|  |  |  |
| --- | --- | --- |
| itu_logo | World Telecommunication Standardization Assembly (WTSA-16)Yasmine Hammamet, 25 October - 3 November 2016 | CCITT/ITU-T 60th Anniversary logo |
| INTERNATIONAL TELECOMMUNICATION UNION |  |
|  |  |
| PLENARY MEETING | Revision 1 toDocument 19-E |
|  | 14 October 2016 |
|  | Original: English |
|  |
| ITU-T Study Group 17 |
| Security |
| REPORT of ITU-T sg17 TO THE WORLD TELECOMMUNICATION STANDARDIZATION ASSEMBLY (WTSA-16), PART I: GENERAL |

|  |  |
| --- | --- |
| **Abstract:** | This contribution contains the report of ITU-T Study Group 17 to WTSA-16 concerning its activities during the 2013-2016 study period. |

Note by the TSB:

The report of Study Group 17 to the WTSA-16 is presented in the following documents:

Part I: **Document 19** – General; including proposed changes to WTSA Resolution 2 in Annex 2

Revision 1 of Part I provides updates reflecting the outcome of 8th Study Group 17 meeting,
Status: 14 October 2016.

Part II: **Document 20** – Questions proposed for study during the study period 2017-2020

**CONTENTS**

|  Page |
| --- |
| [1 Introduction 3](#_Toc464191837)[2 Organization of work 8](#_Toc464191838)[3 Results of the work accomplished during the 2013-2016 study period 12](#_Toc464191839)[4 Observations concerning future work 44](#_Toc464191840)[5 Updates to the WTSA Resolution 2 for the 2017-2020 study period 45](#_Toc464191841)[ANNEX 1 List of Recommendations, Supplements and other materials produced or deleted during the study period 46](#_Toc464191842)[ANNEX 2 Proposed updates to the Study Group 17 mandate and Lead Study Group roles 62](#_Toc464191843) |

# 1 Introduction

## 1.1 Responsibilities of Study Group 17

Study Group 17 was entrusted by the World Telecommunication Standardization Assembly (Dubai, 2012) with the study of 12 Questions in the area of security including cybersecurity, countering spam and identity management. SG17 is also responsible for the application of open system communications including directory and object identifiers, and for technical languages, the method for their usage and other issues related to the software aspects of telecommunication systems.

Annex A to WTSA-12 Resolution 2 states the following mandate for Study Group 17, Security:

*ITU-T Study Group 17 is responsible for building confidence and security in the use of information and communication technologies (ICT). This includes studies relating to cybersecurity, security management, countering spam and identity management. It also includes security architecture and framework, protection of personally identifiable information, and security of applications and services for the Internet of things, smart grid, smartphone, Internet Protocol television (IPTV), web services, social network, cloud computing, mobile financial system and telebiometrics. Study Group 17 is also responsible for the application of open system communications, including directory and object identifiers, and for technical languages, the method for their usage and other issues related to the software aspects of telecommunication systems, and for conformance testing to improve the quality of Recommendations.*

Annex A to WTSA-12 Resolution 2 states the following lead study group responsibilities for Study Group 17, Security:

*- Lead study group on security*

*- Lead study group on identity management (IdM)*

*- Lead study group on languages and description techniques.*

Annex B to WTSA-12 Resolution 2 defines the following responsibilities of SG17:

*ITU-T Study Group 17 is responsible for building confidence and security in the use of information and communication technologies (ICT). This includes studies relating to security, including cybersecurity, countering spam and identity management. It also includes security architecture and framework, security management, protection of personally identifiable information (PII), and security of applications and services for the Internet of things (IoT), smart grid, smartphone, Internet Protocol television (IPTV), web services, social network, cloud computing, mobile financial system and telebiometrics. Study Group 17 is also responsible for the application of open system communications, including directory and object identifiers, and for technical languages, the method for their usage and other issues related to the software aspects of telecommunication systems, and for conformance testing to improve quality of Recommendations.*

*In the area of security, Study Group 17 is responsible for developing the core Recommendations on ICT security, such as security architecture and frameworks; the fundamentals related to cybersecurity, including threats, vulnerabilities and risks, incident handling/response and digital forensics; security management, including management of PII; countering spam by technical means. In addition, Study Group 17 provides overall coordination of security work in ITU-T.*

*In addition, Study Group 17 is responsible for developing the core Recommendations on security aspects of applications and services in the areas of IPTV, smart grid, IoT, social network, cloud computing, smartphone, mobile financial system and telebiometrics.*

*Study Group 17 is also responsible for developing the core Recommendations on a generic identity management model that is independent of network technologies and supports the secure exchange of identity information between entities. This work also includes studying the process for discovery of authoritative sources of identity information; generic mechanisms for the bridging/interoperability of a diverse set of identity information formats; identity management threats, the mechanisms to counter them, the protection of PII and the development of mechanisms to ensure that access to PII is only authorized when appropriate.*

*In the area of open system communication, Study Group 17 is responsible for Recommendations in the following areas:*

* *directory services and systems, including public key infrastructure (PKI) (ITU-T F.500- and ITU-T X.500-series);*
* *object identifiers (OIDs) and associated registration authorities (ITU-T X.660/ITU-T X.670-series);*
* *open systems interconnection (OSI), including Abstract Syntax Notation One (ASN.1) (ITU-T F.400-, ITU-T X.200-, ITU-T X.400-, ITU-T X.600-, ITU-T X.800-series); and*
* *open distributed processing (ODP) (ITU-T X.900-series).*

*In the area of languages, Study Group 17 is responsible for studies on modelling, specification and description techniques. This work, which includes languages such as ASN.1, SDL, MSC and URN, will be developed in line with the requirements of and in cooperation with the relevant study groups such as Study Group 2, Study Group 9, Study Group 11, Study Group 13, Study Group 15 and Study Group 16.*

Annex C to WTSA-12 Resolution 2 (as modified by TSAG) defines the list of Recommendations under the responsibility of Study Group 17 in the 2013-2016 study period:

* *ITU-T E.104, ITU-T E.115, ITU-T E.409 (in conjunction with Study Group 2)*
* *ITU-T F.400-series; ITU-T F.500 − ITU-T F.549*
* *ITU-T X-series, except those under the responsibility of Study Groups 2, 11, 13, 15, and 16*
* *ITU-T Z-series except ITU-T Z.300-series and ITU-T Z.500-series.*

## 1.2 Management team and meetings held by Study Group 17

WTSA-12 appointed Mr Arkadiy KREMER (Russian Federation) as Study Group 17 chairman and appointed the following nine vice-chairmen Khalid BELHOUL (United Arab Emirates), Mohamed M.K. ELHAJ (Sudan), Mario German FROMOW RANGEL (Mexico), Antonio GUIMARAES (Brazil), Zhaoji LIN (China), Patrick MWESIGWA (Uganda), Koji NAKAO (Japan), Sacid SARIKAYA (Turkey), and Heung Youl YOUM (Korea). Mr FROMOW RANGEL did not participate in any meetings of Study Group 17.

Study Group 17 met eight times in plenary in the course of the study period (see Table 1).

TABLE 1
Meetings of Study Group 17 and its Working Parties

| Meetings | Date | Reports |
| --- | --- | --- |
| Study Group 17 | Geneva, 17 – 26 April 2013 | COM 17 – R 1 to R 8 |
| Study Group 17 | Geneva, 26 August – 4 September 2013 | COM 17 – R 9 to R 22 |
| Study Group 17 | Geneva, 15 – 24 January 2014 | COM 17 – R 23 to R 29 |
| Study Group 17 | Geneva, 17 – 26 September 2014 | COM 17 – R 30 to R 36 |
| Study Group 17 | Geneva, 8 – 17 April 2015 | COM 17 – R 37 to R 45 |
| Study Group 17 | Geneva, 8 – 17 September 2015 | COM 17 – R 46 to R 57 |
| Study Group 17 | Geneva, 14 – 23 March 2016 | COM 17 – R 58 to R 66 |
| Study Group 17 | Geneva, 29 August – 7 September 2016 | COM 17 – R 67 to R 80 |

Management team meetings took place in conjunction with each Study Group 17 meeting.

In addition many Rapporteurs’ meetings (including e-meetings) took place during the study period in different locations, see Table 1-bis.

TABLE 1-bis
Rapporteur meetings organized under Study Group 17 during the study period

| Dates | Place/Host | Question(s) | Event name |
| --- | --- | --- | --- |
| 2013-01-14 | Korea (Rep. of) [Seoul]/ Soonchunhyang University and KISA | 3/17 | Q3/17 interim Rapporteur group meeting |
| 2013-01-22 to2013-01-24 | China [Beijing]/China Academy of Telecommunication Research of MIIT (CATR) | 8/17 | Q8/17 interim Rapporteur group meeting |
| 2013-01-23 to2013-01-25 | E-Meeting | 4/17 | Q4/17 interim Rapporteur group meeting |
| 2013-02-19 to2013-02-22 | Switzerland [Geneva]/ITU | 8/17 | Q8/17 interim Rapporteur group meeting |
| 2013-06-17 to2013-06-21 | Korea (Rep. of) [Seoul]/Korean Agency for Technology and Standards (KATS) | 11/17 | Q11/17 interim Rapporteur group meeting with ISO/IEC JCT 1/SC 6 |
| 2013-07-02 to2013-07-03 | E-Meeting | 4/17 | Q4/17 interim Rapporteur group meeting |
| 2013-07-08 to2013-07-10 | China [Guangzhou]/China Telecom | 8/17 | Q8/17 interim Rapporteur group meeting |
| 2013-07-09 to2013-07-10 | France [Paris]/LegalBox | 11/17 | Q11/17 interim Rapporteur group meeting |
| 2013-12-04 to2013-12-05 | Korea (Rep. of) [Seoul]/TOZ | 3/17 | Q3/17 interim Rapporteur group meeting |
| 2014-02-17 to2014-02-21 | Canada [Ottawa]/Ericsson | 11/17 | Q11/17 interim Rapporteur group meeting jointly with ISO/IEC JTC 1/SC 6/WG10 |
| 2014-04-07 to2014-04-11 | Hongkong [China]/ISO/IEC JTC 1/SC 27 | 3/17 | Q3/17 interim Rapporteur group meeting jointly with ISO/IEC JTC 1/SC 27/WG5 |
| 2014-05-07 to2014-05-08 | E-Meeting | 10/17 | Q10/17 interim Rapporteur group meeting |
| 2014-06-17 to2014-06-18 | United States [Charlotte, North Carolina]/Bank of America | 10/17 | Q10/17 interim Rapporteur group meeting |
| 2014-06-24 to2014-06-26 | Korea (Rep. of) [Seoul]/KR organizations | 6/17 | Q6/17 interim Rapporteur group meeting |
| 2014-06-25 to2014-06-26 | Korea (Rep. of) [Seoul]/KR organizations | 7/17 | Q7/17 interim Rapporteur group meeting |
| 2014-06-25 to2014-06-26 | Korea (Rep. of) [Seoul]/KR organizations | 3/17 | Q3/17 interim Rapporteur group meeting |
| 2014-07-01 to2014-07-03 | China [Beijing]/China Academy of Telecommunication Research of MIIT (CATR) | 8/17 | Q8/17 interim Rapporteur group meeting |
| 2014-07-16 to2014-07-17 | E-Meeting | 4/17 | Q4/17 interim Rapporteur group meeting |
| 2014-07-16 | E-Meeting | 11/17 | Q11/17 interim Rapporteur group meeting |
| 2014-10-20 to2014-10-24 | United Kingdom [London]/British Standards Institution | 11/17 | Q11/17 interim Rapporteur group meeting jointly with ISO/IEC JTC 1/SC 6/WG10 |
| 2014-12-15 to2014-12-17 | China [Beijing]/China Academy of Telecommunication Research of MIIT (CATR) | 8/17 | Q8/17 interim Rapporteur group meeting |
| 2015-01-15 to2015-01-16 | Korea (Rep. of) [Seoul]/Telecommunications Technology Association (TTA) | 3/17, 6/17 | Q6/17 and Q3/17 interim Rapporteur group meetings |
| 2015-01-27 to2015-01-28 | E-Meeting | 4/17 | Q4/17 interim Rapporteur group meeting |
| 2015-01-29 | E-Meeting | 10/17 | Q10/17 interim Rapporteur group meeting |
| 2015-02-02 | E-Meeting | 10/17 | Q10/17 interim Rapporteur group meeting |
| 2015-02-05 | E-Meeting | 10/17 | Q10/17 interim Rapporteur group meeting |
| 2015-05-25 to2015-05-29 | Belgium [Gent]/Ghent University - iMinds | 11/17 | Q11/17 interim Rapporteur group meeting jointly with ISO/IEC JTC 1/SC 6/WG10 |
| 2015-07-09 to2015-07-10 | E-Meeting | 4/17 | Q4/17 interim Rapporteur group meeting |
| 2015-07-09 to2015-07-10 | Korea (Rep. of) [Seoul]/KISA | 6/17 | Q6/17 interim Rapporteur group meeting |
| 2015-07-09 | Korea (Rep. of) [Seoul]/KISA | 3/17 | Q3/17 interim Rapporteur group meeting |
| 2015-07-16 to2015-07-17 | China [Beijing]/China Academy of Telecommunication Research of MIIT (CATR) | 8/17 | Q8/17 interim Rapporteur group meeting |
| 2015-07-22 to2015-07-24 | United States [New York]/Aetna | 10/17 | Q10/17 interim Rapporteur group meeting |
| 2016-01-07 to2016-01-08 | Korea (Rep. of) [Seoul]/TOZ | 10/17 | Q10/17 interim Rapporteur group meeting |
| 2016-01-07 to2016-01-08 | Korea (Rep. of) [Seoul]/TOZ | 3/17 | Q3/17 interim Rapporteur group meeting |
| 2016-01-07 to2016-01-08 | Korea (Rep. of) [Seoul]/TOZ | 6/17 | Q6/17 interim Rapporteur group meeting |
| 2016-01-18 to2016-01-19 | E-Meeting | 4/17 | Q4/17 interim Rapporteur group meeting |
| 2016-02-29 to2016-03-04 | China [Xian]/Standardization Administration of the People’s Republic of China (SAC) | 11/17 | Q11/17 interim Rapporteur group meeting jointly with ISO/IEC JTC 1/SC 6/WG10 |
|  |  |  |  |
| 2016-06-28 to2016-06-29 | Korea (Rep. of) [Seoul]/KISA | 3/17 | Q3/17 interim Rapporteur group meeting |
| 2016-06-28 to2016-06-29 | Korea (Rep. of) [Seoul]/KISA | 2/17 | Q2/17 interim Rapporteur group meeting |
| 2016-06-28 to2016-06-29 | Korea (Rep. of) [Seoul]/KISA | 7/17 | Q7/17 interim Rapporteur group meeting |
| 2016-06-28 to2016-06-29 | Korea (Rep. of) [Seoul]/KISA | 6/17 | Q6/17 interim Rapporteur group meeting |
| 2016-06-30 to2016-07-01 | China [Guangzhou]/China Telecom | 8/17 | Q8/17 interim Rapporteur group meeting |
| 2016-07-14 to2016-07-15 | United States [New York]/Aetna | 10/17 | Q10/17 interim Rapporteur group meeting |
| 2016-07-18 | E-Meeting | 4/17 | Q4/17 interim Rapporteur group meeting |

# 2 Organization of work

## 2.1 Organization of studies and allocation of work

**2.1.1** At its first meeting of the study period, Study Group 17 decided to establish 5 working parties.

**2.1.2** Table 2 shows the number and title of each Working Party, together with the number of Questions assigned to it and the name of its Chairman.

**2.1.3** Table 3 lists other groups created by Study Group 17 during the study period.

**2.1.4** In line with WTSA-12 Resolution 54, at its April 2015 SG17 meeting, the African Regional Group for SG17 was created; see section 3.3.5.

During the study period, two **Joint Coordination Activities (JCAs)** proposed by Study Group 17 were continued and endorsed by TSAG.

**- Joint Coordination Activity on Identity Management (JCA-IdM)**

The Joint Coordination Activity on Identity Management (JCA-IdM) continued from the former study period with the objective to coordinate the ITU‑T identity management (IdM) work in collaboration with external bodies. Highlights of achievements of the JCA-IdM are given in 3.3.4.1.

**- Joint Coordination Activity on Child Online Protection (JCA-COP)**

The Joint Coordination Activity on Child Online Protection (JCA-COP), continued from the former study period with the objective to coordinate the ITU-T child online protection (COP) work amongst the ITU-T study groups, and to liaise with ITU-R and ITU-D as well as with the Council Working Group on Child Online Protection. Highlights of achievements of the JCA-COP are given in 3.3.4.2.

**2.1.5** During the study period, two **projects** were continued by Study Group 17.

**- ASN.1 Project**

The ASN.1 project, established during the 2001-2004 study period, has continued to assist users of ASN.1 (Recommendations ITU‑T X.680-, X.690- and X.890-series) within and outside of ITU‑T, and to promote the use of ASN.1 across a wide range of industries and standards bodies. Highlights of achievements of the project are given in 3.4.1.

**- OID Project**

The OID Project, established during the 2001-2004 study period, has continued to assist and support users of Object Identifiers (OIDs) registered in accordance with the X.660- and X.670-series of Recommendations within and outside of ITU‑T. Highlights of achievements of the project are given in 3.4.2.

TABLE 2
Organization of Study Group 17

| Designation | Questions to be studied | Title of the Working Party | Working Party Chairmen |
| --- | --- | --- | --- |
| WP 1/17 | 1, 2, 3 | Fundamental security | Koji NAKAO |
| WP 2/17 | 4, 5 | Network and information security | Sacid SARIKAYA |
| WP 3/17 | 8, 10 | Identity management and cloud computing security | Heung Youl YOUM |
| WP 4/17 | 6, 7, 9 | Application security | Antonio GUIMARAES |
| WP 5/17 | 11, 12 | Formal languages | Zhaoji LIN |

TABLE 3
Other Groups (if any)

| Title of the Group | Chairman | Vice-Chairmen |
| --- | --- | --- |
| JCA-IdM | Co-chairmen: Richard BRACKNEY(1), Jon SHAMAH(2), Hiroshi TAKECHI(3), Abbie BARBIR(4) |  |
| JCA-COP | Co-chairman: Ashley HEINEMAN(5), Philip RUSHTON |  |
| SG17-RG-AFR | Michael KATUNDU | **Mohamed M. K. Elhaj,Patrick Mwesigwa,Mohamed Touré** |
| ASN.1 Project | Project leader: Paul THORPE |  |
| OID Project | Project leader: Olivier DUBUISSON |  |

Notes:

(1) Co-chairman passed away 12 September 2013.

(2) Co-chairing until September 2013.

(3) Co-chairing since 4 September 2013.

(4) Co-chairing since 24 January 2014.

(5) Co-chairing until 31 January 2016.

## 2.2 Questions and Rapporteurs

**2.2.1** WTSA-12 assigned to Study Group 17 the following 12 Questions listed in Table 4 and SG17 appointed the listed Rapporteurs and Associate Rapporteurs.

**2.2.2** The Questions listed in Table 5 have been adopted anew during this period.

Note – While no new Questions were adopted, Questions 6/17, 8/17 and 12/17 were modified during the study period.

**2.2.3** The Questions listed in Table 6 have been deleted during this period.

TABLE 4
Study Group 17 – Questions assigned by WTSA-12 and Rapporteurs

| Questions | Title of the Questions | WP | Rapporteur |
| --- | --- | --- | --- |
| Q1/17 | Telecommunication/ICT security coordination | 1/17 | Mohamed M. K. ELHAJAssociate Rapporteurs:Hua JIANG(7),Young Wha KIM(2),Cai CHEN(13),Isaac Kobina KWARKO,Yiwen WANG(12) |
| Q2/17 | Security architecture and framework | 1/17 | Patrick MwesigwaAssociate Rapporteurs:Zhiyuan HU(1),Dmitry V. KOSTROV(7),Heung Ryong Oh |
| Q3/17 | Telecommunication information security management | 1/17 | Miho NaganumaAssociate Rapporteur:Kyeong Hee OH |
| Q4/17 | Cybersecurity | 2/17 | Youki KadobayashiAssociate Rapporteurs:Michael KATUNDU(1),Jong Hyun Kim,Ibrahim Hamza AL MALLOUHI |
| Q5/17 | Countering spam by technical means | 2/17 | Hongwei Luo(10)Yanbin ZHANG(11)Associate Rapporteur:Seokung YOON(3) |
| Q6/17 | Security aspects of ubiquitous telecommunication services | 4/17 | Jonghyun BaekAssociate Rapporteur:Yutaka Miyake,Bo YU(12) |
| Q7/17 | Secure application services | 4/17 | Jae Hoon NahAssociate Rapporteur:Lijun LIU(5)Huirong TIAN(8) |
| Q8/17 | Cloud computing security | 3/17 | Liang WeiAssociate Rapporteurs:Mark JEFFREY(9),Victor KUTUKOV |
| Q9/17 | Telebiometrics | 4/17 | John George CARASAssociate Rapporteur:Yong Nyuo SHIN |
| Q10/17 | Identity management architecture and mechanisms | 3/17 | Abbie BarbirAssociate Rapporteurs:Richard BRACKNEY(6),Hiroshi TAKECHI(4),Junjie XIA(3) |
| Q11/17 | Generic technologies to support secure applications | 5/17 | Erik AndersenAssociate Rapporteur:Jean-Paul LEMAIRE |
| Q12/17 | Formal languages for telecommunication software and testing | 5/17 | Dieter HogrefeAssociate Rapporteurs:Gunter MUSSBACHER,Rick Reed |

Note:

(1) Appointed associate Rapporteur (17 April 2015)

(2) Appointed associate Rapporteur (8 April 2015)

(3) Appointed associate Rapporteur (24 January 2014)

(4) Appointed associate Rapporteur (4 September 2013)

(5) Appointed associate Rapporteur (9 October 2015)

(6) Associate Rapporteur passed away 12 September 2013

(7) Associate Rapporteur until March 2015

(8) Associate Rapporteur stepped-down (27 September 2015)

(9) Associate Rapporteur stepped-down (26 February 2016)

(10) Rapporteur until 17 September 2015

(11) Appointed Rapporteur (14 March 2016)

(12) Appointed associate Rapporteur (23 March 2016)

(13) Appointed associate Rapporteur (17 September 2015).

TABLE 5
Study Group 17 – New Questions adopted and Rapporteurs

| Questions | Title of the Questions | WP | Rapporteur |
| --- | --- | --- | --- |
| None |  |  |  |

TABLE 6
Study Group 17 – Questions deleted

| Questions | Title of Questions | Rapporteurs | Results |
| --- | --- | --- | --- |
| None |  |  |  |

# 3 Results of the work accomplished during the 2013-2016 study period

## 3.1 General

During the study period through to its September 2016 meeting, Study Group 17 examined 592 contributions and a large number of TDs and liaison statements.

On the basis of these documents, by 7 September 2016, Study Group 17:

– developed 49 new Recommendations;

– revised 69 existing Recommendations;

– amended 8 Recommendations;

– deleted 3 Recommendations;

– developed 13 Supplements;

– produced 19 Technical Corrigenda;

- developed 3 Technical Reports (no Handbooks were prepared).

## 3.2 Highlights of achievements

The main results achieved on the various Questions assigned to Study Group 17 are briefly summarized below (see Table 6a). Formal replies to the Questions are given in a synoptic table in Annex 1 of this report.

**Table 6a – Summary of achievements in this study period**

| **Question** | **Recommen­dations** | **Amend­ments** | **Corri­genda** | **Supplements** | **Other public­cations** | **Draft Recommendation consented/ determined at the last meeting****(see Table 8)** |
| --- | --- | --- | --- | --- | --- | --- |
| **New** | **Rev­ised** | **New** | **Rev­ised** |
| **1/17** | --- | --- | --- | --- | --- | --- | 1 TR | --- |
| **2/17** | 4 |  |  |  | 1 |  |  |  |
| **3/17** |  | 1 |  |  | 1 |  |  | X.1058 (X.gpim)\* |
| **4/17** | 9 | 3 | 8 |  | 2 | 1 |  | X.1212 (X.cogent)\*X.1550 (X.nessa)\* |
| **5/17** | 2 |  |  | 1 | 2 |  |  |  |
| **6/17** | 2 |  |  | 2 | 3 |  |  | X.1126 (X.msec-11)\*X.1362 (X.iotsec-1)\*X.1373 (X.itssec-1)\* |
| **7/17** | 8 |  |  |  | 2 |  |  |  |
| **8/17** | 5 | 1 |  |  |  |  |  |  |
| **9/17** | 3 |  |  |  |  |  |  | X.1080.0 (X.pbact)\* |
| **10/17** | 4 |  |  |  |  |  |  |  |
| **11/17** | 4 | 23 |  | 14 |  |  | 1 TR |  |
| **12/17** | 6 | 30 |  |  |  | 1 | 4 IGs | Z.100 Annex F1 (revised)Z.100 Annex F2 (revised)Z.100 Annex F3 (revised) |

Notes:

\* Draft Recommendation under TAP, others are under AAP

TR Technical Report

IG Implementer’s Guide.

**a) Q1/17, Telecommunication/ICT security coordination**

This Question continued to focus on the coordination and organization of the entire range of security activities within ITU‑T and has continued to develop and maintain documentation to support coordination and outreach activities. Q1/17 primarily acts a SG17 contact for security coordination matters.

Q1/17 does not have any Recommendations under its own responsibility.

Q1/17 developed and maintained several outreach, promotion and reference documents during this study period that ITU‑T considers valuable in promoting its security work and its deliverables. Examples include:

- The security manual, *Security in telecommunications and information technology - An overview of issues and the deployment of existing ITU*‑*T Recommendations for secure telecommunications,* highlights the major security work of the ITU‑T study groups. Q1/17 has assisted the TSB in an update to the security manual during the Study Period. The 6th edition was published as a Technical Report.

- The on-line *Compendium of Security Recommendations* is a five-part document comprising: a catalogue of approved ITU‑T Recommendations related to telecommunication security; an extract of ITU‑T approved security definitions; a summary of ITU‑T study groups with security related activities; a summary of security-related texts recently approved or under approval process; and a summary of other ITU security activities.

- The *Security Standards Roadmap* is an on-line resource that provides information about existing Information and Communication Technology (ICT) security standards and work in progress in key standards development organizations. The Roadmap is in six parts:

- ICT Standards Development Organizations and Their Work which contains information about the Roadmap structure and about each of the listed standards organizations. It also provides links to existing security glossaries and vocabularies;

- [Approved ICT Security Standards](http://www.itu.int/ITU-T/studygroups/com17/ict/part02.html) which contains a searchable database of approved security standards;

- [Security standards under development](http://www.itu.int/ITU-T/studygroups/com17/ict/part03.html);

- [Future needs and proposed new security standards](http://www.itu.int/ITU-T/studygroups/com17/ict/part04.html);

- [Best practices](http://www.itu.int/ITU-T/studygroups/com17/ict/part05.html); and

- [Identity Management (IdM) Landscape: IdM standards, organizations and gap analysis](http://www.itu.int/ITU-T/studygroups/com17/ict/part06.html).

In addition to information on the ITU‑T security Recommendations and related work, the Roadmap currently includes information on standards work of ISO/IEC, ATIS, ENISA, ETSI, IEEE, IETF, OASIS, 3GPP, and 3GPP2.

- A Technical Report on *successful use of security standards*, intends to help users, especially those from developing countries, to gain a better understanding of the value of using security-related ITU-T Recommendations in a variety of contexts (e.g. business, commerce, government, industry). It covers the use of security standards in a variety of applications and also introduces readers to the relevance and importance of foundational security standards such as architectural standards, methodology, definitions, and other high-level guidance. The overall focus is to encourage successful and productive use of these standards.

A mini workshop between the Universal Postal Union (UPU) and ITU took place during the ITU-T SG17 meeting on 21 January 2014. Longstanding WTSA-12 Resolution 11 frames the collaboration between the ITU-T and the UPU. The workshop was held on various topics of mutual interest such as .PostID, Digital Object Architecture, telecom finance, secure mobile payment, secure e-mail, and ITU-UPU collaboration.

ITU hosted a workshop on “ICT Security Standardization Challenges for Developing Countries” in Geneva, Switzerland, held on 15 – 16 September 2014. The main objective of the workshop was to present and discuss ICT security challenges, in particular for developing countries. The analysis of ICT security challenges and capacity building in the deployment of international ICT security standards was the focus of the workshop. The workshop aimed to enhance standardization competence by advising on the technical composition and best-practice of international ICT security standards. The event was to deepen collaboration in the security activities of ITU’s standardization and development sectors (ITU-T and ITU-D), in addition benefiting ITU-T collaboration with other standards-setting organizations. The key topics of the workshop were: cybersecurity, data protection, trust services and cloud computing including big data, with a focus on standardization and the role of ICTs in safeguarding critical infrastructure.

ITU hosted the ITU cybersecurity workshop *Global Cybersecurity Challenges: Collaborating for effective enhancement of cybersecurity in developing countries* (8 September 2015 afternoon) organized in collaboration with ITU-D SG2 and in parallel to SG17’s and ITU-D SG2’s meetings. SG17 representatives with leadership roles actively participated in the workshop: Ms Miho Naganuma (workshop moderator), Mr Mohamad Elhaj and Mr Patrick Mwesigwa (moderators of the two main sessions). The workshop produced several important insights into the cybersecurity challenges faced by developing countries as well as best practices in meeting these challenges. The workshop demonstrated the spirit of good collaboration shared by ITU-T and ITU-D, and the workshop concluded in a commitment to expand this collaboration. SG17 liaised the common report of the workshop with all regional organizations.

The ITU-ATU Workshop on Cybersecurity Strategy in African Countries was held in Khartoum, Sudan from 24 to 26 July 2016. This regional workshop was organized by the International Telecommunication Union (ITU) in collaboration with the African Telecommunication Union (ATU) and the National Telecommunication Corporation in Sudan (NTC) host of the event. The main objective of the workshop was to build capacity and to share experiences and best practices in countries and to provide information regarding the status of implementations of existing cyber security strategies; to identify any gaps; and to yield a way forward. This workshop was attended by more than 110 participants from 19 countries, regional and international organization, private sectors and national country stakeholders from Sudan.

Lastly, active coordination has been established with all Study Group 17 Questions, all other study groups with a security component and external standards development organizations engaged in ICT security standards work.

**b) Q2/17, Security architecture and framework**

Recommendations X.800, X.802 and X.803 describe security within the context of open systems. The security architecture for systems providing end-to-end communications is provided in Recommendation X.805. A comprehensive set of detailed security frameworks covering aspects of security such as authentication, access control, non-repudiation, confidentiality, integrity, and security audit and alarms has been established (X.810, X.811, X.812, X.813, X.814, X.815 and X.816). To provide Generic Upper Layers Security (GULS), Recommendations X.830, X.831, X.832, X.833, X.834 and X.835 have been developed. In cooperation with ISO/IEC JTC 1/SC 27, Recommendations X.841, X.842 and X.843 on security information objects and trusted third party services have been established.

In this study period, Q2/17 has developed four new Recommendations, and one new supplement:

* X.1033, *Guidelines on security of the individual information service provided by the operators*, provides guidelines on the security of the individual information service provided by the telecommunication operators. The scope covers the classification of individual information service, the security requirements, the mechanisms, and the coordination.
* X.1037, *Technical security guideline on deploying IPv6,* provides a set of technical security guidelines for telecommunication organizations to deploy and operate IPv6 networks and services. The content of this Recommendation focuses on how to securely deploy network facilities for telecommunication organizations and how to ensure security operations for the IPv6 environment.
* X.1038, *Security requirements and reference architecture for software-defined networking*, supports security protection and provides security requirements and a reference architecture for software-defined networking (SDN). This Recommendation identifies new security threats as well as traditional network security threats to SDN, defines security requirements, provides possible security countermeasures against new security threats, and designs a security reference architecture for SDN.
* X.1039, *Technical security measures for implementation of ITU-T X.805 security dimensions*, is aimed at providing a set of security measures to implement the high-level dimensions. It also provides technical implementation guidance for security measures that can be used to improve organizations’ security response capabilities. A set of security measures described in this Recommendation could assist organizations in managing information security risks and implementing technical dimensions. The audience of this Recommendation includes, but is not limited to, those individuals responsible for implementing an organization's information security dimensions.
* X.Suppl.23, *ITU-T X.1037 – Supplement on Security management guideline for the implementation of an IPv6 environment in telecommunications organizations*, provides security management guidelines for the implementation of IPv6 environment in telecommunication organizations in order to ensure the protection of information in the networks and protection of the supporting network infrastructure when transitioning from IPv4 to IPv6 and implementing an IPv6 environment.

**c) Q3/17, Telecommunication information security management**

Q3/17 studies information security management for telecommunications, in recognition that for telecommunications organizations, information and the supporting processes, telecommunications facilities, networks and transmission media are important telecommunication business assets. A key Recommendation is Rec. ITU-T X.1051 on information security management guidelines that was revised collaboratively with ISO/IEC.

In this study period, Q3/17 has developed one revised Recommendation, and one new supplement:

* X.1051 (revised), *Information technology – Security techniques – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations*, establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security controls in telecommunications organizations based on ISO/IEC 27002; and provides an implementation baseline of information security controls within telecommunications organizations to ensure the confidentiality, integrity and availability of telecommunications facilities, services and information handled, processed or stored by the facilities and services.
* X.Suppl.27, *ITU-T X.1054 - Supplement on Best practice for implementation of Rec. ITU-T X.1054 | ISO /IEC 27014 on governance of information security – Case of Burkina Faso*, documents the implementation of Recommendation ITU-T X.1054 | ISO /IEC 27014 to the governance of information security of e-Council of Ministers in Burkina Faso, and illustrates a case of best practice in the implementation of Recommendation ITU-T X.1054 | ISO /IEC 27014.

Q3/17 closely cooperates with ISO/IEC JTC 1/SC 27/WG1 on information security management.

This Question differs from Questions in Study Group 2 in that Study Group 2 deals with the exchange of network management information between network elements and management systems and between management systems in telecommunications management network (TMN) environment. This Question deals primarily with the protection of business assets, including information and processes in view of information security management.

**d) Q4/17, Cybersecurity**

Q4/17 studies cybersecurity in recognition of that the telecommunications landscape is constantly changing, and with it, requirements for associated telecommunication/ICT security. In this cyber environment, there is a strong need for securing protocols, infrastructures, and applications which are used as an integral part of our daily communications. Cybersecurity involves securing and protecting services, personal information, protecting Personally Identifiable Information, and providing information assurance (IA) among interacting entities. Q4/17 developed an ensemble of key specifications for the trusted exchange of cybersecurity information necessary for making security measurable and enabling continuous security monitoring. These specifications were given the name CYBEX for Cybersecurity Information Exchange. Q4/17 also studies non-CYBEX cybersecurity issues such as abnormal traffic detection, botnet mitigation, and attack source attribution (including traceback).

Q4/17 has undertaken primary responsibility for WTSA-12 Res. 50 (Cybersecurity) and joint responsibility with Q3/17 for Res. 58 (Encourage the creation of national computer incident response teams, particularly for developing countries).

In this study period, Q4/17 has developed nine new Recommendations, three revised Recommendations, eight new Amendments, and two new supplements, and one revised supplement:

* X.1208, *A cybersecurity indicator of risk to enhance confidence and security in the use of telecommunication/information and communication technologies*, describes a methodology for organizations to use cybersecurity indicators when computing a risk measure and it provides a list of potential cybersecurity indicators. X.1208 does not propose the use of an index or a single indicator to express the cybersecurity capabilities of an organization.
* X.1210, *Overview of source-based security troubleshooting mechanisms for Internet protocol-based networks*, provides source-based security troubleshooting mechanisms for security issues, as well as selection criteria and basic security guidelines of troubleshooting mechanisms.
* X.1211, *Techniques for preventing web-based attacks*, describes techniques that can mitigate web-based attacks which occur when the vulnerabilities of the website hosts are exploited and malicious code is introduced that can infect a user's computer.
* X.1303*bis*, *Common alerting protocol (CAP 1.2)*, is a simple but general format for exchanging all-hazard emergency alerts and public warnings over all kinds of networks. CAP allows a consistent warning message to be disseminated simultaneously over many different warning systems, thus increasing warning effectiveness while simplifying the warning task.
* X.1500 *Amendments 3, 4, 5, 6, 7, 8, 9, 10: Revised structured cybersecurity information exchange techniques*, provide a list of revised structured cybersecurity information techniques that has been created to be constantly updated as these techniques evolve, expand, are newly identified or are replaced. The list follows the outline provided in the body of the Recommendation. These amendments reflect the situation of recommended techniques as of April 2013, September 2013, January 2014, September 2014, April 2015, September 2015, March 2016, and September 2016, including bibliographical references.
* X.1520 (revised), *Common vulnerabilities and exposures*, provides a structured means to exchange information security vulnerabilities and exposures that provides common names for publicly known problems in the commercial or open source software used in communications networks, end user devices, or any of the other types of information and communications technology (ICT) capable of running software. CVE makes it easier to share data across separate vulnerability capabilities (tools, repositories, and services) with this common naming.
* X.1521 (revised), *Common vulnerability scoring system 3.0*, provides an open framework for communicating the characteristics and impacts of information and communication technologies (ICT) vulnerabilities in the commercial or open source software used in communications networks, end user devices, or any of the other types of ICT capable of running software.
* X.1525, *Common weakness scoring system*, provides an open framework for communicating the characteristics and impacts of information and communication technologies (ICT) weaknesses during development of software capabilities.
* X.1526 (revised), *Language for the open definition of vulnerabilities and for the assessment of a system state*, includes the three main steps of the assessment process: representing configuration information of endpoints for testing; analysing the endpoint for the presence of the specified machine state (vulnerability, configuration, patch state, etc.) and reporting the results of this assessment. The purpose of OVAL is to provide an international, information security, community standard to promote open and publicly available security content and to standardize the transfer of this information across the entire spectrum of security tools and services. OVAL is a language used to encode endpoint details, and an assortment of content repositories held throughout the community.
* X.1542, *Session information message exchange format*, describes the information model for the session information message exchange format (SIMEF) and provides an associated data model specified with extensible markup language (XML) schema. The SIMEF defines a data model representation for sharing the transport layer session log information regarding the centralized network security management and security information exchange system.
* X.1544, *Common attack pattern enumeration and classification*, is an XML/XSD-based specification for the identification, description, and enumeration of attack patterns.
* X.1546, *Malware attribute enumeration and characterization*, focuses on the creation of the enumeration of low-level malware attributes and includes enumerations of malware attributes and behaviour that provide a common vocabulary.
* X.1582, *Transport protocols supporting cybersecurity information exchange*, provides an overview of transport protocols that have been adopted and adapted for use within the Cybersecurity Information Exchange (CYBEX). X.1582 outlines applications of transport, transport protocol characteristics, as well as security considerations.
* X.Suppl.10 (revised), *ITU-T X.1205 – Supplement on usability of network traceback*, provides an overview of traceback for responsive measures to certain network issues within a single or a more complex array of service providers. Traceback may assist in discovering ingress points, paths, partial paths or sources of problematic network events. This information may aid service providers in mitigating such events.
* X.Suppl.18, *ITU-T X.1205 – Supplement on guidelines for abnormal traffic detection and control on IP-based telecommunication networks*, identifies abnormal traffic detection technologies and control measures for IP based telecommunication networks. X.Suppl.18 aim is to provide telecommunication operators with a comprehensive guidelines for monitoring, detecting and controlling abnormal IP traffic.
* X.Suppl.20, *ITU-T X.1205 – Supplement on framework of security information sharing negotiation*, provides a framework for negotiating agreement on security information sharing between cybersecurity entities such as information requester and information provider. X.Suppl.20 defines functional capabilities and a reference model for security information sharing negotiation, conceptual data modelling of security information sharing agreement (SSA), security information sharing policy (SSP) and the SSA negotiation process.

**e) Q5/17, Countering spam by technical means**

Q5/17 studies technical measures to counter spam, as it relates to the stability and robustness of the telecommunication network. Spam is a problem that has become widespread causing a complex range of problems to users, service providers, and network operators around the globe. Q5/17 though its studies is directly supporting WTSA-12 Resolution 52 and also Resolution 50.

Q5/17 followed its formerly developed three-level Recommendation series-structure for countering spam that covers most of the current and future types of spam. The first level is technical strategies on countering spam. The second level focuses on specific areas of countering spam, including SMS, e-mail and IP multimedia applications. The third level covers general technologies for counting spam.

In this study period, Q5/17 has developed two new Recommendations, two new supplements, and one Corrigendum (X.1243 Cor.1):

* X.1246, *Technologies involved in countering voice spam in telecommunication organizations*, gives an overview of voice spam, and summarizes the existing anti-spam technologies which are used by users and telecommunication networks alike, and the collaboration mechanism between them.
* X.1247, *Technical framework for countering mobile messaging spam*, gives an overview of mobile messaging anti-spam processes, and proposes a technical framework for countering mobile messaging spam. Entity functions and processing procedures are specified in this framework. In addition, this Recommendation provides information sharing mechanisms against mobile messaging spam within the anti-spam domain and among anti-spam domains.
* X.Suppl.25, *ITU-T X.1231 – Supplement on guidance to assist in countering spam for mobile phone developers*, provides guidance to assist in countering spam for mobile phone developers. In addition, this Supplement describes security threats of mobile phones with application level aspects, and provides guidance to assist in countering spam for mobile phone developers.
* X.Suppl.28, ITU-T X.1245 *–* *Supplement on Technical measures and mechanisms on countering spoofed calls in the terminating network of voice over long term evolution*, analyses the threats and recommends technical measures and mechanisms to counter spoofed calls in the terminating network of voice over long term evolution (VoLTE) if the identity of the incoming calls cannot be trusted securely by the terminating network. This Supplement focuses mainly on the protection of the VoLTE users, to prevent them from the risk of receiving spoofed calls or to warn them in advance of suspicious spoofed calls by deploying procedures both on the network side and the user side (smartphone), after having conducted a threat analysis of spoofed calls.

**f) Q6/17, Security aspects of ubiquitous telecommunication services**

Q6/17 studies the security aspects of ubiquitous telecommunication services which refer to the services that allow anyone to access to any desired information in a user-friendly way, anytime and anywhere using any devices. Specifically, Q6/17 studies the security of domain-specific ubiquitous telecommunications between heterogeneous devices using application-level technologies such as ubiquitous web for ubiquitous sensor network, home network, mobile network, multicast network, IPTV network, IoT, SDN, smart grid, and ITS. During this study period, the Q6/17 text was amended through TSAG.

In this study period, Q6/17 has developed two new Recommendations, two technical corrigenda (X.1311 Cor.1, X.1314 Cor.1), and three new supplements:

* X.1198, *Virtual machine-based security platform for renewable IPTV service and content protection*, specifies a virtual machine-based security platform for the renewable service and content protection (SCP) system, and defines a common interface and functional logic in the Internet protocol television (IPTV) terminal device and includes the data structure of SCP client and system components for a terminal device such as an embedded SCP, media client and control client.
* X.1314, *Security requirements and framework of ubiquitous networking*, provides a high-level security framework for ubiquitous networking, analyses security threats and defines the security requirements to mitigate these threats in ubiquitous networking environment.
* X.Suppl.19, *ITU-T X.1120-X.1139 series – Supplement on security aspects of smartphones*, aims to protect the personal privacy of users and to improve information security of smartphones. In order to satisfy these security objectives, this Supplement specifies a hierarchical security framework and relevant security considerations for smartphones. X.Suppl.19 identifies smartphone threats, which are categorized into vulnerabilities and attacks. With regard to the security framework, X.Suppl.19 provides necessary security solutions through system improvements and security tools.
* X.Suppl.24, *ITU-T X.1120-X.1139 series – Supplement on a secure application distribution framework for communication devices*, provides a secure application distribution framework for communication devices and security requirements for application distribution sites to enhance the safety of the communication environment for users.
* X.Suppl.26, *ITU-T X.1111, Supplement on security functional architecture for smart grid services using telecommunication networks*, describes a security functional architecture for smart grid (SG) services using telecommunication networks. It identifies security risks and security requirements. This Supplement further defines a security functional architecture for smart grid services using telecommunication networks based on a general functional model.

Q6/17 collaborates with ISO/IEC JTC 1/SCs 6, 25, 27 and 31 on security of USNs.

**g) Q7/17, Secure application services**

Q7/17 studies secure application services such as security of peer-to-peer (P2P) services, secure password-based authentication with key exchange and various trusted third party (TTP) services, and web services.

In this study period, Q7/17 has developed eight new Recommendations, and two new supplements:

* X.1144, *eXtensible Access Control Markup Language (XACML) 3.0*, develops extensible access control markup language (XACML 3.0) which is an updated version of Recommendation ITU-T X.1142 (which is equivalent to OASIS XACML 2.0 (06/2006)), and defines core XACML including syntax of the language, models, context with policy language model, syntax and processing rules.
* X.1154, *General framework of combined authentication on multiple identity service provider environments*, provides the general framework of combined authentication in multiple IdSP environments for a service provider. In this Recommendation, three types of combined authentication methods are considered: multifactor authentication, multi-method authentication and multiple authentications.
* X.1155, *Guidelines on local linkable anonymous authentication for electronic services*, provides guidelines on local linkable anonymous authentication for e-services. This includes the privacy threats of e-services, the requirements of local linkable anonymous authentication, the functions that satisfy these requirements, and a general model of local linkable anonymous authentication for e-services.
* X.1156, *Non-repudiation framework based on a one-time password*, provides a non-repudiation framework based on a one-time password (OTP) to enhance trust between transaction entities.
* X.1157, *Technical capabilities of fraud detection and response for services with high assurance level requirements*, provides capabilities required to support fraud detection and response service in security sensitive information and communication technology (ICT) application services.
* X.1158, *Multi-factor authentication mechanisms using a mobile device*, describes the weaknesses of a single-factor authentication mechanism, the need for a multi-factor authentication mechanism and various combinations of the multi-factor authentication mechanisms using a mobile device, and the threats for the two-factor authentication (TFA) mechanism
* X.1159, *Delegated non-repudiation architecture based on ITU-T X.813*, describes the delegated non-repudiation service models and operations.
* X.1163, *Security requirements and mechanisms of peer-to-peer-based telecommunication networks*, provides a security guideline for a telecommunication network based on P2P technology; briefly introduces the characteristics of the network, it also analyses the security requirements of the network and the services, and it specifies the security mechanisms to fulfil these requirements.
* X.Suppl.21, *ITU-T X.1143 – Supplement on security framework for web mashup services*, describes the security framework for web mashup services and also describes web mashup types and a reference architecture.
* X.Suppl.22, *ITU-T X.1144 – Supplement on enhancements and new features in eXtensible Access Control Markup Language (XACML 3.0)*, summarizes the enhancements and new features of Recommendation ITU-T X.1144 (XACML 3.0) in comparison to Recommendation ITU‑T X.1142 (XACML 2.0).

**h) Q8/17, Cloud computing security**

Q8/17 studies cloud computing security. SG17, through assistance of the chairmen of SG13 and SG17, developed high-level principles for separation of cloud computing security work. During this study period, the Q8/17 text was amended through TSAG.

In this study period, Q8/17 has developed five new Recommendations, and one revised Recommendation:

* X.1601 and X.1601 (revised), *Security framework for cloud computing*, describes the security framework for cloud computing. The Recommendation analyses security threats and challenges in the cloud computing environment, and describes security capabilities that could mitigate these threats and address security challenges. A framework methodology is provided for determining which of these security capabilities will require specification for mitigating security threats and addressing security challenges for cloud computing.
* X.1602, *Security requirements for software as a service application environments*, analyses the maturity levels of software as a service (SaaS) application and proposes security requirements to provide a consistent and secure service execution environment for SaaS applications. These proposed requirements originate from cloud service providers (CSP) and cloud service partners (CSN) as they need a SaaS application environment to meet their demands on security. The requirements are general and independent of any service or scenario specific model (e.g. web services, or representational state transfer (REST)), assumptions or solutions.
* X.1631, *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services*, provides guidelines for information security controls applicable to the provision and use of cloud services by providing additional implementation guidance for relevant controls specified in ISO/IEC 27002, and additional controls with implementation guidance that specifically relate to cloud services. This Recommendation | International Standard provides controls and implementation guidance for both cloud service providers and cloud service customers.
* X.1641, *Guidelines for cloud service customer data security*, provides generic security guidelines for the cloud service customer (CSC) data in cloud computing. It analyses the CSC data security lifecycle and proposes security requirements at each stage of the data lifecycle. Furthermore, the Recommendation provides guidelines on when each control should be used for best security practice.
* X.1642, *Guidelines for the operational security of cloud computing*, provides generic operational security guidelines for cloud computing from the perspective of cloud service providers (CSPs). It analyses the security requirements and metrics for the operation of cloud computing. A set of security measures and detailed security activities for the daily operation and maintenance are provided to help CSPs mitigate security risks and address security challenges for the operation of cloud computing.
1. **Q9/17, Telebiometrics**

Q9/17 studies telebiometrics, and security requirements and guidelines for applications of telebiometrics including requirements of appropriate generic protocols providing safety, security, privacy protection, and consent “for manipulating biometric data” in applications of telebiometrics, e.g., e-health, telemedicine

In this study period, Q9/17 has developed three new Recommendations:

* X.1085, *Information technology — Security techniques — Telebiometric authentication framework using biometric hardware security module*, Recommendation ITU-T X.1085 | ISO/IEC 17992 describes a telebiometric authentication scheme using biometric hardware security module (BHSM) for the telebiometric authentication of proving owner of X.509 certificate registered individual at RA (Register Authority). This Recommendation | International Standard provides the requirements for deploying the BHSM scheme to securely operate the telebiometric authentication under PKI environments. The scheme focuses on providing how to assure the telebiometric authentication with biometric techniques and hardware security module and it also suggests ASN.1 standard format for including the proposed scheme in X.509 framework when telebiometric authentication and X.509 certificate are combined to prove the owner of the certificate.
* X.1087, *Technical and operational countermeasures for telebiometric applications using mobile devices*, specifies the implementation model and threats in the operating telebiometric systems in mobile devices and provides a general guideline for security countermeasures from both the technical and operational perspectives in order to establish a safe mobile environment for the use of telebiometric systems.
* X.1092, *Integrated framework for telebiometric data protection in e-health and telemedicine*, provides an integrated framework to protect biometric data and private information in e-health and telemedicine.

**j) Q10/17, Identity management architecture and mechanisms**

This Question is dedicated to the vision setting and the coordination and organization of the entire range of IdM activities within ITU‑T. A top-down approach to the IdM is used with collaboration with other study groups and other standards development organizations (SDOs). Other Questions are involved in specific aspects of IdM, i.e., protocols, requirements, network device identifiers, etc.

In this study period, Q10/17 has developed four new Recommendations:

* X.1255, *Framework for discovery of identity management information*, provides an open architecture framework in which identity management information can be discovered. The core components of the framework set forth in this Recommendation include: 1) a digital entity data model, 2) a digital entity interface protocol, 3) one or more identifier/resolution systems and 4) one or more metadata registries. These components form the basis of the open architecture framework.
* X.1256, *Guidelines and framework for sharing network authentication results with service applications*, develops guidelines for network operators and service providers to share network authentication results, and provides a framework for sharing minimum attributes across multiple services within an established trust relationship.
* X.1257, *Identity and access management taxonomy*, develops a specification to ensure that necessary business meaning is assigned to IAM roles and permissions and that this business meaning is traceable and reference-able throughout IAM process lifecycle so that permissions can be efficiently assigned to user, separation of duties (SoD) controls successfully implemented across applications, and access review and reconciliation processes can be carried out efficiently.
* X.1258, *Enhanced entity authentication based on aggregated attributes*, introduces the concept of attribute aggregation to allow an entity to aggregate attributes from multiple identity service providers (IdSPs). Attribute aggregation is the mechanism of collecting attributes of an entity retrieved from multiple identity service providers. Attribute aggregation is needed to aggregate the attributes dynamically on demand. IdSP can realize the aggregation request when an entity wants to get a service. Further on, an entity-centric attribute aggregation mechanism could also be applied to the authentication for mitigating privacy leakage.

**k) Q11/17, Generic technologies to support secure applications**

Q11/17 studies the directory services and systems including public-key/attribute certificates. Updating of the X.500 series Recommendations comprises a large part of the work that is undertaken jointly with ISO/IEC JTC 1/SC 6/WG 10.

Significant work has been undertaken on Rec. ITU-T X.509 during the current study period, such as:

a) Making it a clean PKI and PMI (privilege management infrastructure) specification by moving X.500 directory sections to other parts of the X.500 series thereby making Rec. ITU-T X.509 a stand-alone document.

b) Aligned style and terminology to what is currently used in the industry and provided a clear separation between PKI and PMI.

c) Added a so-called Authorization and Validation list capability requested by and referenced by IEC 62351-9, *IEC TC 57 Power Systems Management and Associated Information Exchange – Part 9 – Data and Communication Security – Key Management*.

d) Several other adjustments to prepare Rec. ITU-T X.509 for future requirements imposed by smart grid security and Internet of things.

Q11/17 is also maintaining the ASN.1 Recommendations and is further elaborating Recommendations on OIDs. This work is also done collaboratively with ISO/IEC JTC 1/SC 6/WG10. ASN.1 is stable with the revision approved September 2015. The ASN.1 module database continues to have new additions, enabling implementers to obtain syntax-checked, machine-readable, published ASN.1 specifications.

Study Group 17 has developed, over several study periods, a world-wide identifications scheme based on hierarchical registration authorities called the “Object Identifier Tree”. This is extensively used in many applications by both ITU‑T and ITU‑R Recommendations and ISO/IEC International Standards. More than 954046 identifications have been recorded publicly, and many more have been issued for internal use by various organizations. The original Object Identifier Tree identified arcs of the tree using numbers and names from the Latin alphabet.

Q11/17 in collaboration with ISO/IEC JTC 1/SC 7/WG19 developed two revisions of the Open Distributed Processing (ODP) Recommendations ITU-T X.906 and X.911.

Q11/17 is maintaining the X-series Open Systems Interconnection (OSI) Recommendations. In this study period, Q11/17 has not developed any new OSI Recommendations or revisions thereof; but developed two Technical Corrigenda X.226 Cor.1andX.227*bis* Cor.1.

In this study period, Q11/17 has developed 4 new Recommendations, 23 revised Recommendations, and 14 (X.226 Cor.1, X.227*bis* Cor.1, X.509 Cor.1, X.509 Cor.2, X.509 Cor.3, X.680 Cor.2, X.682 Cor.1, X.683 Cor.1, X.690 Cor.2, X.694 Cor.2, X.520 Cor.1, X.691 Cor.1, X.691 Cor.3, X.691 Cor.4) Technical Corrigenda to the X.500-, X.680-, and X.690-series of Recommendations, and one Technical Report:

* X.500 (revised), *Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services*, introduces the concepts of the Directory and the DIB (Directory Information Base) and overviews the services and capabilities which they provide.
* X.501 (revised), *Information technology – Open Systems Interconnection – The Directory: Models*, provides a number of different models for the Directory as a framework for the other Recommendations in the ITU-T X.500-series. 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.
* X.509 (revised), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*, defines frameworks for public-key infrastructure (PKI) and privilege management infrastructure (PMI). It introduces the basic concept of asymmetric cryptographic techniques. It specifies the following data types: public-key certificate, attribute certificate, certificate revocation list (CRL) and attribute certificate revocation list (ACRL). It also defines several certificates and CRL extensions, and it defines directory schema information allowing PKI and PMI related data to be stored in a directory. In addition, it defines entity types, such as certification authority (CA), attribute authority (AA), relying party, privilege verifier, trust broker and trust anchor. It specifies the principles for certificate validation, validation path, certificate policy, etc. It includes a specification for authorization validation lists that allow for fast validation and restrictions on communications. It includes protocols necessary for maintaining authorization validation lists and a protocol for accessing a trust broker.
* X.511 (revised), *Information technology – Open Systems Interconnection – The Directory: Abstract service definition*, defines in an abstract way the externally visible services provided by the Directory, including bind and unbind operations, read operations, search operations, modify operations, operations to support password policies and operations to support interworking with LDAP. It also defines errors.
* X.518 (revised), *Information technology – Open Systems Interconnection – The Directory: Procedures for distributed operation*, specifies the procedures required for a distributed directory consisting of a mix of Directory System Agents (DSAs) and lightweight directory access protocol (LDAP) servers acting together to provide a consistent service to its users, independent of the point of access. It also describes procedures for protocol conversion between the directory access protocol/directory system protocol (DAP/DSP) protocols and the LDAP protocol.
* X.519 (revised), *Information technology – Open Systems Interconnection – The Directory: Protocol specifications*, specifies the Directory Access Protocol, the Directory System Protocol, the Directory Information Shadowing Protocol and the Directory Operational Binding Management Protocol which fulfil the abstract services specified in Recommendation ITU-T X.501 | ISO/IEC 9594-2, Recommendation ITU T X.511 | ISO/IEC 9594-3, Recommendation ITU-T X.518 | ISO/IEC 9594-4 and Recommendation ITU-T X.525 | ISO/IEC 9594-9. It includes specifications for supporting underlying protocols to reduce the dependency on external specifications. The protocols may be encoded using all standard ASN.1 encoding rules.
* X.520 (revised), *Information technology – Open Systems Interconnection – The Directory: Selected attribute types*, 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 objects defined in Rec. ITU-T X.521 | ISO/IEC 9594-7. Other attributes types, called notification attributes, provide diagnostic information. This Recommendation | International Standard defines context types which supply characteristics associated with attribute values. It also includes definitions for LDAP syntaxes relevant for attribute types and matching rules.
* X.521 (revised), *Information technology – Open Systems Interconnection – The Directory: Selected object classes*, 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.
* X.525 (revised), *Information technology – Open Systems Interconnection – The Directory: Replication*, 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.
* F.511, *Directory Service – Support of tag-based identification services*, provides guidance for the use of directory services to support tag‑based identification applications by reference to the directory capabilities specified in the ITU‑T X.500 series of Recommendations | ISO/IEC 9594 (all parts), and in the lightweight directory access protocol (LDAP) specifications as developed within Internet Engineering Task Force (IETF).
* X.667 (revised), *Information technology – Procedures for the operation of object identifier registration authorities: Generation of universally unique identifiers and their use in object identifiers*, specifies procedures for the generation of universally unique identifiers (UUIDs) and for their use in the international object identifier tree under the joint UUID arc.
* X.675, *OID-based resolution framework for heterogeneous identifiers and locators*, analyses the requirements, such as identifier independence, identifier separation, compatibility, uniqueness, tolerance, stability, and security. The general architecture for the object identifier-based resolution framework is specified with several scenarios. The scenarios show how to operate the resolution framework for heterogeneous identifiers and locators.
* X.680 (revised), *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*, provides a notation called Abstract Syntax Notation One (ASN.1) for defining the syntax of information data. It defines a number of simple data types and specifies a notation for referencing these types and for specifying values of these types. The ASN.1 notations can be applied whenever it is necessary to define the abstract syntax of information without constraining in any way how the information is encoded for transmission.
* X.681 (revised), *Information technology – Abstract Syntax Notation One (ASN.1): Information object specification,* provides the ASN.1 notation which allows information object classes as well as individual information objects and sets thereof to be defined and given reference names.
* X.682 (revised), *Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification,* provides the ASN.1 notation for the general case of constraint and exception specification by which the data values of a structured data type can be limited.
* X.683 (revised), *Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications,* defines the provisions for parameterized reference names and parameterized assignments for data types which are useful for the designer when writing specifications where some aspects are left undefined at certain stages of the development to be filled in at a later stage to produce a complete definition of an abstract syntax.
* X.690 (revised), *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER),* defines a set of Basic Encoding Rules (BER) that may be applied to values of types defined using the ASN.1 notation, a set of Distinguished Encoding Rules (DER) and a set of Canonical Encoding Rules (CER) both of which provide constraints on the Basic Encoding Rules (BER).
* X.691 (revised), *Information technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)*, describes a set of encoding rules that can be applied to values of all ASN.1 types to achieve a much more compact representation than that achieved by the Basic Encoding Rules and its derivatives (described in Rec. ITU-T X.690 | ISO/IEC 8825-1).
* X.692 (revised), *Information technology – ASN.1 encoding rules: Specification of Encoding Control Notation (ECN)*, defines the Encoding Control Notation (ECN) used to specify encodings (of ASN.1 types) that differ from those provided by standardized encoding rules such as the Basic Encoding Rules (BER) and the Packed Encoding Rules (PER).
* X.693 (revised), *Information technology – ASN.1 encoding rules: XML Encoding Rules (XER)*, specifies rules for encoding values of ASN.1 types using the Extensible Markup Language (XML).
* X.694 (revised), *Information technology – ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1*, defines rules for mapping an XSD Schema (a schema conforming to the W3C XML Schema specification) to an ASN.1 schema in order to use ASN.1 encoding rules such as the Basic Encoding Rules (BER), the Distinguished Encoding Rules (DER), the Packed Encoding Rules (PER) or the XML Encoding Rules (XER) for the transfer of information defined by the XSD Schema.
* X.695 (revised), *Information technology – ASN.1 encoding rules: Registration and application of PER encoding instructions*, specifies the rules for applying PER encoding instructions using either type prefixes or an encoding control section.
* X.696, *Information technology – ASN.1 encoding rules: Specification of Octet Encoding Rules (OER)*, specifies two sets of binary encoding rules that can be applied to values of all ASN.1 types using less processing resources than the Basic Encoding Rules and its derivatives.
* X.696 (revised), *Information technology – ASN.1 encoding rules: Specification of Octet Encoding Rules (OER)*, specifies two sets of binary encoding rules that can be applied to values of all ASN.1 types using less processing resources than the Basic Encoding Rules and its derivatives (described in Rec. ITU‑T X.690 | ISO/IEC 8825-1) and the Packed Encoding Rules (described in Rec. ITU-T X.691 | ISO/IEC 8825‑2).
* X.906 (revised), *Information technology – Open distributed processing – Use of UML for ODP system specifications*, refines and extends the definition of how open distributed processing (ODP) systems are specified by defining the use of the Unified Modelling Language for the expression of ODP system specifications.
* X.911 (revised), *Information technology – Open distributed processing – Reference model – Enterprise language*, refines and extends the definition of how ODP systems are specified from the enterprise viewpoint, and is intended for the development or use of enterprise specifications of ODP systems.
* X.1341, *Certified mail transport and certified post office protocols*, defines the certified mail transfer protocol (CMTP) and certified post office protocol (CPOP) in order to foster the exchanges of electronic certified mails in the world in a secure way by providing confidentiality, identification of the correspondents, integrity and non-repudiation.
* Technical Report: Current and new challenges for public-key infrastructure standardization, explores the issues and threats currently facing the deployment of public-key infrastructure (PKI), and the new challenges PKI will experience in areas such as wireless PKI (WPKI), cloud computing, smart grid, and machine-to-machine (M2M) in general.

**l) Q12/17, Formal languages for telecommunication software and testing**

Q12/17 covers formal languages to define the requirements, architecture, and behaviour of telecommunications systems: requirements languages, specification and implementation languages. Q12/17 is also studying testing languages as a means to support interoperability and conformance.

In this study period, SG11 and SG17 agreed through TSAG on:

* Revision of Question 11/11 to add work on conformance and interoperability testing methodologies and framework.
* Revision of Question 12/17 to remove work on conformance testing methodologies and framework and to add work on TTCN-3.
* Revision of Annex C of Resolution 2 to reflect Z.160/Z.170-series under SG17 and reflect X.290-series (except X.292), X.Suppl.4, X.Suppl.5 and Z.500 under SG11.

In this study period, Q12/17 has developed six new Recommendations, 30 revised Recommendations, four revised implementer’s guides, and one revised Supplement:

* Z.100 (revised), *Specification and Description Language – Overview of SDL 2010*, introduces the Specification and Description Language, intended for unambiguous specification and description of telecommunication systems.
* Z.100 Annex F1 (revised), *SDL‑2010 formal definition: General overview*, provides motivation, gives an overview of the structure of the formal semantics, and contains an introduction to the Abstract State Machine (ASM) formalism, which is used to define the SDL‑2010 semantics.
* Z.100 Annex F2 (revised), *SDL-2010 formal definition: Static semantics*, describes the static semantic constraints, and transformations as identified by the Model clauses of Recommendations ITU-T Z.101, Z.102, Z.103, Z.104, Z.105 and Z.107 that are included by reference in Recommendation Z.100.
* Z.100 Annex F3 (revised), *SDL-2010 formal definition: Dynamic semantics*, defines the SDL‑2010 dynamic semantics.
* Z.101 (revised), *Specification and Description Language – Basic SDL 2010*, defines the basic features of the Specification and Description Language. The language defined in this document covers the essential features of the language, which is further defined in other Recommendations in the ITU-T Z.100 series.
* Z.102 (revised), *Specification and Description Language – Comprehensive SDL-2010*, defines the comprehensive features of the Specification and Description Language. The language defined in this document covers features of the language not included in Basic SDL 2010 in Recommendation ITU-T Z.101. These features provide comprehensive coverage of abstract grammar of the language except some data features covered in ITU-T Z.104 (and ITU-T Z.107 for object oriented data).
* Z.103 (revised), *Specification and Description Language – Shorthand notation and annotation in SDL 2010*, defines the shorthand and annotation features of the Specification and Description Language. The language defined in this document covers features of the language not included in Basic SDL 2010 in Recommendation ITU-T Z.101 or Comprehensive SDL 2010 in Recommendation ITU-T Z.102. Features defined in this Recommendation either do not have their own abstract grammar and are transformed to concrete grammar defined by Recommendations ITU T Z.101, ITU-T Z.102 and ITU-T Z.104 (and ITU-T Z.107 for object oriented data), or are annotations with no formal meaning.
* Z.104 (revised), *Specification and Description Language – Data and action language in SDL-2010*, defines the data features of the Specification and Description Language so that data definitions and expressions are well defined. The language defined in this document partially overlaps features of the language included in Basic SDL 2010 in Recommendation ITU T Z.101 and used in Comprehensive SDL 2010 in Recommendation ITU T Z.102 and the features of Recommendation ITU T Z.103.
* Z.105 (revised), *Specification and Description Language – SDL 2010 combined with ASN.1 modules*, defines how Abstract Syntax Notation One (ASN.1) modules are usable in combination with Specification and Description Language 2010 (SDL-2010). This text replaces Recommendation ITU-T Z.105 (2003) to align with Recommendations ITU-T Z.100, ITU‑T Z.101, ITU-T Z.102, ITU-T Z.103, ITU-T Z.104, ITU‑T Z.106 and ITU‑T Z.107 for SDL‑2010. Recommendation ITU-T Z.105 (2003) replaced the semantic mappings from ASN.1 to SDL‑2000 defined in Recommendation ITU-T Z.105 (1999).
* Z.106 (revised), *Specification and Description Language – Common interchange format for SDL 2010*, defines the common interchange format of Specification and Description Language (SDL‑CIF). The SDL‑CIF is intended for the interchange of graphical SDL-2010 specifications (SDL‑GR) made on different tools that do not use the same storage format. This Recommendation introduces two further levels of SDL CIF. Two further conformance levels are defined, one at a more liberal SDL PR level and the second including graphical information.
* Z.107 (revised), *Specification and Description Language – Object-oriented data in SDL 2010*, defines the object-oriented data features of the Specification and Description Language building on the foundation of the data definitions and expressions defined in Recommendation ITU T Z.104. The language defined in this Recommendation partially overlaps features of the language included in Basic SDL 2010 in Recommendation ITU T Z.101 and used in Comprehensive SDL 2010 in Recommendation ITU T Z.102, and the features of Recommendations ITU T Z.103 and ITU-T Z.104.
* Z.109 (revised), *Specification and description language: Unified Modeling Language (UML) profile for SDL*‑*2010*, defines a unified odelling 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. ITU‑T Z.109 Recommendation is revised to be consistent with the rest of the Recommendation ITU‑T Z.100 series for SDL‑2010.
* Z.109 (revised), *Specification and Description Language – Unified odelling language profile for SDL-2010*, defines a unified odelling language (UML) profile that maps to SDL 2010 semantics so that UML is able to be used in combination with the ITU T Specification and Description Language. Appendix I includes an (informative) Example language specification for a concrete grammar and its mapping to the UML profile.
* Z.111 (revised), *Notations and guidelines for the definition of ITU-T languages*, provides meta-grammars for ITU-T Recommendations that define ITU-T languages in the X.680 series and the Z series of ITU-T Recommendations on languages for specification, implementation, modelling and testing. This allows the description of these meta-grammars that define the abstract or concrete grammar (syntax, constraints and semantics) of languages without having to repeat the meta-grammar (such as lexical naming rules, or the description of Backus-Naur Form syntax) as a preamble or annex to each language definition.
* Z.161 (revised), *Testing and Test Control Notation version 3: TTCN*‑*3 core language*, 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. The first revision of Z.161 adds numerous extensions to the language (parameter default values, type parameterization is moved to another document (Advanced parameterization), special real values and exclusive range bounds, visibility restrictions of imported definitions, template restrictions, implicitly omitting fields of values and templates, break/continue statements, new predefined functions etc.) and contains numerous clarifications (e.g. on subtyping structured types, type compatibility, execution of the alt statement etc.), corrigenda and editorial corrections.
* Z.161 (revised), *Testing and Test Control Notation version 3: TTCN-3 core language*, 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 Common Object Request Broker Architecture (CORBA) based platforms and application programming interfaces (APIs). This revision of the Recommendation contains amendments, clarifications, corrigenda and editorial corrections.
* Z.161.1, Z.161.1 (revised), *Testing and Test Control Notation version 3: TTCN-3 Language Extensions: Support of interfaces with continuous signals*, defines the “Continuous Signal support” package of TTCN 3. TTCN 3 can be used for the 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, APIs, etc. TTCN 3 is not restricted to conformance testing and can be used for many other kinds of testing including interoperability, robustness, regression, system and integration testing. The specification of test suites for physical layer protocols is outside the scope of the present document.
* Z.161.2, Z.161.2 (revised), *Testing and Test Control Notation version 3: TTCN-3 language extensions: Configuration and deployment support*, defines the configuration and deployment support package of TTCN-3.
* Z.161.3, Z.161.3 (revised), *Testing and Test Control Notation version 3: TTCN-3 language extensions: Advanced parameterization*, defines the advanced parameterization package of TTCN-3.
* Z.161.4, Z.161.4 (revised), *Testing and Test Control Notation version 3: TTCN-3 language extensions: Behaviour types*, defines the behaviour types package of TTCN 3.
* Z.161.5, Z.161.5 (revised), *Testing and Test Control Notation version 3: TTCN-3 Language extensions: Performance and real time testing*, defines the real-time and performance testing support package of TTCN-3.
* Z.164 (revised), *Testing and Test Control Notation version 3: TTCN-3 operational semantics*, 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 Recommendation ITU T Z.161. This revision of the Recommendation contains amendments, clarifications, corrigenda and editorial corrections.
* Z.165 (revised), *Testing and Test Control Notation version 3: TTCN*‑*3 runtime interface (TRI)*, provides the specification of the runtime interface for TTCN‑3 (Testing and Test Control Notation 3) test system implementations. The second revision of Z.165 contains amendments, clarifications, corrigenda and editorial corrections.
* Z.165.1, Z.165.1 (revised), *Testing and Test Control Notation version 3: Extension Package: Extended TRI*, defines the Extended TRI package of TTCN 3. TTCN 3 can be used for the 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, APIs, etc. TTCN 3 is not restricted to conformance testing and can be used for many other kinds of testing including interoperability, robustness, regression, system and integration testing. The specification of test suites for physical layer protocols is outside the scope of the present document.
* Z.166 (revised), *Testing and Test Control Notation version 3: TTCN*‑*3 control interface (TCI)*, specifies the control interfaces for TTCN‑3 test system implementations. The second revision of Z.166 contains amendments, clarifications, corrigenda and editorial corrections.
* Z.166 (revised), *Testing and Test Control Notation version 3: TTCN-3 control interface (TCI)*, specifies the control interfaces for TTCN-3 test system implementations. The TTCN-3 control interfaces (TCIs) 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 of ETSI ES 201 873-6 V4.8.1). The interface definition uses the Common Object Request Broker Architecture (CORBA) Interface Definition Language (IDL) to specify the TCI completely. Clauses 8, 9 and 9.7 of [ETSI ES 201 873-6 V4.8.1] present language mappings for this abstract specification to the target languages Java and ANSI C. This revision of the Recommendation contains amendments, clarifications, corrigenda and editorial corrections.
* Z.167 (revised), *Testing and Test Control Notation version 3: TTCN*‑*3 mapping from ASN.1*, 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 second revision of Z.167 contains amendments (conformance and compatibility, requirements and descriptions related to the object identifier type have been moved to this document from all other Z.16x Recommendations, supporting XML values within ASN.1 modules, conversion of the OID-IRI and RELATIVE-OID-IRI types, special real values and subtypes containing special values and exclusive bounds, updated predefined language strings etc.), clarifications (e.g. on visibility of imported ASN.1 definitions, on the transformation rules) corrigenda and editorial corrections.
* Z.168 (revised), *Testing and Test Control Notation version 3: TTCN*‑*3* mapping from CORBA IDL, defines the mapping rules for CORBA IDL (as defined in chapter 3 in Draft Approved Specification ptc/06-05-01 (2006)) to TTCN‑3 (as defined in Recommendation ITU‑T Z.161) to enable testing of CORBA-based systems. The second revision of Z.168 contains amendments, clarifications, corrigenda and editorial corrections.
* Z.169 (revised), *Testing and Test Control Notation version 3: TTCN*‑*3 Using XML schema with TTCN*‑*3*, defines the mapping rules for W3C Schema to TTCN‑3 to enable testing of XML-based systems, interfaces and protocols. The third revision of Z.169 contains amendments, clarifications, corrigenda and editorial corrections.
* Z.169 (revised), *Testing and Test Control Notation version 3: Using XML schema with TTCN-3*, defines the mapping rules for W3C Schema to TTCN-3 to enable testing of XML-based systems, interfaces and protocols. This revision of the Recommendation contains amendments, clarifications, corrigenda and editorial corrections.
* Z.170 (revised), *Testing and Test Control Notation version 3: TTCN*‑*3 documentation comment specification*, defines a documentation of TTCN‑3 source code using special documentation comments. The second revision of Z.170 contains amendments, clarifications, corrigenda and editorial corrections.
* Z.Sup1(revised), *ITU-T Z.100-series – Supplement on methodology on the use of description techniques*, (that is, Recommendations ITU-T Z.100 to Z.107, Z.109, Z.110, Z.120, Z.121, Z.150, Z.151, Z.160 to Z.170), outlines a methodology (called SDL+) for the use of these languages in combination, in particular where the ITU Specification and Description Language is used.
* Z.Imp100 (revised), *Specification and Description Language implementer’s guide – Version 2.0.1*, is a compilation of reported defects and their resolutions to the Specification and Description Language Recommendations ITU‑T Z.100, Z.101, Z.102, Z.103, Z.104, Z.105, Z.106, Z.109, Z.111 and Z.119. This Guide is intended to be an additional authoritative source of information for implementers to be read in conjunction with the Recommendations themselves. This Guide itself is not an ITU‑T Recommendation. However, it records agreed corrections to reported defects. This Guide is for the SDL‑2010 version of the language
* Z.Imp100 (revised), *Specification and Description Language implementer’s guide – Version 2.0.2*, is a compilation of reported defects and their resolutions to the Specification and Description Language Recommendations ITU‑T Z.100, Z.101, Z.102, Z.103, Z.104, Z.105, Z.106, Z.109, Z.111 and Z.119. This Guide is intended to be an additional authoritative source of information for implementers to be read in conjunction with the Recommendations themselves. This Guide itself is not an ITU‑T Recommendation. However, it records agreed corrections to reported defects. This Guide is for the SDL‑2010 version of the language.
* Z.100Imp (revised), *Specification and Description Language implementer’s guide – Version 3.0.0*, includes all changes agreed by Q12/17 to the texts of the relevant Recommendations consented or in-force at the date the guide is approved by SG17 and applies until either the implementer’s guide is updated to following version or all the changes are incorporated into the relevant Recommendations and the implementer’s guide is updated to version 3.0.1.
* Z.100Imp (revised), *Specification and Description Language implementer’s guide – Version 3.0.1*, includes all changes agreed by Q12/17 to the texts of the relevant Recommendations consented or in-force at the date the guide is approved by SG17 and applies until either the implementer’s guide is updated to following version or all the changes are incorporated into the relevant Recommendations and the implementer’s guide is updated to version 3.0.2.

## 3.3 Report of lead study group activities, GSIs, JCAs, regional groups, and projects

Study Group 17 is the lead study group on telecommunication security, on identity management and on languages and description techniques. The lead study group activities are shared as follows:

- Security, which is managed by Question 1/17

- Identity management, which is managed by Question 10/17

- Languages and description techniques, which is managed by WP 5/17.

### 3.3.1 Lead study group activities on security

Study Group 17 has been designated the Lead Study Group (LSG) for Security in accordance with World Telecommunication Standardization Assembly (WTSA-12) Resolution 2.

As the lead study group for telecommunication security, Study Group 17 is responsible for the study of the appropriate core Questions on security. In addition, in consultation with other relevant study groups and in collaboration, where appropriate, with other standards bodies, Study Group 17 has the responsibility to define and maintain the overall framework and to coordinate, assign (recognizing the mandates of the study groups) and prioritize the studies to be carried out by the study groups, and to ensure the preparation of consistent, complete and timely Recommendations.

Within SG17, Question 1/17 is the coordinator for the LSG for security activities. This effort is carried out closely with other study groups to identify and develop security solutions. However, specific expertise to integrate these solutions with individual technologies under development can come only from the Question carrying out the development.

As the lead study group on security, Study Group 17 has engaged in on-going liaison with all ITU‑T study groups that have a security dimension to their work. SG17 also collaborates with a broad array of standardization bodies and forums on ICT and telecommunication security. Particular focus has been placed upon avoiding potential conflicts in the work being undertaken by study groups and external bodies.

In addition, security coordination meetings have been held during each Study Group 17 meeting and a list of security contacts has been established for all study groups with security-related work.

Concerning SG17 lead study group matters, internal liaison statements on security matters were received and treated from ITU CITS, CT-CCVOCAB, ITU SCV, ITU-D Question 26/2, ITU-D SG 1 (Q22-1/1), ITU-D SG 2 (Q3/2, Q5/2), ITU-R SG6, ITU-R WP (4B, 5A, 5B, 5C, 5D, 7C), , ITU-T FG-(AC, DFS, DR&NRR, Innovation, SmartCable, SSC), ITU-T JCA-(AHF, CIT, Cloud, COP, IoT, Res178, SDN, SG&HN), ITU-T RevCom, ITU-T SGs (2, 3, 5, 9, 11, 12, 13 (WP 3/13), 15, 16 (Q14/16, Q27/16, Q28/16), 20), and ITU-T TSAG).

Concerning SG17 lead study group matters, external liaison statements were treated, received from 3GPP (SA3, TSG GERAN), CSA, ETSI ISG (ISI, QSC), ETSI TC (CYBER, ITS, M2M, MTS), GSMA SG, ICANN SSAC, IEC TC (25 (JWG 1, WG 5, WG 6), 57/WG15), IETF (IAB, Security Area, STIR WG), ISO TC 12 (JWG 20, WG 18), ISO/IEC JTC 1/SCs (6/WG 7, 7/WG 19, 27 (SC27/WG 1, WG 2), 37, 38), ISO/IEC JTC 1/WG 10, MEF, OASIS, oneM2M WG4, and UPU.

SG17 sent internal liaison statements to ITU CITS, ITU-D SGs (1 (Q22-1/1), 2 (Q3/2, Q5/2)), ITU‑R SGs (4, (WPs 4A, 4B, 4C), 5 (WP 5A), 7), ITU-T FGs (DFS, Innovation, SSC), ITU-T JCAs (AHF, CIT, Cloud, COP, IoT, Res178, SDN, SG&HN), ITU-T RevCom, ITU-T SCV, ITU-T SGs (2, 3, 5, 9, 11, 12, 13, 15, 16, 20), and ITU-T TSAG.

SG17 sent external liaison statements to: 3GPP (SA3, TSG GERAN), CSA, ENISA, ETSI (ISG ISI, SAGE, TC (CYBER, ITS (WG2, WG5), M2M, MTS, SmartM2M)), BIPM, FIDO Alliance, GSMA (MMG, FASG, SG), ICRU, IEC SEG, IEC TC (25 (JWG 1), 57 WG 15, 65/WG10), IESG, IETF (SEC Area, ACE WG, CORE WG, DICE WG, STIR WG), ISO SAG-S, ISO TC (12 (JWG 20, WG 18), TC 68/SC2, 154, 204, 215, 292), ISO TMB, ISO/IEC JTC 1/SC (6 (WG 10), 27 (SG on IoT, WG 1, WG 2, WG 3, WG 4, WG 5), 37 (WG 4)), JTC 1/WG 9, M3AAWG, NIST, NSTIC, OASIS TC (Identity in the cloud, IBOPS, MQTT, Trust Elevation), OIDF, OMA, oneM2M (WG4), UpnP, UPU.

In response to WTSA-12 Resolution 7, *Collaboration with the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)*, Study Group 17 maintains an on-line table that lists its relationships with Technical Committees (TCs) of ISO and IEC and Subcommittees (SCs) of ISO/IEC JTC 1 that also includes identification of the nature of the relationship as joint work (e.g., common texts or twin texts), technical collaboration by liaison mechanism, or informational liaison.

In 2013, on behalf of ITU, SG17 participated in two workshops on countering spam (ITU Workshop on Countering and Combating Spam, Durban, South Africa, 8 July 2013 and Joint CITEL (PCC.I), ITU and the Internet Society workshop on Combating SPAM, Mendoza, Argentina, 7 October 2013), both were productive and made remarkable impact.

In 2014, SG17 organized in a 1 and ½ day ITU workshop on ICT security standardization challenges for developing countries, Geneva, 15-16 September 2014. More than 90 participants participated in the workshop with majority of the participants coming from developing countries. The workshop enhanced standardization competence by advising on the technical composition and best-practice if international ICT security standards, The event deepened collaboration in the security activities of ITU’s standardization and development sectors (ITU-T and ITU-D), in addition benefiting ITU-T collaboration with other standards-setting organizations. One result of this security workshop was the establishment of a correspondence group on investigation of new topics for SG17 standardization.

In 2015, the ITU cybersecurity workshop on *Global Cybersecurity Challenges – Collaborating for effective enhancement of cybersecurity in developing countries*, was held in the afternoon of 8 September 2015 in conjunction with the overlapping ITU-D Study Group 2 and ITU-T Study Group 17 meetings. The workshop produced several important insights into the cybersecurity challenges faced by developing countries as well as best practices in meeting these challenges. The workshop demonstrated the spirit of good collaboration shared by ITU-T and ITU-D, and the workshop concluded in a commitment to expand this collaboration.

In particular, SG17 plan of work on security considers:

 implementation of WTSA-12 Resolutions 7, 11, 40, 50, 52, 58, 64, 65, 67, 70, 73, 75, 76 and 78;

 implementation of PP-10 and PP-14 Resolutions 101, 130, 136, 174, 177, 178, 179, 181, 188, 189, 197, 199, 200, and 201; and

 implementation of WTDC-10 and WTDC-14 Resolutions 23, 30, 34, 45, 47, 54, 63, 67, 69, 79, and 80.

A Study Group 17 action plan in support of WTSA-12 Resolutions has been developed and is updated at each meeting of Study Group 17.

In addition, a lead study group on security homepage is maintained on the Study Group 17 website with direct links to the key security products and services.

SG17 actively updates the ICT security standards database of approved standards of the ICT Security Standards Roadmap, which is an important tool for standard developers in respect of avoiding duplication. The webpages of the Roadmap Part1, Part 2, and Part3 were updated.

SG17 also updated the Security Compendia which provides information on ITU security standardization activities including the catalogue of ITU-T Recommendations dealing with security and the catalogue of ITU-T approved security definitions and abbreviations

Work item X.Trsuss was completed to develop a Technical Report on the successful use of security standards which is intended to help users, especially those from developing countries, to gain a better understanding of the value of using security-related ITU-T Recommendations in a variety of contexts (e.g. business, commerce, government, industry). The TR covers the use of security standards in a variety of applications and also introduces readers to the relevance and importance of foundational security standards such as architectural standards, methodology, definitions, and other high-level guidance. The overall focus is to encourage successful and productive use of these standards.

Work was finished on preparing the 6th edition of the Security Manual as a Technical Report. The Security Manual is a major ITU-T promotion tool that highlights in an easy-to-understand fashion the important security work of all ITU-T study groups.

ITU-T SGs (other than SG17) achieved the following results concerning its work on security Recommendations:

**Recommendations approved:**

| **SG** | **Recommen­dation** | **Title** |
| --- | --- | --- |
| SG5 | K.58 | EMC, resistibility and safety requirements and guidance for determining responsibility under co-located information and communication technology installations |
| SG5 | K.87 | Guide for the application of electromagnetic security requirements – Overview |
| SG9 | J.1002 | Pairing protocol specification for renewable conditional access system |
| SG9 | J.1003 | Specifications of network protocol for renewable conditional access system |
| SG9 | J.1004 | Specifications of authorization centre interfaces for renewable conditional access system |
| SG9 | J.1005 | Architecture and requirements of digital rights management (DRM) for cable television multiscreen |
| SG13 | Y.2705 | Minimum security requirements for the interconnection of the Emergency Telecommunications Service (ETS) |
| SG13 | Y.2725 | Support of OpenID in Next Generation Networks |
| SG13 | Y.2770 | Requirements for deep packet inspection in next generation networks |
| SG13 | Y.2771 | Framework for deep packet inspection |
| SG13 | Y.2772 | Mechanisms for the network elements with support of deep packet inspection |
| SG13 | Y.3032 | Configurations of node identifiers and their mapping with locators in future networks |
| SG13 | Y.3520 (revised) | Cloud computing framework for end-to-end resource management |
| SG15 | G.808.1 | Generic protection switching – Linear trail and subnetwork protection |
| SG15 | G.808.3 | Generic protection switching – Shared mesh protection |
| SG15 | G.873.1 | Optical Transport Network (OTN) Linear protection |
| SG15 | G.873.1 Amd.1 | Optical Transport Network (OTN): Linear protection – Amendment 1: New Appendix III – Optical layer protection |
| SG15 | G.873.2 | ODUk shared ring protection |
| SG15 | G.8031/Y.1342 (revised) | Ethernet linear protection switching |
| SG16 | F.748.1 | Requirements and common characteristics of IoT identifier for IoT services |
| SG16 | F.771 Amd.1 | Service description and requirements for multimedia information access triggered by tag-based identification – Amendment 1: Supporting multiple air interfaces |
| SG16 | H.235.0 (revised) | H.323 security: Framework for security in H-series (H.323 and other H.245-based) multimedia systems |
| SG16 | H.235.6 (revised) | H.323 security: Encryption profile with native H.235/H.245 key management |
| SG16 | H.248.50 | Gateway control protocol: NAT traversal toolkit packages |
| SG16 | H.248.84 | Gateway control protocol NAT traversal for peer-to-peer services |
| SG16 | H.248.86 | Gateway control protocol: H.248 Support for deep packet inspection |
| SG16 | H.248.90 | Gateway control protocol: H.248 packages for control of transport security using TLS |
| SG16 | H.248.91 | Gateway control protocol: Guidelines on the use of ITU-T H.248 capabilities for transport security in TLS networks in ITU-T H.248 profiles |
| SG16 | H.248.93 | Gateway control protocol: H.248 support for control of transport security using DTLS |
| SG16 | H.460.18 | Traversal of H.323 signalling across network address translators and firewalls |
| SG16 | H.460.19 | Traversal of H.323 media across network address translators and firewalls |
| SG16 | H.460.22 | Negotiation of security protocols to protect H.225.0 call signalling messages |
| SG16 | H.621 Amd.1 | Architecture of a system for multimedia information access triggered by tag-based identification: Amendment 1: Supporting multiple air interfaces |
| SG16 | H.751 | Metadata for rights information interoperability in IPTV services |
| SG16 | H.810 | Interoperability design guidelines for personal health systems |
| SG16 | H.812.4 | Interoperability design guidelines for personal health systems: WAN interface: Authenticated persistent session device class |

**Note:**

**\*** Marked Recommendations were approved using TAP.

**Supplements and Appendices agreed**

| **SG** | **Number** | **Title** |
| --- | --- | --- |
| SG13 | Y.Sup19 | ITU-T Y.2200-series – Supplement on the risk analysis service in next generation networks |
| SG13 | Y.Sup18 | ITU-T Y.2700-series – Supplement on next generation network certificate management |
| SG13 | Supplement 23 to Y.2770-series | ITU-T Y.2770-series – Supplement on DPI terminology |
| SG13 | Supplement 25 | ITU-T Y.2770-series – Supplement on DPI use cases and application scenarios |
| SG15 | G.Suppl.52 | ITU-T G-series Recommendations – Supplement on Ethernet ring protection switching |
| SG15 | G.sup54 | ITU-T G-series Recommendations – Supplement on Ethernet linear protection switching |
| SG16 | H.460.24 (2009) Amd.2 | Point-to-point media through network address translators and firewalls within ITU-T H.323 systems: Support for ITU-T H.460.19 multiplex media mode for point-to-point media |

### 3.3.2 Lead study group activities on Identity Management

Study Group 17 has been designated the Lead Study Group for Identity Management (IdM) in accordance with World Telecommunication Standardization Assembly (WTSA-12) Resolution 2.

As the lead study group for Identity Management, Study Group 17 is responsible for the study of the appropriate core Questions on IdM. In addition, in consultation with other relevant study groups and in collaboration, where appropriate, with other standards bodies, Study Group has the responsibility to define and maintain the overall framework and to coordinate, assign (recognizing the mandates of the study groups) and prioritize the studies to be carried out by the study groups, and to ensure the preparation of consistent, complete and timely Recommendations.

In particular, Study Group 17 is responsible for studies relating to the development of a generic identity management model that is independent of network technologies and supports the secure exchange of identity information between entities. This work also includes studying the process for discovery of authoritative sources of identity information; generic mechanisms for the bridging/interoperability of a diverse set of identity information formats; identity management threats, the mechanisms to counter them, the protection of personally identifiable information (PII) and to develop mechanisms to ensure that access to PII is only authorized when appropriate.

The following is the status of work on IdM across the study groups of ITU‑T:

ITU-T SGs (other than SG17) achieved the following results concerning its work on IdM Recommendations:

**Approved Recommendations**

| **SG** | **Recommendation** | **Title** |
| --- | --- | --- |
| SG13 | Y.2084 | Distributed service networking content distribution functions |
| SG13 | Y.2723 | Support for Oauth in next generation networks |
| SG13 | Y.2724 | Framework for supporting Oauth and OpenID in next generation networks |
| SG13 | Y.2725 | Support of OpenID in Next Generation Networks |
| SG13 | Y.3031 | Identification framework in future networks |
| SG13 | Y.3032 | Configurations of node identifiers and their mapping with locators in future networks |
| SG13 | Y.3034 | Architecture for interworking of heterogeneous component networks in ID/locator split-based future networks |
| SG16 | F.748.1 | Requirements and common characteristics of IoT identifier for IoT services |
| SG16 | F.771 Amd.1 | Service description and requirements for multimedia information access triggered by tag-based identification – Amendment 1: Supporting multiple air interfaces |
| SG16 | H.621 Amd.1 | Architecture of a system for multimedia information access triggered by tag-based identification: Amendment 1: Supporting multiple air interfaces |
| SG16 | H.642.1 | Multimedia information access triggered by tag-based identification – Identification scheme |
| SG16 | H.642.2 | Multimedia information access triggered by tag-based identification – Registration procedures for identifiers |
| SG16 | H.642.3 | Information technology – Automatic identification and data capture technique – Identifier resolution protocol for multimedia information access triggered by tag-based identification |
| SG16 | H.642.2 | Multimedia information access triggered by tag-based identification – Registration procedures for identifiers |

**Agreed Supplements**

| **SG** | **Supplement** | **Title** |
| --- | --- | --- |
| SG13 | Y.Suppl.18 | ITU-T Y.2700-series – Supplement on next generation network certificate management |

A WIKI with the IdM Roadmap has been launched on the SG17 web page that provides a compilation of existing and ongoing IdM standards globally. This IdM Roadmap reflects coordination with other SDOs and fora on identity management and helps to avoid duplication of work.

In addition, a lead study group on Identity management homepage is maintained on the Study Group 17 website with direct links to key resources.

### 3.3.3 Lead study group activities on languages and description techniques

Study Group 17 has been designated the Lead Study Group for languages and description techniques in accordance with World Telecommunication Standardization Assembly (WTSA-12) Resolution 2.

As Lead Study Group for Languages and Description Techniques, Study Group 17 has the responsibility with respect to languages and description techniques for telecommunications:

* to provide guidance to ITU‑T members and other Study Groups on the use of languages and description techniques;
* to maintain the set of ITU‑T Recommendations and other guidelines for languages and description techniques used for telecommunications;
* to advise on suitable languages available through other channels to be used if an appropriate language is not defined by a Recommendation of ITU‑T;
* to interact with other recognized bodies such as IETF and OMG that use or define complementary languages and description techniques.

Questions 11/17, and Q12/17 of WP 5/17 have been productive on languages and description techniques for ASN.1, ODP, SDL, MSC, URN and TTCN. Extensive collaboration with other study groups and organizations has helped progress the work.

Question 11/17 works collaboratively with ISO/IEC JTC 1/SC 6/WG 10 on Abstract Syntax Notation One (ASN.1), which are published as common texts in the X.680/X.690/X.890- series. The entire X.680/X.690 suite of ASN.1 Recommendations was revised in 2015.

Question 11/17 also works collaboratively with ISO/IEC JTC 1/SC 7/WG 19 in developing common texts on Open Distributed Processing (ODP). X.906 (UML for ODP) and X.911 (Enterprise Language) were revised.

Question 12/17 Rapporteurs have engaged in and organized workshops to engage more participation from industry and academia in the development of language Recommendations and supporting tools. The following workshops were held during this study period:

- 16th International System Design Languages Forum, Model-driven dependability engineering, 26-28 June 2013, Montreal, Canada.

- 8th System Analysis and Modeling (SAM) conference (SAM-2014), within MODELS-2014, 29-30 September 2014, Valencia, Spain.

- 17th International System Design Languages Forum – 12 – 14 October 2015, Berlin, Germany.

- 9th System Analysis and Modelling (SAM) Conference 2016, 3-4 October in St Malo, France.

The ITU is a ‘supporting organization’ for these events – as approved by SG17 and the ITU helps with publicity. Society members are involved in ongoing Q12/17 work on the revision of the Standardization and Description Language (SDL‑2010) in the Z.100-series.

Question 12/17 has a close relationship with ETSI TC MTS and collaboratively maintains the Z.160- and Z.170 series of Recommendation on TTCN‑3. Six new and 24 revised texts were approved.

In addition, a lead study group on Languages and description techniques homepage is maintained on the Study Group 17 website with an overview of each of each of the languages.

ITU-T SGs (other than SG17) achieved the following results concerning its work on language Recommendations:

**Approved Recommendations**

| **SG** | **Recommendation** | **Title** |
| --- | --- | --- |
| SG13 | Y.3320 | Requirements for applying formal methods to software-defined networking |

### 3.3.4 GSIs and JCAs

SG17 does not have a global standards initiative (GSI) under its responsibility during this study period. Two Joint Coordination Activities (JCAs) under the auspices of SG17 underscore the lead study group functions given to SG17.

#### 3.3.4.1 JCA-IdM

The Joint Coordination Activity on Identity Management (JCA-IdM) from the former study period has been continued during this study period; as proposed to and endorsed by TSAG. The purpose of the JCA-IdM to ensure that the ITU-T IdM work is progressed in a well-coordinated way between study groups (in particular with SG2, SG13, SG17, and SG20) and to act as a point of contact within ITU-T and with other SDOs/Fora/Consortia on IdM in order to avoid duplication of work and assist in implementing the IdM tasks assigned by WTSA-12 Resolution 2 and in implementing GSC-16 Resolution 4 on identity management. JCA-IdM agreed the direction to change the operations of the JCA-IdM such as to focus more on showstoppers in IdM standardization, and to leverage better working together.

Representatives from Study Groups 13 and 17 as well as a number of key relevant external bodies participated in ten meetings of the JCA-IdM, where 44 documents were handled, and significant coordination was accomplished among study groups and a variety of external standards bodies. Overall, participation at the JCA-IdM meetings was very good and significant progress was made. Some of the external standards bodies that participated in the JCA-IdM meetings were: ISO/IEC JTC 1/SC 27/WG5, ETSI/ISG, ENISA, OASIS/IdCloud TC, OASIS Trust Elevation TC, OASIS IBOPS, OpenID Foundation, FIDO Alliance, OASIS TC IBOPS, Kantara Initiative, American Bar Association, GLEIF, STORK 2.0 project, and UPU.

SG17 approved qualification of the OpenID Foundation according to Recommendations ITU-T A.4 and A.5, and initated A.4 and A.5 qualifications for FIDO Alliance.

A WIKI with the IdM Roadmap has been launched on the SG17 web page that provides a compilation of existing and on-going IdM standards globally. This IdM Roadmap reflects coordination with other SDOs and fora on identity management and helps to avoid duplication of work.

#### 3.3.4.2 JCA‑COP

The scope of JCA‑COP is to coordinate the ITU‑T child online protection (COP) work amongst the ITU‑T study groups, and to liaise with ITU‑R and ITU‑D as well as with the Council Working Group on Child Online Protection. JCA-COP brings together various stakeholders with the purpose to learn activities and best practices, but also to identify gaps and develop roadmap towards future COP standards.

JCA-COP conducted eight meetings (six of them face-to-face and co-located with the SG17 meetings, and two e-meetings) in this study period; all the JCA-COP meetings were well attended.

Input presentations were received from ISO/IEC JTC 1/SC 27/WG5, IETF/ISOC, ITU-D Q3/2, DeafKidzInternational, ECPAT, EFC, FCACP, FOSI, GSMA, ICMEC, I-KiZ, and Iran (Islamic Republic of).

Incoming liaison statements were received from ITU-D SG1 Q22-1/1, ITU-T FGs (SSC, DR&NRR), ITU-T JCAs (AHF, SG&HN), ITU-T SGs (2, 3, 9, 16, 17, and 20), ITU-T RevCom, and regular reports from ITU CWG-COP.

Outgoing liaison statements were sent to ITU-T FG-SSC, ITU-T JCA-AHF, and ITU-D Q22-1/1.

### 3.3.5 Study Group 17 Regional Group for Africa (SG17-RG-AFR)

At its April 2015 SG17 meeting, the African Regional Group for SG17 was created. Mr Michael KATUNDU (Kenya) is the chairman of the African Regional Group and Mr Mohamed ELHAJ (Sudan) and Mr Patrick MWESIGWA (Uganda) and Mr Mohamed TOURÉ (Guinea) are the Vice Chairmen of the group. SG17-RG-AFR met twice in Abidjan, Côte d’Ivoire, from 21 to 22 January 2016, and in Khartoum, Sudan (Republic of), from 27 – 28 July 2016. The first meeting identified number of hot topics of interest to Africa. In addition, the meeting generated several ideas for a structure of the regional group including candidate topics for focal points. The meeting discussed three input contributions and prepared two output contributions to be sent to the next SG17 meeting in March 2016. The second meeting agreed a structure of the regional group having three working groups:

WG 1: Cybersecurity, co-chaired by Mr Adetunji BASORUN (Nigeri’), and Mr N’takpe Ernest ’OKA (Côte d’Ivoire, République du)).

WG 2: Electronic Transaction and Mobile Security, co-chaired by Mr Abubakar MAINA (Nigeria), and Mr William K’DIO (Côte d’Ivoire, République du)).

WG 3: Internet Infrastructure Security, co-chaired by Mr Mutaz ISHAG (Sudan, Republic of), and Mr Egide NDAYIZEYE (Burundi), Mr Bertrand Kisito NGA (Cameroon).

## 3.4 Projects

The SG17 ASN.1 & OID projects continue to assist:

* existing users of ASN.1 and object identifiers (OID), within and outside of ITU‑T (e.g., ITU‑T SG16, ISO/IEC JTC 1/SC 27, ISO TC 215, 3GPP, etc.).
* countries and in particular developing countries, in setting a national registration authority for OIDs.

These projects provided speakers and tutorial material, and coordinates the provision of tool support to users and the contents of related websites.

### 3.4.1 ASN.1 Project

The ASN.1 project, under the leadership of Mr Paul Thorpe, provides assistance to users of ASN.1 (Rec. ITU-T X.680, X.690 and X.890 series) within and outside the ITU-T (e.g., ITU-T SG16, ISO/IEC JTC 1/SC27, ISO/TC 215, ETSI LI, 3GPP, etc.). It also helps the TSB in the maintenance of an up-to-date database of error-free ASN.1 modules. The ASN.1 module database continues to have new additions, enabling implementers to obtain syntax-checked, machine-readable, published ASN.1 specifications. This database contains more than 840 modules of more than 200 ITU-T Recommendations and the modules of other SDOs referenced by them.

In cooperation with the TSB, a database is being maintained that contains a machine-processable copy of the current version of all ASN.1 modules that are included in ITU‑T Recommendations. The provision of an on-line ASN.1 module database is a great value-added tool for the ITU‑T compared to other standardization organizations. It improves industry efficiency by saving time and money. Implementations of the associated ITU‑T Recommendations require an electronic format (using ASCII encoding) in order to directly process the formal definitions in current tools. Obtaining an ASCII encoding from a printed or a post-script document involves re-typing, hinders speedy implementation and can introduce errors. Having all ASN.1 modules in one place greatly eases implementation of the corresponding protocols. The ASN.1 database also contains selected modules from several other standards bodies.

**3.4.2 OID Project**

OIDs are a means to universally and unambiguously reference objects used or defined in standards. The work in Question 11/17 on ITU-T’s Object Identifier (OID) hierarchical registration (ITU-T X.660 and X.670 series) has continued to be actively developed collaboratively with ISO/IEC JTC 1/SC 6.

The International OID tree has more than 966 000 registrations recorded in the OID repository at <http://www.oid-info.com>, and provides for the identification of objects (of any sort) via a hierarchical allocation scheme controlled jointly by ITU-T and ISO/IEC. OIDs allow for the identification of objects using any of the languages of the world (in a structured and hierarchical fashion).

The OID Project, under the leadership of Mr Olivier Dubuisson, helps national administrations and ISO/IEC National Bodies settle a registration authority for their country OID, such as Algeria, Andorra, Argentina, Bolivia, Bosnia and Herzegovina, Brazil, Honduras, Lithuania, Malaysia, Mongolia, Nicaragua, Oman, Philippines, Rwanda, and Sri Lanka.

## 3.5 Other Activities

### 3.5.1 Bridging the standardization gap

Since September 2013, SG17 regularly organizes a session on bridging the standardization gap during its study group meetings. The sessionsbrought a wealth of information about the ITU BSG programme, activities and projects, and are an excellent venue for developing countries to bring their suggestions to SG17. The sessions serve as a catalyst for developing countries to express their interests and requirements.

### 3.5.2 MoU on E-business

The memorandum of understanding (MoU) on electronic business was signed between the International Electrotechnical Commission (IEC), the International Organization for Standardization (ISO), the ITU‑T and the United Nations Economic Commission for Europe (UN/ECE). International user groups as well as some forums and consortia also participate in implementation of the MoU. The purpose of the MoU is to minimize the risk of divergent and competitive approaches to standardization, avoid duplication of efforts and avoid confusion amongst users.

Participation to the MoU management group has provided for a better coordination of and sharing of information on the work of Study Group 17 on security, telebiometrics, identity management, ubiquitous sensor networks (USN), ASN.1, object identifiers (OIDs) as well as relevant work from other study groups.

### 3.5.3 ITU‑T/ISO/IEC/ Strategic Advisory Group on Security (SAG-S)

The reconstituted SAG-S was a group under ISO Technical Management Board. ITU-T SG17, in its capacity as ITU-T lead study group on security, participated in the SAG-S e-meetings throughout 2013, and has contributed input material on published ITU-T security Recommendations and drafts to SAG-S, as reflected in the Threat Collection deliverable. The reconstituted SAG-S was ISO focused and unfortunately did not play any coordination role between ISO, IEC and ITU-T as it did previously. ISO TMB terminated SAG-S in 2014.

# 4 Observations concerning future work

Study Group 17’s work on security has had continued and remarkable growth throughout this study period resulting in a center of excellence – a core competency in security. Study Group 17 is the Standardization Sector’s lead study group in security. The work of SG17 has been maintained throughout this study period. A foundation of security Recommendations has been established, collaboration arrangements with other bodies are in place, and an ongoing work program of security Questions for the next study period is proposed in Part II of the Study Group 17 report. Given that building confidence and security in the use of information and communication technologies (ICTs) is one of the top priorities of the ITU, it is critical that this security competence in ITU‑T be nurtured and enhanced, and not fragmented.

The distinction between telecommunication networks and information networks and applications continues to blur. The work that has been done in Study Group 17 on security (including generic security architecture, framework, mechanisms and management guidelines for heterogonous networks/systems/services) needs to be continued and there needs to be a lead study group for security to coordinate within the ITU and with other SDOs. Study Group 17 also anticipates an increasing need for developing guidelines on security that meet the needs of all countries.

Strengthening the trust framework, authentication, and protection of personally identifiable information is a prerequisite for the development of the Information Society and for building confidence among users of ICTs. Security of and for telecommunications and Information and Communication Technologies (ICT security) remains an area where security standards will be needed. New emerging technologies such as cloud computing, smart grid, intelligent transportation systems the 5th generation of cellular network, software-defined networks, Big Data analytics, Internet of things, need technical measures to protect the personally identifiable information (PII) of citizens, as well as technical measures to protect children online. New security approaches to adequately address security threats may be required. Study Group 17 has a key role to play in development of international Recommendations in these areas. Much-needed development of security approaches for evolving technologies is best undertaken in the study group with expertise in existing security approaches.

Through its activities as lead study group for security and as a result of SG17’s liaison and coordination activities, SG17 maintains awareness of other study group’s security activities as well as the work of other standardization bodies and consortia. It is anticipated that the liaison and coordination activities of SG17 will continue to be important in the future. SG17 has a proven track record of collaborating with other standards developing organizations in jointly developing Recommendations/standards. Generally, SG17 in its function of a lead study group and in order to be able to better support its security standardization activities makes good use of liaison facilities (correspondence, formal A.4/A.5/A.6 liaison cooperation) as well as referencing and joint development (A.23/A.25).

SG17 is also the lead study group for identity management (IdM), a key global enabler for managing digital identities, establishing trust, protecting personally identifiable information, operating networks including controlling access to a network or service, performing online e-transactions and digital financial services, etc. As it plays such a critical role in building confidence and security in the use of ICTs, identity management is integral to the activities of Study Group 17 as the ITU‑T security lead. SG17 continues to coordinate IdM within ITU and with other SDOs. Its work relating to PKI, ASN.1, and OIDs has been useful across multiple ICT sectors.

To enable security to be effective, new standards will be needed. It has long been recognized by ITU that structured expression platforms such as Abstract Syntax Notation One (ASN.1) are important. In the case of ASN.1 a major step forward has been made by ensuring the ASN.1 in ITU‑T Recommendations conforms to the ASN.1 definition and made available as machine-readable files. Extending this approach (and the supporting ITU resources) to the other specification languages such as the Specification and Description Language (SDL) could further increase the security inherent in good quality Recommendations. Products can benefit from using these Recommendations. Along with the formal languages for writing Recommendations, ITU has also provided the Testing and Test Control Notation (TTCN) for writing conformance (and other) tests.

New environment, such as Internet of things (IoT) and smart grid security put requirements on PKI that are not yet covered by the current Rec. ITU-T X.509. The current PKI that was originally to secure only banking. E-government and was not designed to cope with environments with low capacity entities, millions or billions of entities with no human interaction. Without enhancement to PKI to adapt to this new environments, major aspects of IoT and smart grid security will fail with great impact for the society as it will affect the stability of major part of essential infrastructures. The work on enhancing PKI to cope with new environment should have high priority during the next study period.

# 5 Updates to the WTSA Resolution 2 for the 2017-2020 study period

Annex 2 contains the updates to WTSA Resolution 2 proposed by Study Group 17 concerning the general areas of study, title, mandate, lead roles and points of guidance in the next study period.

ANNEX 1

List of Recommendations, Supplements and
other materials produced or deleted during the study period

The list of new and revised Recommendations approved during the study period is found in Table 7.

Table 7 lists **Recommendations, amendments and corrigenda** approved during this study period **as of the date** of table generation. Texts are ordered by Recommendation (alphanumeric) and then by date of approval (oldest versions first). A double numbered Recommendation will appear once. A Recommendation that was followed by other study groups will appear only under the study group that approved it.

The list of Recommendations determined/consented at the last meeting of Study Group 17 is found in Table 8.

Texts are ordered by Recommendation (alphanumeric). A double numbered Recommendation will appear once. A Recommendation that was followed by other study groups will appear only under the study group that consented or determined it.

Note – The last meeting in this report refers to 7 September 2016..

The list of Recommendations deleted by Study Group 17 during the study period is found in Table 9. Texts are ordered by Recommendation (alphanumeric). A double numbered Recommendation will appear once.

The List of Recommendations submitted by Study Group 17 to WTSA-16 for approval is found in Table 10.

Tables 11 onwards list other publications approved and/or deleted by Study Group 17 during the study period.

Table 11 lists supplements agreed during this study period **as of the date** of table generation.

TABLE 7
Study Group 17 – Recommendations approved during the study period

| **Recommendation** | **Approval** | **N/R** | **Status** | **AAP/****TAP** | **Title** |
| --- | --- | --- | --- | --- | --- |
| F.511 | 2014-04-06 | New | In force | AAP | Direct–ry Service – Support of tag-based identification services |
| X.226 Cor.1 | 2015-07-16 |  | In force | AAP | Information Technology – Open Systems Interconnection – Connection-Oriented Presentation Protocol: Protocol Specification – Technical Corrigendum 1 |
| X.227*bis* Cor.1 | 2015-07-16 |  | In force | AAP | Information technology – Open Systems Interconnection – Connection-mode protocol for the Application Service Object Association Control Service Element – Technical Corrigendum 1 |
| X.500 | 2016-10-14 | Revised | In force | AAP | Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services |
| X.501 | 2016-10-14 | Revised | In force | AAP | Information technology – Open Systems Interconnection – The Directory: Models |
| X.509 (2012) Cor.1 | 2015-05-28 |  | In force | AAP | Information technology – Open Systems Interconnection – The Directory – Public-key and attribute certificate frameworks – Technical Corrigendum 1 |
| X.509 (2012) Cor.2 | 2016-04-29 |  | In force | AAP | Information technology – Open Systems Interconnection – The Directory – Public-key and attribute certificate frameworks – Technical Corrigendum 2 |
| X.509 (2012) Cor.3 | 2016-10-14 |  | In force | AAP | Information technology – Open Systems Interconnection – The Directory – Public-key and attribute certificate frameworks – Technical Corrigendum 3 |
| X.509 | 2016-10-14 | Revised | In force | AAP | Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks |
| X.511 | 2016-10-14 | Revised | In force | AAP | Information technology – Open Systems Interconnection – The Directory: Abstract service definition |
| X.518 | 2016-10-14 | Revised | In force | AAP | Information technology – Open Systems Interconnection – The Directory: Procedures for distributed operation |
| X.519 | 2016-10-14 | Revised | In force | AAP | Information technology – Open Systems Interconnection – The Directory: Protocol specifications |
| X.520 (2012) Cor.1 | 2014-11-13 |  | In force | AAP | Information technology – Open Systems Inte–connection - The Directory: Selected Attribute Types – Technical Corrigendum 1 |
| X.520 | 2016-10-14 | Revised | In force | AAP | Information technology – Open Systems Interconnection – The Directory: Selected attribute types |
| X.521 | 2016-10-14 | Revised | In force | AAP | Information technology – Open Systems Interconnection – The Directory: Selected object classes |
| X.525 | 2016-10-14 | Revised | In force | AAP | Information technology – Open Systems Interconnection – The Directory: Replication |
| X.667 | 2012-10-14 | Revised | In force | AAP | Information–technology - Procedures for the operation of Object Identifier Registration Authorities: Generation of Universally Unique identifier (UUIDS) and their use in object identifiers |
| X.675 | 2015-06-15 | New | In force | AAP | OID-based resolution framework for heterogeneous identifiers and locators |
| X.680 | 2015-08-13 | Revised | In force | AAP | Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation |
| X.680 (2008) Cor.2 | 2014-03-01 |  | Superseded | AAP | Information–technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation – Technical Corrigendum 2 |
| X.681 | 2015-08-13 | Revised | In force | AAP | Information technology – Abstract Syntax Notation One (ASN.1): Information object specification |
| X.682 | 2015-08-13 | Revised | In force | AAP | Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification |
| X.682 (2008) Cor.1 | 2014-03-01 |  | Superseded | AAP | Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification – Technical Corrigendum 1 |
| X.683 | 2015-08-13 | Revised | In force | AAP | Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications |
| X.683 (2008) Cor.1 | 2014-03-01 |  | Superseded | AAP | Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications – Technical Corrigendum 1 |
| X.690 | 2015-08-13 | Revised | In force | AAP | Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) |
| X.690 (2008) Cor.2 | 2014-03-01 |  | Superseded | AAP | Information technology – ASN.1 encoding rules: specification of basic encoding rules (BER), canonical encoding rules (CER) and distinguished encoding rules (DER) – Technical Corrigendum 2 |
| X.691 | 2015-08-13 | Revised | In force | AAP | Information technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER) |
| X.691 (2008) Cor.3 | 2014-11-13 |  | Superseded | AAP | Information technology – Specification of Packed Encoding Rules (PER) – Technical Corrigendum 3 |
| X.691 (2008) Cor.4 | 2014-11-13 |  | Superseded | AAP | Information technology – Specification of Packed Encoding Rules (PER) – Technical Corrigendum 4 |
| X.691 (2015) Cor.1 | 2016-10-14 |  | In force | AAP | Information technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER) – Technical Corrigendum 1 |
| X.692 | 2015-08-13 | Revised | In force | AAP | Information technology – ASN.1 encoding rules: Specification of Encoding Control Notation (ECN) |
| X.693 | 2015-08-13 | Revised | In force | AAP | Information technology – ASN.1 encoding rules: XML Encoding Rules (XER) |
| X.693 (2008) Cor.2 | 2014-03-01 |  | Superseded | AAP | Information technology – ASN.1 encoding rules: XML Encoding Rules (XER) – Technical Corrigendum 2 |
| X.694 | 2015-08-13 | Revised | In force | AAP | Information technology – ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1 |
| X.694 (2008) Cor.2 | 2014-03-01 |  | Superseded | AAP | Information technology – ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1 – Technical Corrigendum 2 |
| X.695 | 2015-08-13 | Revised | In force | AAP | Information technology – ASN.1 encoding rules: Registration and application of PER encoding instructions |
| X.696 | 2014-08-29 | New | Superseded | AAP | Information technology – ASN.1 encoding rules: Specification of Octet Encoding Rules (OER) |
| X.696 | 2015-08-13 | Revised | In force | AAP | Information technology – ASN.1 encoding rules: Specification of Octet Encoding Rules (OER) |
| X.906 | 2014-10-07 | Revised | In force | AAP | Information technology – Open distributed processing – Use of UML for ODP system specifications |
| X.911 | 2014-09-13 | Revised | In force | AAP | Information technology – Open distributed processing – Reference model – Enterprise language |
| X.1033 | 2016-04-29 | New | In force | AAP | Guidelines on security of the individual information service provided by the operators |
| X.1037 | 2013-10-07 | New | In force | AAP | Technical security guideline on deploying IPv6 |
| X.1038 | 2016-10-14 | New | In force | AAP | Security requirements and reference architecture for software-defined networking |
| X.1039 | 2016-10-14 | New | In force | AAP | Technical security measures for implementation of ITU-T X.805 security dimensions |
| X.1051 | 2016-04-29 | Revised | In force | AAP | Information technology – Security techniques – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations |
| X.1085 | 2016-10-14 | New | In force | AAP | Information technology — Security techniques — Telebiometric authentication framework using biometric hardware security module |
| X.1087 | 2016-10-14 | New | In force | AAP | Technical and operational countermeasures for telebiometric applications using mobile devices |
| X.1092 | 2013-06-13 | New | In force | AAP | Integrated framework for telebiometric data protection in e-health and telemedicines |
| X.1144 | 2013-10-14 | New | In force | AAP | eXtensible Access Control Markup Language (XACML) 3.0 |
| X.1154 | 2013-04-26 | New | In force | TAP | General framework of combined authentication on multiple identity service provider environments |
| X.1155 | 2015-10-29 | New | In force | AAP | Guidelines on local linkable anonymous authentication for electronic services |
| X.1156 | 2013-06-13 | New | In force | AAP | Non-repudiation framework based on a one time password |
| X.1157 | 2015-09-17 | New | In force | TAP | Technical capabilities of fraud detection and response for services with high assurance level requirements |
| X.1158 | 2014-11-13 | New | In force | AAP | Multi-factor authentication mechanisms using a mobile device |
| X.1159 | 2014-11-13 | New | In force | AAP | Delegated non-repudiation architecture based on ITU-T X.813 |
| X.1163 | 2014-05-28 | New | In force | AAP | Security requirements and mechanisms of peer-to-peer-based telecommunication networks |
| X.1198 | 2013-06-13 | New | In force | AAP | Virtual machine-based security platform for renewable IPTV service and content protection |
| X.1208 | 2014-01-24 | New | In force | TAP | A cybersecurity indicator of risk to enhance confidence and security in the use of telecommunication/information and communication technologies |
| X.1210 | 2014-01-24 | New | In force | TAP | Overview of source-based security troubleshooting mechanisms for Internet protocol-based networks |
| X.1211 | 2014-09-26 | New | In force | TAP | Techniques for preventing web-based attacks |
| X.1243 (2010) Cor.1 | 2014-01-24 |  | In force | TAP | Interactive gateway system for countering spam: Corrigendum 1 |
| X.1246 | 2015-09-17 | New | In force | TAP | Technologies involved in countering voice spam in telecommunication organizations |
| X.1247 | 2016-03-23 | New | In force | TAP | Technical framework for countering mobile messaging spam |
| X.1255 | 2013-09-04 | New | In force | TAP | Framework for discovery of identity management information |
| X.1256 | 2016-03-23 | New | In force | TAP | Guidelines and framework for sharing network authentication results with service applications |
| X.1257 | 2016-03-23 | New | In force | TAP | Identity and access management taxonomy |
| X.1258 | 2016-09-07 | New | In force | TAP | Enhanced entity authentication based on aggregated attributes |
| X.1303 *bis* | 2014-03-01 | New | In force | AAP | Common alerting protocol (CAP 1.2) |
| X.1311 (2011) Cor.1 | 2014-11-29 |  | In force | AAP | Information Technology - Security framework for ubiquitous sensor networks - Technical Corrigendum 1 |
| X.1314 | 2014-11-13 | New | In force | AAP | Security requirements and framework of ubiquitous networking |
| X.1314 Cor.1 | 2015-10-29 |  | In force | AAP | Security requirements and framework of ubiquitous networking - Corrigendum 1 |
| X.1341 | 2015-09-17 | New | In force | TAP | Certified mail transport and certified post office protocols |
| X.1500 Amd.3 | 2013-04-26 | New | Superseded | Agreement | Overview of cybersecurity information exchange - Amendment 3 - Revised structured cybersecurity information exchange techniques |
| X.1500 Amd.4 | 2013-09-04 | New | Superseded | Agreement | Overview of cybersecurity information exchange - Amendment 4 - Revised structured cybersecurity information exchange techniques |
| X.1500 Amd.5 | 2014-01-24 | New | Superseded | Agreement | Overview of cybersecurity information exchange - Amendment 5 - Revised structured cybersecurity information exchange techniques |
| X.1500 Amd.6 | 2014-09-26 | New | Superseded | Agreement | Overview of cybersecurity information exchange - Amendment 6 - Revised structured cybersecurity information exchange techniques |
| X.1500 Amd.7 | 2015-04-17 | New | Superseded | Agreement | Overview of cybersecurity information exchange - Amendment 7 - Revised structured cybersecurity information exchange techniques |
| X.1500 Amd.8 | 2015-09-17 | New | Superseded | Agreement | Overview of cybersecurity information exchange - Amendment 8 - Revised structured cybersecurity information exchange techniques |
| X.1500 Amd.9 | 2016-03-23 | New | Superseded | Agreement | Overview of cybersecurity information exchange – Amendment 9 – Revised structured cybersecurity information exchange techniques |
| X.1500 Amd.10 | 2016-03-23 | New | In force | Agreement | Overview of cybersecurity information exchange – Amendment 10 – Revised structured cybersecurity information exchange techniques |
| X.1520 | 2014-01-24 | Revised | In force | TAP | Common vulnerabilities and exposures |
| X.1521 | 2016-03-23 | Revised | In force | TAP | Common vulnerability scoring system 3.0 |
| X.1525 | 2015-04-17 | New | In force | TAP | Common weakness scoring system |
| X.1526 | 2013-04-26 | New | Superseded | TAP | Object vulnerability and assessment language |
| X.1526 | 2014-01-24 | Revised | In force | TAP | Language for the open definition of vulnerabilities and for the assessment of a system state |
| X.1542 | 2016-09-07 | New | In force | TAP | Session information message exchange format |
| X.1544 | 2013-04-26 | New | In force | TAP | Common attack pattern enumeration and classification |
| X.1546 | 2014-01-24 | New | In force | TAP | Malware attribute enumeration and characterization |
| X.1582 | 2014-01-24 | New | In force | TAP | Transport protocols supporting cybersecurity information exchange |
| X.1601 | 2014-01-24 | New | Superseded | TAP | Security framework for cloud computing |
| X.1601 | 2015-10-29 | Revised | In force | AAP | Security framework for cloud computing |
| X.1602 | 2016-03-23 | New | In force | TAP | Security requirements for software as a service application environments |
| X.1631 | 2015-07-15 | New | In force | AAP | Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services |
| X.1641 | 2016-09-07 | New | In force | AAP | Guidelines for cloud service customer data security |
| X.1642 | 2016-03-23 | New | In force | TAP | Guidelines for the operational security of cloud computing |
| Z.100 | 2016-04-29 | Revised | In force | AAP | Specification and Description Language - Overview of SDL-2010 |
| Z.100 Annex F1 | 2015-01-13 | Revised | In force | AAP | Specification and Description Language - Overview of SDL-2010 - Annex F1 - SDL-2010 formal definition: General overview |
| Z.100 Annex F2 | 2015-01-13 | Revised | In force | AAP | Specification and Description Language - Overview of SDL-2010 - Annex F2 - SDL-2010 formal definition: Static semantics |
| Z.100 Annex F3 | 2015-01-13 | Revised | In force | AAP | Specification and Description Language - Overview of SDL-2010 - Annex F3 - SDL-2010 formal definition: Dynamic semantics |
| Z.101 | 2016-04-29 | Revised | In force | AAP | Specification and Description Language - Basic SDL-2010 |
| Z.102 | 2016-04-29 | Revised | In force | AAP | Specification and Description Language - Comprehensive SDL-2010 |
| Z.103 | 2016-04-29 | Revised | In force | AAP | Specification and Description Language - Shorthand notation and annotation in SDL-2010 |
| Z.104 | 2016-04-29 | Revised | In force | AAP | Specification and Description Language - Data and action language in SDL-2010 |
| Z.105 | 2016-04-29 | Revised | In force | AAP | Specification and Description Language - SDL-2010 combined with ASN.1 modules |
| Z.106 | 2016-04-29 | Revised | In force | AAP | Specification and Description Language - Common interchange format for SDL-2010 |
| Z.107 | 2016-04-29 | Revised | In force | AAP | Specification and Description Language - Object-oriented data in SDL-2010 |
| Z.109 | 2013-10-14 | Revised | Superseded | AAP | Specification and Description Language – Unified modelling language profile for SDL-2010 |
| Z.109 | 2016-10-14 | Revised | In force | AAP | Specification and Description Language – Unified modelling language profile for SDL-2010 |
| Z.111 | 2016-04-29 | Revised | In force | AAP | Notations and guidelines for the definition of ITU-T languages |
| Z.161 | 2013-07-14 | Revised | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 core language |
| Z.161 | 2014-11-13 | Revised | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 core language |
| Z.161 | 2015-10-29 | Revised | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 core language |
| Z.161 | 2016-10-14 | Revised | In force | AAP | Testing and Test Control Notation version 3: TTCN-3 core language |
| Z.161.1 | 2014-11-13 | Revised | Superseded  | AAP | Testing and Test Control Notation version 3: TTCN-3 language extensions: Support of interfaces with continuous signals |
| Z.161.1 | 2015-10-29 | Revised | In force | AAP | Testing and Test Control Notation version 3: TTCN-3 language extensions: Support of interfaces with continuous signals |
| Z.161.2 | 2014-11-13 | Revised | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 language extensions: Configuration and deployment support |
| Z.161.2 | 2013-07-14 | New | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 language extensions: Configuration and deployment support |
| Z.161.2 | 2015-10-29 | Revised | In force | AAP | Testing and Test Control Notation version 3: TTCN-3 language extensions: Configuration and deployment support |
| Z.161.3 | 2013-07-14 | New | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 language extensions: Advanced parameterization |
| Z.161.3 | 2014-11-13 | Revised | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 language extensions: Advanced parameterization |
| Z.161.3 | 2015-10-29 | Revised | In force | AAP | Testing and Test Control Notation version 3: TTCN-3 language extensions: Advanced parameterization |
| Z.161.4 | 2013-07-14 | New | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 Language Extensions: Behaviour types |
| Z.161.4 | 2015-10-29 | New | In force | AAP | Testing and Test Control Notation version 3: TTCN-3 Language Extensions: Behaviour types |
| Z.161.5 | 2014-11-13 | New | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 Language extensions: Performance and real time testing |
| Z.161.5 | 2015-10-29 | New | In force | AAP | Testing and Test Control Notation version 3: TTCN-3 Language extensions: Performance and real time testing |
| Z.164 | 2016-10-14 | Revised | In force | AAP | Testing and Test Control Notation version 3: TTCN-3 operational semantics |
| Z.165 | 2013-07-14 | Revised | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 runtime interface (TRI) |
| Z.165 | 2014-11-13 | Revised | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 runtime interface (TRI) |
| Z.165 | 2015-10-29 | Revised | In force | AAP | Testing and Test Control Notation version 3: TTCN-3 runtime interface (TRI) |
| Z.165.1 | 2013-07-14 | Revised | Superseded | AAP | Testing and Test Control Notation version 3: Extension Package: Extended TRI |
| Z.165.1 | 2014-11-13 | Revised | Superseded | AAP | Testing and Test Control Notation version 3: Extension Package: Extended TRI |
| Z.165.1 | 2015-10-29 | Revised | In force | AAP | Testing and Test Control Notation version 3: Extension Package: Extended TRI |
| Z.166 | 2013-07-14 | Revised | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 control interface (TCI) |
| Z.166 | 2014-11-13 | Revised | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 control interface (TCI) |
| Z.166 | 2015-10-29 | Revised | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 control interface (TCI) |
| Z.166 | 2016-10-14 | Revised | In force | AAP | Testing and Test Control Notation version 3: TTCN-3 control interface (TCI) |
| Z.167 | 2013-07-14 | Revised | In force | AAP | Testing and Test Control Notation version 3: Using ASN.1 with TTCN-3 |
| Z.168 | 2013-07-14 | Revised | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 mapping from CORBA IDL |
| Z.168 | 2015-10-29 | Revised | In force | AAP | Testing and Test Control Notation version 3: TTCN-3 mapping from CORBA IDL |
| Z.169 | 2013-07-14 | Revised | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 mapping from XML data definition |
| Z.169 | 2015-10-29 | Revised | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 mapping from XML data definition |
| Z.169 | 2016-10-14 | Revised | In force | AAP | Testing and Test Control Notation version 3: TTCN-3 mapping from XML data definition |
| Z.170 | 2013-07-14 | Revised | In force | AAP | Testing and Test Control Notation version 3: TTCN-3 documentation comment specification |

TABLE 8
Study Group 17 – Recommendations consented/determined at the last meeting (and not yet approved)

| **Recommendation** | **Consent/Determination** | **TAP/AAP** | **Title** |
| --- | --- | --- | --- |
| X.1058 (X.gpim) | 2016-09-07 | TAP | Information technology — Security techniques — Code of practice for personally identifiable information protection |
| X.1080.0 (X.pbact) | 2016-09-07 | TAP | Access control for telebiometrics data protection |
| X.1126 (X.msec-11) | 2016-09-07 | TAP | Guidelines on mitigating the negative effects of infected terminals in mobile networks |
| X.1212 (X.cogent) | 2016-09-07 | TAP | Design considerations for improved end-user perception of trustworthiness indicators |
| X.1362 (X.iotsec-1) | 2016-09-07 | TAP | Simple encryption procedure for Internet of things (IoT) environments |
| X.1373 (X.itssec-1) | 2016-09-07 | TAP | Secure software update capability for intelligent transportation system communication devices |
| X.1550 (X.nessa) | 2016-09-07 | TAP | Access control models for incident exchange networks |
| Z.100 Annex F1 (revised) | 2016-09-07 | AAP | Specification and Description Language – Overview of SDL 2010 – Annex F1: SDL 2010 formal definition: General overview |
| Z.100 Annex F2 (revised) | 2016-09-07 | AAP | Specification and Description Language – Overview of SDL 2010 – Annex F2: SDL 2010 formal definition: Static semantics |
| Z.100 Annex F3 (revised) | 2016-09-07 | AAP | Specification and Description Language – Overview of SDL 2010 – Annex F3: SDL 2010 formal definition: Dynamic semantics |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

TABLE 9
Study Group 17 – Recommendations deleted during study period

| Recommendation | Last version | Withdrawal date | Title |
| --- | --- | --- | --- |
| Z.400 | 1993-03 | 24 December 2015 | Structure and format of quality manuals for telecommunications software |
| Z.600 | 2000-11 | 24 December 2015 | Distributed processing environment architecture |
| Z.601 | 2007-02 | 24 December 2015 | Data architecture of one software system |

TABLE 10
Study Group 17 – Recommendations submitted to WTSA-16

| Recommendation | Proposal | Title | Reference |
| --- | --- | --- | --- |
| None |  |  |  |

TABLE 11
Study Group 17 – Supplements

| **Supplement** | **Approval** | **Status** | **Title** |
| --- | --- | --- | --- |
| X.Suppl.10 (09/2011) (revised) | 2014-01-24 | In force | ITU-T X.1205 – Supplement on usability of network traceback |
| X.Suppl.18 | 2013-04-26 | In force | ITU-T X.1205 – Supplement on guidelines for abnormal traffic detection and control on IP-based telecommunication networks |
| X.Suppl.19 | 2013-04-26 | In force | ITU-T X.1120 series - Supplement on security aspects of smartphones |
| X.Suppl.20 | 2013-04-26 | In force | ITU-T X.1205 – Supplement on framework of security information sharing negotiation |
| X.Suppl.21 | 2014-01-24 | In force | ITU-T X.1143 – Supplement on security framework for web mashup services |
| X.Suppl.22 | 2014-01-24 | In force | ITU-T X.1144 – Supplement on enhancements and new features in eXtensible Access Control Markup Language (XACML 3.0) |
| X.Suppl.23 | 2014-09-26 | In force | ITU-T X.1037 – Supplement on Security management guideline for the implementation of an IPv6 environment in telecommunications organizations |
| X.Suppl.24 | 2014-09-26 | In force | ITU-T X.1120-X.1139 series – Supplement on a secure application distribution framework for communication devices |
| X.Suppl.25 | 2016-03-23 | In force | ITU-T X.1231 – Supplement on guidance to assist in countering spam for mobile phone developers |
| X.Suppl.26 | 2016-03-23 | In force | ITU-T X.1111 – Supplement on security functional architecture for smart grid services using telecommunication networks |
| X.Suppl.27 | 2016-09-07 | In force | ITU-T X.1054 – Supplement on Best practice for implementation of Rec. ITU-T X.1054 | ISO /IEC 27014 on governance of information security – Case of Burkina Faso |
| X.Suppl.28 | 2016-09-07 | In force | ITU-T X.1245 – Supplement on Technical measures and mechanisms on countering spoofed calls in the terminating network of voice over long term evolution |
| Z.Sup1 (revised) | 2015-04-17 | In force | ITU-T Z.100-series – Supplement on methodology on the use of description techniques |

TABLE 12
Study Group 17 – Non-normative publications (Handbooks, Manuals) agreed

| Publication | Approval | Status | Title |
| --- | --- | --- | --- |
| Technical Report | 2014-09-26 | Published | Current and new challenges for public-key infrastructure standardization |
| Technical Report | 2015-09-17 | Published | Security in telecommunications and information technology – An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications; 6th edition |
| Technical Report | 2016-09-07 | Published | Successful use of security standards |

TABLE 13
Study Group 17 – Recommendations, determined/consented and rejected

| **Recommendation** | **Consent / Determination** | **TAP / AAP** | **Title** |
| --- | --- | --- | --- |
| Draft X.1126 (ex X.msec-6)(Note 1) | 2013-04 | TAP | Security aspects of smartphones |
| Draft Rec. ITU-T X.894 (ex X.cms)(Note 2) | 2016-03-23 | AAP | Information technology - Generic applications of ASN.1 - Cryptographic Message Syntax - Generic applications of ASN.1 - Cryptographic Message Syntax |

Note 1 - X.1126 (ex X.msec-6) standardization activity has ceased (2013-04) within SG17, re‑vectored as X.Suppl.19.

Note 2 – On 15 September 2016 Draft Rec. ITU-T X.894 (X.cms) was delegated from AAP Last Call Judgement to the next SG17 meeting for dis-approval; a new work item X.CMS-prof is being developed.

ANNEX 2

Proposed updates to the Study Group 17 mandate and Lead Study Group roles

**(WTSA Resolution 2)**

The following are the proposed changes to the Study Group 17 mandate and Lead Study Group roles agreed at the last Study Group 17 meeting in this study period, based on the relevant portions of [WTSA-12 Resolution 2](http://www.itu.int/en/ITU-T/wtsa16/Documents/CPI/ITU-T_Res2_2016-E.docx).

Part 1 – General areas of study

**…**

**ITU-T Study Group 17**

**Security**

ITU-T Study Group 17 is responsible for building confidence and security in the use of information and communication technologies (ICT). This includes studies relating to cybersecurity, security management, countering spam and identity management. It also includes security architecture and framework, protection of personally identifiable information, and security of applications and services for the Internet of things (IoT), smart grid, smartphone, software-defined networking (SDN), Internet Protocol television (IPTV), web services, social network, cloud computing, big data analytics, mobile financial system and telebiometrics. Study Group 17 is also responsible for the application of open system communications, including directory and object identifiers, and for technical languages, the method for their usage and other issues related to the software aspects of telecommunication systems, and for conformance testing to improve the quality of Recommendations.

**…**

Part 2 – Lead ITU-T study groups in specific areas of study

**…**

SG17 Lead study group on security
Lead study group on identity management (IdM)
Lead study group on languages and description techniques

**…**

Annex B
(to Resolution 2)

**Points of guidance to ITU-T study groups for development
of the post-2012 work programme**

**…**

**ITU-T Study Group 17**

ITU-T Study Group 17 is responsible for building confidence and security in the use of information and communication technologies (ICT). This includes studies relating to security, including cybersecurity, countering spam and identity management. It also includes security architecture and framework, security management, protection of personally identifiable information (PII), and security of applications and services for the Internet of things (IoT), smart grid, smartphone, software-defined networking (SDN), Internet Protocol television (IPTV), web services, social network, cloud computing, mobile financial system and telebiometrics. Study Group 17 is also responsible for the application of open system communications, including directory and object identifiers, and for technical languages, the method for their usage and other issues related to the software aspects of telecommunication systems, and for conformance testing to improve quality of Recommendations.

In the area of security, Study Group 17 is responsible for developing the core Recommendations on ICT security, such as security architecture and frameworks; the fundamentals related to cybersecurity, including threats, vulnerabilities and risks, incident handling/response and digital forensics; security management, including management of PII; countering spam by technical means. In addition, Study Group 17 provides overall coordination of security work in ITU‑T.

In addition, Study Group 17 is responsible for developing the core Recommendations on security aspects of applications and services in the areas of IPTV, smart grid, IoT, software-defined networking (SDN), social network, cloud computing, big data analytics, smartphone, mobile financial system and telebiometrics.

Study Group 17 is also responsible for developing the core Recommendations on a generic identity management model that is independent of network technologies and supports the secure exchange of identity information between entities. This work also includes studying the process for discovery of authoritative sources of identity information; generic mechanisms for the bridging/interoperability of a diverse set of identity information formats; identity management threats, the mechanisms to counter them, the protection of personally-identifiable information (PII) and the development of mechanisms to ensure that access to PII is only authorized when appropriate.

In the area of open system communication, Study Group 17 is responsible for Recommendations in the following areas:

• directory services and systems, including public key infrastructure (PKI) (ITU-T F.500- and ITU-T X.500-series);

• object identifiers (OIDs) and associated registration authorities (ITU-T X.660/ITU-T X.670-series);

• open systems interconnection (OSI), including Abstract Syntax Notation One (ASN.1) (ITU-T F.400-, ITU-T X.200-, ITU-T X.400-, ITU-T X.600-, ITU-T X.800-series); and

• open distributed processing (ODP) (ITU-T X.900‑series).

In the area of languages, Study Group 17 is responsible for studies on modelling, specification and description techniques. This work, which includes languages such as ASN.1, SDL, MSC and URN, will be developed in line with the requirements of and in cooperation with the relevant study groups such as Study Group 2, Study Group 9, Study Group 11, Study Group 13, Study Group 15 and Study Group 16.

**…**

Annex C
(to Resolution 2)

**List of Recommendations under the responsibility of the respective
ITU-T study groups and TSAG in the 2013-2016 study period**

**…**

**ITU-T Study Group 17**

ITU-T E.104, ITU-T E.115, ITU-T E.409 (in conjunction with Study Group 2)

ITU-T F.400-series; ITU-T F.500 − ITU-T F.549

ITU-T X-series, except those under the responsibility of Study Groups 2, 11, 13, 15 and 16

ITU-T Z-series, except ITU-T Z.300-series and ITU-T Z.500-series

NOTE 1 – Changes in assignment of Z-series Recommendations were agreed by TSAG after WTSA-12.

**…**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_