test language;

2) as a standardized interchange format of TTCN test suites between TTCN tools;

3) as the semantic basis (and where relevant, the syntactical basis) for the various presentation formats.

The core language may be used independently of the presentation formats. However, neither the tabular format nor the graphical format can be used without the core language. Use and implementation of these presentation formats shall be done on the basis of the core language.

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 operational semantics are necessary to unambiguously interpret the specifications made with TTCN-3. This 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.

The interface is defined to be compatible with ITU-T Z.161. This Recommendation uses the CORBA interface definition language (IDL) to specify the TRI completely. Clauses 6 and 7 specify language mappings of the abstract specification to the target languages Java and ANSI-C. A summary of the IDL-based interface specification is provided in Annex A.

Z.166 (revised), Testing and Test Control Notation version 3: TTCN-3 control interface (TCI)

This Recommendation specifies the control interfaces for TTCN-3 test system implementations. The TTCN-3 control interfaces provide a standardized 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.

The interfaces are defined to be compatible with the TTCN-3 standards (see clause 2). The interface definition uses the CORBA interface definition language (IDL) to specify the TCI completely. Clauses 8 and 9 present language mappings for this abstract specification to the target languages Java and ANSI C. A summary of the IDL-based interface specification is provided in Annex A.

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, ITU-T X.681, ITU-T X.682 and ITU-T X.683 with TTCN-3. The harmonization of other languages with TTCN-3 is not covered by this Recommendation.

Z.168 (revised), Testing and Test Control Notation version 3: TTCN-3 mapping from CORBA IDL

This Recommendation defines the mapping rules for CORBA interface definition language (IDL) to TTCN-3 (as defined in ITU-T Z.161) to enable testing of CORBA-based systems. The principles of mapping CORBA IDL to TTCN-3 can be also used for the mapping of interface specification languages of other object-/component-based technologies.

The specification of other mappings is outside the scope of this Recommendation.

Z.169 (revised), Testing and Test Control Notation version 3: TTCN-3 mapping from XML data definition

This Recommendation defines the mapping rules for W3C Schema to TTCN-3 to enable testing of XML-based systems, interfaces and protocols.

_____