|  |  |  |
| --- | --- | --- |
| ITU logo | INTERNATIONAL TELECOMMUNICATION UNION**TELECOMMUNICATION STANDARDIZATION SECTOR**STUDY PERIOD 2017-2021 | TSAG-TD1048 |
| **TSAG** |
| **Original: English** |
| **Question(s):** | N/A | E-Meeting, 25-29 October 2021 |
| **TD(Ref.:** [SG17-LS305](http://handle.itu.int/11.1002/ls/sp16-sg17-oLS-00305.docx)) |
| **Source:** | ITU-T Study Group 17 |
| **Title:** | LS on ITU-T SG17 Lead Study 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 2021) |
| **Deadline:** | - |
| **Contact:** | Heung-Youl YoumITU-T SG17 chairmanKorea (Republic of) | Tel: +82 41 530 1328E-mail: hyyoum@sch.ac.kr  |
| **Contact:** | Mohamed ElhajCo-Rapporteur of Q1/17 | E-mail: mohamed.elhaj@tpra.gov.sd  |
| **Contact:** | Abbie BarbirCo-Rapporteur 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  |

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-00305.docx>.

|  |  |  |
| --- | --- | --- |
| ITU logo | INTERNATIONAL TELECOMMUNICATION UNION**TELECOMMUNICATIONSTANDARDIZATION SECTOR**STUDY PERIOD 2017-2020 | **SG17-LS305** |
| **STUDY GROUP 17** |
| **Original: English** |
| **Question(s):** | 1/17 | Virtual, 24 August - 3 September 2021 |
| **(Ref.:** [**SG17-TD3927R4**](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3927/en)**,** [**TD3928R3**](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3928/en)**,** [**TD3929**](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3929/en)**R1)** |
| **Source:** | ITU-T Study Group 17 |
| **Title:** | LS on SG17 Lead Study Reports  |
| **LIAISON STATEMENT** |
| **For action to:** | - |
| **For comment to:** |  |
| **For information to:** | TSAG |
| **Approval:** | ITU-T Study Group 17 meeting (Virtual, 3 September 2021) |
| **Deadline:** | - |
| **Contact:** | Heung-Youl YoumITU-T SG17 chairmanKorea (Republic of) | Tel: +82 41 530 1328E-mail: hyyoum@sch.ac.kr |
| **Contact:** | Mohamed ElhajCo-Rapporteur of Q1/17 | E-mail: mohamed.elhaj@tpra.gov.sd |
| **Contact:** | Abbie BarbirCo-Rapporteur 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 |

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 4 September 2020 and 3 September 2021.

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-TD3927R4**](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3927/en)**)**

ITU-T Study Group 17 is very active in fulfilling its lead role on security. Twelve Questions in SG17, 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 the SG17 August/September 2020 e-meeting sent LSG report to TSAG, of ITU-T SGs concerning their work on security Recommendations:

SG17 at its January 2021 e-plenary: approved 3 new Recommendations.

SG17 at its 20-30 April 2021 e-meeting: approved 2 Recommendations, determined 1 Recommendation, consented 2 Recommendations and agreed 1 text.

SG17 at its 24 August – 3 September 2021 e-meeting: approved 1 Recommendation, determined 11 Recommendations, consented 6 Recommendations and agreed 2 texts.

# **2 Ongoing work**

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

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

SG17 work on security considers:

* Implementation of WTSA-16 Resolutions 2, 7, 11, 18, 32, 40, 44, 50, 52, 54, 58, 64, 65, 67, 73, 75, 76 77, 78, 80, 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, 201, 204, 205, 206.
* Implementation of WTDC-17 Resolutions 30, 34, 43, 45, 47, 63, 67, 69, 79, 80, and 84.

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-2020-PDF-E.pdf)

SG17 agreed the 7th edition of the Security Manual in September 2020. It is now published as ITU-T Technical Report XSTR-SEC-MANUAL. The Security Manual is a major ITU-T promotion tool that highlights in an easy-to-understand fashion the important security work of ITU-T. The 7th edition includes information on 43 new ITU-T Recommendations.

Discussion was held on the best way to timely include future work that would benefit from being part of the next edition.

b) [Successful use of security standards](https://www.itu.int/pub/T-TUT-SEC-2020-1)

SG17 agreed the 2nd edition to XSTR-SUSS, *Technical Report on successful use of security standards* in September 2020. The 2nd edition presents further 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).

c) [ICT Security Standards Roadmap](https://www.itu.int/en/ITU-T/studygroups/com17/ict/Pages/default.aspx)

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) of approved standards, which is an important tool for standard developers in respect of avoiding duplication.

At the April 2021 SG17 meeting, 168 standards were added to Part 2 of the roadmap. In addition, a proposal was received as a first attempt at updating IdM related standard efforts in Part 6 of the roadmap; refer to the Lead Study Group report on identity management.

At the Aug/Sep 2021 SG17 meeting, 57 standards were added to Part 2 of the roadmap.

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

SG17 also continues updating the Security Compendium that provides information on ITU security standardization activities, including the catalogue of ITU-T Recommendations dealing with security and the catalogue of ITU-T approved security definitions.

At the April 2021 SG17 meeting, 198 definitions, 157 abbreviations and 23 Recommendations were added to the Compendium.

At the Aug/Sep 2021 SG17 meeting, 99 definitions, 89 abbreviations and 13 Recommendations were added to the Compendium.

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

1. No new update to security contacts (see Annex 3) since SG17 March 2018 meeting.
2. In this reporting period, SG17 received and treated liaison statements on security matters coming from: ITU-D Q3/2; ITU-R WP4C, WP 5A, WP 5D; ITU-T SG2, SG3, SG5, SG11, SG13, SG15, SG16, Q22/16, SG20, TSAG, FG-AI4EE, FG-AN, FG-QIT4N, FG-VM; JCA-IMT2020; SCV.
3. In this reporting period, SG17 sent liaison statements to: ITU FIGI; ITU-R WP 5D; ITU-T SG2, SG3, SG5, SG9, SG11, SG12, SG13, SG15, SG16, SG20, FG-QIT4N WG1/2, FG-VM, JCA-IMT2020, SCV.

# **5 Collaboration with other organizations**

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

a) In this reporting period, SG17 received and treated liaison statements on security matters coming from 3GPP TSG SA3; ETSI TC ITS, ETSI SAGE, ETSI ISG QKD; IEEE 802.1; ISO/IEC JTC1/SC27/WG1, WG3, WG4, WG5; OASIS.

b) In this reporting period, SG17 sent liaison statements to: OASIS; ISO/TC 307/WG2, ISO/TC 307/JWG 4, ISO/IEC JTC 1/SC27/WG2, ISO/IEC JTC 1/SC27/WG1, 2, 3, 5, ISO/IEC JTC 1 SC41; ETSI ISG-QKD; 3GPP TSG SA3; GSMA FASG/GSG; W3C DID WG; NIST; FIDO Alliance; UPU; RAISE Forum.

## **Annex 1 Achievements of ITU-T Study Groups on Security (4 September 2020 – 3 September 2021)**

**a) Recommendations approved**

|  |  |  |
| --- | --- | --- |
| **SG** | **No.** | **Title** |
| SG9 | J.1204J.stov-sec | The security framework of a smart TV operating system *(Approved 2020-08-13)* |
| SG13 | Y.3055Y.trust-pdm | Framework for trust based personal data management *(Approved 2020-09-29)* |
| SG13 | Y.3802Y.QKDN\_Arch | Quantum key distribution networks - Functional architecture *(Approved 2020-12-07)* |
| SG13 | Y.3803Y.QKDN\_KM | Quantum key distribution networks – Key management *(Approved 2020-12-07)* |
| SG13 | Y.3804Y.QKDN-CM | Quantum key distribution networks - Control and management *(Approved 2020-09-29)* |
| SG17 | X.1046X.SDSec | Framework of software-defined security in software-defined networks/network functions virtualization networks *(Approved 2020-12-14)* |
| SG17 | X.1052 | Information security management processes for telecommunication organizations *(Approved 2020-10-29)* |
| SG17 | X.1054rev | Information security, cybersecurity and privacy protection - Governance of information security *(Approved 2021-04-30)* |
| SG17 | X.1060 X.framcdc | Framework for the creation and operation of a cyber defence center *(Approved 2021-06-29)* |
| SG17 | X.1061 X.ciag | Cyber insurance acquisition guideline *(Approved 2021-08-21)* |
| SG17 | X.1217 X.fgati | Guidelines for applying threat intelligence in telecommunication network operation *(Approved 2021-01-07)* |
| SG17 | X.1218X.rdmase | Requirements and Guidelines for Dynamic Malware Analysis in a Sandbox Environment *(Approved 2020-10-29)* |
| SG17 | X.1233 X.gcims | Guidelines for countering spam over instant messaging *(Approved 2021-09-03)* |
| SG17 | X.1368 X.secup-iot | Secure firmware/software update for Internet of things (IoT) devices *(Approved 2021-01-07)* |
| SG17 | X.1374X.itssec-3 | Security requirements for external interfaces and devices with vehicle access capability *(Approved 2020-10-29)* |
| SG17 | X.1375X.itssec-4 | Guidelines for intrusion detection system for in-vehicle networks *(Approved 2020-10-29)* |
| SG17 | X.1376 X.mdcv | Security-related misbehaviour detection mechanism using big data for connected vehicles *(Approved 2021-01-07)* |
| SG17 | X.1400X.dlt-td | Terms and definitions for distributed ledger technology *(Approved 2020-10-29)* |
| SG17 | X.1404X.sa-dlt | Security assurance for distributed ledger technology *(Approved 2020-10-29)* |
| SG17 | X.1405 X.str-dlt | Security threats and requirements for digital payment services based on distributed ledger technology *(Approved 2021-06-29)* |
| SG17 | X.1406 X.stov | Security threats to online voting system using distributed ledger technology *(Approved 2021-07-14)* |
| SG17 | X.1452X.tfss | Guidelines for security services provided by operators *(Approved 2020-10-29)* |
| SG17 | X.1710X.sec-QKDN\_ov | Security framework for quantum key distribution networks *(Approved 2020-10-29)* |
| SG17 | X.1714X.cf-QKDN | Key combination and confidential key supply for quantum key distribution networks *(Approved 2020-10-29)* |
| SG17 | X.1811 X.5Gsec-q | Security guidelines for applying quantum-safe algorithms in 5G systems *(Approved 2021-04-30)* |
| SG20 | Y.4808 Y.IoT-DA-Counterfeit | Digital entity architecture framework to combat counterfeiting in IoT *(Approved 2020-08-29)* |

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

| **SG** | **No.** | **Title** |
| --- | --- | --- |
| SG17 | Cor.1 to XTR.SEC-QKD | Security considerations for quantum key distribution network, Corrigendum *1 (Agreed 2021-04-30)* |
| SG17 | X.sup-csc | Supplement to X.1051: Critical security controls for telecommunication organization information and network security management in support of ITU-T X.1051 *(Agreed 2021-09-03)*  |
| SG17 | TR.XAASL | Framework for security standardization for virtualized services *(Agreed 2021-09-03)* |

**c) Draft Recommendations determined**

|  |  |  |
| --- | --- | --- |
| **SG** | **No.** | **Title** |
| SG17 | X.1234X.gcmms | Guideline for countering Multimedia Messaging Service spam *(Determined 2021-09-03)* |
| SG17 | X.1235X.tecwes | Technologies in countering website spoofing for telecommunication organizations *(Determined 2021-09-03)* |
| SG17 | X.1246 Amd.1 | Technologies involved in countering voice spam in telecommunication organizations *(Determined 2021-09-03)* |
| SG17 | X.1247 Amd.1  | Technical framework for countering mobile messaging spam *(Determined 2021-09-03)* |
| SG17 | X.1333X.sg-rat | Security guidelines for use of remote access tools in Internet-connected control system *(Determined 2021-09-03)* |
| SG17 | X.1369X.ssp-iot | Security requirements and framework for IoT service platform *(Determined 2021-09-03)* |
| SG17 | X.1407X.srip-dlt | Security requirements for intellectual property management based on distributed ledger technology *(Determined 2021-09-03)* |
| SG17 | X.1453X.strvms | Security threats and requirements for video management system *(Determined 2021-09-03)* |
| SG17 | X.1643X.sgcc | Security guidelines for container in cloud computing environment *(Determined 2021-09-03)* |
| SG17 | X.1752X.sgBDIP | Security guidelines for big data infrastructure and platform *(Determined 2021-09-03)* |
| SG17 | X.1812X.5Gsec-t | Security framework based on trust relationship in 5G ecosystem *(Determined 2021-09-03)* |

**d) 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.3057 Y.trust-index | A trust index model for ICT infrastructures and services *(Consented 2021-07-16)* |
| SG13 | Y.3805Y.QKDN\_SDNC | Quantum key distribution networks - Software defined networking control *(Consented 2021-07-16)* |
| SG13 | Y.3806Y.QKDN-qos-req | Quantum key distribution networks - Requirements for QoS assurance *(Consented 2021-07-16)* |
| SG17 | X.1011X.rf-csap | Reference framework for continuous protection of service access process *(Consented 2021-09-03)* |
| SG17 | X.1047X.nsom-sec | Security requirements and architecture for network slice orchestration and management *(Consented 2021-09-03)* |
| SG17 | X.1408X.das-mgt | Security framework for the data access and sharing management system based on DLT *(Consented 2021-09-03)* |
| SG17 | X.1470X.sgos | Security guidelines of web-based online customer service *(Consented 2021-09-03)* |
| SG17 | X.1712X.sec-QKDN\_km | Security requirements and designs for quantum key distribution networks - key management *(Consented 2021-09-03)* |
| SG17 | X.1770X.tf-mpc | Technical framework and application for secure multi-party computation *(Consented 2021-09-03)* |

## **Annex 2 Current work plan of ITU-T Study Groups on Security(status 3 September 2021)**

**a) Recommendations planned for TAP determination**

| **SG** | **Q** | **No.** | **Title** |
| --- | --- | --- | --- |
| SG17 | 2/17 | X.5Gsec-ecs | Security framework for 5G edge computing services |
| SG17 | 2/17 | X.5Gsec-guide | Security guideline for 5G communication system |
| SG17 | 2/17 | X.5Gsec-netec | Security capabilities of network layer for 5G edge computing |
| SG17 | 2/17 | X.5Gsec-message | Security requirements for 5G message service |
| SG17 | 2/17 | X.5Gsec-ssl | Guidelines for classifying security capabilities in 5G network slice |
| SG17 | 2/17 | X.5G-vs | Security requirements for the operation of vertical services supporting ultra reliable and low latency communication (URLLC) in the 5G private networks |
| SG17 | 4/17 | X.tsfpp | Technical security framework for protection of users' personal information while countering mobile messaging spam |
| SG17 | 6/17 | X.iotsec-4 | Security requirements for IoT devices and gateway |
| SG17 | 6/17 | X.sc-iot | Security controls for Internet of Things (IoT) systems |
| SG17 | 6/17 | X.ztd-iot | Security methodology for zero-touch massive IoT deployment |
| SG17 | 6/17 | X.ra-iot\* | Security risk analysis framework for IoT devices *(NWI agreed 2021-09-03)* |
| SG17 | 7/17 | X.rdda | Requirements for data de-identification assurance |
| SG17 | 7/17 | X.sec-grp-mov | Security guideline for group movement service platform |
| SG17 | 7/17 | X.sles | Security measures for location enabled smart office services |
| SG17 | 8/17 | X.BaaS-sec | Guideline on blockchain as a service (BaaS) security |
| SG17 | 8/17 | X.gecds | Guideline on edge computing data security |
| SG17 | 8/17 | X.nssa-cc | Requirements of network security situational awareness platform for cloud computing |
| SG17 | 8/17 | X.sgcnp | Security guidelines for cloud native PaaS |
| SG17 | 8/17 | X.sgdc | Security guidelines for distributed cloud |
| SG17 | 8/17 | X.sgmc | Security guidelines for multi-cloud |
| SG17 | 13/17 | X.1373rev | Secure software update capability for intelligent transportation system communication devices |
| SG17 | 13/17 | X.edrsec | Security guidelines for cloud-based event data recorders in automotive environment |
| SG17 | 13/17 | X.eivnsec | Security guideline for Ethernet-based In-Vehicle networks |
| SG17 | 13/17 | X.evtol-sec | Security guidelines for electric vertical take-off and landing (eVTOL) vehicle in an urban air mobility environment |
| SG17 | 13/17 | X.fstiscv | Framework of security threat information sharing for connected vehicles |
| SG17 | 13/17 | X.itssec-5 | Security guidelines for vehicular edge computing |
| SG17 | 13/17 | X.srcd | Security requirements for categorized data in V2X communication |
| SG17 | 14/17 | X.sa-dsm | Security architecture of data sharing management based on the distributed ledger technology |

**b) Recommendations planned for AAP consent**

| **SG** | **Q** | **No.** | **Title** |
| --- | --- | --- | --- |
| SG9 | 5/9 | J.1204-rev | The security framework of a smart TV operating system |
| SG13 | 6/13 | Y.QKDN-qos-gen | General aspects of QoS (quality of service) on the quantum key distribution network |
| SG13 | 16/13 | Y.QKDN\_BM | Quantum key distribution networks - Business role-based models |
| SG13 | 16/13 | Y.trust-arch | Functional architecture for trust enabled service provisioning |
| SG13 | 19/13 | Y.ccrm | Cloud computing - Framework of risk management |
| SG13 | 23/13 | Y.SBN-TR | Service brokering network framework for trusted reality |
| SG16 | 11/16 | H.235.10 H.235.DTLS | H.323 security: Support of DTLS for media streams |
| SG17 | 1/17 | X.arch-design | Design principles and best practices for security architectures |
| SG17 | 3/17 | X.1051rev2 | Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations |
| SG17 | 4/17 | X.arc-ev | Security architecture for evaluation of technical vulnerabilities |
| SG17 | 7/17 | X.1144rev | eXtensible Access Control Markup Language (XACML) 3.0 |
| SG17 | 7/17 | X.guide-cdd | Security guidelines for combining de-identified data using trusted third party |
| SG17 | 7/17 | X.scpa | Security measures for countering password related online attacks |
| SG17 | 7/17 | X.sg-dtn | Security guidelines for digital twin network |
| SG17 | 7/17 | X.smdtsc | Security measures for digital twin system of smart cities |
| SG17 | 7/17 | X.smsrc | Security measures for smart residential community services |
| SG17 | 7/17 | X.vide | Guideline of visual feature protection and secure sharing mechanisms for de-identification |
| SG17 | 7/17 | X.websec-7 | Reference monitor for online analytics services |
| SG17 | 7/17 | X.saf-dsf | Security assurance framework for digital financial services *(NWI agreed 2021-09-03)* |
| SG17 | 8/17 | X.sa-ec | Security architecture of edge cloud |
| SG17 | 8/17 | X.sr-cphr | Security requirements of cloud-based platform under low latency and high reliability application scenarios |
| SG17 | 13/17 | X.ipscv | Methodologies for intrusion prevention systems for connected vehicles |
| SG17 | 13/17 | X.rsu-sec | Security requirements for road-side units in intelligent transportation systems |
| SG17 | 13/17 | X.idse | Evaluation methodology for in-vehicle intrusion detection system *(NWI agreed 2021-09-03)* |
| SG17 | 14/17 | X.tf-spd-dlt | Technical framework for secure software programme distribution mechanism based on distributed ledger technology *(Deleted 2021-09-03)* |
| SG17 | 14/17 | X.sc-dlt | Security controls for distributed ledger technology |
| SG17 | 14/17 | X.ss-dlt | Security services based on DLT |
| SG17 | 14/17 | X.srcsm-dlt | Security Requirements for Smart Contract Management based on the distributed ledger technology |
| SG17 | 15/17 | X.icd-schemas | Security data schemas for integrated cyber defence solutions |
| SG17 | 15/17 | X.sec\_QKDN\_AA | Authentication and authorization in QKDN using quantum safe cryptography  |
| SG17 | 15/17 | X.sec\_QKDN\_CM | Security requirements and measures for quantum key distribution networks - control and management |
| SG17 | 15/17 | X.sec-QKDN-intrq | Security requirements for integration of QKDN and secure network infrastructures |
| SG17 | 15/17 | X.sec\_QKDN\_tn | Security requirements for quantum key distribution networks - trusted node |
| SG20 | 6/20 | Y.Data.Sec.IoT-Dev | Requirements of data security for the heterogeneous IoT devices |
| SG20 | 6/20 | Y.oneM2M.SEC.SOL | oneM2M Security Solutions |

**c) Technical Reports and Technical Papers planned for agreement**

| **SG** | **Q** | **No.** | **Title** |
| --- | --- | --- | --- |
| SG13 | 16/13 | Y.supp.trust-roadmap | Standardization roadmap on Trustworthy Networking and Services including Quantum Enhanced Networks |
| SG15 | 11/15 | G.Sup.otnsec | OTN security |
| SG17 | 1/17 | TP.sec-arch | Technical Paper: Implications and further considerations of security architecture patterns *(Deleted 2021-09-03)* |
| SG17 | 2/17 | TR.zt-acp | Technical Report: Guideline for zero trust based access control platform in telecommunication network *(NWI agreed 2021-09-03)* |
| SG17 | 4/17 | X.Suppl.cs-MLTR.cs-ml | Supplement to X.1231: Countering spam based on machine learning *(WI change agreed 2021-09-03)* |
| SG17 | 2/17 | XSTP-5gsec-RM | 5G security standardization roadmap *(NWI agreed 2021-09-03)* |
| SG17 | 6/17 | TR.ibc-cd | Technical report: Guideline for identity-based cryptosystems used for cross-domain secure communications |
| SG17 | 7/17 | TR-cta | Technical Report: Use cases of contact tracing applications to prevent spread of infectious diseases |
| SG17 | 14/17 | TR.qs-dlt | Technical Report: Guidelines for quantum-safe DLT system |
| SG17 | 15/17 | TR.hybsec-qkdn | Technical Report: Overview of hybrid security approaches applicable to QKD |
| SG17 | 15/17 | TR.sec-ai | Technical Report: Guidelines for security management of using artificial intelligence technology  |
| SG17 | 15/17 | TR.sgfdcml | Technical Report: Security guidelines for FHE-based data collaboration in machine learning |

## **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 | - Fernando Masami MatsubaraRapporteur Q27/16 | m.matsubara@fr.merce.mee.com  |
| ITU-T SG17 | - Heung Youl YoumSG17 Chairman- Mohamed ElhajCo-Rapporteur Q1/17- Juhee KiCo-Rapporteur Q1/17- Xiaoya YangITU-T SG17 Counsellor | hyyoum@sch.ac.krmohamed.elhaj@tpra.gov.sd eye@iitp.krxiaoya.yang@itu.inttsbsg17@itu.int |
| ITU-T SG20 | - Abdulhadi AbouAlmalLiaison officer from SG20 to SG17 | aalmal@etisalat.ae |
| 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-TD3928R3**](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3928/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 as well as related biometrics applications. Other ITU-T study groups (SG2, SG3, SG11, SG13, SG 16 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 2020 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 2021):

# **2 Ongoing work**

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

# **3 Workshops**

SG17 held two workshops in the IdM area during this reporting period:

* The first workshop took place during the *BDT Emerging technology week 2021*, held 5-9 July 2021. The session SG17 organized was on *Blockchain and Decentralized Identity for enabling online trust and accountability*. The report, including presentation slides, is in [TD3957](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3957/en).
* The second was held 11 August 2021 in conjunction with SG16 and SG20 and WHO on *digital vaccination certificate*. The report is in [TD3868](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3868/en).

# **4 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, SG13 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.

JCA-IdM met twice during this reporting period. At the 23 April 2021 e-meeting, reports were shared from FIDO Alliance, FIGI, ISO/IEC JTC1/SC27/WG5, ISO/TC307/JWG 4, NIST, RAISE Forum, W3C DID WG, ITU-T SG3 and SG17. At the 27 August 2021 e-meeting, reports were shared from FIDO Alliance, ISO/IEC JTC1/SC27/WG5, ISO/TC307/JWG 4, NIST, RAISE Forum, W3C DID WG and ITU-T Q10/17.

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

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

SG17 agreed to have the dual numbering of the SG3 Recommendation D.1140, *Policy Framework including principles for digital identity infrastructure*, as X.1261.

In this reporting period, SG17 received and treated liaison statements on identity management matters coming from ITU-T SG2, SG5, SG11, SG13, SG16, SG20; ISO/IEC JTC 1/SC 27/WG 4 and ISO/IEC JTC 1/SC 27/WG 5.

In this reporting period, SG17 sent liaison statements to FIDO Alliance, W3C DID WG, OASIS, RAISE Forum, NIST, UPU, ISO/IEC JTC 1/SC 27/WG 5, ISO/TC 307/WG 2&JWG 4, ITU-T SGs 2, 3, 5, 9, 11, 12, 13, 15, 16, 20, ITU FIGI.

## **Annex 1 Achievements of ITU-T Study Groups on Identity Management (4 September 2020 - 3 September 2021)**

1. **Approved Recommendations**

|  |  |  |
| --- | --- | --- |
| **SG** | **No** | **Title** |
| SG3SG17 | D.1140X.1261\*\*\* | Policy Framework including principles for digital identity infrastructure *(Approved 2020-08-28)* |
| SG17 | X.1252rev | Baseline identity management terms and definitions *(Approved 2021-04-30)* |
| SG17 | X.1254rev | Entity authentication assurance framework *(Approved 2020-09-03)* |
| SG17 | X.1279X.eaasd | Framework of enhanced authentication using telebiometrics with anti-spoofing detection mechanisms *(Approved 2020-09-03)* |
| SG20 | Y.4476Y.IoT-rf-dlt | OID-based Resolution framework for transaction of distributed ledger assigned to IoT resources *(Approved 2021-02-06)* |

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

1. **Approved Supplements, Technical Reports**

|  |  |  |
| --- | --- | --- |
| **SG** | **No** | **Title** |
|  |  |  |

1. **Consented/Determined Recommendations**

|  |  |  |
| --- | --- | --- |
| **SG** | **No** | **Title** |
| SG17 | X.501Amd.1 | Information technology - Open Systems Interconnection -The Directory: Models *(Consented 2021-09-03)* |
| SG17 | X.509Cor.1 | Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks *(Consented 2021-09-03)* |
| SG17 | X.672rev | Information technology – Open Systems Interconnection – Object identifier resolution system (ORS) *(Consented 2021-09-03)* |
| SG17 | X.1080.2X.b2m | Biology to machine protocol *(Consented 2021-09-03)* |
| SG20 | Y.4809Y.IoT-ITS-ID\* | IoT Identifiers for Intelligent Transport Systems *(Determined 2021-05-27)*  |

Notes:

\* Marked draft Recommendations were determined; all non-marked were consented.

## **Annex 2 Current work plan of ITU-T Study Groups on Identity Management (status 3 September 2021)**

|  |  |  |
| --- | --- | --- |
| **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.510Amd.1 | Information Technology – Open systems Interconnection - The Directory: Protocol specifications for secure operations |
| SG17 | X.1250rev | Baseline capabilities for enhanced global identity management and interoperability |
| SG17 | X.1251rev | A framework for user control of digital identity |
| SG17 | X.gpwd | Threat analysis and guidelines for securing password and password-less authentication solutions |
| SG17 | X.pet\_auth | Entity authentication service for pet animals using telebiometrics |
| SG17 | X.pki-em | Information technology – Public-Key Infrastructure: Establishment and maintenance |
| SG17 | X.oob-sa | Framework for out-of-band server authentication using mobile devices *(NWI agreed 2021-09-03)* |
| SG17 | X.srdidm | Security requirements for decentralized identity management systems using distributed ledger technology *(NWI agreed 2021-09-03)* |
| SG17 | X.tec-idms | Management and protection techniques for user data protection in distributed identity systems |
| 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 | 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-TD3929R1**](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3929/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., Question 11/17) 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 2020 meeting sent its previous LSG report to TSAG, of ITU-T SGs concerning their work on languages and description techniques (status: 3 September 2021).

# **2 Ongoing work**

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

# **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).

**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.

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 and subsequently approved.

**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.

The set of revised SDL Recommendations Z.100 to Z.107 were consented on 30 April 2020 and subsequently approved. The updated Z.100 Implementer’s guide Z.Imp100 version 4.0.1 was also approved. 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 11/17 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 and subsequently approved. Another set of nine revised TTCN-3 Recommendations were consented on 3 September 2021.

# **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 11/17 has a close relationship with the SDL Forum Society, which focuses on the ITU-T System Design Languages (SDL). Society members are involved in ongoing Q11/17 work.

Question 11/17 also has a close relationship with ETSI TC MTS on TTCN-3.

## **Annex 1Achievements of ITU-T Study Groups on languages and description techniques (4 September 2020 – 3 September 2021)**

1. **Recommendations approved**

| **SG** | **No** | **Title** |
| --- | --- | --- |
| SG17 | X.680 (revised) | Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation *(Approved 2021-02-13)* |
| SG17 | X.681 (revised) | Information technology - Abstract Syntax Notation One (ASN.1): Information object specification *(Approved 2021-02-13)* |
| SG17 | X.682 (revised) | Information technology - Abstract Syntax Notation One (ASN.1): Constraint specification *(Approved 2021-02-13)* |
| SG17 | X.683 (revised) | Information technology - Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications *(Approved 2021-02-13)* |
| SG17 | X.690 (revised) | Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) *(Approved 2021-02-13)*  |
| SG17 | X.691 (revised) | Information technology - ASN.1 encoding rules: Specification of Packed Encoding Rules (PER) *(Approved 2021-02-13)*  |
| SG17 | X.692 (revised) | Information technology - ASN.1 encoding rules: Specification of Encoding Control Notation (ECN) *(Approved 2021-02-13)* |
| SG17 | X.693 (revised) | Information technology - ASN.1 encoding rules: XML Encoding Rules (XER) *(Approved 2021-02-13)* |
| SG17 | X.694 (revised) | Information technology - ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1 *(Approved 2021-02-13)*  |
| SG17 | X.695 (revised) | Information technology - ASN.1 encoding rules: Registration and application of PER encoding instructions *(Approved 2021-02-13)* |
| SG17 | X.696 (revised) | Information technology - ASN.1 encoding rules: Specification of Octet Encoding Rules (OER) *(Approved 2021-02-13)* |
| SG17 | X.697 (revised) | Information technology - ASN.1 encoding rules: Specification of JavaScript Object Notation Encoding Rules (JER) *(Approved 2021-02-13)* |
| SG17 | X.894 Cor. 2 | Generic applications of ASN.1 – Cryptographic Message Syntax – Cor. 2 *(Approved 2021-02-13)* |
| SG17 | Z.100 (revised) | Specification and Description Language - Overview of SDL-2010 *(Approved 2021-06-13)* |
| SG17 | Z.100 Annex F2(revised) | Specification and Description Language - Overview of SDL-2010 - SDL formal definition: Static semantics *(Approved 2021-06-13)* |
| SG17 | Z.100 Annex F3(revised) | Specification and Description Language - Overview of SDL-2010 - SDL formal definition: Dynamic semantics *(Approved 2021-06-13)* |
| SG17 | Z.101 (revised) | Specification and Description Language - Basic SDL-2010 *(Approved 2021-06-13)* |
| SG17 | Z.102 (revised) | Specification and Description Language - Comprehensive SDL-2010 *(Approved 2021-06-13)* |
| SG17 | Z.103 (revised) | Specification and Description Language - Shorthand notation and annotation in SDL-2010 *(Approved 2021-06-13)* |
| SG17 | Z.104 (revised) | Specification and Description Language - Data and action language in SDL-2010 *(Approved 2021-06-13)* |
| SG17 | Z.105 (revised) | Specification and Description Language - SDL-2010 combined with ASN.1 modules *(Approved 2021-06-13)* |
| SG17 | Z.106 (revised) | Specification and Description Language - Common interchange format for SDL-2010 *(Approved 2021-06-13)* |
| SG17 | Z.107 (revised) | Specification and Description Language - Object-oriented data in SDL-2010 *(Approved 2021-06-13)* |
| SG17 | Z.161 (revised) | Testing and Test Control Notation version 3: TTCN-3 core language *(Approved 2020-10-29)* |
| SG17 | Z.161.3 (revised) | Testing and Test Control Notation version 3: TTCN-3 language extensions: Advanced parameterization *(Approved 2020-10-29)* |
| SG17 | Z.161.4 (revised) | Testing and Test Control Notation version 3: TTCN-3 language extensions: Behaviour types *(Approved 2020-10-29)* |
| SG17 | Z.161.6 (revised) | Testing and Test Control Notation version 3: TTCN-3 Language extensions: Advanced Matching *(Approved 2020-10-29)* |
| SG17 | Z.161.7 (revised) | Testing and Test Control Notation version 3: TTCN-3 Language extensions: Object-Oriented Features *(Approved 2020-10-29)* |
| SG17 | Z.165.1 (revised) | Testing and Test Control Notation version 3: TTCN-3 language extensions: Extended TRI *(Approved 2020-10-29)* |
| SG17 | Z.166 (revised) | Testing and Test Control Notation version 3: TTCN-3 control interface (TCI) *(Approved 2020-10-29)* |
| SG17 | Z.167 (revised) | Testing and Test Control Notation version 3: Using ASN.1 with TTCN-3 *(Approved 2020-10-29)* |
| SG17 | Z.169 (revised) | Testing and Test Control Notation version 3: Using XML schema with TTCN-3 *(Approved 2020-10-29)* |

1. **Recommendations consented**

| **SG** | **No** | **Title** |
| --- | --- | --- |
| SG17 | Z.161 (revised) | Testing and Test Control Notation version 3: TTCN-3 core language (*Consented 2021-09-03)* |
| SG17 | Z.161.2 (revised) | Testing and Test Control Notation version 3: TTCN-3 language extensions: Configuration and deployment support (*Consented 2021-09-03)* |
| SG17 | Z.161.3 (revised) | Testing and Test Control Notation version 3: TTCN-3 language extensions: Advanced parameterization (*Consented 2021-09-03)* |
| SG17 | Z.161.4 (revised) | Testing and Test Control Notation version 3: TTCN-3 language extensions: Behaviour types |
| SG17 | Z.161.7 (revised) | Testing and Test Control Notation version 3: TTCN-3 language extensions: Object-oriented features (*Consented 2021-09-03)* |
| SG17 | Z.167 (revised) | Testing and Test Control Notation version 3: Using ASN.1 with TTCN-3 (*Consented 2021-09-03)* |
| SG17 | Z.168 (revised) | Testing and Test Control Notation version 3: The IDL to TTCN-3 mapping (*Consented 2021-09-03)* |
| SG17 | Z.169 (revised) | Testing and Test Control Notation version 3: Using XML schema with TTCN-3 (*Consented 2021-09-03)* |
| SG17 | Z.171 (revised) | Testing and Test Control Notation version 3: Using JSON with TTCN-3 (*Consented 2021-09-03)* |

## **Annex 2Current work plan of ITU-T Study Groups on languages and description techniques (status 3 September 2021)**

**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.

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