|  |  |  |
| --- | --- | --- |
| ITU logo | INTERNATIONAL TELECOMMUNICATION UNION**TELECOMMUNICATION STANDARDIZATION SECTOR**STUDY PERIOD 2017-2020 | TSAG-TD806 |
| **TSAG** |
| **Original: English** |
| **Question(s):** | N/A | E-Meeting, 21-25 September 2020 |
| **TD(Ref.:** [SG17-LS260](http://handle.itu.int/11.1002/ls/sp16-sg17-oLS-00260.docx)) |
| **Source:** | ITU-T Study Group 17 |
| **Title:** | LS on SG17 lead study group reports [from ITU-T SG17] |
| **Purpose:** | Information |
| **LIAISON STATEMENT** |
| **For action to:** | - |
| **For comment to:** | - |
| **For information to:** | TSAG |
| **Approval:** | ITU-T Study Group 17 meeting (Virtual, 3 September 2020) |
| **Deadline:** | N/A |
| **Contact:** | Heung Youl YoumITU-T SG17 chairman | Tel: +82 41 530 1328E-mail: hyyoum@sch.ac.kr |
| **Contact:** | Mohamed ElhajRapporteur of Q1/17 | E-mail: mohamed.elhaj@tpra.gov.sd |
| **Contact:** | Abbie BarbirRapporteur of Q10/17 | Tel: +1 613-697-0865E-mail: abarbir@live.ca |
| **Contact:** | Jean Paul LemaireRapporteur of Q11/17 | Tel: +33 672 197 819E-mail: jean-paul.lemaire@univ-paris-diderot.fr |
| **Contact:** | Dieter HogrefeRapporteur of Q12/17 | Tel: +49 551 39172001Fax: +49 551 391 4403E-mail: hogrefe@informatik.uni-goettingen.de |

A new liaison statement has been received from SG17.

This liaison statement follows and the original file can be downloaded from the ITU ftp server at <http://handle.itu.int/11.1002/ls/sp16-sg17-oLS-00260.docx>.

|  |  |  |
| --- | --- | --- |
| ITU logo | INTERNATIONAL TELECOMMUNICATION UNION**TELECOMMUNICATIONSTANDARDIZATION SECTOR**STUDY PERIOD 2017-2020 | **SG17-LS260** |
| **STUDY GROUP 17** |
| **Original: English** |
| **Question(s):** | 1, 10, 11, 12/17 | Virtual, 24 August - 3 September 2020 |
| **(Ref.: SG17-**[**TD3158**](https://www.itu.int/md/T17-SG17-200824-TD-PLEN-3158/en)**,** [**TD3159**](https://www.itu.int/md/T17-SG17-200824-TD-PLEN-3159/en)**,** [**TD3160**](https://www.itu.int/md/T17-SG17-200824-TD-PLEN-3160/en)**)** |
| **Source:** | ITU-T Study Group 17 |
| **Title:** | LS on SG17 lead study group reports |
| **Purpose:** | Information |
| **LIAISON STATEMENT** |
| **For action to:** | - |
| **For comment to:** | - |
| **For information to:** | TSAG |
| **Approval:** | ITU-T Study Group 17 meeting (Virtual, 3 September 2020) |
| **Deadline:** | N/A |
| **Contact:** | Heung Youl YoumITU-T SG17 chairman | Tel: +82 41 530 1328E-mail: hyyoum@sch.ac.kr |
| **Contact:** | Mohamed ElhajRapporteur of Q1/17 | E-mail: mohamed.elhaj@tpra.gov.sd |
| **Contact:** | Abbie BarbirRapporteur of Q10/17 | Tel: +1 613-697-0865E-mail: abarbir@live.ca |
| **Contact:** | Jean Paul LemaireRapporteur of Q11/17 | Tel: +33 672 197 819E-mail: jean-paul.lemaire@univ-paris-diderot.fr |
| **Contact:** | Dieter HogrefeRapporteur of Q12/17 | Tel: +49 551 39172001Fax: +49 551 391 4403E-mail: hogrefe@informatik.uni-goettingen.de |
|  |

SG17 has the following lead roles:

* [Lead study group on security](https://www.itu.int/en/ITU-T/studygroups/com17/Pages/telesecurity.aspx)
* [Lead study group on identity management (IdM)](https://www.itu.int/en/ITU-T/studygroups/com17/Pages/idm.aspx)
* [Lead study group on languages and description techniques](https://www.itu.int/en/ITU-T/studygroups/com17/Pages/ldt.aspx)

Please find attached three reports from SG17 on each of these roles since last SG17 report to TSAG (LS194), i.e. between 5 September 2019 and 3 September 2020.

Attachments (3):

1. Report on SG17 as the lead study group on security
2. Report on SG17 as the lead study group on identity management (IdM)
3. Report on SG17 as the lead study group on languages and description techniques

**Attachment 1
Report on SG17 as the lead study group on security (Ref.:** [**SG17-TD3160**](https://www.itu.int/md/T17-SG17-200824-TD-PLEN-3160/en)**)**

ITU-T Study Group 17 is very active in fulfilling its lead role in security. In particular, Questions 1/17 through 14/17, as well as certain security activities within Questions of other study groups work to shape the ICT security landscape and interact with a wide range of related standards bodies. SG17 is the parent group of JCA-COP (which is dormant since March 2017).

For additional information, please see the Lead Study Group on security web page at: <http://www.itu.int/ITU-T/studygroups/com17/tel-security.html>

# **1 Achievements**

Annex 1 provides a set of tables that list the results, since previous SG17 August/September 2019 meeting sent LSG report to TSAG, of ITU-T SGs concerning their work on security Recommendations:

SG17 took action on a number of security Recommendations in its March 2020 e-meeting plus its 29 May 2020 e-plenary: approved 12 new Recommendations and two Technical reports.

SG17 took action on a number of security Recommendations in its August/September 2020 e-meeting: approved 10 Recommendations, determined 4 Recommendations, consented 32 Recommendations and agreed 5 texts.

# **2 Ongoing work**

Recommendations and other texts on security currently under development in ITU-T SGs are listed in Annex 2.

# **3 SG17 as Lead Study Group on Security**

SG17 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 and 97;
* Implementation of PP-14 Resolutions 101, 123, 130, 136, 174, 177, 178, 179, 181, 188, 189, 197, 199, 200, and 201.
* Implementation of WTDC-14 Resolutions 23, 30, 34, 45, 47, 54, 63, 67, 69, and 80.

SG17 promotes the work on security and has many considerable efforts on this regard, including:

1. [Security Manual](https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-SEC-2015-PDF-E.pdf)

SG17 revised the Security Manual to the 7th edition in September 2020. The Security Manual is a major promotion tool that highlights in an easy-to-understand fashion the important security work of ITU-T. It provides a broad introduction and it summarizes how the ITU-T is responding to global cybersecurity challenges with Recommendations, technical reports and guidance documents. Ms Kyeong Hee Oh is the editor and all study groups were invited to provide updated information. The 7th edition includes information on 43 new ITU-T standards since the previous edition.

b) [Successful use of security standards](https://www.itu.int/pub/T-TUT-SEC-2016)

SG17 revised its Technical Report on Successful use of security standards to the 2nd edition in September 2020. The report presents examples of how ITU-T Recommendations are used today in the marketplace to help protect networks, people, data, and critical infrastructure. 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). Mr. Abbie Barbir is the master editor.

1. [ICT Security Standards Database](https://www.itu.int/net4/ITU-T/landscape#?topic=0.1&workgroup=1.3935&searchValue=&page=1&sort=Revelance)

SG17 actively maintains the [ICT security standards database](https://www.itu.int/net4/ITU-T/landscape#?topic=0.1&workgroup=1.3935&searchValue=&page=1&sort=Revelance) (i.e., Part 2 of the [ICT Security Standards Roadmap](https://www.itu.int/en/ITU-T/studygroups/com17/ict/Pages/default.aspx)) of approved standards, which is an important tool for standard developers in respect of avoiding duplication. The database provides information on approved ICT security standards of the ITU-T and other standards organizations including ATIS, ETSI, IEEE, IETF, ISO/IEC JTC 1, OASIS, 3GPP and 3GPP2. Ms Yiwen Wang is editor.

At March 2020 SG17 meeting, 56 new security standards in eight SDOs were added into the databases. At Aug/Sept 2020 SG17 meeting, 24 new security standards in eight SDOs were added into the database.

1. [Security Compendium](https://www.itu.int/en/ITU-T/studygroups/com17/Pages/Security_Compendia.aspx)

SG17 also continues updating the [Security Compendium](https://www.itu.int/en/ITU-T/studygroups/com17/Pages/Security_Compendia.aspx) that provides information on security related ITU standardization activities, including the catalogue of ITU-T Recommendations dealing with security and the catalogue of ITU-T approved security definitions. Mr. Sandor Mazgon is editor.

At March 2020 SG17 meeting, 275 definitions and 11 Recommendations were added to the Compendium. At Aug/Sept 2020 SG17 meeting, 279 definitions and 16 Recommendations were added to the Compendium.

# **4 Collaboration with other SGs and other Sectors**

1. No new update to security contacts (see Annex 3) for this study period were provided since SG17 March 2018 meeting.
2. In this reporting period, SG17 received and treated liaison statements on security matters coming from: ITU-D SG2; ITU-R WP5D; ITU-T CITS, FG-AI4EE, FG-AI4H, FG-ML5G, FG-NET2030, FG-QIT4N, FG-VM, FIGI, JCA-IMT2020, CCV, SCV, SG2, SG3, SG5, SG9, SG11, SG12, SG13, SG15, SG16, SG20 and TSAG.
3. In this reporting period, SG17 sent liaison statements to: ITU-D SG2; ITU-R WP 5D; ITU-T CITS, FG-AI4EE, FG-QIT4N, FG-VM, FIGI, JCA-IMT2020, SCV, SG2, SG3, SG5, SG9, SG11, SG13, SG16, SG20, TSAG and TSB Director’s Ad Hoc Group on IPR.

# **5 Collaboration with other organizations**

SG17 collaborates with a broad array of standardization bodies and forums on telecommunication security.

1. In this reporting period, concerning telecommunication security matters, liaison statements were received and treated from: 3GPP TSG SA3; CEN-CENELEC JTC 19; ETSI (ISG ETI, ISG F5G, ISG NIN, ISG SAI; TC Cyber, TC ITS); FIDO Alliance; IETF WG TLS, ISO/IEC JTC 1(SC 27 and itsWG1, WG3, WG4, WG5; SC 29/WG1), MEF, OASIS (OpenC2 TC) and W3C Verifiable claims WG.
2. In this reporting period, SG17 sent liaisons to 3GPP (TSG SA3, SA5); CEN-CENELEC JTC 19; ETSI (ISG QKD, ISG ZSM; SAGE; TC Cyber and its WG QSC); FIDO Alliance; GSMA; ICAO; IEEE Blockchain Initiative; IETF (ANIMA); ISO (TC 20, TC 307); ISO/IEC JTC 1 (WG11, SC 27 and its WG1, WG3, WG4, WG5, SC 29/WG1); MEF; MITRE; NIST; OASIS (CTI TC, OpenC2 TC); OIX; OPIX Foundation; UNECE (GRVA, WP.29); UPU; W3C (DID, Verifiable claims WG, Credentials community Group); WIPO.

## Annex 1Achievements of ITU-T Study Groups on security (5 September 2019 – 3 September 2020)

**a) Recommendations approved**

|  |  |  |
| --- | --- | --- |
| **SG** | **No.** | **Title** |
| SG9 | J.1014 (J.dmcd-eci-as) | Embedded common interface for exchangeable CA/DRM solutions; Advanced Security - ECI­ - specific functionalities |
| SG9 | J.1015 (J.dmcd-kl-as) | Embedded common interface for exchangeable CA/DRM solutions: The advanced security system - Key ladder block |
| SG9 | J.1015.1 (J.dmcd-kl-as Annex A) | Embedded common interface for exchangeable CA/DRM solutions: The advanced security system - Key ladder block: Authentication of control word-usage rules information and associated data 1 |
| SG11 | Q.3057 (Q.SR-trust) | Signalling requirements and architecture for interconnection between trustable network entities |
| SG11 | Q.5050 (Q.FW-CCF) | Framework for solution to combat counterfeit ICT Devices |
| SG13 | Y.3800 (Y.QKDN\_FR) | Overview on networks supporting quantum key distribution |
| SG13 | Y.3801 (Y.QKDN-req) | Functional requirements for quantum key distribution networks |
| SG17 | X.500-series (revised) | Edition 9 of Rec. ITU-T X.500 | ISO/IEC 9594-1 Information technology - Open Systems Interconnection - The Directory |
| SG17 | X.1044 (X.srnv) | Security requirements of network virtualization |
| SG17 | X.1045 (X.ssc) | Security service chain architecture and its application |
| SG17 | X.1052 (revised) | Organization information security management guideline |
| SG17 | X.1059 (X.grm) | Risk management implementation guidance on the assets of telecommunication organizations accessible by global IP-based networks |
| SG17 | X.1148 (X.fdip) | Framework of de-identification process for telecommunication service providers |
| SG17 | X.1149 (X.sfop) | Security framework of open platform for FinTech services |
| SG17 | X.1216 (X.gcpie) | Guidelines for Collection and Preservation of Cyber Security Incident Evidence |
| SG17 | X.1232 (X.tfcas) | Technical framework for countering advertising spam in user generated information  |
| SG17 | X.1254rev | Entity authentication assurance framework |
| SG17 | X.1279 | Framework of enhanced authentication using telebiometrics with anti-spoofing detection mechanisms |
| SG17 | X.1332 (X.sgsec-3) | Security guidelines for smart metering service in smart grids |
| SG17 | X.1363 (X.iotsec-3) | Technical framework of personally identifiable information (PII) handling system in IoT environment |
| SG17 | X.1364 (X.nb-iot) | Security requirements and framework for narrow band internet of things |
| SG17 | X.1365 (X.ibc-iot) | Security framework for use of identity-based cryptography in support of IoT services over telecom networks |
| SG17 | X.1366 (X.amas-iot) | Aggregate message authentication schemes with group authentication capability for IoT environment |
| SG17 | X.1367 (X.elf-iot) | Standard format of IoT error logs for security incident operations |
| SG17 | X.1371 (X.stcv) | Security threats in connected vehicles |
| SG17 | X.1372 (X.itssec-2) | Security guidelines for V2X communication systems |
| SG17 | X.1401 (X.sct-dlt) | Security threats to Distributed Ledger Technology |
| SG17 | X.1402 (X.sra-dlt) | Security framework for distributed ledger technology |
| SG17 | X.1403 (X.dlt-sec) | Security guidelines for using DLT for decentralized identity management |
| SG17 | X.1451 (X.tfrca) | Risk identification to optimize authentication |
| SG17 | X.1604 (X.SRNaaS) | Security requirements of network as a service (NaaS) in cloud computing |
| SG17 | X.1605 (X.SRIaaS) | Security requirements of public infrastructure as a service (IaaS) in cloud computing |
| SG17 | X.1606 (X.SRCaaS) | Security requirements for communications as a service application environments |
| SG17 | X.1750 (X.GSBDaaS) | Guidelines on security of big data as a service for big data service providers |
| SG17 | X.1751 (X.sgtBD) | Security guidelines on big data lifecycle management for telecommunication operators |
| SG17 | X.1702 (X.qrng-a) | Quantum noise random number generator architecture |
| SG20 | Y.4807 (Y.IoT-agility) | Agility by design for Telecommunications/ICT Systems Security used in the Internet of Things |
| SG20 | Y.4808 (Y.IoT-DA-Counterfeit) | Information Management Digital Architecture to combat counterfeiting in IoT |

 **b) Supplements, Appendices, and Technical Report agreed**

| **SG** | **No.** | **Title** |
| --- | --- | --- |
| SG9 | J.Suppl.8 (J.sup-te) | Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Trust Environment (TE) |
| SG11 | TR-SS7-DFS | Technical Report: SS7 vulnerabilities and mitigation measures for digital financial services transactions |
| SG13 | Supplement 49 to Y.3500-series (Y.sup.ccsr) | Cloud Computing Standardization Roadmap |
| SG17 | TR.sec-qkd | Technical Report: Security considerations for quantum key distribution network |
| SG17 | Security Manual | Security in telecommunications and information technology (7th edition) |
| SG17 | TR.suss | Technical Report: Successful use of security standards (2nd edition) |
| SG17 | TP.inno | Technical Report: Description of the incubation mechanism and ways to improve it |
| SG17 | TP.sgstruct | Technical Report: Strategic approaches to the transformation of security studies |
| SG17 | TR.usm | Technical Report: Unified Security Model (USM) - a neutral integrated system approach to Cybersecurity |

**c) Draft Recommendations determined**

|  |  |  |
| --- | --- | --- |
| **SG** | **No.** | **Title** |
| SG17 | X.1054rev | Information technology - Security techniques - Governance of information security |
| SG17 | X.1217 (X.fgati) | Framework and guidelines for applying threat intelligence in telecom network operation |
| SG17 | X.1368 (X.secup-iot) | Secure software update procedure for IoT devices |
| SG17 | X.1376 (X.mdcv) | Security-related misbehaviour detection mechanism based on big data analysis for connected vehicles |
| SG17 | X.1811 (X.5Gsec-q) | Security guidelines for applying quantum-safe algorithms in 5G systems |

**d) Draft Recommendations consented**

|  |  |  |
| --- | --- | --- |
| **SG** | **No.** | **Title** |
| SG9 | J.1204 (J.stvos-sec) | The security framework of smart TV operating system |
| SG13 | Y.3055 (Y.trust-pdm) | Framework for Trust based Personal Data Management |
| SG13 | Y.3802 (Y.QKDN\_Arch) | Functional architecture of the Quantum Key Distribution network |
| SG13 | Y.3803 (Y.QKDN\_KM) | Key management for Quantum Key Distribution network |
| SG13 | Y.3804 (Y.QKDN\_CM) | Control and Management for Quantum Key Distribution Networks  |
| SG17 | X.1046 (X.SDSec) | Guideline on software-defined security in SDN (Software-defined Networking)/NFV (Network Function Virtualization) network |
| SG17 | X.1052rev | Organization information security management guideline |
| SG17 | X.1218 (X.rdmase) | Requirements and guidelines for dynamic malware analysis in a sandbox environment |
| SG17 | X.1374 (X.itssec-3) | Security requirements for external device with vehicle access capability |
| SG17 | X.1375 (X.itssec-4) | Methodologies for intrusion detection system on in-vehicle system |
| SG17 | X.1400 (X.dlt-td) | Terms and definitions for distributed ledger technology |
| SG17 | X.1404 (X.sa-dlt) | Security assurance for distributed ledger technology |
| SG17 | X.1452 (X.tfss) | Technical framework for security services provided by operators |
| SG17 | X.1710 (X.sec-QKDN\_ov) | Security requirements for QKD networks - Overview |
| SG17 | X.1714 (X.cf-QKDN) | Use of cryptographic functions on a key generated by a Quantum Key Distribution networks |

## Annex 2 Current work plan of ITU-T Study Groups on security (status 3 September 2020)

| **SG** | **Q** | **No.** | **Title** |
| --- | --- | --- | --- |
| SG13 | 2 | Y.DNI-fr | Framework and Requirements of Decentralized Trustworthy Network Infrastructure |
| SG13 | 6 | Y.QKDN-qos-arc | Functional architecture of QoS assurance for quantum key distribution networks |
| SG13 | 6 | Y.QKDN-qos-gen | General Aspects of QoS on the Quantum Key Distribution Network |
| SG13 | 6 | Y.QKDN-qos-ml-req | Requirements of machine learning based QoS Assurance for quantum key distribution networks |
| SG13 | 6 | Y.QKDN-qos-req | Requirements for QoS Assurance of the Quantum Key Distribution Network |
| SG13 | 16 | Y.QKDN\_BM | Business role-based models in Quantum Key Distribution Network |
| SG13 | 16 | Y.QKDN\_frint | Framework for integration of QKDN and secure network infrastructures |
| SG13 | 16 | Y.QKDN-SDNC | Software Defined Network Control for Quantum Key Distribution Networks |
| SG13 | 16 | Y.energ-brokerage | Framework of trusted electricity brokerage for distributed energy resources |
| SG13 | 16 | Y.SNS-trust | Framework for Evaluation of Trust and Quality of Media in Social Networking Services |
| SG13 | 16 | Y.supp.trust-roadmap | Standardization roadmap on trustworthy networking and services including quantum enhanced networks |
| SG13 | 16 | Y.trust-arch | Functional architecture for trust enabled service provisioning |
| SG13 | 16 | Y.trust-index | Trust index for ICT infrastructures and services |
| SG13 | 16 | Y.PII-Did | Prioritization based De-Identification Methods for Personally Identifiable Information |
| SG13 | 19 | Y.ccrm | Cloud computing - Framework of risk management |
| SG13 | 23 | Y.SBN-TR | Service brokering network framework for Trusted Reality |
| SG15 | 11 | G.Sup.otnsec | OTN Security |
| SG16 | 11 | H.235.10 | H.323 security: Support of DTLS for media streams |
| SG17 | 2 | TP.sec-arch\*\* | Implications and further considerations of security architecture patterns |
| SG17 | 2 | X.arch-design | Design principles and best practices for security architectures |
| SG17 | 2 | X.nsom-sec | Security requirements and architecture for network slice orchestration and management |
| SG17 | 2 | X.rf-csap | Reference framework for continuous protection of service access process |
| SG17 | 3 | X.1041rev2 | Code of practice for Information security controls based on ISO/IEC 27002 for telecommunication organizations |
| SG17 | 3 | X.ciag | Cyber insurance acquisition guideline for Information and Communication Technologies (ICT) services provider |
| SG17 | 3 | X.framcdc | Framework for the creation and operation of a cyber defence center |
| SG17 | 3 | X.sup-csc\*\* | ITU-T X.1051 - Supplement on critical security controls for telecommunication organizations |
| SG17 | 4 | TR.sgfdm\*\* | Technical Report: Security guidelines for FHE-based machine learning |
| SG17 | 4 | X.arc-ev | Security architecture for evaluation of technical vulnerabilities |
| SG17 | 4 | X.icd-schemas | Security data schemas for integrated cyber defence solutions |
| SG17 | 4 | X.sec-QKDN-intrq | Security requirements for integration of QKDN and secure network infrastructures |
| SG17 | 4 | X.sec-QKDN-km | Security requirements for quantum key distribution networks - key management |
| SG17 | 4 | X.sec-QKDN-tn | Security requirements for quantum key distribution networks – trusted node |
| SG17 | 4 | X.tf-mpc | Technical framework and application for secure multi-party computation |
| SG17 | 5 | TR.cs-ml\*\* | Technical Report: Countering spam based on AI |
| SG17 | 5 | X.1246rev\* | Technologies involved in countering voice spam in telecommunication organizations |
| SG17 | 5 | X.1247rev\* | Technical framework for countering mobile messaging spam |
| SG17 | 5 | X.gcims\* | Guidelines for countering instant messaging spam |
| SG17 | 5 | X.gcmms\* | Guideline for countering multimedia messaging service spam |
| SG17 | 5 | X.tecwes\* | Technologies in countering website spoofing for telecommunication organizations |
| SG17 | 5 | X.tsfpp\* | Technical security framework for protection of users' personal information while countering mobile messaging spam |
| SG17 | 6 | X.5Gsec-ecs\* | Security framework for 5G edge computing services |
| SG17 | 6 | X.5Gsec-guide\* | Security guideline for 5G communication system based on ITU-T X.805 |
| SG17 | 6 | X.5Gsec-netec\* | Security capabilities of network layer for 5G edge computing |
| SG17 | 6 | X.5Gsec-ssl\* | Guidelines for classifying security capabilities in 5G network slice |
| SG17 | 6 | X.5Gsec-t\* | Security framework based on trust relationship in 5G ecosystem |
| SG17 | 6 | X.5Gsec-vs\* | Security requirements for vertical services supporting ultra reliable and low latency communication (URLLC) in the 5G non-public networks |
| SG17 | 6 | X.iotsec-4\* | Security requirements for IoT devices and gateway |
| SG17 | 6 | X.sc-iot\* | Security controls for Internet of Things (IoT) systems |
| SG17 | 6 | X.sg-rat\* | Security guidelines for use of remote access tools in Internet-connected control system |
| SG17 | 6 | X.ssp-iot\* | Security requirements and framework for IoT service platform |
| SG17 | 6 | X.strvms\* | Security threats and requirements for video management system |
| SG17 | 6 | X.ztd-iot\* | Security methodology for zero-touch massive IoT deployment |
| SG17 | 7 | TR.cta\*\* | Technical Report: Use cases of contact tracing applications to prevent spread of infectious diseases |
| SG17 | 7 | X.rdda\* | Requirements for data de-identification assurance |
| SG17 | 7 | X.scpa | Security measures for countering password related online attacks |
| SG17 | 7 | X.sec-grp-mov\* | Proposal for new work item: Security guideline for group movement service platform |
| SG17 | 7 | X.sgos | Security guidelines of web-based online customer service |
| SG17 | 7 | X.sles\* | Security measures for location enabled smart office services |
| SG17 | 7 | X.smdtsc | Proposal for new work item: Security Measures for Digital Twin System of Smart Cities |
| SG17 | 7 | X.smsrc | Proposal for new work item: Security Measures for Smart Residential Community Services |
| SG17 | 7 | X.websec-7 | Reference monitor for online analytics services |
| SG17 | 8 | TR.fssvs | Framework for Security Standardization for Virtualized Services |
| SG17 | 8 | X.BaaS-sec\* | Guideline on blockchain as a service (BaaS) security |
| SG17 | 8 | X.nssa-cc\* | Requirements of network security situational awareness platform for cloud computing |
| SG17 | 8 | X.sgBDIP\* | Security guidelines for big data infrastructure and platform |
| SG17 | 8 | X.sgcc\* | Security guidelines for container in cloud computing environment |
| SG17 | 8 | X.sgdc\* | Security guidelines for distributed cloud |
| SG17 | 8 | X.sgmc\* | Security guidelines for multi-cloud |
| SG17 | 8 | X.sr-cphr | Security requirements of cloud-based platform under low latency and high reliability application scenarios |
| SG17 | 9 | X.b2m | Biology to machine protocol |
| SG17 | 9 | X.pet\_auth | Entity authentication service for pet animals using telebiometrics |
| SG17 | 9 | X.tas | Telebiometric authentication using speaker recognition |
| SG17 | 13 | X.1373rev\* | Secure software update capability for intelligent transportation system communication devices |
| SG17 | 13 | X.edrsec\* | Security guidelines for cloud-based event data recorders in automotive environment |
| SG17 | 13 | X.eivnsec\* | Security guidelines for the Ethernet-based in-vehicle networks |
| SG17 | 13 | X.evtol-sec\* | Security guidelines for electric vertical take-off and landing (eVTOL) vehicle in an urban air mobility environment |
| SG17 | 13 | X.fstiscv\* | Framework of security threat information sharing for connected vehicles |
| SG17 | 13 | X.ipscv | Methodologies for intrusion prevention systems for connected vehicles |
| SG17 | 13 | X.itssec-5\* | Security guidelines for vehicular edge computing |
| SG17 | 13 | X.rsu-sec | Security guidelines for vehicular edge computing |
| SG17 | 13 | X.srcd\* | Security requirements for categorized data in V2X communication |
| SG17 | 14 | TR.qs-dlt\*\* | Guidelines for quantum-safe DLT system |
| SG17 | 14 | X.das-mgt | Security framework for data access and sharing management system based on distributed ledger technology |
| SG17 | 14 | X.sa-dsm\* | Security architecture of data sharing management based on the distributed ledger technology |
| SG17 | 14 | X.sc-dlt | Security controls for distributed ledger technology |
| SG17 | 14 | X.srcsm-dlt | Security Requirements for Smart Contract Management based on the distributed ledger technology |
| SG17 | 14 | X.srip-dlt\* | Security requirements for intellectual property management based on distributed ledger technology |
| SG17 | 14 | X.ss-dlt | Security Services based on Distributed Ledger Technology |
| SG17 | 14 | X.stov | Security threats to online voting using distributed ledger technology |
| SG17 | 14 | X.str-dlt | The security threats and requirements for digital payment services based on distributed ledger technology |
| SG17 | 14 | X.tf-spd-dlt | Technical framework for secure software programme distribution mechanism based on distributed ledger technology |
| SG20 | 2 | Y.IoT-ITS-framework | Framework of Cooperative Intelligent Transport Systems based on the Internet of Things |
| SG20 | 6 | Y.Data.sec.IoT-Dev | Requirements of data security for the heterogeneous IoT devices |
| SG20 | 6 | Y.IoT-Ath-SC | Framework of IoT-devices authentication in smart city |
| SG20 | 6 | Y.oneM2M.SEC.SOL | oneM2M Security Solutions |

Notes:
\* Marked draft Recommendations are for determination; all non-marked are for consent.

\*\* Texts for approval by agreement (AAP/TAP not applicable)

## Annex 3 Security Contacts List

|  |  |  |
| --- | --- | --- |
| **Study Group** | **Contact** | **E-mail** |
| ITU-T SG2 | - Yanchuan WangChina Telecom (P.R. China)- Ping ZhaoChina Telecom (P.R.China) | wangych@chinatelecom.cnzhaop@gsta.com |
| ITU-T SG3 | - Linjuan HuangMIIT (P.R. China) | huanglinjuan@catr.cn |
| ITU-T SG5 | - Yuichiro OkugawaNTT (Japan) | [No email was provided]. |
| ITU-T SG9 | - Han-Seung Koo Korea | koohs@etri.re.kr |
| ITU-T SG11 | - Andrey KucheryavyChairman SG11 | akouch@mail.ru |
| ITU-T SG12 | - Al Morton | acmorton@att.com |
| ITU-T SG13 | - Leo LehmannChairman SG13 | Leo.Lehmann@bakom.admin.ch |
| ITU-T SG15 | - Tomer Cohen | tomer.cohen72@gmail.com |
| ITU-T SG16 | - Paul JonesChairman WP1/16 | paulej@packetizer.com |
| ITU-T SG17 | - Heung Youl YoumSG17 Chairman- Mohamed ElhajRapporteur, ITU-T Q1/17- Xiaoya YangCounsellor, ITU/TSB- ITU-T SG17 Secretariat | hyyoum@sch.ac.krmohamed elhaj@tpra.gov.sdxiaoya.yang@itu.inttsbsg17@itu.int |
| ITU-T SG20 | - Giampiero Nanniliaison officer from SG20 to SG17 | Giampiero\_Nanni@symantec.com |
| TSAG | - Bruce GracieChairman TSAG | bruce.gracie@ericsson.com |
| ITU-D SG 2 | - Marco Obiso, BDTFocal Point for Q.3/2, Cybersecurity and ICT Applications Division- Miho Naganuma NEC (Japan) | marco.obiso@itu.intm-naganuma@bx.jp.nec.com |
| ITU-R SG 4 | - Chris HoferChairman ITU-R SG 4 | chris.hofer@viasat.com |
| ITU-R SG 5 | - Martin FentonChairman ITU-R SG 5 | martin.fenton@ofcom.org.uk |

# **Attachment 2Report on SG17 as the lead study group on identity management (ref. SG17-**[**TD3159**](https://www.itu.int/md/T17-SG17-200824-TD-PLEN-3159/en)**)**

ITU-T Study Group 17 continues to be very active in fulfilling its lead role in identity management (IdM). In particular, elements within SG17 responsibility (i.e., Questions 10, 11/17, and JCA-IdM) played an active role in shaping the IdM landscape and interacting with a wide range of standards bodies that are addressing IdM. Other ITU-T study groups (SG2, SG3, SG11, and SG20) also have IdM related activities.

For additional information, please see the lead study group on identity management web page at: <http://www.itu.int/en/ITU-T/studygroups/com17/Pages/idm.aspx> and the JCA-IdM web page at  [http://www.itu.int/en/ITU-T/jca/idm/Pages/default.aspx](%20http%3A//www.itu.int/en/ITU-T/jca/idm/Pages/default.aspx).

# **1 Achievements**

Since SG17 Sept 2019 meeting sent last SG17 LSG report to TSAG, ITU-T SGs achieved the results listed in Annex 1 concerning their work on IdM Recommendations (Status: 3 Sept 2020):

# **2 Ongoing work**

Recommendations and other texts concerning IdM that are currently under development in ITU-T SGs are listed in Annex 2.

# **3 Collaboration and outreach**

SG17 is the parent group of JCA-IdM. The purpose of the JCA-IdM is coordination of the ITU-T identity management (IdM) work, and to ensure that the ITU-T IdM work is progressed in a well-coordinated way between study groups, in particular with SG2, SG3, SG11, and SG20, and to act as a point of contact within ITU-T and with other SDOs/Fora on IdM in order to avoid duplication of work and assist in implementing the IdM tasks assigned by WTSA-16 Resolution 2 and in implementing GSC-16 Resolution 4 on identity management.

SG17 developed X.Suppl.35 Supplement to ITU-T X.1254 on use cases of entity authentication assurance (EAA) framework.

SG17 approved X.1279, *Framework of enhanced authentication using telebiometrics with anti-spoofing detection mechanisms* and X.1403, *Security guidelines for using DLT for decentralized identity management.*

SG17 approved a revision of X.1254, *Entity authentication assurance framework* in conjunction with ISO/IEC JTC 1/SC 27 work for revision of ISO/IEC 29115.

SG17 determined a revision of X.1252, *Baseline identity management terms and definitions.*

SG17 agreed to have the dual numbering of the SG3 Recommendation D.267, *Guidelines for digital identity*, as X.1261.

Q10/17 collaborated with FIGI to develop a hands on sessions on strong authentication and decentralized identity during the [FIGI Security Clinic December 2019 meeting](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201912/Pages/default.aspx). In addition, Q10/17 worked with FIGI to address how identity solutions can help in the fight against Covid-19. This was done through the workshop on “[FIGI Security, Infrastructure and Trust Working Group (SIT WG)](https://www.itu.int/en/ITU-T/extcoop/figisymposium/Pages/FIGISITWG.aspx)”.

In this reporting period, SG17 received and treated liaison statements on identity management matters coming from ITU-T FIGI, SG11, SG13, SG20; FIDO Alliance, NIST, ISO/IEC JTC 1/SC 27/WG 1 and ISO/IEC JTC 1/SC 27/WG 4.

In this reporting period, SG17 sent liaison statements to ITU-T FIGI, SG2, SG3, SG5, SG13, SG16, SG20; W3C Verifiable claims WG, FG AI4EE, IEEE Blockchain Initiative, W3C DID, ETSI TC Cyber, , ISO TC 307, ISO/IEC JTC 1/SC 27/WG1 and WG 5, Kantara Initiative, NIST, FIDO Alliance, OASIS, OPIX Foundation, OIX and UPU.

## Annex 1 Achievements of ITU-T Study Groups on Identity Management (5 September 2019 - 3 September 2020)

1. **Approved Recommendations**

|  |  |  |
| --- | --- | --- |
| **SG** | **No** | **Title** |
| SG3 | D.267 (D.DigID)/X.1261\*\*\* | Guidelines for digital identity |
| SG17 | X.509 (ninth edition) | Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks |
| SG17 | X.510 (X.509prot) | Information technology – Open Systems Interconnection – The Directory: Protocol specifications for secure operations |
| SG17 | X.677 (X.uav-oid) | Identification mechanism for unmanned aerial vehicles using object identifiers |
| SG17 | X.1254rev | Entity authentication assurance framework |
| SG17 | X.1279 (X.eaasd) | Framework of enhanced authentication using telebiometrics with anti-spoofing detection mechanisms |
| SG17 | X.1365 (X.ibc-iot) | Security framework for use of identity-based cryptography in support of IoT services over telecom networks |
| SG17 | X.1403 (X.dlt-sec) | Security guidelines for using DLT for decentralized identity management |
| SG20 | Y.4462 (Y.IoT-ics) | Requirements and functional architecture of Open IoT identity correlation service |

1. **Approved Supplements, Technical Reports**

|  |  |  |
| --- | --- | --- |
| **SG** | **No** | **Title** |
| SG11 | TR-RLB-IMEI | Reliability of IMEI |
| SG17 | TR.ors | OID Resolution system: Problems, Requirements and Potential solutions |

1. **Consented/Determined Recommendations**

|  |  |  |
| --- | --- | --- |
| **SG** | **No** | **Title** |
| SG11 | Q.5052 (Q.DEV\_DUI) | Addressing mobile devices with duplicate unique identifier |
| SG17 | X.1252rev\* | Baseline identity management terms and definitions |

Notes:

\* Marked draft Recommendations are for determination; all non-marked are for consent.

\*\*\* Dual numbering of D.267 (SG3) as X.1261 (SG17)

## Annex 2 Current work plan of ITU-T Study Groups on Identity Management (status 3 September 2020)

|  |  |  |
| --- | --- | --- |
| **SG** | **No** | **Title** |
| SG2 | TR.OTTnum\*\* | Current use of E.164 numbers as identifiers for OTTs |
| SG2 | E.sup.OTTnum | Guidance on the use of E.164 numbers as identifiers for OTTs |
| SG2 | E.IoT-NNAI\* | Internet of Things Naming Numbering Addressing and Identifiers |
| SG13 | Y.SCid-fr | Requirements and converged framework of self-controlled identity based on blockchain |
| SG17 | X.510 Amd.1 | Extensions |
| SG17 | X.672rev | Information technology – Open systems interconnection – Object identifier resolution system |
| SG17 | X.1250rev | Baseline capabilities for enhanced global identity management and interoperability |
| SG17 | X.gpwd | Guidelines for securing password and password-less authentication solutions |
| SG17 | X.pki-em | Information technology – Public-Key Infrastructure: Establishment and maintenance |
| SG17 | X.tec-idms | Management and protection techniques for user data protection in distributed identity systems |
| SG17 | X.upu\* | Postal identity management framework |
| SG20 | Y.FW.IC.MDSC | Framework of identification and connectivity of moving devices in smart city |
| SG20 | Y.IoT-CSIADE-fw | Reference framework of converged service for identification and authentication for IoT devices in decentralized environment |
| SG20 | Y.IoT-IoD-PT | Identity of IoT devices based on secure procedures and ensures privacy and trust of IoT systems |
| SG20 | Y.IoT-ITS-ID | IoT Identifiers for Intelligent Transport Systems |
| SG20 | Y.IoT-rf-dlt | OID-based Resolution framework for transaction of distributed ledger assigned to IoT resources |
| SG20 | YSTR.Feas-DID-IoT | Feasibility of Decentralised Identifiers (DIDs) in IoT |

Notes:

\* Marked draft Recommendations are for determination; all non-marked are for consent.

\*\* Texts for approval by agreement (AAP/TAP not applicable)

# **Attachment 3Report on SG17 as the lead study group on languages and description techniques (ref.** [**SG17-3158**](https://www.itu.int/md/T17-SG17-200824-TD-PLEN-3158/en)**)**

ITU-T Study Group 17 is active in fulfilling its lead study group role in languages and description techniques. In particular elements within SG17 responsibility (i.e., Questions 11/17 and 12/17) play an active role in shaping the landscape and interacting with other bodies.

For additional information, please see the Lead Study Group on Languages and description techniques web page at: <http://www.itu.int/en/ITU-T/studygroups/com17/Pages/ldt.aspx>

# **1 Achievements**

Annex 1 provides a set of tables that list the results, since SG17 Aug/Sep 2019 meeting sent its previous LSG report to TSAG, of ITU-T SGs concerning their work on languages and description techniques (status: 3 September 2020).

# **2 Ongoing work**

Recommendations and other texts on languages and description techniques currently under development in ITU-T SGs are listed in Annex 2.

# **3 SG17 as Lead Study Group on Languages and description techniques**

Languages include Abstract Syntax Notation One (ASN.1), Message Sequence Chart (MSC), User Requirements Notation (URN), Specification and Description Language (SDL-2010), and Testing and Test Control Notation (TTCN-3). Q11/17 covers Abstract Syntax Notation One (ASN.1) in collaboration with ISO/IEC, while the other languages are covered by Question 12/17.

**a) Abstract Syntax Notation One (ASN.1, ITU-T X.680, X.690 and X.890 series)**

ASN.1 provides a widely used notation for the definition of protocols and file formats, supported by both compact binary, XML and JSON encodings for the messages and file formats. Question 11/17 develops all ASN.1 Recommendations as common texts with ISO/IEC JTC 1/SC6.

The ASN.1 project provides assistance to users of ASN.1 within and outside the ITU-T (e.g., ITU-T SG16, ISO/IEC JTC 1/SC 27, ISO/TC 215, ETSI TC LI, 3GPP, etc.) and helps the TSB in the maintenance of an up-to-date database of error-free ASN.1 modules. 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 set of revised ASN.1 Recommendations (X.680 and X.690 series) were consented on 3 September 2020.

**b) ITU-T Specification and Description Language (Z.100-series)**

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. Revised Z.100 to Z.107 and Z.Imp100 version 4.0.0 were approved in Oct 2019. The net result is a better-defined SDL‑2010 with a consistent formal definition. No further work is currently planned.

**c) User Requirements Notation (URN, Z.150-series)**

URN has remained stable since the revision of Z.151 approved in October 2018. No further work is currently planned.

**d) Testing and Test Control Notation (TTCN-3, Z.160/170-series)**

Test specification languages can be used in testing ITU-T Recommendations developed by the relevant ITU-T SGs and especially SG11, as the lead group on test specifications, conformance and interoperability testing. Question 12/17 continues its close relationship with ETSI TC MTS on revisions of the ITU-T Z.160/Z.170 series Recommendations on TTCN-3.

Nine revised TTCN-3 Recommendations were consented on 3 September 2020.

# **4 Collaboration with other SGs and external organizations**

Question 11/17 develops all ASN.1 Recommendations collaboratively with ISO/IEC JTC 1/SC 6 as common texts.

Question 12/17 has a close relationship with the SDL Forum Society, which focuses on the ITU-T System Design Languages. Society members are involved in ongoing Q12/17 work.

Question 12/17 also has a close relationship with ETSI TC MTS on TTCN-3.

## Annex 1 to Attachment 3Achievements of ITU-T Study Groups on languages and description techniques (5 September 2019 – 3 September 2020)

1. **Recommendations approved**

| **SG** | **No** | **Title** |
| --- | --- | --- |
| SG17 | Z.100 (revised) | Specification and Description Language - Overview of SDL-2010 |
| SG17 | Z.100 Annex F1(revised) | Specification and Description Language - Overview of SDL-2010 - SDL formal definition: General overview |
| SG17 | Z.100 Annex F2(revised) | Specification and Description Language - Overview of SDL-2010 - SDL formal definition: Static semantics |
| SG17 | Z.100 Annex F3(revised) | Specification and Description Language - Overview of SDL-2010 - SDL formal definition: Dynamic semantics |
| SG17 | Z.101 (revised) | Specification and Description Language - Basic SDL-2010 |
| SG17 | Z.102 (revised) | Specification and Description Language - Comprehensive SDL-2010 |
| SG17 | Z.103 (revised) | Specification and Description Language - Shorthand notation and annotation in SDL-2010 |
| SG17 | Z.104 (revised) | Specification and Description Language - Data and action language in SDL-2010 |
| SG17 | Z.105 (revised) | Specification and Description Language - SDL-2010 combined with ASN.1 modules |
| SG17 | Z.106 (revised) | Specification and Description Language - Common interchange format for SDL-2010 |
| SG17 | Z.107 (revised) | Specification and Description Language - Object-oriented data in SDL-2010 |
| SG17 | Z.161 (revised) | Testing and Test Control Notation version 3: TTCN-3 core language |
| SG17 | Z.161.2 (revised) | Testing and Test Control Notation version 3: TTCN-3 language extensions: Configuration and deployment support |
| SG17 | Z.161.6 (revised) | Testing and Test Control Notation version 3: TTCN-3 Language extensions: Advanced Matching |
| SG17 | Z.161.7 (new) | Testing and Test Control Notation version 3: TTCN-3 Language extensions: Object-Oriented Features |
| SG17 | Z.166 (revised) | Testing and Test Control Notation version 3: TTCN-3 control interface (TCI) |
| SG17 | Z.169 (revised) | Testing and Test Control Notation version 3: Using XML schema with TTCN-3 |

1. **Recommendations consented**

| **SG** | **No** | **Title** |
| --- | --- | --- |
| SG17 | X.680rev | Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation |
| SG17 | X.681rev | Information technology - Abstract Syntax Notation One (ASN.1): Information object specification |
| SG17 | X.682rev | Information technology - Abstract Syntax Notation One (ASN.1): Constraint specification  |
| SG17 | X.683rev | Information technology - Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications |
| SG17 | X.690rev | Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)  |
| SG17 | X.691rev | Information technology - ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)  |
| SG17 | X.692rev | Information technology - ASN.1 encoding rules: Specification of Encoding Control Notation (ECN) |
| SG17 | X.693rev | Information technology - ASN.1 encoding rules: XML Encoding Rules (XER) |
| SG17 | X.694rev | Information technology - ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1  |
| SG17 | X.695rev | Information technology - ASN.1 encoding rules: Registration and application of PER encoding instructions |
| SG17 | X.696rev | Information technology - ASN.1 encoding rules: Specification of Octet Encoding Rules (OER) |
| SG17 | X.697rev | Information technology - ASN.1 encoding rules: Specification of JavaScript Object Notation Encoding Rules (JER) |
| SG17 | X.894 Cor. 2 | Generic applications of ASN.1 – Cryptographic Message Syntax – Cor. 2 |
| SG17 | Z.161 (revised) | Testing and Test Control Notation version 3: TTCN-3 core language |
| SG17 | Z.161.3 (revised) | Testing and Test Control Notation version 3: TTCN-3 language extensions: Advanced parameterization |
| SG17 | Z.161.4 (revised) | Testing and Test Control Notation version 3: TTCN-3 language extensions: Behaviour types |
| SG17 | Z.161.6 (revised) | Testing and Test Control Notation version 3: TTCN-3 language extensions: Advanced matching |
| SG17 | Z.161.7 (revised) | Testing and Test Control Notation version 3: TTCN-3 language extensions: Object-oriented features |
| SG17 | Z.165.1 (revised) | Testing and Test Control Notation version 3: TTCN-3 language extensions: Extended TRI |
| SG17 | Z.166 (revised) | Testing and Test Control Notation version 3: TTCN-3 control interface (TCI) |
| SG17 | Z.167 (revised) | Testing and Test Control Notation version 3: Using ASN.1 with TTCN-3 |
| SG17 | Z.169 (revised) | Testing and Test Control Notation version 3: Using XML schema with TTCN-3 |

## Annex 2 to Attachment 3Current work plan of ITU-T Study Groups on languages and description techniques (status 3 September 2020)

**a) Abstract Syntax Notation One (ASN.1)**

|  |  |  |
| --- | --- | --- |
| **SG** | **No** | **Title** |
| SG17 | X.680-X.683 | ASN.1 (new Edition)  |
| SG17 | X.690-X.697 | ASN.1 encoding rules (new Edition) |

Note: All texts are for consent.

**b) TTCN-3**

| **SG** | **No** | **Title** |
| --- | --- | --- |
| SG17 | Z.161-Z.171 | Testing and Test Control Notation version 3 (new Edition) |

Note: All texts are for consent.

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