|  |  |
| --- | --- |
| World Telecommunication Standardization Assembly (WTSA-20)Geneva, 1-9 March 2022 |  |
|  |  |
|  |  |
| PLENARY MEETING | Document  | 19-E |
|  | December 2021 |
|  | Original: English |
|  |
| ITU‑T Study Group 17 |
| Security |
| Report of ITU-T SG17 to the World Telecommunication Standardization Assembly (WTSA-20), Part I: GENERAL |

|  |  |
| --- | --- |
| **Abstract:** | This contribution contains the report of ITU-T Study Group 17 to WTSA-20 concerning its activities during the 2017-2021 study period. |
| **Contact:** | Heung Youl YoumChairman, ITU-T SG17Korea (Republic of) | E-mail: hyyoum@sch.ac.kr |

Note by the TSB:

The report of Study Group 17 to the WTSA-20 is presented in the following documents:

Part I: **Document 19** – General

Part II: **Document 20** – Questions proposed for study during the study period 2022-2024

**CONTENTS**

|  Page |
| --- |
| [1 Introduction 4](#_Toc91228243)[1.1 Responsibilities of Study Group 17 4](#_Toc91228244)[1.2 Management team and meetings held by Study Group 17 5](#_Toc91228245)[2 Organization of work 12](#_Toc91228246)[2.1 Organization of studies and allocation of work 12](#_Toc91228247)[2.2 Questions and Rapporteurs 14](#_Toc91228248)[3 Results of the work accomplished during the 2017-2020 study period 21](#_Toc91228249)[3.1 General 21](#_Toc91228250)[3.2 Highlights of achievements 21](#_Toc91228251)[a) Q1/17, Telecommunication/ICT security coordination (2017 – 2020) / Security standardization strategy and coordination (2021 -) 21](#_Toc91228252)[b) Q2/17, Security architecture and framework (2017 – 2020) / Security architecture and network security (2021 -) 22](#_Toc91228253)[c) Q3/17, Telecommunication information security management (2017 – 2020) / Telecommunication information security management and security services (2021 -) 23](#_Toc91228254)[d) Q4/17, Cybersecurity (2017 – 2020) / Cybersecurity and countering spam (2021 -) 25](#_Toc91228255)[e) Q5/17, Countering spam by technical means (2017 – 2020) 27](#_Toc91228256)[f) Q6/17, Security aspects of telecommunication services, networks and Internet of Things (2017 – 2020) / Security for telecommunication services and Internet of Things (2021 -) 28](#_Toc91228257)[g) Q7/17, Secure application services 30](#_Toc91228258)[h) Q8/17, Cloud computing and Big data infrastructure security 31](#_Toc91228259)[i) Q9/17, Telebiometrics (2017 – 2020) 32](#_Toc91228260)[j) Q10/17, Identity management architecture and mechanisms (2017 – 2020) / Identity management and telebiometrics architecture and mechanisms (2021 -) 33](#_Toc91228261)[k) Q11/17, Generic technologies (Directory, public key infrastructure (PKI), privilege management infrastructure (PMI), Abstract Syntax Notation One (ASN.1), object identifiers (OIDs)) to support secure applications (2017 – 2020) / Generic technologies (such as Directory, PKI, Formal languages, Object Identifiers) to support secure applications (2021 -) 34](#_Toc91228262)[l) Q12/17, Formal languages for telecommunication software and testing (2017 – 2020) 39](#_Toc91228263)[m) Q13/17, Security aspects for Intelligent Transport System (2017 – 2020) / Intelligent transport system (ITS) security (2021 -) 43](#_Toc91228264)[n) Q14/17, Security aspects for Distributed Ledger Technologies (2018 - 2020) / Distributed ledger technology (DLT) security (2021 -) 44](#_Toc91228265)[o) Q15/17, Security for/by emerging technologies including quantum-based security 45](#_Toc91228266)[3.3 Report of lead study group activities, GSIs, JCAs, regional groups, and projects 45](#_Toc91228267)[3.3.1 Lead study group activities on security 46](#_Toc91228268)[3.3.2 Lead study group activities on Identity Management 49](#_Toc91228269)[3.3.3 Lead study group activities on languages and description techniques 50](#_Toc91228270)[3.3.4 Joint Coordination Activity on Identity Management (JCA-IdM) 51](#_Toc91228271)[3.3.5 Study Group 17 Regional Group for Africa (SG17RG-AFR) 51](#_Toc91228272)[3.3.6 Study Group 17 Regional Group for Arab (SG17RG-ARB) 51](#_Toc91228273)[3.4 Projects 52](#_Toc91228274)[3.4.1 ASN.1 Project 52](#_Toc91228275)[3.4.2 OID Project 52](#_Toc91228276)[3.5 Bridging the standardization gap 53](#_Toc91228277)[4 Observations concerning future work 53](#_Toc91228278)[5 Updates to WTSA Resolution 2 for the 2022-2024 study period 55](#_Toc91228279)[ANNEX 1 List of Recommendations, Supplements and other materials produced or deleted during the study period 56](#_Toc91228280)[ANNEX 2 SG17 Proposed Revisions to WTSA Resolution 2 74](#_Toc91228281)  |

#

# 1 Introduction

## 1.1 Responsibilities of Study Group 17

Study Group 17 was entrusted by the World Telecommunication Standardization Assembly (Hammamet, 2016) with the study of 12 Questions for building confidence and security in the use of information and communication technologies (ICT).

Annex A to WTSA-16 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 (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 test specification languages in support of conformance testing to improve the quality of Recommendations.*

Annex A to WTSA-16 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-16 Resolution 2 provides the following points of guidance for 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, 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, which includes languages such as ASN.1, SDL, MSC, URN and TTCN-3.*

*This work 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, Study Group 16, and Study Group 20 (for IoT and SC&C security issues).*

*Study Group 17 will work on relevant identity management aspects in collaboration with Study Group 20 for IoT and Study Group 2, as per the mandate of each study group.*

Annex C to WTSA-16 Resolution 2 (as modified by TSAG) defines the list of Recommendations under the responsibility of Study Group 17 in the 2017-2020 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-16 appointed Mr YOUM Heung Youl (Korea, Republic of) as Study Group 17 Chairman and appointed the following nine vice-chairmen of Study Group 17: Mr DOLMATOV Vasiliy (Russian Federation), Mr ISHAG Muataz Elsadig (Sudan), Mr EVREN Gökhan (Turkey), Ms FUREY Inette (USA), Ms LATROUS Wala Turki (Tunisia), Mr LIN Zhaoji (China), Mr MIGUAL Hugo Darío (Argentina), Mr MIYAKE Yutaka (Japan), and Mr KETTIN ZANGA Patrick-Kennedy (Central Africa). Mr KETTIN ZANGA Patrick-Kennedy did not participate in any meetings of Study Group 17 in this study period.

In March 2018, Ms FUREY Inette (USA) was replaced by Mr GONZALES Juan (USA) for Study Group 17 Vice-chairmanship. In March 2020, Mr MIGUEL Hugo Darío (Argentina) was replaced by Ms MOLINARI Lia (Argentina) for Study Group 17 Vice-chairmanship. In August 2020, Mr KETTIN ZANGA Patrick-Kennedy (Central Africa) was replaced by Mr Eric Anicet MBATHAS (Central Africa) for Study Group 17 Vice-chairmanship.

Study Group 17 met 13 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** |
| --- | --- | --- |
| SG/WP 17 | Geneva, 22-30 March 2017 | SG17-R1 to R9 |
| SG/WP 17 | Geneva, 29 August - 6 September 2017 | SG17-R10 to R17 |
| SG/WP 17 | Geneva, 20-29 March 2018 | SG17-R18 to R24 |
| SG/WP 17 | Geneva, 29 August - 7 September 2018 | SG17-R25 to R32 |
| SG/WP 17 | Geneva, 22-30 January 2019 | SG17-R33 to R37 |
| SG/WP 17 | Geneva, 27 August - 5 September 2019 | SG17-R38 to R50 |
| SG/WP 17 | Virtual, 17-26 March 2020 | SG17-R51 to R66 |
| SG17 | Virtual, 29 May 2020 | SG17-R67 |
| SG/WP 17 | Virtual, 24 August - 3 September 2020 | SG17-R68 to R77 |
| SG17 | Virtual, 7 January 2021 | SG17-R78 |
| SG/WP 17 | Virtual, 20 - 30 April 2021 | SG17-R79 to R85 |
| SG/WP 17 | Virtual, 24 August - 3 September 2020 | SG17-R86 to R102 |
| SG17 | Virtual, 7 January 2022 | SG17-R103 |

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** | **Question(s)** | **Event name** |
| --- | --- | --- | --- |
| 2016-12-12to2016-12-13 | China [Beijing] | [Q8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=5710&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-170322-TD-PLEN-0057)] | Q8/17 interregnum Rapporteur group meeting |
| 2017-01-12to2017-01-13 | *E-Meeting* | [Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=5711&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-170322-TD-PLEN-0054)] | Q4/17 interregnum Rapporteur group e-meeting |
| 2017-02-06to2017-02-10 | Tunisia [Tunis] | [Q11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=5716&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-170322-TD-PLEN-0058)] | Joint Rapporteur Group meeting of Question 11/17 with ISO/IEC JTC 1/SC 6/ WG10 |
| 2017-02-08to2017-02-09 | Korea (Rep. of) [Seoul] | [Q3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=5712&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-170322-TD-PLEN-0053)] | Q3/17 interregnum Rapporteur group meeting |
| 2017-02-08to2017-02-09 | Korea (Rep. of) [Seoul] | [Q6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=5713&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-170322-TD-PLEN-0056)] | Q6/17 interregnum Rapporteur group meeting |
| 2017-06-22to2017-06-23 | Korea (Rep. of) [Seoul] | [Q3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6903&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0392)] | Q3/17 interim Rapporteur Group meeting |
| 2017-06-22to2017-06-23 | Korea (Rep. of) [Seoul] | [Q6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6904&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0393)] | Q6/17 interim Rapporteur Group meeting |
| 2017-06-27to2017-06-28 | China [Beijing] | [Q8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6909&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0394)] | Q8/17 interim Rapporteur Group meeting |
| 2017-06-29 | Japan [Tokyo] | [Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6916&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0395)] | Q4/17 interim Rapporteur Group meeting |
| 2017-06-30 | Japan [Tokyo] | [Q3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6905&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0390)][Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6906&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0390)][Q10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6907&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0390)] | Joint Rapporteur Group meeting of Q3/17, Q4/17 and Q10/17 on DFS |
| 2017-07-03 | Japan [Tokyo] | [Q10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=7916&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0396)] | Q10/17 interim Rapporteur Group meeting |
| 2017-07-14 | Korea (Rep. of) [Seoul] | [Q13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=8918&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0397)] | Q13/17 interim Rapporteur Group meeting |
| 2017-10-30to2017-11-03 | Korea (Rep. of) | [Q11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9047&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-0817)] | Joint Q11/17 meeting with ISO/IEC JTC1/SC6 |
| 2017-11-30to2017-12-01 | Korea (Rep. of) [**Bundang]** | [Q14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9048&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-0817)] | Q14/17 Rapporteur group meeting |
| 2017-12-13to2017-12-14 | China [Beijing] | [Q7/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9050&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-0822)] | Q7/17 Rapporteur group meeting |
| 2018-01-09 | Canada [Vancouver] | [Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9051&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-0821)][Q10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9052&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-1006)] | Joint Q4/17 and Q10/17 meeting |
| 2018-01-22to2018-01-23 | China [Beijing] | [Q14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9057&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-0823)] | Q14/17 Rapporteur group meeting |
| 2018-01-24to2018-01-25 | Korea (Rep. of) [Seoul] | [Q13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9056&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-0818)] | Q13/17 Rapporteur group meeting |
| 2018-01-25to2018-01-26 | Korea (Rep. of) [Seoul] | [Q3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9054&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-0820)] | Q3/17 Rapporteur group meeting |
| 2018-01-25to2018-01-26 | Korea (Rep. of) [Seoul] | [Q6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9055&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-0819)] | Q6/17 Rapporteur group meeting |
| 2018-06-04to2018-06-06 | China [Beijing] | [Q14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9265&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-180829-TD-PLEN-1252)] | Q14/17 interim Rapporteur group meeting |
| 2018-06-07to2018-06-08 | Korea (Rep. of) [Seoul] | [Q6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9261&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-180829-TD-PLEN-1246)][Q13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9262&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-180829-TD-PLEN-1251)] | Q6/17 and Q13/17 interim Rapporteur group meetings |
| 2018-06-20to2018-06-21 | China [Yinchuan] | [Q7/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9259&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-180829-TD-PLEN-1247)] | Q7/17 Rapporteur group meeting |
| 2018-06-26to2018-06-27 | United States [Seattle, Washington] | [Q10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9264&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-180829-TD-PLEN-1249)] | Q10/17 interim Rapporteur group meeting |
| 2018-06-27to2018-06-28 | China [Beijing] | [Q8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9263&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-180829-TD-PLEN-1248)] | Q8/17 interim Rapporteur group meeting |
| 2018-08-27to2018-08-31 | Japan [Tokyo] | [Q11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9260&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-180829-TD-PLEN-1250)] | Q11/17 interim Rapporteur group meeting jointly with ISO/IEC JTC 1/SC 6/WG 10 |
| 2018-11-08to2018-11-09 | Singapore | [Q13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9405&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-190122-TD-PLEN-1727)] | Q13/17 Interim Rapporteur group meetings |
| 2018-11-12to2018-11-13 | Japan [Tokyo] | [Q10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9406&Group=17)[[meeting report](http://www.itu.int/md/T17-SG17-190122-TD-PLEN-1726)] | Q10/17 Interim Rapporteur group meetings |
| 2018-11-12to2018-11-13 | Japan [Tokyo] | [Q14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9407&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-190122-TD-PLEN-1726)] | Q14/17 Interim Rapporteur group meetings |
| 2019-04-22to2019-04-26 | China [Beijing] | [Q11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9560&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2057)] | Q11/17 interim Rapporteur group meeting jointly with ISO/IEC JTC 1/SC 6/WG 10 |
| 2019-06-04to2019-06-05 | *E-Meeting* | [Q10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9559&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2056)] | Q10/17 interim Rapporteur group e-meeting |
| 2019-06-04to2019-06-05 | *E-Meeting* | [Q14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9563&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2059)] | Q14/17 interim Rapporteur group |
| 2019-06-10to2019-06-12 | China [Shanghaï] | [Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9574&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2051)] | Q4/17 interim Rapporteur group |
| 2019-06-11to2019-06-12 | China [Beijing] | [Q13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9561&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2058)] | Q13/17 interim Rapporteur group |
| 2019-06-18to2019-06-19 | China [Chongqing] | [Q7/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9556&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2053)] | Q7/17 interim Rapporteur group |
| 2019-06-24to2019-06-25 | China [Beijing] | [Q8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9557&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2054)] | Q8/17 interim Rapporteur group |
| 2019-06-27to2019-06-28 | Japan [Tokyo] | [Q6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9555&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2052)] | Q6/17 interim Rapporteur group |
| 2019-06-27 | *E-Meeting* | [Q3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9554&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2050)] | Q3/17 interim Rapporteur group e-meeting |
| 2019-10-22to2019-10-23 | China [Haikou] | [Q7/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9763&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2564)] | Q7/17 interim Rapporteur group meeting |
| 2019-12-05to2019-12-06 | Switzerland [**Fribourg**] | [Q11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9767&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2762)][Q14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9768&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2762)] | Joint meeting of Q11/17 and Q14/17 |
| 2019-12-11to2019-12-13 | China [Jinan] | [Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9882&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2562)] | Q4/17 interim Rapporteur group meeting |
| 2019-12-11 | *E-Meeting* | [Q11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9766&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2567)] | Q11/17 interim Rapporteur group meeting |
| 2019-12-11 | China [Jinan] | [Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9760&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2754)] | Q4/17 and Q16/13 collocated Rapporteur group meeting |
| 2019-12-12 | Japan [Tokyo] | [Q10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9765&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2566)] | Q10/17 interim Rapporteur group meeting |
| 2019-12-13 | Japan [Tokyo] | [Q3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9759&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2561)] | Q3/17 interim Rapporteur group meeting |
| 2020-01-07to2020-01-08 | China [Beijing] | [Q8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9764&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2565)] | Q8/17 interim Rapporteur group meeting |
| 2020-01-07to2020-01-08 | Japan [Fukuoka] | [Q13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9769&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2569)] | Q13/17 interim Rapporteur group meeting |
| 2020-01-08 | *E-Meeting* | [Q14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9771&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2570)] | Q14/17 interim Rapporteur group meeting |
| 2020-01-13to2020-01-14 | Malaysia [Kuala Lumpur] | [Q6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9783&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2563)] | Q6/17 interim Rapporteur group meeting |
| 2020-02-03to2020-02-07 | United Kingdom [London] | [Q11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9770&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2568)] | Q11/17 interim Rapporteur group meeting jointly with ISO/IEC JTC 1/SC 6/WG 10 |
| 2020-04-17 | *E-Meeting* | [Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10081&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-200529-TD-PLEN-2963)] | Q4/17 interim Rapporteur group meeting |
| 2020-04-22 | *E-Meeting* | [Q11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10087&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-200529-TD-PLEN-2966)] | Q11/17 interim Rapporteur group meeting |
| 2020-05-11to2020-05-12 | *E-Meeting* | [Q6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10083&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-200824-TD-PLEN-3093)] | Q6/17 interim Rapporteur group meeting |
| 2020-05-13 | *E-Meeting* | [Q13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10088&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-200529-TD-PLEN-2979)] | Q13/17 interim Rapporteur group meeting |
| 2020-06-02to2020-06-03 | *E-Meeting* | [Q3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10080&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-200824-TD-PLEN-3090)] | Q3/17 interim Rapporteur group meeting |
| 2020-06-10to2020-06-11 | *E-Meeting* | [Q13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10089&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-200824-TD-PLEN-3096)] | Q13/17 interim Rapporteur group meeting |
| 2020-06-19 | *E-Meeting* | [Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10347&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-200824-TD-PLEN-3091)] | Q4/17 interim Rapporteur group meeting |
| 2020-06-22to2020-06-23 | *E-Meeting* | [Q14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10090&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-200824-TD-PLEN-3097)] | Q14/17 interim Rapporteur group meeting |
| 2020-07-13 | *E-Meeting* | [Q10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10086&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-200824-TD-PLEN-3095)] | Q10/17 interim Rapporteur group meeting |
| 2020-07-16to2020-07-17 | *E-Meeting* | [Q8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10084&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-200824-TD-PLEN-3094)] | Q8/17 interim Rapporteur group meeting |
| 2020-10-19to2020-10-30 | *E-Meeting* | [Q11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11694&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-210107-TD-PLEN-3447)] | Q11/17 interim Rapporteur group meeting jointly with ISO/IEC JTC 1/SC 6/WG 10 |
| 2020-11-18 | *E-Meeting* | [Q10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11588&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-210107-TD-PLEN-3462)] | Q10/17 interim Rapporteur group meeting |
| 2020-11-25to2020-11-26 | *E-Meeting* | [Q13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11589&Group=17) [[meeting report](https://www.itu.int/md/T17-SG17-210107-TD-PLEN-3467)] | Q13/17 interim Rapporteur group meeting |
| 2020-11-26to2020-11-27 | *E-Meeting* | [Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11570&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-210107-TD-PLEN-3460)] | Q4/17 interim Rapporteur group meeting |
| 2020-12-07to2020-12-08 | *E-Meeting* | [Q2/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11569&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-210107-TD-PLEN-3459)] | Q2/17 interim Rapporteur group meeting |
| 2020-12-09to2020-12-10 | *E-Meeting* | [Q3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11727&Group=17) [[meeting report](https://www.itu.int/md/T17-SG17-210107-TD-PLEN-3468)] | Q3/17 interim Rapporteur group meeting |
| 2020-12-21to2020-12-22 | *E-Meeting* | [Q6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11571&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-210107-TD-PLEN-3463)] | Q6/17 interim Rapporteur group meeting |
| 2021-01-04to2021-01-05 | *E-Meeting* | [Q14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11590&Group=17) [[meeting report](https://www.itu.int/md/T17-SG17-210107-TD-PLEN-3469)] | Q14/17 interim Rapporteur group meeting |
| 2021-02-01to2021-02-02 | *E-Meeting* | [Q3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11832&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-210420-TD-PLEN-3547)] | Q3/17 interim Rapporteur group meeting |
| 2021-02-01to2021-02-02 | *E-Meeting* | [Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11830&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-210420-TD-PLEN-3548)] | Q4/17 interim Rapporteur group meeting |
| 2021-02-04 | *E-Meeting* | [Q6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11836&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-210420-TD-PLEN-3549)] | Q6/17 interim Rapporteur group meeting |
| 2021-06-17to2021-06-18 | *E-Meeting* | [Q15/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12574&Group=17) [[meeting report](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3876)] | Q15/17 interim Rapporteur group meeting |
| 2021-06-17to2021-06-18 | *E-Meeting* | [Q8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12539&Group=17) [[meeting report](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3875)] | Q8/17 interim Rapporteur group meeting |
| 2021-06-24to2021-06-25 | *E-Meeting* | [Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12534&Group=17) [[meeting report](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3877)] | Q4/17 interim Rapporteur group meeting |
| 2021-06-24 | *E-Meeting* | [Q10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12575&Group=17) [[meeting report](http://www.itu.int/md/T17-SG17-210824-TD-PLEN-3878)] | Q10/17 interim Rapporteur group meeting |
| 2021-06-28to2021-06-29 | *E-Meeting* | [Q14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12592&Group=17) [[meeting report](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3879)] | Q14/17 interim Rapporteur group meeting |
| 2021-07-01to2021-07-02 | *E-Meeting* | [Q2/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12533&Group=17) [[meeting report](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3880)] | Q2/17 interim Rapporteur group meeting |
| 2021-10-05 | *E-Meeting* | [Q3/17 [meeting report]](https://www.itu.int/md/T17-SG17-220107-TD-PLEN-4199/en) | Q3/17 interim Rapporteur group meeting |
| 2021-11-19 | *E-Meeting* | [Q10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12744&Group=17) [[meeting report](https://www.itu.int/md/T17-SG17-220107-TD-PLEN-4178)] | Q10/17 interim Rapporteur group meeting |
| 2021-11-24to2021-11-25 | *E-Meeting* | [Q2/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12733&Group=17) [[meeting report](https://www.itu.int/md/T17-SG17-220107-TD-PLEN-4159)] | Q2/17 interim Rapporteur group meeting |
| 2022-01-20to2022-01-21 | *E-Meeting* | Q15/17 [meeting report] | Q15/17 interim Rapporteur group meeting |
| 2022-02-07 | *E-Meeting* | Q3/17 [meeting report] | Q3/17 interim Rapporteur group meeting |
| 2022-02-15 | *E-Meeting* | Q10/17 [meeting report] | Q10/17 interim Rapporteur group meeting |
| 2022-02-17 | *E-Meeting* | Q6/17 [meeting report] | Q6/17 interim Rapporteur group meeting |
| 2022-02-23to2022-02-24 | *E-Meeting* | Q2/17 [meeting report] | Q2/17 Interim Rapporteur group meeting  |
| 2022 -02-?? | *E-Meeting* | Q4/17 [meeting report] | 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 4 working parties. Table 2 shows the number and title of each working party, together with the Questions assigned to it and the name of its Chairman and Vice-chairmen between 2017 and 2020.

**TABLE 2
Organization of Study Group 17 (2017-2020)**

| **Designation** | **Questions to be studied** | **Title of the Working Party** | **Chairmanand Vice-Chairmen** |
| --- | --- | --- | --- |
| PLEN | Q1/17; |  |  |
| WP1/17 | Q2/17; Q3/17; Q6/17; Q13/17(7); | Telecommunication/ICT Security | Mr Miyake Yutaka (Chairman)Mr Dolmatov Vasiliy (Vice-chairman)Mr Evren Gökhan (Vice-chairman) |
| WP2/17 | Q4/17; Q5/17; Q14/17(8); | Cyberspace security | Mr Nakao Koji (Chairman)Ms Furey Inette (Vice-chairman) (1) Mr Gonzalez Juan (Vice-chairman) (2) |
| WP3/17 | Q7/17; Q8/17; Q12/17; | Application security | Mr Taddei Arnaud (Chairman)Mr Lin Zhaoji (Vice-chairman) (3)Ms Bai Xiaoyuan (Vice-chairman) (4) |
| WP4/17 | Q9/17; Q10/17; Q11/17; | Identity management and authentication | Mr Li Kepeng (Chairman) (5)Mr Nah Jae Hoon (Vice-chairman/Co-chairman) (5, 6)Mr Lin Zhaoji (Co-chairman) (6) |

Notes:

(1) Vice-chairing until September 2017.

(2) Vice-chairing since March 2018.

(3) Vice-chairing until September 2018.

(4) Vice-chairing since January 2019.

(5) Chair/Vice-chairing until September 2018.

(6) Co-chairing since Jan 2019.

(7) Q13/17 was established by SG17 in September 2017.

(8) Q14/17 was established by SG17 in March 2018.

**2.1.2** Due to the outbreak of global pandemic of COVID-19, the World Telecommunication Standardization Assembly (WTSA-20) planned to be held in 2020 was postponed to 2022, and the 2017-2020 study period was extended accordingly until WTSA-20. In August/September 2020 meeting SG17 agreed a set of 12 Questions for approval by WTSA-20 (see section 2.2) and to establish a task force on preparation for the next study period.

With the postponement of WTSA-20 to March 2022, TSAG meeting on 11-18 January 2021 endorsed this new set of SG17 Questions (ref. [TSB Circular 295](https://www.itu.int/md/T17-TSB-CIR-0295/en)). At 20-30 April 2021 meeting, SG17 agreed to organize the set of 12 Questions into a new structure of five Working Parties.

Table 3 shows the number and title of each working party, together with the Questions assigned to it and the name of its Chairman from 2021.

**TABLE 3
Organization of Study Group 17 (2021-)**

| **Designation** | **Questions to be studied** | **Title of the Working Party** | **Chairmanand Vice-Chairmen** |
| --- | --- | --- | --- |
| WP1/17 | Q1/17; Q15/17 | Security strategy and coordination | Chairman: Mr Dolmatov Vasily (Russia)Vice-Chairman: Mr Kim Jonghyun (Korea)  |
| WP2/17 | Q2/17; Q6/17; Q13/17; | 5G, IoT and ITS security | Chairman: Mr Miyake Yutaka (KDDI)Vice-Chairmen: Ms Hu Zhiyuan (Nokia Shanghai Bell)Mr Mills Philip (UK)  |
| WP3/17 | Q3/17; Q4/17;  | Cybersecurity and management | Chairman: Mr Nakao Koji (NICT)Vice-Chairman: Ms Molinari Lia (Argentina) |
| WP4/17 | Q7/17; Q8/17; Q14/17 | Service and application security | Chairman: Mr Nah Jae Hoon (ETRI)Vice-Chairman: Ms Bai Xiaoyuan (Alibaba)  |
| WP5/17 | Q10/17; Q11/17 | Fundamental security technologies | Chairman: Mr Lin Zhaoji (ZTE)Vice-Chairman: *vacant* |

**2.1.3** Table 4 lists other groups created by Study Group 17 during the study period.

**2.1.4** In line with WTSA-16 Resolution 54, at its March 2017 SG17 meeting, the Arab Regional Group for SG17 was created; see section 3.3.5.

**2.1.5** 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.

**- 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 was set to dormant in the first meeting of SG17 in March 2017.

**2.1.6** 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 4
Other Groups (if any)**

| **Title of the Group** | **Chairman** | **Vice-Chairmen** |
| --- | --- | --- |
| JCA-IdM | Co-chairmen: Mr Barbir Abbie (1), Mr Park Keundug (1), Mr Takechi Hiroshi (1) Mr Youm Heung Youl (8) |  |
| JCA-COP | NA |  |
| SG17RG-AFR | Mr Katundu Michael (2)Ms Njiraini Mwende (3) | Mr Elhaj Mohamed **(**2)**,**Mr Mwesigwa Patrick (2)**,**Mr Toure Mohamed (2) |
| SG17RG-ARB | Ms Latrous Wala Turki (4)**,**Mr Al Salehi Badar Ali Said (5) | Ms Abdelkader Manel (6)**,**Ms Abouche Chehrazed (6)**,**Ms Almansoury Laial (7) |
| ASN.1 Project | Project leader: Mr Thorpe Paul |  |
| OID Project | Project leader: Mr Dubuisson Olivier  |  |

Notes:

(1) Co-chairing since March 2017.

(2) Chairing/Vice-chairing until September 2018.

(3) Chairing since April 2019.

(4) Co-chairing from December 2017 to October 2018.

(5) (Co-)Chairing since December 2017.

(6) Vice-chairing from December 2017 to October 2018.

(7) Vice-chairing since December 2017.

(8) Acting-cochair since April 2021.

**2.2 Questions and Rapporteurs**

**2.2.1** WTSA-16 assigned to Study Group 17 the following 12 Questions listed in Table 5 and SG17 appointed the listed Rapporteurs and Associate Rapporteurs through this study period.

**TABLE 5
Study Group 17 – Questions assigned by WTSA-16 and Rapporteurs (2017-2020)**

| **Questions** | **Title of the Questions** | **WP** | **Rapporteur(19)** |
| --- | --- | --- | --- |
| Q1/17 | Telecommunication/ICT security coordination | PLEN  | Ms Latrous Wala (Rapporteur) **(13)**Mr Elhaj Mohamed M. K. (Rapporteur) **(1)**Ms Ki Juhee (Associate rapporteur) **(2)**Mr Najarian Paul (Associate rapporteur) **(3)**Mr Senga Wataru (Associate rapporteur) **(3)**Ms Wang Yiwen (Associate rapporteur) **(3)** |
| Q2/17 | Security architecture and framework | WP1/17 | Ms Hu Zhiyuan (Co-rapporteur) **(3)**Mr Oh Heung Ryong (Co-rapporteur) **(3)**Ms Chaabane Emna (Associate rapporteur) **(10)**Mr Lee Jinmyung (Associate rapporteur) **(16)** |
| Q3/17 | Telecommunication information security management | WP1/17 | Ms Naganuma Miho (Rapporteur) **(3)**Mr Min Jinghua (Associate rapporteur) **(7)**Mr Mustafa Thaib (Associate rapporteur) **(5)**Mr Fischer Andres (Associate rapporteur) **(4)** |
| Q4/17 | Cybersecurity | WP2/17 | Mr Kadobayashi Youki (Rapporteur) **(6)**Mr Kim Jong-Hyun (Rapporteur) **(7)**Mr Sim Dong-Hi (Associate rapporteur) **(2)**Mr Zhang Chen (Associate rapporteur) **(15)**Mr Casanovas Eduardo (Associate rapporteur) **(4)** |
| Q5/17 | Countering spam by technical means | WP2/17 | Mr Zhang Yanbin (Rapporteur) **(3)**Mr Kim ChangOh (Associate rapporteur) **(3)** |
| Q6/17 | Security aspects of telecommunication services, networks and Internet of Things (17)  | WP1/17 | Mr Baek Jonghyun (Co-rapporteur) **(3)**Ms Zuo Min (Co-rapporteur) **(14)**Mr Yan Junzhi (Co-rapporteur) **(8)**Mr Lee Gunhee (Associate rapporteur) **(9)**Mr Takahashi Takeshi (Associate rapporteur) **(3)**Mr Yu Bo (Associate rapporteur) **(3)**Ms Pazo Robles Maria Eugenia (Associate rapporteur) **(4)** |
| Q7/17 | Secure application services | WP3/17 | Mr Nah Jae Hoon (Rapporteur) **(3)**Ms Gao Feng (Associate rapporteur) **(7)**Mr Liu Lijun (Associate rapporteur) **(3)** |
| Q8/17 | Cloud computing and Big data infrastructure security (18)  | WP3/17 | Mr Wei Liang (Rapporteur) **(3)**Mr Sang-Woo Lee (Associate rapporteur) **(9)**Mr McFadden Mark (Associate rapporteur) **(5)** |
| Q9/17 | Telebiometrics | WP4/17 | Mr Caras John George (Rapporteur) **(3)**Mr Li Kepeng (Associate rapporteur) **(11)**Ms Wang Mengxi (Associate rapporteur) **(12)** |
| Q10/17 | Identity management architecture and mechanisms | WP4/17 | Mr Barbir Abbie (Rapporteur) **(3)**Mr Park Keundug (Associate rapporteur) **(3)**Mr Takechi Hiroshi (Associate rapporteur) **(3)**Mr Xia Junjie (Associate rapporteur) **(3)** |
| Q11/17 | Generic technologies (Directory, public key infrastructure (PKI), privilege management infrastructure (PMI), Abstract Syntax Notation One (ASN.1), object identifiers (OIDs)) to support secure applications | WP4/17 | Mr Lemaire Jean-Paul (Rapporteur) **(3)**Ms Kaddachi Olfa (Associate rapporteur) **(18)** |
| Q12/17 | Formal languages for telecommunication software and testing | WP3/17 | Mr Hogrefe Dieter (Rapporteur) **(3)**Mr Mussbacher Gunter (Associate rapporteur) **(5)**Mr Duhalde Enacom Martin (Associate rapporteur) **(4)** |

Note:

(1) Appointed 5 September 2019

(2) Appointed 30 January 2019

(3) Appointed 30 March 2017

(4) Appointed 30 March 2017, dismissed 29 March 2018

(5) Appointed 6 September 2017

(6) Appointed 30 March 2017, removed (reassigned) 29 March 2018

(7) Appointed 29 March 2018

(8) Appointed 30 January 2019

(9) Appointed 7 September 2018

(10) Appointed 30 March 2017, dismissed 7 September 2018

(11) Appointed 30 March 2017, resigned 7 September 2018

(12) Appointed 6 September 2017, dismissed 7 September 2018

(13) Appointed 30 March 2017, dismissed January 2019

(14) Appointed 29 March 2018, resigned 30 January 2019

(15) Appointed 7 September 2018

(16) Appointed 6 September 2017, dismissed 7 September 2018

(17) Q6/17 title was changed from ‘Security aspects of telecommunication services, networks’ to ‘Security aspects of telecommunication services, networks and Internet of Things’.

(18) Q8/17 title was changed from ‘Cloud computing security’ to ‘Cloud computing and Big data infrastructure security’.

(19) Appointment valid before 20 April 2021.

**2.2.2** With the postponement of WTSA-20 to March 2022, TSAG meeting on 11-18 January 2021 endorsed a new set of 12 Questions listed in Table 5a that were agreed by SG17 in SG17 August/September 2020 meeting (ref. [TSB Circular 295](https://www.itu.int/md/T17-TSB-CIR-0295/en)).

**TABLE 5a
Study Group 17 – Questions endorsed by TSAG (from 18 January 2021)**

| **New number** | **New Question title** | **Status** | **Previous number** | **Previous Question title** | **WP** | **Rapporteur** **(1)** |
| --- | --- | --- | --- | --- | --- | --- |
| 1/17 | Security standardization strategy and coordination | Continued | 1/17 | Telecommunication/ICT security coordination | WP1/17 | Co-Rapporteurs:- Mr Elhaj Mohamed M. K- Ms Ki JuheeAssociate rapporteurs:- Mr Najarian Paul- Mr Senga Wataru- Ms Wang Yiwen**)** |
| 2/17 | Security architecture and network security | Continued | 2/17 | Security architecture and framework | WP2/17 | Co-Rapporteurs- Ms Hu Zhiyuan- Mr Oh Heung Ryong |
| 3/17 | Telecommunication information security management and security services | Continued | 3/17 | Telecommunication information security management | WP3/17 | Rapporteur:- Ms Naganuma MihoAssociate rapporteurs:- Mr Min Jinghua - Mr Mustafa Thaib  |
| 4/17 | Cybersecurity and countering spam | Continuation of Q4/17 and Q5/17 | 4/17 | Cybersecurity | WP3/17 | Co-Rapporteurs:- Mr Kim Jong-Hyun- Mr Zhang YanbinAssociate rapporteurs:- Mr Kim ChangOh |
| 5/17 | Countering spam by technical means |
| 6/17 | Security for telecommunication services and Internet of Things | Continued | 6/17 | Security aspects of telecommunication services, networks and Internet of Things | WP2/17 | Co-Rapporteurs:- Mr Baek Jonghyun - Mr Yan JunzhiAssociate rapporteurs:- Mr Lee Gunhee- Mr Takahashi Takeshi- Mr Yu Bo  |
| 7/17 | Secure application services | Continued | 7/17 | Secure application services | WP4/17 | Rapporteur:- Mr Nah Jae Hoon Associate rapporteurs:- Ms Gao Feng- Mr Liu Lijun |
| 8/17 | Cloud computing and big data infrastructure security | Continued | 8/17 | Cloud computing and big data infrastructure security | WP4/17 | Rapporteur:- Mr Wei LiangAssociate rapporteurs:- Mr McFadden Mark |
| 10/17 | Identity management and telebiometrics architecture and mechanisms | Continuation of Q9/17 and Q10/17 | 9/17 | Telebiometrics | WP5/17 | Co-Rapporteurs:- Mr Barbir Abbie- Mr Caras John GeorgeAssociate rapporteurs:- Mr Kim Jason- Mr Park Keundug- Mr Takechi Hiroshi- Mr Xia Junjie |
| 10/17 | Identity management architecture and mechanisms |
| 11/17 | Generic technologies (such as Directory, PKI, Formal languages, Object Identifiers) to support secure applications | Continuation of Q11/17 and Q12/17 | 11/17 | Generic technologies (Directory, public key infrastructure (PKI), privilege management infrastructure (PMI), Abstract Syntax Notation One (ASN.1), object identifiers (OIDs)) to support secure applications | WP5/17 | Rapporteur:- Mr Lemaire Jean-Paul Associate rapporteur:- Mr Hogrefe Dieter |
| 12/17 | Formal languages for telecommunication software and testing |
| 13/17 | Intelligent transport system (ITS) security | Continued | 13/17 | Security aspects for Intelligent Transport System | WP2/17 | Rapporteur:- Mr Lee Sang-Woo Associate rapporteurs:- Mr Park Seungwook - Ms Zhang Yi  |
| 14/17 | Distributed ledger technology (DLT) security | Continued | 14/17 | Security aspects for distributed ledger technologies | WP4/17 | Co-Rapporteurs:- Mr Kadobayashi Youki- Ms Oh Kyeong HeeAssociate rapporteurs:- Ms Bai Xiaoyuan- Ms Wang Ke |
| 15/17 | Security for/by emerging technologies including quantum-based security | New | – | – | WP1/17 | Rapporteur:- Mr Sim DongheeAssociate rapporteurs:- Mr Kenyoshi Kaoru- Mr Yoon ChunSeok- Mr Zhang Chen |

(1) (re-)appointed in SG17 20-30 April 2021 meeting

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

**TABLE 5b
Study Group 17 – New Questions adopted and Rapporteurs**

| **Questions** | **Title of the Questions** | **WP** | **Rapporteur** |
| --- | --- | --- | --- |
| Q13/17 | Security aspects for Intelligent Transport System **(10)** /Intelligent transport system (ITS) security **(11)**  | WP1/17**(10) /** WP2/17**(11)**   | Mr Lee Sang-Woo (Rapporteur) **(1)**Mr Park Seungwook (Associate rapporteur) **(1)**Ms Zhang Yi (Associate rapporteur) **(2)** |
| Q14/17 | Security aspects for Distributed Ledger Technologies **(10)** Distributed ledger technology (DLT) security **(11)** | WP2/17**(10) /** WP3/17**(11)**   | Mr Kadobayashi Youki (Co-rapporteur) **(3)**Ms Oh Kyeong Hee (Co-rapporteur) **(3)**Ms Bai Xiaoyuan (Associate rapporteur) **(4)**Ms Wang Ke (Associate rapporteur) **(4)** Ms Zuo Min (Associate rapporteur) **(5)** |
| Q15/17 | Security for/by emerging technologies including quantum-based security | WP1/17**(11)**  | Mr Sim Dong-hi (Rapporteur) **(6)**Mr Kenyoshi Kaoru (Associate rapporteur) **(7)**Mr Yoon Chun Seok (Associate rapporteur) **(8)**Mr Zhang Chen (Associate rapporteur) **(9)** |

(1) Appointed 30 March 2017

(2) Appointed 7 Sep 2018

(3) Appointed 6 September 2017

(4) Appointed 29 March 2018

(5) Appointed 6 September 2017, removed (reassigned) 29 March 2018

(6) Appointed 20 April 2021

(7) Appointed 20 April 2021

(8) Appointed 20 April 2021, responsible for incubation task.

(9) Appointed 20 April 2021

(10) 2017 – 2020

(11) 2021 – 2022

**2.2.4** The Questions listed in Table 6 have been merged into other Questions of SG17 during this period.

**TABLE 6
Study Group 17 – Questions deleted**

| **Questions** | **Title of the Questions** | **Rapporteur** | **Note** |
| --- | --- | --- | --- |
| Q5/17 (deleted) | Countering spam by technical means | Mr Zhang Yanbin (Rapporteur)Mr Kim ChangOh (Associate rapporteur) | Q5/17 was merged with Q4/17 on 18 January 2021, following endorsement by TSAG |
| Q9/17 (deleted) | Telebiometrics | Caras John George (Rapporteur) | Q9/17 was merged with Q10/17 on 18 January 2021, following endorsement by TSAG |
| Q12/17 (deleted) | Formal languages for telecommunication software and testing | Mr Hogrefe Dieter (Rapporteur)Mr Mussbacher Gunter (Associate rapporteur) | Q12/17 was merged with Q11/17 on 18 January 2021, following endorsement by TSAG |

# 3 Results of the work accomplished during the 2017-2020 study period

## 3.1 General

During the study period through to its 7 January 2022 e-meeting, Study Group 17 examined a large number of contributions and TDs and liaison statements.

On the basis of these documents, by 7 January 2022, Study Group 17:

– developed 53 AAP + 47 TAP new Recommendations; (3 TAP determined)

– revised 93 AAP + 3 TAP existing Recommendations;

– amended 4 Recommendations;

– developed 8 new Supplements, one revised Supplement and one corrigendum to one existing Supplement;

– produced 17 Technical Corrigenda;

– developed 2 Technical papers and 6 Technical Reports (no Handbooks were prepared).

During the study period through to 7 January 2022 e-meeting, SG17:

– attracted 2163 (2063+100) participants (past meetings: 100, 223, 231, 91, 262, 69, 225, 206, 178, 168, 130, 134, 146)

– established 162 new work items (past meetings: 7, 15, 0, 15, 7, 26, 13, 25, 21, 26, 7)

– received 1179 Contributions (past meetings: 1, 98, 104, 2, 110, 121, 151, 118, 144, 113, 106, 78)

– produced 4220 TDs (past meetings: 106, 336, 305, 44, 434, 35, 439, 508, 380, 420, 395, 426, 368)

– received 585 incoming liaison statements and produced 328 outgoing liaison statements (past meetings: 55+1, 51+23, 36+17, 21+0, 58+32, 1+2, 77+24, 64+42, 47+30, 40+37, 46+37, 49+40, 40+38)

## 3.2 Highlights of achievements

The main results achieved on the various Questions assigned to Study Group 17 are briefly summarized below:

Formal replies to the Questions are given in a synoptic table in Annex 1 of this report.

**a) Q1/17, Telecommunication/ICT security coordination (2017 – 2020) / Security standardization strategy and coordination (2021 -)**

Q1/17 acts as a SG17 focal point for coordination of telecommunications/ICT security matters both within SG17 and with other study groups and outside organizations. Q1/17 also develops and maintains several outreach and reference documents 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. In this study period, Q1/17 prepared the 7th edition.

– The Technical Report on *Successful Use of Security Standards* focuses on how approved security-related ITU-T Recommendations can be successfully deployed. Both individual Recommendations (such as ITU-T X.805) and families of Recommendations (such as CYBEX) are considered and the potential benefits that can be gained from their use are described. In this study period, Q1/17 prepared the 2nd edition.

– The *ICT Security Standards Roadmap* contains an online searchable database of over 2,600 approved ICT security standards from ITU-T study groups and from external SDOs including 3D@home, 3GPP, 3GPP2, ATIS, ETSI, IEEE, IETF, ISO/IEC JTC 1, OASIS, oneM2M, SmartBan and TETRA. In this study period, Q1/17 approved many updates.

– The *Compendium of Security Recommendations* that provides in Part I a catalogue of approved ITU‑T Recommendations related to telecommunication security and in Part II an extract of ITU‑T approved security definitions. In this study period, the compendium was updated at each Q1/17 meeting.

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.

Q1/17 also promoted workshops on Security, supported SG17’s two regional groups (Africa and Arab) and improved the efficiency of SG17 work by creating templates, tools, and procedures. In this study period, Q1/17 has assisted ITU in holding 13 ITU workshops by end of 2021.

**b) Q2/17, Security architecture and framework (2017 – 2020) / Security architecture and network security (2021 -)**

Q2/17 develops a comprehensive set of security architecture and framework Recommendations for providing standard security solutions for telecommunications. Included are security for 5G, security frameworks for software defined networking, voice-over-long-term-evolution and network virtualization.

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

– X.1011, *Guidelines for continuous protection of the service access process*,analyzes security threats to service access process, specifies security protection measures to detect the abnormal access activities and introduces an enhanced authorization mechanism for service access.

– X.1040, *Security reference architecture for lifecycle management of e-commerce business data,* analyses the main features and typical threats faced by e‑commerce service ecosystems, and provides a security reference architecture for lifecycle management of e‑commerce business data.

– X.1041, *Security framework for voice-over-long-term-evolution (VoLTE) network operation,* analyses security threats encountered by the VoLTE network and recommends countermeasures for telecommunication operators to ensure the secure operation. It also provides a security reference framework for VoLTE network.

– X.1043, *Security framework and requirements for service function chaining based on software-defined networking,* analyses security threats to and specifies security requirements for service function chaining based on software-defined networking (SDN). The corresponding security countermeasures are also given. Recommendation ITU-T X.1043 also aims to help understanding of security risks encountered when using SDN-based service function chaining and implementation of secured SDN-based service function chains.

– X.1044, *Security requirements of network virtualization,* analyses security challenges and threats to network virtualization (NV) and specifies security requirements for the physical resources layer, the virtual resources layer and the logically isolated network partition (LINP) layer in network virtualization.

– X.1045, *Security service chain architecture for networks and applications,* supports provision of customized dynamic and adaptive security services for networks and applications. This Recommendation defines the security service chain and an architecture design for the security service chain. This Recommendation applies the security service chain to networks and applications. This Recommendation also enables tracing network attacks to their resources in a service function chain (SFC) overlay network with high performance and the mitigating/preventing of those attacks automatically.

– X.1046, *Framework for software-defined security in software-defined networks/network functions virtualization networks*, specifies a framework of software-defined security – in software defined networking (SDN) and the network functions virtualization (NFV) network. This Recommendation analyses the main security challenges including technical and operational aspects in operators’ SDN/NFV based networks. This Recommendation defines security requirements to address these challenges in SDN/NFV networks. This Recommendation introduces the concept of ‘software-defined security’ and designs a framework for ‘software-defined security’. This Recommendation provides implementation of software-defined security.

– X.1047, *Security requirements and architecture for network slice management and orchestration* establishes security requirements and architecture for network slice management and orchestration, as well as automatic creation of end-to-end (E2E) network slices with customized security capabilities, to deploy full-scale E2E network slicing for consumer, business and government segments.

– X.Suppl.30, *ITU-T X.805 - Security guidelines for mobile virtual network,* provides security guidelines for mobile virtual network operators (MVNOs). Security is very important to MVNOs and most MVNOs have a lot of security similarities. This Supplement analyses the main features of MVNOs and the typical security threats that they face. Based on the structure of MVNOs, this Supplement provides a security framework for MVNOs, including security objectives and security requirements.

**c) Q3/17, Telecommunication information security management (2017 – 2020) / Telecommunication information security management and security services (2021-)**

Q3/17 develops Recommendations on telecommunication information security management such as code of practices for PII, telecommunication organizations, and small and medium-sized telecommunication organizations.

In this study period, Q3/17 has developed five new Recommendations, one corrigendum, two revised and three new Supplements:

– Corrigendum 1 to X.1051 (revised), *Information technology – Security techniques – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations*.

– X.1052 (revised), *Information security management processes for telecommunication organizations,* provides best practices for information security management for telecommunication organizations to support Recommendation ITU-T X.1051. This recommendation is based on a process approach to describe a set of security management areas, which gives guidelines of telecommunication organizations to fulfil the control objectives defined in Recommendation ITU T X.1051. The management areas including asset management, incident management, risk management policy management and map the controls defined by Recommendation ITU-T X.1051 to achieve methodologies.

– X.1053, *Code of practice for information security controls based on ITU-T X.1051 for small and medium-sized telecommunication organizations,* establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security controls in small and medium-sized telecommunication organizations (SMTOs) based on Recommendation ITU-T X.1051. This Recommendation also provides an implementation baseline of information security controls for SMTOs to ensure the confidentiality, integrity and availability of telecommunication facilities and services and information handled, processed or stored by the facilities and services.

– X.1058, *Information technology - Security techniques - Code of practice for Personally Identifiable Information protection,* establishes control objectives, controls and guidelines for implementing controls, to meet the requirements identified by a risk and impact assessment related to the protection of PII. In particular, this Specification specifies guidelines based on ISO/IEC 27002, taking into consideration the requirements for processing PII that may be applicable within the context of an organization's information security risk environment(s).

– X.1059, *Implementation guidance for telecommunications organizations on risk management of their assets globally accessible in IP-based networks,* provides guidance for telecommunication organizations on the risk management of their assets globally accessible in IP-based networks, the assets which are exposed directly to hackers and attackers. These assets may also be connected to the traditional (and even old) assets of legacy telecommunication networks, which might have some design level vulnerabilities that could be difficult to fix. Therefore, it would be practical to consider all the assets globally accessible in IP-based networks (AGIT) of a telecommunication organization as a whole, and to introduce some specific security controls to continuously reduce the overall risks and to strengthen the overall security of telecommunication services and networks.

– X.1060, *Framework for the creation and operation of a Cyber Defence Centre,* defines Cyber Defence Centre as the entity that plays a central role in an organization to address cybersecurity risks. The three processes of build, management and evaluation that CDC should practically implement are described as a framework, and the services that the organization should have in order to implement more specific cybersecurity measures are also provided.

– X.1061, *Cyber insurance acquisition guideline for Information and Communication Technologies (ICT) services provider*

This cyber insurance acquisition guideline provides the understanding of cyber insurance coverage and the requirements of cyber security risks assessments, selection of insurer, assessment by the insurer, and evaluation of insurer for organisations that adopt cyber insurance as a risk treatment option to manage the impact of a cybersecurity incident.

– X.Suppl.13 (revised), *ITU-T X.1051 - Information security management users' guide*

– X.Suppl.32, *ITU-T X.1058 - Code of practice for personally identifiable information protection for telecommunications organizations,* aims to complement the information provided in ITU‑T X.1058 by providing additional implementation guidance for personally identifiable information (PII) protection, which are not described in ITU-T X.1058, but should further be applicable to telecommunications organizations to address PII protection.

– X.Suppl.34, *ITU-T X.1051 - Code of practice for information security controls for telecommunication organizations,* highlights and shares the implementation of a code of practice for information and network security management by the Malaysian information and communication industry, based on Recommendation ITU-T X.1051.

– X.Suppl.36, *ITU-T X.1051 – Critical security controls for telecommunication organizations information and network security management*, provides cyber security best practices for security management using critical security controls within the scope of the recommendation ITU-T X.1051. The use of Critical Security Controls (CSC) framework and the associated critical security controls is supporting and complimentary to ITU-T X.1051 Recommendation.

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

**d) Q4/17, Cybersecurity (2017 – 2020) / Cybersecurity and countering spam (2021 -)**

Q4/17 develops Recommendations on cybersecurity frameworks and requirements on how telecommunication/ICT providers secure their infrastructure and maintain secure operations, and exchange cybersecurity information. In this study period Q4/17 also incorporated an incubation function to address emerging issues such as security in a quantum environment until 2020 and transferred this function to Q15/17 in January 2021. Also in January 2021, Q4/17 assumed the ongoing work on countering spam previously studied in Q5/17.

In this study period, Q4/17 has developed 14 new Recommendations, one revised Recommendation, two new Amendments, two new Technical Papers and two new Technical Reports:

– X.1212, *Design considerations for improved end-user perception of trustworthiness indicators*, describes design consideration for improved end-user perception of trustworthiness indicators. The appendices describe representative techniques for measuring end-user perception of such indicators.

– X.1213, *Security capability requirements for countering smartphone-based botnets,* analyses the background and potential security threats of smartphone-based botnets, and provides security capability requirements.

– X.1214, *Security assessment techniques in telecommunication/information and communication technology networks,* describes a security assessment methodology for software-based telecommunication/information and communication technology (ICT) network elements and best practices for developers, manufacturers, operators and individual security experts in the telecommunication domain to address the security of their software-based elements. Both traditional circuit-switched networks and packet-based networks are exposed to different threats and attacks – from external as well as internal sources – that target the various parts of the telecommunication/ICT network. In telecommunication/ICT networks, this Recommendation covers both detection of vulnerabilities and methodology of security assessment.

– X.1215, *Use cases for structured threat information expression,* provides various use cases for how the structured threat information expression (STIX) language may be used to support cyber threat intelligence (CTI) and information sharing.

– X.1216, *Requirements for collection and preservation of cybersecurity incident evidence*, describes a general procedure for cybersecurity incident response and investigation. It also analyses sources of cybersecurity incident evidence and specifies capability requirements for tools used for collection and preservation of such evidence in an investigative process. This Recommendation also specifies reliability assurance requirements for these tools as guidelines to developers who design tools for such purpose.

– X.1217, *Guidelines for applying threat intelligence in telecommunication network operation*, Threat intelligence from a telecommunication operator’s point of view is a collection of organized, analysed, and refined information about potential and current attacks that may threaten an organization. This information can also include attackers’ motivations, intentions, characteristics, and methods, along with their modus operandi or techniques, tactics, and procedures. In network and information security area, the occurrence of large-scale and unexpected cybersecurity incidents has triggered the urgent need for threat intelligence. Threat intelligence can help an organization to reduce risk and improve its overall security. A unified taxonomy, grammar, and presentation of threat intelligence has been defined so that threat intelligence can be shared between different organizations. This Recommendation specifies guidelines for applying threat intelligence in telecommunication network operation after an overview analysis.

– X.1218, *Requirements and guidelines for dynamic malware analysis in a sandbox environment*. Unknown malware is commonly used in advanced attacks, in particular advanced persistent threats (APTs), to avoid being detected. For example, a targeted attack using phishing email weaponized with unknown malwares can easily achieve a successful initial compromise. Thus, for detection of advanced attacks, special attention and defence measurements should be taken to detect unknown malwares. Recommendation ITUT-T X.1218 analyses threats related to unknown malwares and specifies requirements of unknown malware detection based on dynamic behaviour analysis.

– X.1233, *Guidelines for countering spam over instant messaging,* specifies guidelines for instant messaging (IM) service providers and users to counter spam over instant messaging (SPIM). It covers instant messaging spam scenarios, technical measures and mechanisms to counter SPIM for IM service providers, and emergency response disposal measures to counter SPIM for IM users, etc.

– X.1234, *Guideline for countering Multimedia Messaging Service (MMS) spam*, specifies guidelines for countering MMS spam. It analyses typical scenarios, characteristics, and recognition methods of MMS spam, and provides a technical framework, work flows and some key technologies of MMS spam recognition, to help MMS providers and MMS users to counter spam.

– X.1235, *Technologies in countering website spoofing for telecommunication organizations*, recommends technologies for telecommunication organizations to identify website spoofing in time and protect their websites from being spoofed.

– Amd.11 and 12 to X.1500, *Overview of cybersecurity information exchange,* provides a list of structured cybersecurity information techniques that have been created to be continually updated as these techniques evolve, expand, are newly identified or are replaced. The list follows the outline provided in the body of the Recommendation. Situation of recommended techniques as of March 2017 and March 2018 respectively, including bibliographical references, were reflected.

– X.1541 (revised), *Incident object description exchange format version 2,* describes the information model for the incident object description exchange format (IODEF) version 2 and provides an associated data model specified with XML schema. The IODEF specifies a data model representation for sharing commonly exchanged information about computer security or other incident types. This is achieved by listing the relevant clauses of IETF RFC 7970 and showing whether they are normative or informative.

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

– X.1702, *Quantum noise random number generator architecture,* defines a generic functional architecture of a quantum entropy source, a common method to estimate and validate the entropy of a noise source under evaluation, and a common method to specify randomness extractors when they are part of the implemented system.

– X.1710, *Security framework for quantum key distribution networks*, specifies a framework including requirements and measures to combat security threats for quantum key distribution networks (QKDNs). It specifies a simplified QKDN structure for analysis of the relevant security threats. Security requirements and corresponding security measures are then specified on that basis.

– X.1714, *Key combination and confidential key supply for quantum key distribution networks*, describes key combination methods for quantum key distribution network (QKDN) and specifies security requirements for both the key combination and the key supply from QKDN to cryptographic applications.

– TP.inno, *Description of the incubation mechanism and ways to improve it*, describes entirely the incubation mechanism established by SG17. It then inventories other ways and mechanisms in ITU and other SDOs to accept innovation.

– TP.sgstruct, *Strategic approaches to the transformation of security studies*, covers the short, mid and long-term aspects of the transformation of security studies.

– TR.sec-qkd, *Security considerations for quantum key distribution network,* develops a QKD framework to satisfy requirements from the telecom network's perspective.

– TR.usm, *Unified Security Model (USM) - a neutral integrated system approach to Cybersecurity*, presents a universal “all matters security” architecture, that is neutral and agnostic. It has the potential to facilitate security control mass interoperability and security response automation.

In this study period, Q4/17 held a mini workshop on Secure Quantum Communications, Geneva, 24 January 2019.

**e) Q5/17, Countering spam by technical means (2017 – 2020)**

Q5/17 develops Recommendations for countering spam by technical means, such as countering advertising spam, countering instant messaging spam, countering mobile in-application advertising spam, countermeasures against short message service phishing and smishing attack, and countering telephone service scams.

In this study period, Q5/17 has developed three new Recommendations and two new supplements:

– X.1232, *Technical framework for countering advertising spam in user-generated information*, analyses scenarios and characteristics of advertising spam, and specifies a reference framework and process flows to help Internet service providers to counter advertising spam.

– X.1248, *Technical requirements for countering instant messaging spam,* identifies characteristics of spam over instant messaging (SPIM) and specifies technical requirements for countering it. As instant messaging (IM) increases in popularity, the proliferation of SPIM becomes an increasingly serious problem. The characteristics of IM, such as being Internet protocol (IP)-based with widespread usage that is free of charge, potentially allows SPIM to spread widely and uncontrollably. If SPIM problems are not carefully addressed, they can have negative impacts on the utilization of the IM service itself.

– X.1249, *Technical framework for* *countering mobile in-application advertising spam,* provides a technical framework for countering mobile in‑application advertising spam. Mobile in-application advertising spam is the sending of unsolicited advertisements, which are displayed within a mobile phone application. This unsolicited advertising can appear on the display screen of a mobile device as a banner at the top or bottom of the screen, a mobile interstitial or an overlay.

– X.Suppl.29, *ITU-T X.1242 - Supplement on guidelines on* *countermeasures against short message service phishing and smishing attacks,* provides universal guidelines on short message service (SMS) phishing which is a fraudulent technique through mobile phones by causing phishing frauds with smartphones, acquiring personal information on the smartphones, or by enabling small amounts of money to be approved and paid while the account holder is not aware of the approval.

– X.Suppl.33, *ITU-T X.1231 - Supplement on technical framework for countering telephone service scams,* provides a technical framework and related best practices for countering telephone service scams. In the framework, entity functions and processing procedures are specified. The best practices cover those found to be the most effective in stopping known telephone service scam methods.

**f) Q6/17, Security aspects of telecommunication services, networks and Internet of Things (2017 – 2020) / Security for telecommunication services and Internet of Things (2021 -)**

Q6/17 develops Recommendations on security requirements and frameworks for telecommunication services, mobile networks, smart grid network, IPTV and Internet of Things.

In this study period, Q6/17 has developed 17 new Recommendations, one Amendment and one corrigendum to an existing Supplement:

– X.1042, *Security services using software-defined networking*, supports the protection of network resources using security services based on software-defined networking (SDN). This Recommendation first classifies the network resources for SDN-based security services: SDN application, SDN controller, SDN switch and security manager (SM). Recommendation ITU-T X.1042 then defines security services based on SDN.

– X.1126, *Guidelines on mitigating the negative effects of infected terminals in mobile networks,* provides guidelines to mobile operators to restrain the infected terminals by utilizing technologies in the mobile network to protect both subscribers and mobile operators.

– X.1127, *Functional security requirements and architecture for mobile phone anti-theft measures,* focuses on the functional security requirements and functional architecture for smartphone anti-theft mechanisms based on the general requirements described by the GSMA.

– Amendment 1 to X.1197, *Guidelines on criteria for selecting cryptographic algorithms for IPTV service and content protection,* updates Appendices I and II to reflect the state of the art as of August 2019, including bibliographical references.

– X.1331, *Security guidelines for home area network (HAN) devices in smart grid systems,* provides threat analysis for a HAN in smart grid systems, security requirements and security functions. Since the role and functions of each HAN device are different, the security requirements and security functions by device are provided.

– X.1332*, Security guidelines for smart metering service in smart grids,* provides security guidelines for smart metering services, so that the service providers can implement security measures properly in order to assure the security of the service. It analyses the general model of smart metering service from the perspective of service level. Based on the general model, this Recommendation discusses security threats and attack method against smart metering services, and it identifies security requirements and capabilities to mitigate these risks. In addition, this Recommendation introduces useful security standards that can be considered when service provider implements the security capabilities.

– X.1333, *Security guidelines for use of remote access tools in Internet-connected control systems*, describes a whole picture to employ RATs (Remote access tools) securely for monitoring, control and maintenance.

– X.1361, *Security framework for the Internet of things based on the gateway model,* describes a security framework for the Internet of things (IoT) using security gateways. The IoT is a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies. This Recommendation analyses security threats and challenges in an IoT environment and describes capabilities that could address and mitigate these threats and challenges. A framework methodology is provided for determining which security capabilities are required for mitigating and addressing these threats and challenges for the IoT.

– X.1362*, Simple encryption procedure for Internet of things (IoT) environments,* specifies encryption with associated mask data (EAMD) for the Internet of things (IoT) devices. It describes EAMD and how it provides a set of security services for traffic using it.

– X.1363*, Technical framework of personally identifiable information (PII) handling system in Internet of things (IoT) environment,* specifies a technical framework for PII handling in IoT environment with single or multiple service providers.

– X.1364*, Security requirements and framework for narrow band Internet of things,* specifies security threats and requirements specific to the NB-IoT deployments and thus establishes a security framework for the operator to safeguard these new technology applications.

– X.1365*, Security methodology for use of identity-based cryptography in support of Internet of Things (IoT) services over telecommunication networks,* provides a security methodology for the use of IBC public key technology in support of IoT services over telecommunications networks including mechanisms of identity management, key management architecture, key management operations and authentication.

– X.1366, *Aggregate message authentication schemes for Internet of things environment*, specifies two message authentication schemes. One is an aggregate message authentication (AMA) scheme for IoT as a basic mechanism. The other is an interactive aggregate message authentication (IAMA) scheme with interactive protocol in a lightweight and secure manner. Both aggregate message authentication schemes can be applied for ensuring "entity (identity) authentication" as well as for ensuring "message authentication".

– X.1367, *Standard format for Internet of things error logs for security incident operations*, specifies a standardized error log format that can be placed in a protocol payload, such as syslog (see IETF RFC 5424) to be used for converting an error log information issued by an edge device to the standard error log format. This Recommendation also specifies a standardized error code table to solve the second issue. As a result, security incidents across computer networks and networks for IoT edge devices can be integrally managed.

– X.1368, *Secure firmware or software update for Internet of things devices*, specifies: 1) basic models and procedures for securely updating firmware/software (FW/SW) of Internet of things (IoT) devices; and 2) requirements and capabilities for updating IoT FW.

– X.1369, *Security Requirements for IoT Service Platform*, specifies security requirements for IoT service platform. It assesses security threats and challenges to IoT business service platform and describes security measures that could mitigate security threats and challenges.

– X.1453, *Security threats and requirements for video management systems*, analyzes the security threats to server platform based VMS (Video management system) running on an IP network and specifies security requirements to counteract identified security threats.

– X.1811, *Security guidelines for applying quantum-safe algorithms in IMT-2020 systems*, identifies threats raised by quantum computing to International Mobile Telecommunications-2020 (IMT-2020) systems through assessing the security strength of currently used cryptographic algorithms. This Recommendation briefly reviews quantum safe algorithms, including both symmetric and asymmetric types, and provides guidelines for applying quantum safe algorithms in IMT-2020 systems.

– X.Suppl.26 Cor.1, *ITU-T X.1111 - Supplement on security functional architecture for smart grid services using telecommunication networks.*

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

Q7/17 develops Recommendations on security requirements for secure application services such as value-added services and Fintech services.

In this study period, Q7/17 has developed nine new Recommendations:

– X.1145, *Security framework and requirements for open capabilities of telecommunication services*, focuses on an analysis of the security requirements of open capabilities of telecommunication services and provides a security framework.

– X.1146, *Secure protection guidelines for value-added services provided by telecommunication operators,* provides secure protection guidelines for value-added services provided by telecommunication operators. In addition to analysing typical service scenarios, security threats and attack methods, Recommendation ITU-T X.1146 provides technical measures to counter threats and attacks. This will help the operators to assure the security of the value-added service and will also protect the users' benefits.

– X.1147, *Security requirements and framework for big data analytics in mobile Internet services,* will analyse the security requirements of big data analytics in mobile Internet services and provide security framework.

– X.1148, *Framework of de-identification process for telecommunication service providers*, describes a framework of de-identification process with operational steps and specifies data release models and data stages in a de-identification process for telecommunication service providers based on data lifecycle model and the roles of stakeholders.

– X.1149, *Security framework of open platform for FinTech services,* describes an open platform architecture for financial technology (FinTech) services, threats and vulnerabilities of open platform, and open API usage procedure for FinTech services. It also specifies security requirements of open platform of FinTech services for both financial company and FinTech company sides. Use cases of the proposed open platform are found in Appendix to this Recommendation.

– X.1450, *Guidelines on hybrid authentication and key management mechanisms in the client-server model,* provides guidelines for hybrid authentication and key exchange mechanisms in the client-server model. The underlying mechanism suggests the use of shared secrets and public key techniques for authentication and key exchange. This Recommendation covers service scenarios, and security threats and methods to mitigate such attacks.

– X.1451, *Risk identification to optimize authentication,* specifies a risk identification function in an ICT service system as a pre-processor before the authentication function is invoked. It enables the ICT service system to optimize user authentication based on identified risks. With this specific risk identification function, the ICT service system can make choices on authentication mechanisms adaptively to its users and achieve multiple benefits such as: 1) to improve user experiences; 2) to increase the capacity and reduce the per transaction cost of user authentication; 3) to reduce the risk of user identity forgery.

– X.1452, *Guidelines for security services provided by operators*, classifies potential use cases of security services provided by operators and analyse specific requirements for security services, thus providing guidelines for operators to safeguard and improve their security services.

– X.1470, *Security guidelines of web-based online customer service*, analyses the security threats of web-based online customer service in three aspects: network security, system security, service security. It specifies security guidelines of web-based online customer service and corresponding security measures. It also proposes test procedures to verify the specified security requirements are satisfied by corresponding security measures.

**h) Q8/17, Cloud computing and Big data infrastructure security**

Q8/17 develops Recommendations on security threats and requirements for cloud computing and big data infrastructure.

In this study period, Q8/17 has developed eight new Recommendations:

– X.1603, *Data security requirements for the monitoring service of cloud computing,* analyses data security requirements for the monitoring service of cloud computing which includes monitoring data scope requirements, monitoring data lifecycle, security requirements of monitoring data acquisition and security requirements of monitoring data storage.

– X.1604, *Security requirements of network as a service (NaaS) in cloud computing,* analyses security threats and challenges on network as a service (NaaS) in cloud computing and specifies security requirements of NaaS in NaaS application, NaaS platform and NaaS connectivity aspects based on corresponding cloud capability types.

– X.1605, *Security requirements of public infrastructure as a service (IaaS) in cloud computing,* aims to document security requirements of public IaaS in order to help IaaS providers to improve security of IaaS platform throughout the planning, building and operating stages.

– X.1606, *Security requirements for ‘communications as a service’ application environments*, identifies security threats and recommends security requirements for communications as a service (CaaS) application environments. The Recommendation describes scenarios and features of CaaS containing multi-communication capabilities. Then it identifies specific threats arising from unique CaaS features and recommends appropriate CaaS security requirements.

– X.1643, *Security requirements and guidelines of virtualization container in cloud computing environment*, analyses security threats and challenges on virtualization container in cloud computing environment and specifies a reference framework with security guidelines for virtualization container in cloud.

– X.1750, Guidelines on security of ‘big data as a service’ for big data service providers, analyses security challenges Big data as a service (BDaaS) faces, identifies security roles and responsibilities for provision of BDaaS, as well as a security framework for a big data infrastructure. It also specifies security protection measures that should be satisfied for services and components related to BDaaS.

– X.1751, *Security guidelines for big data lifecycle management by telecommunication operators*, analyses security vulnerabilities and establishes security guidelines for big data lifecycle management by telecommunication operators. It introduces specific characteristics of telecommunication big data services and data categories, analyses security vulnerabilities of big data lifecycle management and specifies security guidelines for telecommunication operators.

– X.1752, *Security guidelines for big data infrastructure and platform*, analyses security threats and challenges on big data infrastructure and platform and specifies a reference framework to mapping security guidelines against threats for big data infrastructure and platform.

– TR.XAASL, *Framework for security standardization for virtualized services*, is a document for discussion regarding the development of standards considerations, requirements and frameworks for virtualized services.

**i) Q9/17, Telebiometrics (2017 – 2020)**

Q9/17 develops Recommendations on telebiometrics to authenticate users using telebiometrics and to protect telebiometric information against unauthorized access.

In this study period, Q9/17 has developed three new Recommendations, one revised Recommendation and one corrigendum:

– X.1080.0 and X.1080.0 Cor.1, *Access control for telebiometrics data protection,* provides specifications on how to protect telebiometrics information against unauthorized access. A service-oriented view is taken, where only information necessary for a particular purpose is provided, i.e., access is given not only on a right-to-know basis, but also on a need-to-know basis. The core of this Recommendation is an attribute specification included in an attribute certificate or public-key certificate that specifies in detail what privileges a particular entity has for one or more service types. Security is provided by using a profile of the cryptographic message syntax (CMS). The CMS profile provides authentication, integrity and, when required, confidentiality (encryption). This profile is intended to provide security support for telebiometrics specifications in general. The profile assumes, and is dependent upon, the correct deployment of a public-key infrastructure (PKI). This Recommendation is also dependent on the deployment of a privilege management infrastructure (PMI).

– X.1080.1 (revised), *e-Health and world-wide telemedicines - Generic telecommunication protocol,* defines the framework for other parts of the ITU-T 1080.x series of Recommendations by providing the overall model for communications aspects of telebiometrics. It provides the basic allocation of object identifiers for uniquely identifying pieces of information during data transfer and it defines a generic telecommunication protocol. It provides a technique for a formal specification of objects and it specifies a generic protocol that supports interactions between a medical station local to a patient and a remote medical centre providing greater expertise. This protocol is to be used and extended by other parts of the ITU-T X.1080.x series Recommendations.

– X.1093, *Telebiometric access control with smart ID cards*, describes the general scheme for logical and/or physical access control using the biometrics-on-card. This Recommendation can be applied to the recent emerging area of requiring secure physical and also logical access control management.

– X.1094, *Telebiometric authentication using bio-signals,* specifies new secure and strong telebiometric authentication methods using bio-signals.

**j) Q10/17, Identity management architecture and mechanisms (2017 – 2020) / Identity management and telebiometrics architecture and mechanisms (2021 -)**

Q10/17 develops Recommendations on identity management subjects including authentication frameworks. In January 2021, Q10/17 assumed the ongoing work on telebiometrics previously studied in Q9/17.

In this study period, Q10/17 has developed five new Recommendations, two revised Recommendations and one new supplement:

– X.1080.2, *Biology-to-machine (B2M) protocol*, defines a general protocol for exchange of biometric information from a patient facility to a medical expert facility so that a medical centre could remotely monitor a patient and retrieve information from that patient.

– X.1252 (revised), *Baseline identity management terms and definitions*, provides definitions of key terms used in identity management (IdM). The terms are drawn from many sources but all are believed to be in common use in IdM work. This Recommendation is not intended to be a huge compendium of IdM-related terms. Instead, the terms defined here are limited to those considered to constitute a baseline list of the most important and commonly-used IdM-specific terms. This Recommendation includes Annex A that explains the rationale for some of these key terms.

– X.1254 (revised), Entity authentication assurance framework, specifies three entity authentication assurance levels (AALs), and criteria for and threats to each of them. Additionally, it:

• establishes a framework for managing AALs;

• provides guidance concerning control technologies that are to be used to mitigate authentication threats, based on a risk assessment;

• provides guidance for mapping the three AALs to other authentication assurance schemas; and

• provides guidance for exchanging the results of authentication that are based on the three AALs.

– X.1276, *Authentication step-up protocol and metadata Version 1.0*, proposes simple trust elevation architectural patterns demonstrating the use of trust elevation in modern access control architectures, describes a common metadata set mechanisms and protocol elements for trust elevation information exchanges and promotes the use of trust elevation elements to facilitate standardization among the many technologies and approaches currently in use for credential and authentication risk mitigation.

– X.1277, *Universal authentication framework,* describes the FIDO universal authentication framework (UAF) that enables online services and websites, whether on the open Internet or within enterprises, to transparently leverage native security features of end-user computing devices for strong user authentication and to reduce the problems associated with creating and remembering many online credentials.

– X.1278, *Client to authenticator protocol/Universal 2-factor framework,* describes an application layer protocol for communication between an external authenticator and another client/platform, as well as bindings of this application protocol to a variety of transport protocols using different physical media.

– X.1279, *Framework of enhanced authentication using telebiometrics with anti-spoofing detection mechanisms*, provides an architectural framework of enhanced authentication using telebiometrics with anti-spoofing detection. This Recommendation analyses threats to traditional telebiometric authentication solutions and specifies an architectural framework, authentication process flows and security considerations for enhanced authentication using telebiometrics with anti-spoofing detection mechanisms.

– X.Suppl.35, *ITU-T X.1254 - Supplement on use cases of entity authentication assurance (EAA) framework,* contains three use cases of applying the entity authentication assurance framework in security implementation, including detailed security considerations in risk assessment, choice of appropriate assurance level and selection of authentication technologies.

SG17 agreed at its 29 May 2020 SG17 e-plenary to assign X.1261 to ITU-T D.1140, *Policy Framework including Principles for digital identity infrastructure*, to become a dual numbered Recommendation numbering in the ITU-T D-series and in the ITU-T X-series Recommendations on identity management.

**k) Q11/17, Generic technologies (Directory, public key infrastructure (PKI), privilege management infrastructure (PMI), Abstract Syntax Notation One (ASN.1), object identifiers (OIDs)) to support secure applications (2017 – 2020) / Generic technologies (such as Directory, PKI, Formal languages, Object Identifiers) to support secure applications (2021 -)**

Q11/17 develops Recommendations on the directory services and systems including public-key/attribute certificates in the X.500-series. Q11/17 maintains the ASN.1 Recommendations and is further elaborating Recommendations on OIDs, a world-wide identifications scheme based on hierarchical registration authorities called the “Object Identifier Tree”. In January 2021, Q11/17 assumed the ongoing work on languages previously studied in Q12/17.

In this study period, Q11/17 has developed five new Recommendations, twenty revised Recommendations, one Amendment and fourteen Technical Corrigenda (X.680 Cor.1, X.680 Cor.2, X.680 Amd.1, X.680 Cor.3, X.681 Cor.1, X.682 Cor.1, X.682 Cor.2, X.683 Cor.1,, X.693 Cor.1, X.694 Cor.1, X.696 Cor.1, X.696 Cor.2, X.696 Cor.3, X.893 Cor.1, X.894 Cor.1) to the X.500-, X.680-, and X.690-series of Recommendations, one Supplement and one new 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.

– Amd.1 to X.501, *Information technology – Open Systems Interconnection – The Directory: Models*, updates clause 9.2 and Annex A.

– 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.

– Cor.1 to X.509, *Information Technology - Open systems Interconnection - The Directory: Public-key and attribute certificate frameworks*, corrects defects in clause 6.2.2 and Annex B.

– X.510, *Information technology – Open Systems Interconnection – The Directory:* Protocol specifications for secure operations, defines a general protocol, called the wrapper protocol, that provides cyber security for protocols designed for wrapper protocol protection by providing for authentication, integrity and optionally confidentiality (encryption). The wrapper protocol allows cyber security to be provided independently of the protected protocols, which means that the security may be enhanced without affecting the protected protocol specification.

– 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 attribute 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.

– X.676, *Object identifier-based resolution framework for IoT grouped services*, specifies an object identifier (OID)-based resolution framework for identifying various services in IoT environments. OID is an identifier to name an object with a hierarchically assigned namespace. In Internet of things (IoT), thousands of IoT services based on heterogeneous resources will be provided as combinations of various services. For efficiency, various technologies, such as service binding, dynamic services or frequently switching services will be required, along with resolution and identification of grouped services. This Recommendation describes the concepts of IoT grouped services, considerations, architectures, and procedures for an OID-based resolution framework for IoT grouped services.

– X.677, *Identification mechanism for unmanned aerial vehicles using object identifiers*, analyses requirements for full life-cycle management and operating identity recognition of unmanned aerial vehicles (UAVs) with security considerations and specifies an identification mechanism for UAVs using object identifiers (OIDs), including detailed specifications of assignment rules and registration procedures of OIDs used for UAVs.

– X.680 (revised and its Amd.1 and Cor.1-3 before the revision), *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.

– X.681 (revised and its Cor.1 before the revision), *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. An information object class defines the form of a conceptual table (an information object set) with one column for each field in the information object class, and with each complete row defining an information object.

– X.682 (revised and its Cor.2 before the revision), *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. The notation also provides for signalling if and when a constraint is violated.

– X.683 (revised and its Cor.1 before the revision), *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. Application of these encoding rules produces a transfer syntax for such values. It is implicit in the specification of these encoding rules that they are also used for decoding. This Recommendation | International Standard defines also 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). The key difference between them is that DER uses the definite length form of encoding while CER uses the indefinite length form. DER is more suitable for the small, encoded values, while CER is more suitable for the large ones. It is implicit in the specification of these encoding rules that they are also used for decoding.

– 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 and its Cor.1 before the revision), *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 and its Cor.1 before the revision), *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. Encoding instructions are a means of modifying the encodings of ASN.1 types for some specified encoding rule (in this case PER). They can be inserted in an ASN.1 specification in square brackets (much like a tag in the Basic Encoding Rules, BER) immediately before the type that they affect (type prefixes), or they can be collected together at the end of an ASN.1 module (an encoding control section).

– X.696 (revised and its Cor.1-3 before the revision), *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.697, *Information technology - ASN.1 encoding rules: Specification of JavaScript Object Notation Encoding Rules (JER),* specifies a set of JavaScript Object Notation Encoding Rules (JER) that may be used to derive a transfer syntax for values of types defined in Rec. ITU-T X.680 | ISO/IEC 8824-1, Rec. ITU‑T X.681 | ISO/IEC 8824-2, Rec. ITU-T X.682 | ISO/IEC 8824-3, Rec. ITU-T X.683 | ISO/IEC 8824-4. It is implicit in the specification of these encoding rules that they are also to be used for decoding.

– Cor.1 to X.893 *Information technology - Generic applications of ASN.1: Fast infoset security,* provides corrections to the informative annexes and bibliography removing references to the obsolete triple DES algorithm.

– X.894 and its Cor.1 and Cor.2, *Information technology - Generic applications of ASN.1: Cryptographic message syntax,* provides Abstract Syntax Notation One (ASN.1) modules for using cryptographic syntax in ITU-T Recommendations. Cryptographic message syntax (CMS) provides data integrity, confidentiality, origin authenticity, and non-repudiation services needed for reliable information exchange and for strong authentication. It also brings together a set of cryptographic key management techniques to support flexible key establishment mechanisms, such as constructive key management, key agreement, key exchange, and password-based encryption. These techniques can be used to prevent fraud, and to protect personally identifiable and other sensitive information. This Recommendation | International Standard supports digital signature, encryption, and signcryption techniques based on the public-key technology defined in the ITU-T X.500 series | ISO/IEC 9594 multipart standard. All of the standardized encoding rules for ASN.1 are supported.

– Z.161 (revised), *Testing and Test Control Notation version 3: TTCN-3 core language*, defines Testing and Test Control Notation 3 (TTCN-3) intended for specification of test suites that are independent of platforms, test methods, protocol layers and protocols. TTCN-3 can be used for the specification of all types of reactive system tests over a variety of communication ports.

– 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. TTCN-3 can be used for the specification of all types of reactive system tests over a variety of communication ports.

– 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. TTCN‑3 can be used for the specification of all types of reactive system tests over a variety of communication ports.

– 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. TTCN‑3 can be used for the specification of all types of reactive system tests over a variety of communication ports.

– Z.161.7 (revised), *Testing and Test Control Notation version 3: TTCN-3 language extensions: object-oriented features*, defines the support for object-oriented features in TTCN-3. TTCN‑3 can be used for the specification of all types of reactive system tests over a variety of communication ports.

– Z.167 (revised), *Testing and Test Control Notation version 3: Using ASN.1 with TTCN-3*, defines a normative way of using Abstract Syntax Notation One (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.

– Z.168 (revised), *Testing and Test Control Notation version 3: The IDL to TTCN-3 mapping*, defines the mapping rules for Common Object Request Broker Architecture (CORBA) Interface Definition Language (IDL) to TTCN-3 (as defined in Recommendation ITU-T Z.161) to enable testing of CORBA-based systems. The principles of mapping CORBA IDL to TTCN-3 can be also used for the mapping of interface specification languages of other object‑/component-based technologies.

– Z.169 (revised), *Testing and Test Control Notation version 3: Using XML schema with TTCN-3*, defines the mapping rules for the world wide web consortium (W3C) schema to Testing and Test Control Notation 3 (TTCN-3) to enable testing of XML-based systems, interfaces, and protocols.

– Z.171 (revised), *Testing and Test Control Notation version 3: Using JSON with TTCN-3*, specifies the rules to define schemas for JSON data structures in TTCN 3, to enable testing of JSON-based systems, interfaces and protocols, and the conversion rules between TTCN-3 and JSON to enable exchanging TTCN 3 data in JSON format between different systems.

– X.Suppl.31, *ITU-T X.660 - Guidelines for using object identifiers for the Internet of things*, provides guidelines on how to use object identifiers (OIDs) to identify objects in the Internet of things (IoT). It includes guidelines on how to structure OIDs, how to implement resolution systems as well as how to establish management procedures based on existing ITU-T Recommendations and international standards.

– XSTP-OID-ORS, *OID Resolution system: Problems, Requirements and Potential solutions,* identifies problems, requirements and potential solutions for OID resolution. The problems include local performance and global resolution of missing OID sub-trees. Technical requirements for possible solutions are also discussed. Finally, potential technical solutions, administrative and operational guidance are provided.

– Z.Imp100 (revised), *Specification and Description Language implementer’s guide – Version 4.0.1*, provides a compilation of reported defects and maintenance issues with their resolutions for the Specification and Description Language ITU-T Recommendations Z.100, Z.101, Z.102, Z.103, Z.104, Z.105, Z.106, Z.107, Z.109, Z.111 and Z.119.

**l) Q12/17, Formal languages for telecommunication software and testing (2017 – 2020)**

Q12/17 develops Recommendations on formal languages (e.g., SDL, MSC, URN) to define the requirements, architecture, and behaviour of telecommunications systems: requirements languages, specification and implementation languages. Q12/17 also develops Recommendations on testing languages (e.g., TTCN-3) as a means to support interoperability and conformance.

In this study period, Q12/17 has developed three new Recommendations, 64 revised Recommendations, and two revised implementer’s guides:

– 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.151 (revised), U*ser Requirements Notation (URN) - Language definition*, defines the User Requirements Notation (URN) intended for the elicitation, analysis, specification, and validation of requirements. URN combines modelling concepts and notations for goals (mainly for non-functional requirements and quality attributes) and scenarios (mainly for operational requirements, functional requirements and performance and architectural reasoning). The goal sub-notation is called Goal-oriented Requirements Language (GRL) and the scenario sub‑notation is called Use Case Map (UCM).

– Z.161 (revised), *Testing and Test Control Notation version 3: TTCN-3 core language*, defines Testing and Test Control Notation 3 (TTCN-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).

– 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 (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 (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 (revised), *Testing and Test Control Notation version 3: TTCN-3 language extensions: Behaviour types*, defines the behaviour types package of TTCN 3.

– Z.161.6 (new and revised), *Testing and Test Control Notation version 3: TTCN-3 language extensions: Advanced matching*, defines the support of advance matching of Testing and Test Control Notation-3 (TTCN-3).

– Z.161.7 (new and revised), *Testing and Test Control Notation version 3: TTCN-3 language extensions: Object-oriented features,* defines the support for object-oriented features in Testing and Test Control Notation 3 (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 TTCN-3 Runtime Interface (TRI) provides the recommended adaptation for timing and communication of a test system to a particular processing platform and the system under test, respectively. This Recommendation defines the interface as a set of operations independent of target language.

The interface is defined to be compatible with Recommendation ITU‑T Z.161. This Recommendation uses the Common Object Request Broker Architecture (CORBA) Interface Definition Language (IDL) to specify the TRI completely. Clauses 6, 7 and 8 of ETSI ES 201 873-5 V4.8.1 specify language mappings of the abstract specification to the target languages Java and ANSI-C. A summary of the IDL-based interface specification is provided in Appendix A of ETSI ES 201 873-5 V4.8.1.

This revision of the Recommendation contains amendments, clarifications, corrigenda and editorial corrections.

– Z.166 (revised), *Testing and Test Control Notation version 3: TTCN*‑*3 control interface (TCI)*, specifies specifies the control interfaces for Testing and Test Control Notation 3 (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 V4.11.1). 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 V4.11.1 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 harmonization of other languages with TTCN-3 is not covered by this Recommendation.

The first revision of the Recommendation contains amendments (conformance and compatibility, requirements and descriptions related to the object type have been moved to this Recommendation from all other ITU-T 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.

This revision of the Recommendation contains amendments, clarifications, 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 Common Object Request Broker Architecture (CORBA) Interface Definition Language (IDL) to TTCN-3 (as defined in Recommendation ITU-T Z.161) to enable testing of CORBA-based systems. The principles of mapping CORBA IDL to TTCN-3 can be also used for the mapping of interface specification languages of other object‑/component-based technologies. The specification of other mappings is outside the scope of this Recommendation. This revision of the Recommendation 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. This revision of Z.170 contains amendments, clarifications, corrigenda and editorial corrections.

– Z.171 (new and revised), *Testing and Test Control Notation version 3: Using JSON with TTCN-3,* specifies the rules to define schemas for JSON data structures in TTCN 3, to enable testing of JSON-based systems, interfaces and protocols, and the conversion rules between TTCN-3 and JSON to enable exchanging TTCN 3 data in JSON format between different systems.

– Z.Imp100 (revised), *Specification and Description Language implementer’s guide – Version 3.0.2*, provides a compilation of reported defects and maintenance issues with their resolutions for the Specification and Description Language ITU-T Recommendations Z.100, Z.101, Z.102, Z.103, Z.104, Z.105, Z.106, Z.107, Z.109, Z.111 and Z.119.

– Z.Imp100 (revised), *Specification and Description Language implementer’s guide – Version 4.0.0*, provides a compilation of reported defects and maintenance issues with their resolutions for the Specification and Description Language ITU-T Recommendations Z.100, Z.101, Z.102, Z.103, Z.104, Z.105, Z.106, Z.107, Z.109, Z.111 and Z.119.

**m) Q13/17, Security aspects for Intelligent Transport System (2017 – 2020) / Intelligent transport system (ITS) security (2021 -)**

Q13/17 was established in Sept 2017 and develops Recommendations on security aspects for Intelligent Transport System (ITS). Included are various types of communications in vehicles, between vehicles and between vehicles and fixed locations

In this study period, Q13/17 has developed six new Recommendations:

– X.1371, *Security threats to connected vehicles*, describes security threats to connected vehicles and vehicle eco-system.

– X.1372, *Security guidelines for Vehicle-to-Everything (V2X) communication*, provides security guidelines for Vehicle-to-Everything (V2X) communication systems. It identifies threats in V2X communications environments and specifies security requirements for V2X communication systems based on the threats. This Recommendation also provides use cases for V2X communication security services.

– X.1373, *Secure software update capability for intelligent transportation system communication devices*, provides secure software update procedures between a software update server and vehicles with appropriate security controls. This Recommendation can be practically utilized by car manufacturers and ITS-related industries as a set of standard capabilities for best practices.

– X.1374, *Security requirements for external interfaces and devices with vehicle access capability*, analyses security threats to connected vehicles in two parts: threats against interfaces which are used to communicate between a vehicle and its external devices, and threats against external devices which communicate with the vehicle. Recommendation ITU-T X.1374 specifies security requirements for such external interfaces and external devices with vehicle access capability in telecommunication network environments to address identified threats depending on types of access interfaces. Interfaces and external devices with vehicle access capability include the remote keyless entry (RKE) system with smart key, diagnostic tools and wireless dongles using on-board diagnostic II (OBD‑II) port, telematics control units with wireless communication devices and so on.

– X.1375, *Guidelines for an intrusion detection system for in-vehicle networks*, establishes guidelines for an intrusion detection system (IDS) for in‑vehicle networks (IVNs). It mainly focuses on how to detect intrusion and malicious activities on IVNs such as those using a controller area network (CAN) that cannot be supported by general IDSs currently deployed on the Internet. Recommendation ITU-T X.1375 includes classifications and analyses of attacks targeting IVNs. It then proposes methodologies and implementation guidelines for detecting intrusions and malicious activities within CAN-based IVNs that cannot be supported by general IDSs.

– X.1376, *Security-related misbehaviour detection mechanism using big data for connected vehicles*, describes a security-related misbehaviour detection mechanism for connected vehicles to help stakeholders to utilize automotive data to improve vehicle security. As connectivity of vehicles increases, the number of vulnerabilities is rising due to the development of complex technology. These vulnerabilities bring more threats to connected vehicles. Analysis of a large amount of automotive data is very useful for assessing security of connected vehicles.

In this study period, Q13/17 held a mini workshop on Cybersecurity Challenges in Automated Driving, Geneva, 26 August 2019.

**n) Q14/17, Security aspects for Distributed Ledger Technologies (2018 - 2020) / Distributed ledger technology (DLT) security (2021 -)**

Q14/17 was established in March 2018 and develops Recommendations on security aspects for Distributed Ledger Technologies (DLT), also known as blockchain. This includes providing comprehensive security solutions for DLT based applications and services.

In this study period, Q14/17 has developed nine new Recommendations:

– X.1400, *Terms and definitions for distributed ledger technology*, contains a baseline set of terms and definitions for distributed ledger technology (DLT). The definitions provide a basic characterization of the term, and where appropriate, a note is included to provide additional clarity.

– X.1401, *Security threats of distributed ledger technology,* identifies possible threats to various functional components of distributed ledger system, such as protocol, network and data. This Recommendation can be considered in the design or implementation of a DLT system as a reference baseline.

– X.1402, Security framework for distributed ledger technology, describes security capabilities that could mitigate the related security threats and specifies a security framework methodology to determine how to use these security capabilities to mitigate security threats for a specific DLT system.

– X.1403, *Security guidelines for using distributed ledger technology for decentralized identity management*. Distributed Ledger Technology and its specific implementations such as Blockchain offer a unique opportunity for utilizing a trust infrastructure and a platform that could be useful in enabling trusted federation for exchanging identity attributes and identity information. This Recommendation provides a telecom-specific privacy and security considerations for using DLT data in identity management.

– X.1404, *Security assurance for distributed ledger technology*, defines three levels of security assurance for the distributed ledger technology (DLT) in order to facilitate design and development of security assurance mechanisms. It further defines ten security assurance components encompassing the security assurance and specifies criteria and guidelines for achieving each of the three levels of a security assurance component. Finally, it also provides a mapping between specific threats and security assurance components and a mapping between specific security capabilities and security assurance components.

– X.1405, *Security threats and requirements for digital payment services based on distributed ledger technology*. Based on analysis of payment services use cases, Recommendation ITU-T X.1405 described a service model, analysed security threats and challenges, then it specified security requirements against identified threats and challenges.

– X.1406, *Security threats to online voting system using distributed ledger technology*, identifies security threats to online voting system using DLT based on telecommunication/ICT infrastructure. It proposes a reference model of online voting system using DLT based on telecommunication/ICT infrastructure and analyses security threats in online voting process described in the models.

– X.1407, *Security requirements for digital integrity proofing service based on distributed ledger technology*, specifies security threats and requirements in digital integrity proofing service based on distributed ledger technology (DLT).

– X.1408, *Security threats and requirements for data access and sharing based on the distributed ledger technology*, specifies a reference model to describe data access and sharing based on the distributed ledger technology (DLT). It identifies entities and their roles and security threats for data access and sharing based on DLT. In addition, security requirements are specified to address these identified security threats.

**o) Q15/17, Security for/by emerging technologies including quantum-based security**

Q15/17 was established in January 2021 and develops Recommendations on Security for/by emerging technologies including quantum-based security. Q15/17 also hosts the SG17 incubation mechanism (TP.inno) which offers controlled agility in studying emerging security areas in order to secure new emerging telecommunication/ICT based services and applications.

In this study period, Q15/17 has developed two new Recommendations and one Corrigenda to Technical report:

– X.1712, *Security requirements and designs for quantum key distribution networks - key management,* specifies security threats and security requirements for key management in quantum key distribution networks (QKDNs), and then it specifies security measures of key management to meet the security requirements.

– X.1770, *Technical Guidelines for Secure Multi-party Computation*, specifies technical guidelines for MPC and provides a technical standard basis for ICT stakeholders to use MPC to protect data in data collaboration and big data analysis scenarios. It also describes applications where MPC can be used for and how as a reference for ICT stakeholders to develop MPC applications.

– Cor.1 to TR.sec-qkd, *Security considerations for quantum key distribution network,* changes relevant expressions regarding to “IT-secure”, changes ‘qubits’ into ‘quantum states’, changes “co-fiber” into “co-propagation” and modify related contents.

## 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 jointly managed by Q11/17 and Q12/17 until 2020 and by Q11/17 after 2021.

### 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-16) 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, ITU-D (SG 1, SG 2, TDAG), ITU-R (SG1,SG5, SG6, WP (4C, 5A, 5D, 6C)), ITU-T FIGI, ITU-T FG-(AI4EE, AI4H, AN, DFC, DLT, DPM, ML5G, NET2030, QIT4N, VM), ITU-T JCA-(IMT2020, IoT and SC&C, MMeS, SDN), ITU-T SCV, ITU-T SGs (2, 3, 5, 9, 11, 12, 13, 15, 16, 20), and ITU-T TSAG.

Concerning SG17 lead study group matters, external liaison statements were treated, received from 3GPP (SA3), BIPM, CEN-CENELEC JTC 19, ETSI ISG (CIM, ETI, F5G, IPE, NIN, QSC, SAI), ETSI SAGE, ETSI TC (CYBER, ITS, MTS), FIDO Alliance, IEEE 802.1, IETF WG TLS, ISO TC 307, ISO/IEC JTC 1/SCs (6, 27/WG 1-5, 29/WG1), MEF, NIST, OASIS, OMA, oneM2M, SAE and W3C.

SG17 sent internal liaison statements to ITU CITS, IPRAHG, ITU-D (SG 1, SG 2, TDAG), ITU‑R SGs (4, 5 (WP (5A, 5D))), ITU-T FIGI, ITU-T FGs (AI4EE, DFC, DLT, NET2030, DPM, QIT4N,VM), ITU-T JCAs (IMT2020, IoT and SC&C, MMeS, SDN), 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), APT ASTAP, BSI, CEN-CENELEC JTC 19, CIS, ETSI (ISG CIM, MEC, QKD, ZSM; SAGE), ETSI TC (CYBER, ITS, MTS)), FIDO Alliance, GSMA (FASG, SIM), ICAO, IEEE Blockchain Initiative, IETF, IRTF, ISO TC (12, 20, 22, 37, 204, 307), ISO/IEC JTC 1/WG9, ISO/IEC JTC 1/SC (6 (WG 10), 7, 27 (WG 1, WG 2, WG 3, WG 4, WG 5), 29, 38, 42), Kantara Initiative, MEF, MITRE, NGMN, NIST, OASIS TC (CTI, OpenC2, Trust Elevation), OIX, oneM2M, ONF, OPIX Foundation, RAISE Forum, SAE, UNECE, UPU, W3C, WIPO, WHO.

In response to WTSA-16 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.

SG17 organized the following workshops:

– [2nd joint ITU/WHO workshop on digital COVID-19 certificate](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2021/1126/Pages/default.aspx)
Virtual, 13:00-18:00 CEST, 26 November 2021

– [Joint ITU/WHO workshop on digital vaccination certificate](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2021/0811/Pages/default.aspx)
Virtual, 13:00-18:00 CEST, 11 August 2021

– "Decentralized identifiers and blockchain" of [BDT](https://www.itu.int/en/ITU-D/Conferences/ET/2021/Pages/Programme.aspx) [Emerging Technology Week 2021](https://www.itu.int/en/ITU-D/Conferences/ET/2021/Pages/Programme.aspx)
Virtual, 14:00-15:00, 08-07-2021

– [SG17 Mini workshop on Cybersecurity Challenges in Automated Driving](https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/mini-workshop_ITS.aspx)
Geneva, 14:30-17:30, 26 August 2019

– [ITU Workshop on Fintech Security](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20190826/Pages/default.aspx)
Geneva, Switzerland, 26 August 2019

– [ITU Workshop on Quantum Information Technology (QIT) for Networks](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Pages/default.aspx)
Shanghai, China, 5-7 June 2019

– [SG17 Mini workshop on Secure Quantum Communications](https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/Secure%20quantum%20communication.aspx)
Geneva, 14:30-17:30, 24 January 2019

– [ITU Workshop on Artificial Intelligence/Machine Learning and Security](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20190121/Pages/default.aspx)
Geneva, Switzerland, 21 Jan 2019

– [ITU Workshop on Advanced Cybersecurity Attacks and Ransomware](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180828/Pages/default.aspx)
Geneva, Switzerland, 28 August 2018

– [ITU Workshop on 5G Security](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180319/Pages/default.aspx)
Geneva, Switzerland, 19 March 2018

– [ITU Workshop on Security Aspects of Intelligent Transport System](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201708/Pages/default.aspx)
Geneva, Switzerland, 28 August 2017

– [ITU Workshop on Security Aspects of Blockchain](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201703/Pages/default.aspx)
Geneva, Switzerland, 21 March 2017

In particular, SG17 plan of work on security considers:

– Implementation of WTSA-16 Resolutions 7, 11, 18, 32, 40, 44, 50, 52, 54, 58, 64, 65, 67, 70, 73, 75, 76 77, 78, 84, 86, 89, 90, 92, 93, 94, 96, 97 and 98;

– Implementation of PP-18 Resolutions 101, 123, 130, 136, 174, 177, 178, 179, 181, 188, 189, 197, 199, 200, and 201.

– Implementation of WTDC-17 Resolutions 23, 30, 34, 45, 47, 54, 63, 67, 69, and 80.

A Study Group 17 action plan in support of PP-14/18, WTSA-16, WTDC-17 Resolutions has been developed and is updated at each meeting of Study Group 17. At its March 2020 SG17 meeting, an editor for these works has been assigned to facilitate work.

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.

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

The 2nd edition of the Technical Report on the successful use of security standards was published. It 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 7th edition of the Security Manual was published 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** |
| --- | --- | --- |
| SG9 | J.1204 | The security framework of a smart TV operating system |
| SG13 | Y.2241  | Service framework to support web objects based ubiquitous self-directed learning |
| SG13 | Y.2774  | Functional Requirements of Deep Packet Inspection for Future Networks |
| SG13 | Y.3051 | The basic principles of trusted environment in ICT infrastructure |
| SG13 | Y.3052 | Overview of trust provisioning for ICT infrastructures and services |
| SG13 | Y.3053  | Framework of trustworthy networking with trust-centric network domains |
| SG13 | Y.3054  | Framework of Trust-based Media Services |
| SG13 | Y.3055 | Framework for trust based personal data management*)* |
| SG13 | Y.3056 | Framework for bootstrapping of devices and applications for open access to trusted services in distributed ecosystems |
| SG13 | Y.3057 | A trust index model for ICT infrastructures and services |
| SG13 | Y.3302  | Functional architecture of software-defined networking |
| SG13 | Y.3514  | Cloud computing - Trusted inter-cloud computing framework and requirements |
| SG13 | Y.3516  | Functional Architecture of inter-cloud computing |
| SG13 | Y.3517  | Cloud computing - Overview of inter-cloud trust management |
| SG13 | Y.3650  | Framework of big data driven networking based on Deep Packet Inspection |
| SG13 | Y.3802 | Quantum key distribution networks - Functional architecture |
| SG13 | Y.3803 | Quantum key distribution networks – Key management*)* |
| SG13 | Y.3804 | Quantum key distribution networks - Control and management |
| SG13 | Y.3805 | Quantum Key Distribution Networks - Software Defined Networking Control |
| SG13 | Y.3806 | Quantum key distribution networks - Requirements for QoS assurance  |
| SG15 | G.873.1 | Optical Transport Network (OTN): Linear protection |
| SG15 | G.873.3  | Optical Transport Network (OTN) - Shared Mesh Protection |
| SG15 | G.8132/ Y.1383 (revised) | MPLS-TP Ring Protection |
| SG15 | G.9978  | Unified high-speed wire-line based home networking transceivers - Secure admission |
| SG16 | H.248.77 | Gateway control protocol: Secure real-time transport protocol (SRTP) package and procedures |
| SG20 | Y.4457 | Architectural framework for providing transportation safety service |
| SG20 | Y.4808  | Digital entity architecture framework to combat counterfeiting in IoT |
| SG20 | Y.4810  | Requirements of data security for the heterogeneous IoT devices |

**Supplements and Appendices agreed**

| **SG** | **Number** | **Title** |
| --- | --- | --- |
| SG13 | Y.3100-series Supplement 44 | Standardization and open source activities related to network softwarization of IMT-2020 |

**Draft Recommendations consented**

|  |  |  |
| --- | --- | --- |
| **SG** | **No.** | **Title** |
| SG13 | Y.2086 (Y.DNI-fr) | Framework and requirements of decentralized trustworthy network infrastructure *(Consented 2021-07-16)* |
| SG13 | Y.3807 (Y.QKDN-QoS-pa) | Quantum Key Distribution networks - QoS parameters*(Consented 2021-12-10)* |
| SG13 | Y.3808 (Y.QKDN-frint) | Framework for integration of quantum key distribution network and secure storage network*(Consented 2021-12-10)* |
| SG13 | Y.3809 (Y.QKDN-BM) | Quantum Key Distribution Networks - Business role-based models*(Consented 2021-12-10)* |

### 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-16) 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** |
| --- | --- | --- |
| SG3SG17 | D.1140X.1261\*\*\* | Policy Framework including principles for digital identity infrastructure  |
| SG2 | E.217rev | Maritime communications - Ship Station identity |
| SG11 | Q.4063 | The framework of testing of identification systems used in IoT |
| SG11 | Q.5052 | Addressing mobile devices with duplicate unique identifier |
| SG15 | L.207  | Passive node elements with automated ID tag detection |
| SG16 | H.273 | Coding-independent code points for video signal type identification |
| SG17 | X.1252rev | Baseline identity management terms and definitions |
| SG17 | X.1403 | Security guidelines for using DLT for decentralized identity management |
| SG20 | Y.4805 | Identifier service requirements for the interoperability of Smart City applications |
| SG20 | Y.4476 | OID-based Resolution framework for transaction of distributed ledger assigned to IoT resources  |
| SG20 | Y.4809 | IoT Identifiers for Intelligent Transport Systems  |
| SG20 | Y.4811 | Reference framework of converged service for identification and authentication for IoT devices in decentralized environment |

**\*\*\*** Dual numbering of D.1140 (SG3) as X.1261 (SG17)

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-16) 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 12/17 have been productive on languages and description techniques for ASN.1, 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 [ASN.1 module database](http://www.itu.int/ITU-T/recommendations/fl.aspx?lang=1) continues to have new additions, enabling implementers to obtain syntax-checked, machine-readable, published ASN.1 specifications. This database contains about 900 modules of more than 200 ITU-T Recommendations and the modules of other SDOs referenced by them.

The Specification and Description Language (SDL‑2010) is used to define systems both as reference models in Recommendations and as implementations. SDL‑2010 grammar is defined in Z.101 to Z.107 and there is a formal definition in Annex F of Z.100. Question 12/17 updated the formal definition. The benefit of this study has been to detect and resolve ambiguities, errors and inconsistencies in the Z.101 to Z.107 texts. A formal definition completely aligned with SDL‑2010 was consented for AAP approval on 5 September 2019. At the same time updated Z.100 to Z.107 texts were consented for AAP approval to remove the ambiguities, errors and inconsistencies. A revised Z.Imp100 was agreed on 5 September 2019 with an empty list changes to Z.100 to Z.107 texts consented for AAP approval and listing the previous texts in force. The net result is a better-defined SDL‑2010 with a consistent formal definition. No further work is currently planned.

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. Three new and 25 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.

### 3.3.4 Joint Coordination Activity on Identity Management (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. JCA-IdM held six meetings during SG17 Aug/Sept 2017, March 2018, Aug/Sept 2018, Aug/Sept 2019, April 2021, and Aug/Sept 2021 meetings to coordinate ITU-T identity management (IdM) work with ITU-T internal groups and relevant external organizations, e.g, Decentralized Identify Foundation, FIDO Alliance, ISO/IEC JTC 1/SC 27/WG 5, ISO TC 307, Kantara Initiative, Mobile Driving Licence, NH-ISAC Identity working group, OASIS, OpenIdD Foundation, Sovrin Fondation, SSI Open Standards and UPU.

### 3.3.5 Study Group 17 Regional Group for Africa (SG17RG-AFR)

SG17 Regional Group for Africa (SG17RG-AFR) created in April 2015 in last study period was carried on in this study period. It held one meeting in this study period as a joint meeting with SG17RG-ARB in 2-3 April 2019.

### 3.3.6 Study Group 17 Regional Group for Arab (SG17RG-ARB)

At SG17 March 2017 meeting, SG17 Regional Group for Arab (SG17RG-ARB) was created. Its first meeting was held in Muscat, Oman in December 2017. Its second meeting was held in Kuwait in October 2018 and third meeting was held in Tunis in 2-3 April 2019. Its third meeting was a joint meeting with SG17RG-AFR.

In all SG17 Regional Group meetings, bridging standardization gap and SG17 tutorials were given by SG17 Counsellor. Participants from countries in the regions held brainstorming discussions on cybersecurity topics and identified topics of their specific interest for further study.

## 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 the 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 1 643 596registrations as of 16 November 2021 (<http://www.oid-info.com/cgi-bin/display?a=count_nodes>) 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).

In particular, X.677, Identification mechanism for unmanned aerial vehicles using object identifiers, was approved to analyse requirements for full life-cycle management and operating identity recognition of unmanned aerial vehicles (UAVs) with security considerations and specifies an identification mechanism for UAVs using object identifiers (OIDs).

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 Bahrain, Benin, Ecuador, Jamaica, and Vietnam.

## 3.5 Bridging the standardization gap

In all SG17 physical meetings in this study period, TSB organized welcome reception and tour of ITU premises for newcomers to SG17. SG17 Chairman organized ‘SG17 Orientation session for newcomers & Newcomer’s discussion with SG17 management’. In Jan 2019, SG17 Counsellor organized ‘SG17 Counsellor’s Clinic’ to answer questions on SG17 working methods from SG17 delegates. In September 2019, TSB organized ‘ITU-T leadership team training’ for SG17 Rapporteurs and Editors.

From March 2017 to September 2018, SG17 regularly organizes a hands-on training session for delegates from developing countries 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.

In this study period, SG17 regularly organized informal (e-)gatherings of delegates from Africa and Arab states respectively during SG17 (e-)meetings to facilitate discussion on future planning of SG17RG-AFR and SG17RG-ARB.

# 4 Observations concerning future work

Study Group 17’s work on security has had continued and remarkable growth throughout this study period – it is a centre of excellence – a core competency in security. Study Group 17 is the Standardization Sector’s lead study group in security. A foundation of security Recommendations/standards has been established, collaboration and coordination 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, expanded, and enhanced, and not fragmented.

Existing and future threats and vulnerabilities affecting security should be addressed to build confidence and security in the use of ICTs, taking into account new services and emerging applications based on telecommunication/ICT networks, by developing Recommendations and technical reports. Security technologies are fundamental elements of protecting an ICT system from the attack or damage to its hardware, software or information, as well as from disruption or misdirection of the services it provides.

New security approaches and measures to adequately address security threats and risks are required. Study Group 17 has a key role to play in development of international standards in the security area.

Security of and for telecommunications and ICT remains an area where security standards will be needed. Managing new emerging threats in telecommunication and ICTs, including network infrastructure, systems, applications and services, is extremely critical. It is understood the imperative for developing implementable standards and guidelines on security that meet the needs of all countries.

Managing new emerging threats in telecommunication and ICTs infrastructure is extremely critical. The work that has been done in Study Group 17 on security (including generic security architecture, framework, requirements, mechanisms, protocols 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 standards development organizations (SDOs). Study Group 17 understands the imperative for developing implementable standards and guidelines on security that meet the needs of all countries.

Strengthening the security framework and protection of personally identifiable information (PII) is a prerequisite for the development of the highly connected Information Society and for building confidence, trust and security among users of Information and Communication Technologies (ICTs). Data used in applications and services is protected by appropriate security technologies and organizational and physical measures. Security of and by telecommunications and ICT remains an area where security standards will be needed. New emerging technologies such as cloud computing (including edge cloud computing, multi cloud computing), smart grid, smart factory, intelligent transportation systems, the 5th generation of cellular network and beyond, software-defined networks, network function virtualization, network slicing, Big Data analytics, Internet of things, distributed ledger technologies, intelligent transport system, and quantum based security need technical and organizational measures to address various threats and risks, protect the PII of citizens, as well as technical and organizational measures to protect children online. New security risk assessment-based approaches and measures to adequately address security threats and risks may be required. Study Group 17 has a key role to play in development of international standards in these areas. The 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 provides a leading role as a coordinator and maintains awareness of other study group’s security activities as well as the work of other SDOs 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 SDOs 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, Fintech, OTT 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 work including decentralized identity based on DLT within ITU and with other SDOs. Its work relating to PKI, ASN.1, and OIDs has been useful across multiple ICT sectors.

New telecommunication/ICT environments, such as Internet of things (IoT), ITS, smart factory, smart cities/communities, and smart grid, need new security requirements utilizing PKI. The original PKI was to secure only online banking. PKI 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 these new environments, major aspects of IoT, smart factory and smart grid security will fail with great impact for the society and daily life of people 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.

To enable security to be effective, new standards will be needed. It has long been recognized by ITU that structured expression tools 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.

# 5 Updates to WTSA Resolution 2 for the 2022-2024 study period

Annex 2 contains the updates to WTSA Resolution 2 proposed by Study Group 17 concerning the title, general areas of study, lead roles, points of guidance, and Recommendations 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 periodas of 7 January 2022 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 January 2022.

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-20 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 7 January 2022 of table generation.

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

| ***Recommendation*** | ***Approval*** | ***Status*** | ***TAP/AAP*** | ***Title (English)*** |
| --- | --- | --- | --- | --- |
| [X.500](http://handle.itu.int/11.1002/1000/14031) | 2019-10-14 | In force | AAP | Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services |
| [X.501](http://handle.itu.int/11.1002/1000/14032) | 2019-10-14 | In force | AAP | Information technology – Open Systems Interconnection – The Directory: Models |
| [X.501 (2019) Amd. 1](http://handle.itu.int/11.1002/1000/14790) | 2021-10-14 | In force | AAP | Information Technology - Open systems Interconnection - The Directory - Models – Amendment 1: Miscellaneous enhancements |
| [X.509](http://handle.itu.int/11.1002/1000/14033) | 2019-10-14 | In force | AAP | Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks |
| [X.509 (2019) Cor. 1](http://handle.itu.int/11.1002/1000/14791) | 2021-10-14 | In force | AAP | Information Technology - Open systems Interconnection - The Directory – Public-key and attribute certificate frameworks : Corrigendum 1 |
| [X.510](http://handle.itu.int/11.1002/1000/14320) | 2020-08-22 | In force | AAP | Information technology - Open Systems Interconnection - The Directory: Protocol specifications for secure operations |
| [X.511](http://handle.itu.int/11.1002/1000/14034) | 2019-10-14 | In force | AAP | Information technology – Open Systems Interconnection – The Directory: Abstract service definition |
| [X.518](http://handle.itu.int/11.1002/1000/14035) | 2019-10-14 | In force | AAP | Information technology – Open Systems Interconnection – The Directory: Procedures for distributed operation |
| [X.519](http://handle.itu.int/11.1002/1000/14036) | 2019-10-14 | In force | AAP | Information technology – Open Systems Interconnection – The Directory: Protocol specifications |
| [X.520](http://handle.itu.int/11.1002/1000/14037) | 2019-10-14 | In force | AAP | Information technology – Open Systems Interconnection – The Directory: Selected attribute types |
| [X.521](http://handle.itu.int/11.1002/1000/14038) | 2019-10-14 | In force | AAP | Information technology – Open Systems Interconnection – The Directory: Selected object classes |
| [X.525](http://handle.itu.int/11.1002/1000/14047) | 2019-10-14 | In force | AAP | Information technology – Open Systems Interconnection – The Directory: Replication |
| [X.676](http://handle.itu.int/11.1002/1000/13712) | 2018-11-29 | In force | AAP | Object identifier-based resolution framework for IoT grouped services |
| [X.677](http://handle.itu.int/11.1002/1000/14039) | 2020-03-08 | In force | AAP | Identification mechanism for unmanned aerial vehicles using object identifiers |
| [X.680 (2015) Cor. 1](http://handle.itu.int/11.1002/1000/13257) | 2017-05-14 | Superseded | AAP |  |
| [X.680 (2015) Cor. 2](http://handle.itu.int/11.1002/1000/13361) | 2017-10-14 | Superseded | AAP |  |
| [X.680 (2015) Cor. 3](http://handle.itu.int/11.1002/1000/13598) | 2018-05-14 | Superseded | AAP |  |
| [X.680 (2015) Amd. 1](http://handle.itu.int/11.1002/1000/13597) | 2018-05-14 | Superseded | AAP | Relaxing IMPORTS clause to allow importation of definitions from new versions of a given module |
| [X.680](http://handle.itu.int/11.1002/1000/14468) | 2021-02-13 | In force | AAP | Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation |
| [X.681 (2015) Cor. 1](http://handle.itu.int/11.1002/1000/13599) | 2018-05-14 | Superseded | AAP |  |
| [X.681](http://handle.itu.int/11.1002/1000/14469) | 2021-02-13 | In force | AAP | Information technology - Abstract Syntax Notation One (ASN.1): Information object specification |
| [X.682 (2015) Cor. 1](http://handle.itu.int/11.1002/1000/13362) | 2017-10-14 | Superseded | AAP |  |
| [X.682 (2015) Cor. 2](http://handle.itu.int/11.1002/1000/13600) | 2018-05-14 | Superseded | AAP |  |
| [X.682](http://handle.itu.int/11.1002/1000/14470) | 2021-02-13 | In force | AAP | Information technology - Abstract Syntax Notation One (ASN.1): Constraint specification |
| [X.683 (2015) Cor. 1](http://handle.itu.int/11.1002/1000/13601) | 2018-05-14 | Superseded | AAP |  |
| [X.683](http://handle.itu.int/11.1002/1000/14471) | 2021-02-13 | In force | AAP | Information technology - Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications |
| [X.690](http://handle.itu.int/11.1002/1000/14472) | 2021-02-13 | 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.691](http://handle.itu.int/11.1002/1000/14473) | 2021-02-13 | In force | AAP | Information technology - ASN.1 encoding rules: Specification of Packed Encoding Rules (PER) |
| [X.692](http://handle.itu.int/11.1002/1000/14474) | 2021-02-13 | In force | AAP | Information technology - ASN.1 encoding rules: Specification of Encoding Control Notation (ECN) |
| [X.693 (2015) Cor. 1](http://handle.itu.int/11.1002/1000/13363) | 2017-10-14 | Superseded | AAP |  |
| [X.693](http://handle.itu.int/11.1002/1000/14475) | 2021-02-13 | In force | AAP | Information technology - ASN.1 encoding rules: XML Encoding Rules (XER) |
| [X.694 (2015) Cor. 1](http://handle.itu.int/11.1002/1000/14040) | 2019-10-14 | Superseded | AAP |  |
| [X.694](http://handle.itu.int/11.1002/1000/14476) | 2021-02-13 | In force | AAP | Information technology - ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1 |
| [X.695](http://handle.itu.int/11.1002/1000/14477) | 2021-02-13 | In force | AAP | Information technology - ASN.1 encoding rules: Registration and application of PER encoding instructions |
| [X.696 (2015) Cor. 1](http://handle.itu.int/11.1002/1000/13258) | 2017-05-14 | Superseded | AAP |  |
| [X.696 (2015) Cor. 2](http://handle.itu.int/11.1002/1000/13364) | 2017-10-14 | Superseded | AAP |  |
| [X.696 (2015) Cor. 3](http://handle.itu.int/11.1002/1000/13602) | 2018-05-14 | Superseded | AAP |  |
| [X.696](http://handle.itu.int/11.1002/1000/14478) | 2021-02-13 | In force | AAP | Information technology - ASN.1 encoding rules: Specification of Octet Encoding Rules (OER) |
| [X.697](http://handle.itu.int/11.1002/1000/13365) | 2017-10-14 | Superseded | AAP | Information technology - ASN.1 encoding rules: Specification of JavaScript Object Notation Encoding Rules (JER) |
| [X.697](http://handle.itu.int/11.1002/1000/14479) | 2021-02-13 | In force | AAP | Information technology - ASN.1 encoding rules: Specification of JavaScript Object Notation Encoding Rules (JER) |
| [X.893 (2007) Cor. 1](http://handle.itu.int/11.1002/1000/14041) | 2019-10-14 | In force | AAP |  |
| [X.894](http://handle.itu.int/11.1002/1000/12848) | 2018-10-14 | In force | AAP | Information technology – Generic applications of ASN.1: Cryptographic message syntax |
| [X.894 (2018) Cor. 1](http://handle.itu.int/11.1002/1000/13871) | 2019-03-16 | In force | AAP |  |
| [X.894 (2018) Cor. 2](http://handle.itu.int/11.1002/1000/14467) | 2021-02-13 | In force | AAP | Generic applications of ASN.1 cryptographic message syntax Technical Corrigendum 2 |
| [X.1011](http://handle.itu.int/11.1002/1000/14793) | 2021-10-29 | In force | AAP | Guidelines for continuous protection of the service access process |
| [X.1040](http://handle.itu.int/11.1002/1000/13366) | 2017-10-14 | In force | AAP | Security reference architecture for lifecycle management of e-commerce business data |
| [X.1041](http://handle.itu.int/11.1002/1000/13603) | 2018-05-14 | In force | AAP | Security framework for voice-over-long-term-evolution (VoLTE) network operation |
| [X.1042](http://handle.itu.int/11.1002/1000/13803) | 2019-01-30 | In force | TAP | Security services using software-defined networking |
| [X.1043](http://handle.itu.int/11.1002/1000/13872) | 2019-03-16 | In force | AAP | Security framework and requirements for service function chaining based on software-defined networking |
| [X.1044](http://handle.itu.int/11.1002/1000/14042) | 2019-10-29 | In force | AAP | Security requirements of network virtualization |
| [X.1045](http://handle.itu.int/11.1002/1000/14043) | 2019-10-29 | In force | AAP | Security service chain architecture for networks and applications |
| [X.1046](http://handle.itu.int/11.1002/1000/14442) | 2020-12-14 | In force | AAP | Framework of software-defined security in software-defined networks/network functions virtualization networks |
| [X.1047](http://handle.itu.int/11.1002/1000/14794) | 2021-10-29 | In force | AAP | Security requirements and architecture for network slice management and orchestration |
| [X.1051 (2016) Cor. 1](http://handle.itu.int/11.1002/1000/13407) | 2017-09-06 | In force | Agreement |  |
| [X.1052](http://handle.itu.int/11.1002/1000/14044) | 2020-10-29 | In force | AAP | Information security management processes for telecommunication organizations |
| [X.1053](http://handle.itu.int/11.1002/1000/13367) | 2017-11-13 | In force | AAP | Code of practice for information security controls based on ITU-T X.1051 for small and medium-sized telecommunication organizations |
| [X.1058](http://handle.itu.int/11.1002/1000/13182) | 2017-03-30 | In force | TAP | Information technology - Security techniques - Code of practice for personally identifiable information protection |
| [X.1059](http://handle.itu.int/11.1002/1000/14045) | 2019-10-29 | In force | AAP | Implementation guidance for telecommunication organizations on risk management of their assets globally accessible in IP-based networks |
| [X.1060](http://handle.itu.int/11.1002/1000/14721) | 2021-06-29 | In force | AAP | Framework for the creation and operation of a cyber defence centre |
| [X.1061](http://handle.itu.int/11.1002/1000/14733) | 2021-08-22 | In force | AAP | Cyber insurance acquisition guidelines |
| [X.1080.0](http://handle.itu.int/11.1002/1000/13193) | 2017-03-30 | In force | TAP | Access control for telebiometrics data protection |
| [X.1080.0 (2017) Cor. 1](http://handle.itu.int/11.1002/1000/13591) | 2018-03-29 | In force | Agreement |  |
| [X.1080.1](http://handle.itu.int/11.1002/1000/13604) | 2018-05-14 | In force | AAP | e-Health and world-wide telemedicines - Generic telecommunication protocol |
| [X.1080.2](http://handle.itu.int/11.1002/1000/14795) | 2021-10-29 | In force | AAP | Biology-to-machine (B2M) protocol |
| [X.1093](http://handle.itu.int/11.1002/1000/13725) | 2018-11-13 | In force | AAP | Telebiometric access control with smart ID cards |
| [X.1094](http://handle.itu.int/11.1002/1000/13873) | 2019-03-16 | In force | AAP | Telebiometric authentication using biosignals |
| [X.1126](http://handle.itu.int/11.1002/1000/13194) | 2017-03-30 | In force | TAP | Guidelines on mitigating the negative effects of infected terminals in mobile networks |
| [X.1127](http://handle.itu.int/11.1002/1000/13259) | 2017-09-06 | In force | TAP | Functional security requirements and architecture for mobile phone anti-theft measures |
| [X.1145](http://handle.itu.int/11.1002/1000/13260) | 2017-05-14 | In force | AAP | Security framework and requirements for open capabilities of telecommunication services |
| [X.1146](http://handle.itu.int/11.1002/1000/13368) | 2017-10-14 | In force | AAP | Secure protection guidelines for value-added services provided by telecommunication operators |
| [X.1147](http://handle.itu.int/11.1002/1000/13726) | 2018-11-13 | In force | AAP | Security requirements and framework for big data analytics in mobile Internet services |
| [X.1148](http://handle.itu.int/11.1002/1000/14249) | 2020-09-03 | In force | TAP | Framework of de-identification process for telecommunication service providers |
| [X.1149](http://handle.itu.int/11.1002/1000/14250) | 2020-05-29 | In force | AAP | Security framework of an open platform for FinTech services |
| [X.1197 (2012) Amd. 1](http://handle.itu.int/11.1002/1000/14046) | 2019-09-05 | In force | Agreement |  |
| [X.1212](http://handle.itu.int/11.1002/1000/13195) | 2017-03-30 | In force | TAP | Design considerations for improved end-user perception of trustworthiness indicators |
| [X.1213](http://handle.itu.int/11.1002/1000/13261) | 2017-09-06 | In force | TAP | Security capability requirements for countering smartphone-based botnets |
| [X.1214](http://handle.itu.int/11.1002/1000/13404) | 2018-03-29 | In force | TAP | Security assessment techniques in telecommunication/information and communication technology networks |
| [X.1215](http://handle.itu.int/11.1002/1000/13849) | 2019-01-30 | In force | TAP | Use cases for structured threat information expression |
| [X.1216](http://handle.itu.int/11.1002/1000/14259) | 2020-09-03 | In force | TAP | Requirements for collection and preservation of cybersecurity incident evidence |
| [X.1217](http://handle.itu.int/11.1002/1000/14443) | 2021-01-07 | In force | TAP | Guidelines for applying threat intelligence in telecommunication network operation |
| [X.1218](http://handle.itu.int/11.1002/1000/14444) | 2020-10-29 | In force | AAP | Requirements and guidelines for dynamic malware analysis in a sandbox environment |
| [X.1232](http://handle.itu.int/11.1002/1000/14085) | 2019-10-29 | In force | AAP | Technical framework for countering advertising spam in user-generated information |
| [X.1233](http://handle.itu.int/11.1002/1000/14773) | 2021-09-03 | In force | TAP | Guidelines for countering spam over instant messaging |
| X.1234 | 2022-01-07 | In force | TAP | Guideline for countering multimedia messaging service (MMS) spam |
| X.1235 | 2022-01-07 | In force | TAP | Technologies in countering website spoofing for telecommunication organizations |
| [X.1248](http://handle.itu.int/11.1002/1000/13262) | 2017-09-06 | In force | TAP | Technical requirements for countering instant messaging spam |
| [X.1249](http://handle.itu.int/11.1002/1000/13605) | 2019-01-30 | In force | TAP | Technical framework for countering mobile in-application advertising spam |
| [X.1252](http://handle.itu.int/11.1002/1000/14642) | 2021-04-30 | In force | TAP | Baseline identity management terms and definitions |
| [X.1254](http://handle.itu.int/11.1002/1000/14260) | 2020-09-03 | In force | TAP | Entity authentication assurance framework |
| [X.1276](http://handle.itu.int/11.1002/1000/13606) | 2018-05-14 | In force | AAP | Authentication step-up protocol and metadata Version 1.0 |
| [X.1277](http://handle.itu.int/11.1002/1000/13727) | 2018-11-29 | In force | AAP | Universal authentication framework |
| [X.1278](http://handle.itu.int/11.1002/1000/13728) | 2018-11-29 | In force | AAP | Client to authenticator protocol/Universal 2-factor framework |
| [X.1279](http://handle.itu.int/11.1002/1000/14261) | 2020-09-03 | In force | TAP | Framework of enhanced authentication using telebiometrics with anti-spoofing detection mechanisms |
| [X.1331](http://handle.itu.int/11.1002/1000/13405) | 2018-03-29 | In force | TAP | Security guidelines for home area network (HAN) devices in smart grid systems |
| [X.1332](http://handle.itu.int/11.1002/1000/14086) | 2020-03-26 | In force | TAP | Security guidelines for smart metering services in smart grids |
| X.1333 | 2022-01-07 | In force | TAP | Security guidelines for use of remote access tools in Internet-connected control systems |
| [X.1361](http://handle.itu.int/11.1002/1000/13607) | 2018-09-07 | In force | TAP | Security framework for the Internet of things based on the gateway model |
| [X.1362](http://handle.itu.int/11.1002/1000/13196) | 2017-03-30 | In force | TAP | Simple encryption procedure for Internet of things (IoT) environments |
| [X.1363](http://handle.itu.int/11.1002/1000/14087) | 2020-05-29 | In force | TAP | Technical framework of personally identifiable information handling system in Internet of things environment |
| [X.1364](http://handle.itu.int/11.1002/1000/14088) | 2020-03-26 | In force | TAP | Security requirements and framework for narrowband Internet of things |
| [X.1365](http://handle.itu.int/11.1002/1000/14089) | 2020-03-26 | In force | TAP | Security methodology for the use of identity-based cryptography in support of Internet of things (IoT) services over telecommunication networks |
| [X.1366](http://handle.itu.int/11.1002/1000/14262) | 2020-09-03 | In force | TAP | Aggregate message authentication schemes for Internet of things environment |
| [X.1367](http://handle.itu.int/11.1002/1000/14263) | 2020-09-03 | In force | TAP | Standard format for Internet of things error logs for security incident operations |
| [X.1368](http://handle.itu.int/11.1002/1000/14445) | 2021-01-07 | In force | TAP | Secure firmware or software update for Internet of things devices |
| X.1369 | 2022-01-07 | In force | TAP | Security Requirements for IoT Service Platform |
| [X.1371](http://handle.itu.int/11.1002/1000/14090) | 2020-05-29 | In force | TAP | Security threats to connected vehicles |
| [X.1372](http://handle.itu.int/11.1002/1000/14091) | 2020-03-26 | In force | TAP | Security guidelines for vehicle-to-everything (V2X) communication |
| [X.1373](http://handle.itu.int/11.1002/1000/13197) | 2017-03-30 | In force | TAP | Secure software update capability for intelligent transportation system communication devices |
| [X.1374](http://handle.itu.int/11.1002/1000/14446) | 2020-10-29 | In force | AAP | Security requirements for external interfaces and devices with vehicle access capability |
| [X.1375](http://handle.itu.int/11.1002/1000/14447) | 2020-10-29 | In force | AAP | Guidelines for an intrusion detection system for in-vehicle networks |
| [X.1376](http://handle.itu.int/11.1002/1000/14448) | 2021-01-07 | In force | TAP | Security-related misbehaviour detection mechanism using big data for connected vehicles |
| [X.1400](http://handle.itu.int/11.1002/1000/14449) | 2020-10-29 | In force | AAP | Terms and definitions for distributed ledger technology |
| [X.1401](http://handle.itu.int/11.1002/1000/14092) | 2019-11-29 | In force | AAP | Security threats of distributed ledger technology |
| [X.1402](http://handle.itu.int/11.1002/1000/14251) | 2020-07-22 | In force | AAP | Security framework for distributed ledger technology |
| [X.1403](http://handle.itu.int/11.1002/1000/14264) | 2020-09-03 | In force | TAP | Security guidelines for using distributed ledger technology for decentralized identity management |
| [X.1404](http://handle.itu.int/11.1002/1000/14450) | 2020-10-29 | In force | AAP | Security assurance for distributed ledger technology |
| [X.1405](http://handle.itu.int/11.1002/1000/14722) | 2021-06-29 | In force | AAP | Security threats and requirements for digital payment services based on distributed ledger technology |
| [X.1406](http://handle.itu.int/11.1002/1000/14734) | 2021-07-14 | In force | AAP | Security threats to online voting systems using distributed ledger technology |
| X.1407 | 2022-01-07 | In force | TAP | Security requirements for digital integrity proofing service based on distributed ledger technology |
| [X.1408](http://handle.itu.int/11.1002/1000/14801) | 2021-10-29 | In force | AAP | Security threats and requirements for data access and sharing based on the distributed ledger technology |
| [X.1450](http://handle.itu.int/11.1002/1000/13729) | 2018-10-14 | In force | AAP | Guidelines on hybrid authentication and key management mechanisms in the client-server model |
| [X.1451](http://handle.itu.int/11.1002/1000/14252) | 2020-05-29 | In force | AAP | Risk identification to optimize authentication |
| [X.1452](http://handle.itu.int/11.1002/1000/14451) | 2020-10-29 | In force | AAP | Guidelines for security services provided by operators |
| X.1453 | 2022-01-07 | In force | TAP | Security threats and requirements for video management systems |
| [X.1470](http://handle.itu.int/11.1002/1000/14803) | 2021-11-13 | In force | AAP | Security Guidelines of Web-based Online Customer Service |
| [X.1500 (2011) Amd. 11](http://handle.itu.int/11.1002/1000/13263) | 2017-03-30 | Superseded | Agreement | Revised structured cybersecurity information exchange techniques |
| [X.1500 (2011) Amd. 12](http://handle.itu.int/11.1002/1000/13590) | 2018-03-29 | In force | Agreement | Revised structured cybersecurity information exchange techniques |
| [X.1541](http://handle.itu.int/11.1002/1000/13264) | 2017-09-06 | In force | TAP | Incident object description exchange format version 2 |
| [X.1550](http://handle.itu.int/11.1002/1000/13198) | 2017-03-30 | In force | TAP | Access control models for incident exchange networks |
| [X.1603](http://handle.itu.int/11.1002/1000/13406) | 2018-03-29 | In force | TAP | Data security requirements for the monitoring service of cloud computing |
| [X.1604](http://handle.itu.int/11.1002/1000/14093) | 2020-03-26 | In force | TAP | Security requirements of Network as a Service (NaaS) in cloud computing |
| [X.1605](http://handle.itu.int/11.1002/1000/14094) | 2020-03-26 | In force | TAP | Security requirements of public Infrastructure as a Service (IaaS) in cloud computing |
| [X.1606](http://handle.itu.int/11.1002/1000/14265) | 2020-09-03 | In force | TAP | Security requirements for communications as a service application environments |
| X.1643 | 2022-01-07 | In force | TAP | Security requirements and guidelines of virtualization container in cloud computing environment |
| [X.1702](http://handle.itu.int/11.1002/1000/14095) | 2019-11-13 | In force | AAP | Quantum noise random number generator architecture |
| [X.1710](http://handle.itu.int/11.1002/1000/14452) | 2020-10-29 | In force | AAP | Security framework for quantum key distribution networks |
| [X.1712](http://handle.itu.int/11.1002/1000/14805) | 2021-10-29 | In force | AAP | Security requirements and measures for quantum key distribution networks – key management |
| [X.1714](http://handle.itu.int/11.1002/1000/14453) | 2020-10-29 | In force | AAP | Key combination and confidential key supply for quantum key distribution networks |
| [X.1750](http://handle.itu.int/11.1002/1000/14266) | 2020-09-03 | In force | TAP | Guidelines on security of big data as a service for big data service providers |
| [X.1751](http://handle.itu.int/11.1002/1000/14267) | 2020-09-03 | In force | TAP | Security guidelines for big data lifecycle management by telecommunication operators |
| X.1752 | 2022-01-07 | In force | TAP | Security guidelines for big data infrastructure and platform |
| [X.1770](http://handle.itu.int/11.1002/1000/14807) | 2021-10-29 | In force | AAP | Technical guidelines for secure multi-party computation |
| [X.1811](http://handle.itu.int/11.1002/1000/14454) | 2021-04-30 | In force | TAP | Security guidelines for applying quantum-safe algorithms in IMT-2020 systems |
| [Z.100 Annex F1](http://handle.itu.int/11.1002/1000/13732) | 2018-11-13 | Superseded | AAP | Specification and Description Language - Overview of SDL-2010 |
| [Z.100 Annex F2](http://handle.itu.int/11.1002/1000/13733) | 2018-11-13 | Superseded | AAP | Specification and Description Language - Overview of SDL-2010 |
| [Z.100 Annex F3](http://handle.itu.int/11.1002/1000/13734) | 2018-11-13 | Superseded | AAP | Specification and Description Language - Overview of SDL-2010 |
| [Z.100](http://handle.itu.int/11.1002/1000/14048) | 2019-10-14 | Superseded | AAP | Specification and Description Language - Overview of SDL-2010 |
| [Z.100 Annex F2](http://handle.itu.int/11.1002/1000/14050) | 2019-10-14 | Superseded | AAP | Specification and Description Language - Overview of SDL-2010 - SDL-2010 formal definition: Static semantics |
| [Z.100 Annex F3](http://handle.itu.int/11.1002/1000/14051) | 2019-10-14 | Superseded | AAP | Specification and Description Language - Overview of SDL-2010 - SDL-2010 formal definition: Dynamic semantics |
| [Z.100](http://handle.itu.int/11.1002/1000/14670) | 2021-06-13 | In force | AAP | Specification and Description Language - Overview of SDL-2010 |
| [Z.100 Annex F1](http://handle.itu.int/11.1002/1000/14049) | 2019-10-14 | In force | AAP | Specification and Description Language - Overview of SDL-2010 - SDL formal definition: General overview |
| [Z.100 Annex F2](http://handle.itu.int/11.1002/1000/14702) | 2021-06-13 | In force | AAP | Specification and Description Language - Overview of SDL-2010 - SDL formal definition: Static semantics |
| [Z.100 Annex F3](http://handle.itu.int/11.1002/1000/14703) | 2021-06-13 | In force | AAP | Specification and Description Language - Overview of SDL-2010 - SDL formal definition: Dynamic semantics |
| [Z.101](http://handle.itu.int/11.1002/1000/14052) | 2019-10-14 | Superseded | AAP | Specification and Description Language - Basic SDL-2010 |
| [Z.101](http://handle.itu.int/11.1002/1000/14671) | 2021-06-13 | In force | AAP | Specification and Description Language - Basic SDL-2010 |
| [Z.102](http://handle.itu.int/11.1002/1000/14053) | 2019-10-14 | Superseded | AAP | Specification and Description Language - Comprehensive SDL-2010 |
| [Z.102](http://handle.itu.int/11.1002/1000/14672) | 2021-06-13 | In force | AAP | Specification and Description Language - Comprehensive SDL-2010 |
| [Z.103](http://handle.itu.int/11.1002/1000/14054) | 2019-10-14 | Superseded | AAP | Specification and Description Language - Shorthand notation and annotation in SDL-2010 |
| [Z.103](http://handle.itu.int/11.1002/1000/14673) | 2021-06-13 | In force | AAP | Specification and Description Language - Shorthand notation and annotation in SDL-2010 |
| [Z.104](http://handle.itu.int/11.1002/1000/14055) | 2019-10-14 | Superseded | AAP | Specification and Description Language - Data and action language in SDL-2010 |
| [Z.104](http://handle.itu.int/11.1002/1000/14674) | 2021-06-13 | In force | AAP | Specification and Description Language - Data and action language in SDL-2010 |
| [Z.105](http://handle.itu.int/11.1002/1000/14056) | 2019-10-14 | Superseded | AAP | Specification and Description Language - SDL-2010 combined with ASN.1 modules |
| [Z.105](http://handle.itu.int/11.1002/1000/14675) | 2021-06-13 | In force | AAP | Specification and Description Language - SDL-2010 combined with ASN.1 modules |
| [Z.106](http://handle.itu.int/11.1002/1000/14057) | 2019-10-14 | Superseded | AAP | Specification and Description Language - Common interchange format for SDL-2010 |
| [Z.106](http://handle.itu.int/11.1002/1000/14676) | 2021-06-13 | In force | AAP | Specification and Description Language - Common interchange format for SDL-2010 |
| [Z.107](http://handle.itu.int/11.1002/1000/14058) | 2019-10-14 | Superseded | AAP | Specification and Description Language - Object-oriented data in SDL-2010 |
| [Z.107](http://handle.itu.int/11.1002/1000/14677) | 2021-06-13 | In force | AAP | Specification and Description Language - Object-oriented data in SDL-2010 |
| [Z.151](http://handle.itu.int/11.1002/1000/13711) | 2018-10-14 | In force | AAP | User Requirements Notation (URN) - Language definition |
| [Z.161](http://handle.itu.int/11.1002/1000/13369) | 2017-10-14 | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 core language |
| [Z.161](http://handle.itu.int/11.1002/1000/13703) | 2018-10-14 | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 core language |
| [Z.161](http://handle.itu.int/11.1002/1000/14059) | 2019-10-14 | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 core language |
| [Z.161](http://handle.itu.int/11.1002/1000/14480) | 2020-10-29 | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 core language |
| [Z.161](http://handle.itu.int/11.1002/1000/14781) | 2021-10-14 | In force | AAP | Testing and Test Control Notation version 3: TTCN-3 core language |
| [Z.161.1](http://handle.itu.int/11.1002/1000/13370) | 2017-10-14 | In force | AAP | Testing and Test Control Notation version 3: TTCN-3 language extensions: Support of interfaces with continuous signals |
| [Z.161.2](http://handle.itu.int/11.1002/1000/13371) | 2017-10-14 | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 language extensions: Configuration and deployment support |
| [Z.161.2](http://handle.itu.int/11.1002/1000/13704) | 2018-10-14 | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 language extensions: Configuration and deployment support |
| [Z.161.2](http://handle.itu.int/11.1002/1000/14060) | 2019-10-14 | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 language extensions: Configuration and deployment support |
| [Z.161.2](http://handle.itu.int/11.1002/1000/14782) | 2021-10-14 | In force | AAP | Testing and Test Control Notation version 3: TTCN-3 language extensions: Configuration and deployment support |
| [Z.161.3](http://handle.itu.int/11.1002/1000/13372) | 2017-10-14 | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 language extensions: Advanced parameterization |
| [Z.161.3](http://handle.itu.int/11.1002/1000/14481) | 2020-10-29 | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 language extensions: Advanced parameterization |
| [Z.161.3](http://handle.itu.int/11.1002/1000/14783) | 2021-10-14 | In force | AAP | Testing and Test Control Notation version 3: TTCN-3 language extensions: Advanced parameterization |
| [Z.161.4](http://handle.itu.int/11.1002/1000/13373) | 2017-10-14 | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 language extensions: Behaviour types |
| [Z.161.4](http://handle.itu.int/11.1002/1000/13705) | 2018-10-14 | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 language extensions: Behaviour types |
| [Z.161.4](http://handle.itu.int/11.1002/1000/14482) | 2020-10-29 | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 language extensions: Behaviour types |
| [Z.161.4](http://handle.itu.int/11.1002/1000/14784) | 2021-10-14 | In force | AAP | Testing and Test Control Notation version 3: TTCN-3 language extensions: Behaviour types |
| [Z.161.6](http://handle.itu.int/11.1002/1000/13374) | 2017-10-14 | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 language extensions: Advanced matching |
| [Z.161.6](http://handle.itu.int/11.1002/1000/13706) | 2018-10-14 | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 language extensions: Advanced matching |
| [Z.161.6](http://handle.itu.int/11.1002/1000/14061) | 2019-10-14 | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 language extensions: Advanced matching |
| [Z.161.6](http://handle.itu.int/11.1002/1000/14483) | 2020-10-29 | In force | AAP | Testing and Test Control Notation version 3: TTCN-3 language extensions: Advanced matching |
| [Z.161.7](http://handle.itu.int/11.1002/1000/14062) | 2019-10-14 | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 language extensions: Object-oriented features |
| [Z.161.7](http://handle.itu.int/11.1002/1000/14484) | 2020-10-29 | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 Language extensions: Object-oriented features |
| [Z.161.7](http://handle.itu.int/11.1002/1000/14785) | 2021-10-14 | In force | AAP | Testing and Test Control Notation version 3: TTCN-3 language extensions: Object-oriented features |
| [Z.164](http://handle.itu.int/11.1002/1000/13375) | 2017-10-14 | In force | AAP | Testing and Test Control Notation version 3: TTCN-3 operational semantics |
| [Z.165](http://handle.itu.int/11.1002/1000/13376) | 2017-10-14 | In force | AAP | Testing and Test Control Notation version 3: TTCN-3 runtime interface (TRI) |
| [Z.165.1](http://handle.itu.int/11.1002/1000/14485) | 2020-10-29 | In force | AAP | Testing and Test Control Notation version 3: TTCN-3 extension package: Extended TRI |
| [Z.166](http://handle.itu.int/11.1002/1000/13377) | 2017-10-14 | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 control interface (TCI) |
| [Z.166](http://handle.itu.int/11.1002/1000/13707) | 2018-10-14 | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 control interface (TCI) |
| [Z.166](http://handle.itu.int/11.1002/1000/14063) | 2019-10-14 | Superseded | AAP | Testing and Test Control Notation version 3: TTCN-3 control interface (TCI) |
| [Z.166](http://handle.itu.int/11.1002/1000/14486) | 2020-10-29 | In force | AAP | Testing and Test Control Notation version 3: TTCN-3 control interface (TCI) |
| [Z.167](http://handle.itu.int/11.1002/1000/13378) | 2017-10-14 | Superseded | AAP | Testing and Test Control Notation version 3: Using ASN.1 with TTCN-3 |
| [Z.167](http://handle.itu.int/11.1002/1000/13708) | 2018-10-14 | Superseded | AAP | Testing and Test Control Notation version 3: Using ASN.1 with TTCN-3 |
| [Z.167](http://handle.itu.int/11.1002/1000/14487) | 2020-10-29 | Superseded | AAP | Testing and Test Control Notation version 3: Using ASN.1 with TTCN-3 |
| [Z.167](http://handle.itu.int/11.1002/1000/14786) | 2021-10-14 | In force | AAP | Testing and Test Control Notation version 3: Using ASN.1 with TTCN-3 |
| [Z.168](http://handle.itu.int/11.1002/1000/13379) | 2017-10-14 | Superseded | AAP | Testing and Test Control Notation version 3: The IDL to TTCN-3 mapping |
| [Z.168](http://handle.itu.int/11.1002/1000/14787) | 2021-10-14 | In force | AAP | Testing and Test Control Notation version 3: The IDL to TTCN-3 mapping |
| [Z.169](http://handle.itu.int/11.1002/1000/13380) | 2017-10-14 | Superseded | AAP | Testing and Test Control Notation version 3: Using XML schema with TTCN-3 |
| [Z.169](http://handle.itu.int/11.1002/1000/13709) | 2018-10-14 | Superseded | AAP | Testing and Test Control Notation version 3: Using XML schema with TTCN-3 |
| [Z.169](http://handle.itu.int/11.1002/1000/14064) | 2019-10-14 | Superseded | AAP | Testing and Test Control Notation version 3: Using XML schema with TTCN-3 |
| [Z.169](http://handle.itu.int/11.1002/1000/14488) | 2020-10-29 | Superseded | AAP | Testing and Test Control Notation version 3: Using XML schema with TTCN-3 |
| [Z.169](http://handle.itu.int/11.1002/1000/14788) | 2021-10-14 | In force | AAP | Testing and Test Control Notation version 3: Using XML schema with TTCN-3 |
| [Z.170](http://handle.itu.int/11.1002/1000/13381) | 2017-10-14 | In force | AAP | Testing and Test Control Notation version 3: TTCN-3 documentation comment specification |
| [Z.171](http://handle.itu.int/11.1002/1000/13382) | 2017-10-14 | Superseded | AAP | Testing and Test Control Notation version 3: Using JSON with TTCN-3 |
| [Z.171](http://handle.itu.int/11.1002/1000/13710) | 2018-10-14 | Superseded | AAP | Testing and Test Control Notation version 3: Using JSON with TTCN-3 |
| [Z.171](http://handle.itu.int/11.1002/1000/14789) | 2021-10-14 | In force | AAP | Testing and Test Control Notation version 3: Using JSON with TTCN-3 |

**TABLE 8
Study Group 17 – Recommendations consented/determined but not yet approved**

| **Recommendation** | **Consent/ Determination** | **TAP/ AAP** | **Title** |
| --- | --- | --- | --- |
| X.672 | 2021-09-03 | AAP | Object identifier resolution system |
| Amendment 1 to X.1246 | 2021-09-03 | TAP | Technologies involved in countering voice spam in telecommunication organizations |
| Amendment 1 to X.1247 | 2021-09-03 | TAP | Technical framework for countering mobile messaging spam |
| Corrigendum to X.1712 | 2022-01-07 | AAP | Security requirements and measures for QKD networks - key management |
| X.1812 (X.5Gsec-t) | 2021-09-03 | TAP | Security framework based on trust relationship for IMT-2020 ecosystem |

**TABLE 9
Study Group 17 – Recommendations deleted during study period**

| **Recommendation** | **Last version** | **Withdrawal date** | **Title** |
| --- | --- | --- | --- |
| None |  |  |  |

**TABLE 10
Study Group 17 – Recommendations submitted to WTSA-20**

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

**TABLE 11
Study Group 17 – Supplements**

| ***Recommendation*** | ***Approval*** | ***Status*** | ***Title (English)*** |
| --- | --- | --- | --- |
| [X Suppl. 13](http://handle.itu.int/11.1002/1000/13730) | 2018-09-07 | In force | ITU-T X.1051 – Supplement on information security management users' guide for Recommendation ITU-T X.1051 |
| [X Suppl. 26 (2016) Cor. 1](http://handle.itu.int/11.1002/1000/13592) | 2018-03-29 | In force |  |
| [X Suppl. 29](http://handle.itu.int/11.1002/1000/13409) | 2017-09-06 | In force | ITU-T X.1242 – Supplement on guidelines on countermeasures against short message service phishing and smishing attacks  |
| [X Suppl. 30](http://handle.itu.int/11.1002/1000/13410) | 2017-09-06 | In force | ITU-T X.805 – Supplement on security guidelines for mobile virtual network operators  |
| [X Suppl. 31](http://handle.itu.int/11.1002/1000/13411) | 2017-09-06 | In force | ITU-T X.660 – Supplement on guidelines for using object identifiers for the Internet of things |
| [X Suppl. 32](http://handle.itu.int/11.1002/1000/13593) | 2018-03-29 | In force | ITU-T X.1058 - Supplement on code of practice for personally identifiable information (PII) protection for telecommunication organizations  |
| [X Suppl. 33](http://handle.itu.int/11.1002/1000/13731) | 2018-09-07 | In force | ITU-T X.1231 - Supplement on technical framework for countering telephone service scams |
| [X Suppl. 34](http://handle.itu.int/11.1002/1000/13869) | 2019-01-30 | In force | ITU-T X.1051 – Supplement on code of practice for information security controls for telecommunication organizations |
| [X Suppl. 35](http://handle.itu.int/11.1002/1000/14066) | 2019-09-05 | In force | ITU-T X.1254 – Supplement on use cases of entity authentication assurance (EAA) framework |
| [X Suppl. 36](http://handle.itu.int/11.1002/1000/14809) | 2021-09-03 | In force | ITU-T X.1051 – Supplement on critical security controls for telecommunication organizations information and network security management |

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

| ***Designation*** | ***Date*** | ***Title*** | ***Type of publication*** |
| --- | --- | --- | --- |
| [TP.inno](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15153) | 2020-09-03 | Description of the incubation mechanism and ways to improve it | Technical paper |
| [TP.sgstruct](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15154) | 2020-09-03 | Strategic approaches to the transformation of security studies | Technical paper |
| [TR.ors](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15256) | 2020-03-26 | OID Resolution system: Problems, Requirements and Potential solutions | Technical report |
| [TR.sec-manual](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14367) | 2020-09-03 | Security in telecommunications and information technology (7th edition) | Technical report |
| [TR.sec-qkd](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14825) | 2020-03-26 | Security considerations for quantum key distribution network | Technical report |
| [TR.Suss](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14370) | 2020-09-03 | Successful use of security standards (2nd edition) | Technical report |
| [TR.usm](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15241) | 2020-09-03 | Unified Security Model (USM) - a neutral integrated system approach to Cybersecurity | Technical report |
| [TR.XAASL](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16769) | 2021-09-03 | Technical Report: Framework for Security Standardization for Virtualized Services | Technical report |
| [XSTR-SEC-QKD Cor.1](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16969) | 2021-04-30 | Security considerations for quantum key distribution network - Corrigendum 1 | Technical report |
| [Z.Imp100](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16983) | 2021-04-30 | Z.100 Specification and Description Language implementer's guide - Version 4.0.1 | Implementer's guide |
| [Z.Imp100](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14424) | 2018-09-07 | Z.100 Specification and Description Language implementer's guide - Version 3.0.2 | Implementer's guide |
| [Z.Imp100rev](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14816) | 2019-09-05 | Z.100 Specification and Description Language implementer's guide - Version 4.0.0 | Implementer's guide |

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

| **Recommendation** | **Consent / Determination** | **TAP / AAP** | **Title** |
| --- | --- | --- | --- |
|  None |  |  |  |

ANNEX 2

SG17 Proposed Revisions to WTSA Resolution 2

Annex A

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).

Providing security by ICTs and ensuring security for ICTs are both major study areas for Study Group 17. This includes studies relating to cybersecurity, managed security services, endpoint detection and response, security management, countering spam and identity management. It also includes security architecture and framework, quantum based security, distributed ledger technology (DLT) security, intelligent transport system security, security aspects related to AI, and security of networks, applications and services such as Internet of things (IoT) and smart cities, various kinds of networks including IMT2020/5G and beyond, smart grid, industrial control system (ICS), supply chain, smartphone, software‑defined networking (SDN), network function virtualization (NFV), Internet protocol television (IPTV), web services, over-the-top (OTT), social network, cloud computing, big data analytics, digital financial system and telebiometrics.

Building confidence and security in the use of ICTs also includes protecting personally identifiable information (PII) such as technical and operational aspects of data protection with respect to ensuring confidentiality, integrity, and availability of PII.

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 test specification languages in support of 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
Lead study group on languages and description techniques

Annex B
(to WTSA Resolution 2)

Points of guidance to study groups for the development
of the post-2020 work programme

ITU‑T Study Group 17

ITU‑T Study Group 17 is responsible for developing key technical Recommendations in supporting building confidence and security in the use of information and communication technologies (ICT).

To this end this includes studies relating to security, including cybersecurity, countering spam and identity management. It also includes security architecture and framework, security management, and security of networks, applications and services such as the Internet of things (IoT), intelligent transport system, secure application services, social network, cloud computing, distributed ledger technology, 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.

ITU-T Study Group 17’s role is to provide technical solutions for addressing security for ICTs and ensuring security by ICTs. Especially, studies on security for new emerging areas, such as security for IMT2020/5G and beyond, Internet of Things (IoT), smart cities, distributed ledger technologies (DLT), Big data analytics, intelligent transport system, security aspects related to AI, and Quantum related technologies, are focused. Its study areas also include the management of personally identifiable information (PII) such as technical and operational aspects of data protection with respect to ensuring confidentiality, integrity, and availability of PII.

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 such as technical and operational aspects of data protection; and countering spam by technical means.

Study Group 17 provides overall coordination of security work in ITU‑T in its capacity as lead study group on security, on identity management, and on languages and description techniques.

In addition, Study Group 17 is responsible for developing the core Recommendations on security for distributed ledger technologies, security for intelligent transport system, security aspects of applications and services in the areas of IPTV, various kinds of networks including IMT2020/5G and beyond, smart grid, industrial control system (ICS), supply chains, IoT and smart cities, SDN, NFV, social network, cloud computing, big data analytics, smartphone, digital 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 these threats; 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, which includes languages such as ASN.1, SDL, MSC, URN and TTCN-3.

Study Group 17 coordinates security work across all study groups in ITU-T. This work 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, Study Group 16, and Study Group 20.

Study Group 17 will work on relevant identity management aspects in collaboration with Study Group 20 and Study Group 2, as per the mandate of each study group.

Annex C
(to WTSA Resolution 2)

List of Recommendations under the responsibility of the respective
study groups and TSAG in the 2021-2024 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, 3, 11, 13, 15 and 16

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

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