|  |  |  |
| --- | --- | --- |
| ITU logo | INTERNATIONAL TELECOMMUNICATION UNION**TELECOMMUNICATIONSTANDARDIZATION SECTOR**STUDY PERIOD 2017-2020 | TSAG-R21 |
| **TSAG** |
| **Original: English** |
| **Question(s):** | N/A | Virtual, 11-18 January 2021 |
| **REPORT** |
| **Source:** | TSAG |
| **Title:** | Report of the seventh TSAG meeting (virtual, 11-18 January 2021) - Endorsed set of Questions for Study Group 17 |
| **Purpose:** | Admin |
| **Contact:** | TSAG Secretariat | E-mail: tsbtsag@itu.int |

|  |  |
| --- | --- |
| **Keywords:** | TSAG; Updated Questions |
| **Abstract:** | This Report contains the clean text of the Questions agreed by Study Group 17 to be submitted to WTSA, which were endorsed at the virtual TSAG meeting, 11-18 January 2021. This set of Questions became effective on 18 January 2021, for the remainder of the study period. |

**CONTENTS**

1 Introduction 4

2 Wording of Questions 5

A Question 1/17 – Security standardization strategy and coordination 5

A.1 Motivation 5

A.2 Question 6

A.3 Tasks 6

A.4 Relationships 7

B Question 2/17 – Security architecture and network security 9

B.1 Motivation 9

B.2 Question 10

B.3 Tasks 10

B.4 Relationships 11

C Question 3/17 – Telecommunication information security management and security services 12

C.1 Motivation 12

C.2 Question 12

C.3 Tasks 13

C.4 Relationships 13

D Question 4/17 – Cybersecurity and countering spam 15

D.1 Motivation 15

D.2 Question 16

D.3 Tasks 18

D.4 Relationships 19

E Question 6/17 – Security for telecommunication services and Internet of Things 20

E.1 Motivation 20

E.2 Question 20

E.3 Tasks 21

E.4 Relationships 22

F Question 7/17 – Secure application services 23

F.1 Motivation 23

F.2 Question 24

F.3 Tasks 24

F.4 Relationships 24

G Question 8/17 – Cloud computing and big data infrastructure security 26

G.1 Motivation 26

G.2 Question 27

G.3 Tasks 27

G.4 Relationships 28

H Question 10/17 – Identity management and telebiometrics architecture and mechanisms 29

H.1 Motivation 29

H.2 Question 30

H.3 Tasks 31

H.4 Relationships 32

I Question 11/17 – Generic technologies (such as Directory, PKI, Formal languages, Object Identifiers) to support secure applications 33

I.1 Motivation 33

I.2 Question 36

I.3 Tasks 37

I.4 Relationships 38

J Question 13/17 – Intelligent transport system (ITS) security 40

J.1 Motivation 40

J.2 Question 40

J.3 Tasks 41

J.4 Relationships 41

K Question 14/17 – Distributed ledger technology (DLT) security 43

K.1 Motivation 43

K.2 Question 43

K.3 Tasks 44

K.4 Relationships 44

L Question 15/17 – Security for/by emerging technologies including quantum-based security 45

L.1 Motivation 45

L.2 Question 46

L.3 Tasks 46

L.4 Relationships 47

# Introduction

This document contains the clean text of the Questions agreed by Study Group 17 to be submitted to WTSA, which were endorsed at the virtual TSAG meeting, 11-18 January 2021. This set of Questions became effective on 18 January 2021, for the remainder of the study period.

Table 1 lists the Questions endorsed and their relationships to the previously in-force set of Questions. It should be noted that Questions 5/17, 9/17 and 12/17 were deleted, with the remaining study items and tasks transferred to other Questions, as indicated in Table 1.

Table 1 – Map of in-force SG17 Questions (endorsed, left) to the previous ones (right)

| New number | Current Question title | Status | Previous number | Previous Question title |
| --- | --- | --- | --- | --- |
| 1/17 | Security standardization strategy and coordination | Continued | 1/17 | Telecommunication/ICT security coordination  |
| 2/17 | Security architecture and network security | Continued | 2/17 | Security architecture and framework  |
| 3/17 | Telecommunication information security management and security services | Continued | 3/17 | Telecommunication information security management  |
| 4/17 | Cybersecurity and countering spam | Continuation of Questions 4/17 and 5/17 | 4/17 | Cybersecurity  |
| 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  |
| 7/17 | Secure application services | Continued | 7/17 | Secure application services  |
| 8/17 | Cloud computing and Big data infrastructure security | Continued | 8/17 | Cloud computing and big data infrastructure security  |
| 10/17 | Identity management and telebiometrics architecture and mechanisms | Continuation of Questions 9/17 and 10/17 | 9/17 | Telebiometrics  |
| 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 Questions 11/17 and 12/17 | 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  |
| 12/17 | Formal languages for telecommunication software and testing  |
| 13/17 | Intelligent transport system security | Continued | 13/17 | Security aspects for Intelligent Transport System  |
| 14/17 | Distributed Ledger Technology (DLT) security | Continued | 14/17 | Security aspects for distributed ledger technologies  |
| 15/17 | Security for/by emerging technologies including quantum-based security | New | – | – |

# Wording of Questions

## Question 1/17 – Security standardization strategy and coordination

(Continuation of Question 1/17)

### Motivation

Security threats to telecommunication, and Information and Communication Technologies (ICTs) and infrastructure remain increasingly complex. Efforts over the years to secure the infrastructure have been somewhat fragmented and reactionary, and so far have not produced the desired level of protection against threats in a timely manner. The economic impact of such attacks and threats has been huge, resulting in several financial and organizational losses to governments and entities. Intensive, continuous and focused efforts are essential to combat these threats.

This effort is complex and requires the participation of a large number of organizations working on various aspects of security, each within their area of expertise and mandate. This requires coordination, collaboration and cooperation among the various stakeholders, which is a difficult and challenging task.

The subject of security is vast in scope. Security can be applied to almost every aspect of ICTs and networks. There are various approaches to addressing security requirements. These include:

– A bottom-up approach in which experts devise security measures to strengthen and protect a particular domain of the network using specific countermeasures and techniques such as biometrics and cryptography. While fairly common, this is a fragmented approach that often results in uneven determination and application of security measures.

– A top-down approach, which is a high-level and strategic way of addressing security. This approach requires knowledge of the overall picture. It is generally a more difficult approach because it is harder to find experts with comprehensive knowledge of every part of the network and its security requirements than it is to find experts with detailed knowledge of one or two specific areas.

– A combination of bottom-up and top-down approaches, with coordination effort to bring the different pieces together. This has often proved to be extremely challenging when dealing with varying interests and agendas.

This Question produces many deliverables that ITU-T considers as fundamental in promoting its work and deliverables. They also provide valuable resources to the ITU and external organizations. Examples include the ICT Security Standards Roadmap, the Security Manual, the Security Compendia, and the Successful Use of Security Standards. This Question will develop a vision and propose the organizational architecture of SG17. This Question will continue to focus on the coordination and organization of the entire range of telecommunication/ICT security activities within ITU-T and will continue to develop and maintain documentation to support coordination and outreach activities. A top-down approach to security will be used in collaboration and coordination with other study groups and standards development organizations (SDOs). This activity is directed at achieving a more focused effort at the projects and strategic level both internal and external to SG17. This Question supports SG17 activities to ensure that they reflect an efficient process capable of developing high quality, timely, market-driven telecommunication/ICT standards. This Question also addresses the needs of developing countries and Regional Study Groups through the implementation of WTSA Resolution 44 on Bridging the standardization gap.

The security standardization strategy is one of the most important topics across all Questions in SG17. SG17 needs to consider how security standardization architecture and design can improve the development of current and future security work items.

SG17 work on security considers WTSA Resolutions 7, 11, 40, 44, 45, 50, 52, 58, 64, 65, 67, 70, 73, 75, 76, 78, 84, 87, 89, 90, 94, 96, 97 and 98; PP Resolutions 101, 123, 130, 136, 174, 175, 177, 178, 179, 180, 181; 188, 189, 196, 197, 199, 200, 201, 204 and 206; and WTDC Resolutions 21, 23, 34, 45, 47, 54, 58, 59, 63, 64, 67, 69, 78, 79, 80, and 84.

SG17 also supports WSIS action line C5 "Building confidence and security in the use of ICTs" and Objective 2 of the Buenos Aires Action Plan adopted at the 2017 World Telecommunication Development Conference on “Modern and secure telecommunication/ICT infrastructure: Foster the development of infrastructure and services, including building confidence and security in the use of telecommunications/ICTs.”

Technical Reports under responsibility of this Question as of 3 September 2020: TR.sec-manual, XSTR-SUSS.

Texts under development: TP.sec-arch and X.arch-design.

### Question

Study items to be considered include, but are not limited to:

a) What are the deliverables for this Question?

b) What are the processes, work items, work methods and timeline for the Question to achieve the deliverables?

c) What outreach documents (roadmap, security compendia, technical reports, flyers, webpages, etc.) need to be produced and maintained by ITU?

d) What security workshops are needed and how they can be organized?

e) What is needed to build effective relationships with other SDOs in order to advance the work on security?

f) What are the key milestones, success criteria and supporting performance metrics?

g) How can Sector Member and Administration interest in security work be stimulated and how can momentum be sustained?

h) How could telecommunication/ICT security features become more relevant to the marketplace?

i) How can the crucial importance of security and the urgent need to protect global economic interests, which depend on a robust and secure telecommunication/ICT infrastructure, best be promoted to governments and the private sector?

j) What are the security activities under development in other ITU Study Groups and other SDOs?

k) How to address the needs of developing countries and Regional Study Groups in the implementation of WTSA Resolution 44?

l) What is the standardization strategy in support of a comprehensive, coherent telecommunications security solution?

m) How should standardization strategy embrace existing Recommendations on security?

### Tasks

Tasks include, but are not limited to:

a) Act as primary SG17 contact for telecommunication/ICT security coordination matters.

b) Develop and maintain an organizational architecture roadmap – to provide a vision and a detailed plan that determines the level and scope of the security domain for study. The roadmap shall identify all related components (structure, processes) and their inter-relationships, participating organizations and roles. Distinction needs to be made between emerging systems/networks and existing systems/networks

c) Maintain and update the ICT Security Standards Roadmap.

d) Maintain and update the ITU-T Security Compendia.

e) Assist and provide input to TSB in maintaining the Security Manual published as technical report "Security in telecommunications and information technology”.

f) Maintain and update the technical report on the successful use of security standards.

g) Provide guidance on the implementation of telecommunication/ICT security standards.

h) Promote cooperation and collaboration between groups working on telecommunication/ICT security standards development.

i) Review Recommendations and liaisons from other study groups and SDOs as appropriate to assess security coordination implications.

j) Assist in efforts to ensure effective security coordination where necessary.

k) Help direct liaisons from external groups to appropriate study groups in ITU-T.

l) Take ITU-T lead in organizing and planning security workshops and seminars as appropriate.

m) Ensure effective and efficient participation in security coordination efforts with other organizations.

n) Assist in improving the efficiency of SG17 work (e.g., by creating templates, tools, or procedures, performance metrics).

o) Encourage national authorities and operators from developing countries in regions to work together and better contribute to ITU-T SG17 activities in line with the SG17 mandate and in implementing SG17 security Recommendations.

p) Assist SG17 in Bridging Standardization Gap with the aim of supporting WTSA Res. 44, PP Res. 123, and WTDC Res. 47.

q) Achieve effective and efficient participation in security coordination efforts within SG17 to ensure the SG17 work programme reflects the current SG17 security activities and addresses the concerns of the ITU-T membership

r) Development of a comprehensive set of security standardization strategy documents, including architecture documents, for supporting the standardization of security solutions in collaboration with other standards development organizations and ITU-T study groups.

An up-to-date status of work under this Question is contained in the SG 17 work programme at <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

### Relationships

WSIS Action Lines:

C5.

Sustainable Development Goals:

–

Recommendations:

X-series and others related to telecommunication/ICT security.

Questions:

ITU-T Qs 2/17, 3/17, 4/17, 6/17, 7/17, 8/17, 10/17, 11/17, 13/17, 14/17 and 15/17.

Study Groups:

ITU-D; ITU-R; ITU-T SGs 2, 3, 5, 9, 11, 13, 15, 16 and 20; TSAG, including relevant JCAs and FGs.

Standardization bodies:

Alliance for Telecommunications Industry Solutions (ATIS); Cloud Security Alliance (CSA); European Telecommunications Standards Institute (ETSI); Institute of Electrical and Electronics Engineers (IEEE); Internet Engineering Task Force (IETF); ISO/IEC JTC 1/SCs 6 and SC 27, ISO TC 292, ISO TMB; Organization for the Advancement of Structured Information Standards (OASIS); Third Generation Partnership Project (3GPP); Third Generation Partnership Project 2 (3GPP2); Asia-Pacific Telecommunity Standardization Program (ASTAP).

Other bodies:

European Network and Information Security Agency (ENISA); National Institute of Standards and Technology (NIST), one M2M, Regional Asia Information Security Exchange (RAISE) Forum.

## Question 2/17 – Security architecture and network security

(Continuation of Question 2/17)

### Motivation

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

A continued effort to maintain and enhance these security Recommendations to satisfy the needs of emerging technologies (e.g., next generation networks (NGN), security aspects of software-defined networking (SDN)/network function virtualization (NFV), network slicing (NS), service function chain (SFC), multi-access edge computing (MEC),long term evolution/system architecture evolution (LTE/SAE), IMT-2020/5G network and beyond, common security framework and architecture for services/applications, the foundations of artificial intelligence (AI) / machine learning (ML) in supporting the building of confidence and security in the use of ICTs, technical implementation guidance for systems providing end-to-end communications and Internet protocol based networks) and services is required. This effort is reflected by X.1035 and X.1036 that show details of password-authenticated key exchange protocols and policy distribution and enforcement, X.1037 that provides IPv6 security guidelines, X.1038, X.1042, X.1043 and X.1044 that provide security requirements etc. on software-defined networking (SDN) and network function virtualization (NFV), X.1045 that provides customized security services based on service function chain (SFC).

Due to convergence and mobility, telecommunications carrier networks and the associated information systems are exposed to new classes of security threats. The attackers have a deeper reach into networks and require less skill levels with a higher damage propensity. Viruses, hacking and denial of service attacks have become pervasive and they adversely impact network elements and support systems alike.

The telecommunications and information technology industries are seeking cost-effective comprehensive security solutions that are technology agnostic and protect a wide spectrum of networks, services and applications. To achieve such solutions in multi-vendor environment, network security should be designed and optimized around the standard security architectures and standard security technologies. Taking into account the security threats to the telecommunication environment and the current advancement of security countermeasures against the threats, new security requirements and solutions should be investigated. New Recommendations that show how to combine the technology standards and security frameworks are needed to implement comprehensive security for the emerging networks, services and applications.

Recommendations and Supplements under responsibility of this Question as of 3 September 2020: X.800, X.802, X.803, X.805, X.810, X.811, X.812, X.813, X.814, X.815, X.816, X.830, X.831, X.832, X.833, X.834, X.835, X.841, X.842, X.843, X.1031, X.1032, X.1033, X.1034, X.1035, X.1036, X.1037, X.1038, X.1039, X.1040, X.1041, X.1042, X.1043, X.1044, X.1045, and Supplements X.Suppl.2, X.Suppl.3, X.Suppl.15, X.Suppl.16, X.Suppl.23 and X.Suppl.30.

Texts under development: X.nsom-sec, X.rf-csap, X.SDsec (X.1046), X.5GSec-ecs, X.5GSec-guide, X.5Gsec-netec, X.5Gsec-q (X.1811), X.5Gsec-ssl and X.5Gsec-t, X.5Gsec-vs.

### Question

Study items to be considered include, but are not limited to:

a) How should a comprehensive, coherent telecommunications security solution be defined?

b) What is the architecture for a comprehensive, coherent telecommunications security solution?

c) What is the framework for applying the security architecture in order to establish a new security solution?

d) What is the framework for applying the security architecture in order to assess (and consequently improve) an existing security solution?

e) What are the architectural underpinnings for security?

i) What is the architecture for end-to-end security?

ii) What is the open systems security architecture?

iii) What is the security architecture for the mobile environment?

iv) What is the security architecture for evolving networks?

v) What is the security architecture for application services in collaboration with Q7/17?

f) What new security architecture and framework Recommendations are required for providing security solutions in the changing environment?

g) How should architectural standards be structured with respect to existing Recommendations on security?

h) How should architectural standards be structured with respect to the existing advanced security technologies?

i) How should the security framework Recommendations be modified to adapt them to emerging technologies and what new framework Recommendations are required?

j) How are security services applied to provide security solutions?

k) How is telecommunication/ICT infrastructure monitoring applied to provide security solutions?

l) What are the foundations of artificial intelligence / machine learning (AI/ML) in supporting the building of confidence and security in the use of ICT?

m) What are the new security threats and challenges introduced by the emerging network technologies (e.g., SDN, NFV, network slicing, SFC, MEC, LTE/SAE, IMT-2020/5G network and beyond, etc.)?

n) What are the security requirements of IMT-2020/5G network and beyond, and how SG17 can address them?

o) What are common security mechanisms for the emerging networks technologies?

### Tasks

Tasks include, but are not limited to:

a) Development of a comprehensive set of security architecture and framework Recommendations for providing standard security solutions for telecommunications in collaboration with other standards development organizations and ITU-T study groups.

b) Studies and development of Recommendations on a trusted telecommunication network architecture that integrates advanced security technologies.

c) Studies and development of Recommendations on the foundations of AI/ML in supporting the building of confidence and security in the use of ICT.

d) Maintenance and enhancements of Recommendations and Supplements in the X.800-series and X.103x-series.

e) Studies and development of Recommendations on common network security.

f) Study the security requirements of IMT-2020/5G network and beyond, coordinate the related work in various Questions of SG17, be the single point of contact for the security aspect of IMT-2020/5G network and beyond in SG17, and lead the research and development of standards on Security aspects of IMT-2020/5G network and beyond.

An up-to-date status of work under this Question is contained in the SG 17 work programme at <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

### Relationships

WSIS Action Lines:

C5.

Sustainable Development Goals:

–

Recommendations:

X-series and others related to security.

Questions:

ITU-T Qs 1/17, 3/17, 4/17, 6/17, 7/17, 8/17, 10/17, 11/17, 13/17, 14/17 and 15/17.

Study Groups:

ITU-D SG2; ITU-R WP6B; ITU-T SGs 2, 9, 11, 13, 15, 16 and JCA-IMT2020.

Standardization bodies:

Alliance for Telecommunications Industry Solutions (ATIS); European Telecommunications Standards Institute (ETSI); GSM Association (GSMA); Forum for International Irregular Network Access (FIINA); ISO/IEC JTC 1/SC 27 and SC 37; IEC TC 25; ISO TC 12; Internet Engineering Task Force (IETF); Third Generation Partnership Project (3GPP).

## Question 3/17 – Telecommunication information security management and security services

(Continuation of Question 3/17)

### Motivation

For telecommunications organizations, information and the supporting processes, telecommunications facilities, networks and transmission media are important telecommunication business assets. In order for telecommunications organizations to appropriately manage these business assets and to correctly continue the business activity, information security management is extremely necessary. For this reason, Recommendation ITU-T X.1051 was developed to provide code of practice for information security controls for telecommunications organizations.

Based on the code of practice, detailed and specific management areas including risks, assets, governance, management framework and incidents have also been developed together with introducing best practices as Supplement. New areas in relation with Recommendation ITU-T X.1051 should be investigated further. Meanwhile, the series of Recommendations have to be maintained and updated reflecting the latest information security management issues. The aim is to develop a set of Recommendations on security management for telecommunications based on Recommendation ITU-T X.1051 in ITU‑T.

In parallel with developing Recommendations for detailed and specific management areas based on Recommendation ITU-T X.1051, the new areas of telecommunication and ICT security services, e.g., Cyber Defence Center (CDC) services including Security Operation Center (SOC) services, Managed Security Services (MSSs), and Computer Incident Response Teams (CIRTs) services, lifecycle management for security controls and effective risk management, and management of personally identifiable information which request emergent and global countermeasures should be considered. Those areas are not only in information security but also covers aspects in cybersecurity. Therefore, the studies particularly should focus on management aspects on above new areas in information security and cybersecurity.

In the course of the studies, a full collaborative effort between ITU-T and ISO/IEC JTC 1 will be continued to ensure the widest possible compatibility of security solutions. The success of solutions developed as national standards in many countries also need to be considered.

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

Recommendations and Supplements under responsibility of this Question as of 3 September 2020: E.409 (in conjunction with SG2), X.1051, X.1052, X.1053, X.1054, X.1055, X.1056, X.1057, X.1058, X.1059 and Supplements X.Suppl.13, Suppl.27, Suppl.32 and Suppl.34.

Texts under development: X.1051rev2, X.1052-rev, X.1054-rev, X.ciag, X.fram-cdc and X.sup-csc.

### Question

Study items to be considered include, but are not limited to:

a) How should specific security management issues for telecommunications organizations be identified?

b) How should measurement of security management in telecommunications be identified and managed?

c) How should control objectives and controls be mapped and integrated into organizational management and operational aspects in telecommunication organizations?

d) How should concepts and principles for the governance of information security, by which organizations can evaluate, direct, monitor and communicate the information security-related activities within the organization be applied?

e) How should the adoption of risk treatment option to manage the impact of a security incident?

f) How should best practices providing directions in the security services, e.g., CDC services including SOC services, MSSs and CIRT services, be applied?

g) How should information security management for telecommunications organizations be properly implemented by using the existing standards (ITU-T, ISO/IEC and others)?

h) How should management of personally identifiable information be implemented and effective?

i) What enhancements to existing Recommendations under review or new Recommendations under development should be adopted to reduce impact on climate changes (e.g., energy savings, reduction of greenhouse gas emissions, implementation of monitoring systems) either directly or indirectly in telecommunication and ICT or in other industries?

### Tasks

Tasks include, but are not limited to:

a) Study and develop a framework of information security management functions described in Recommendation ITU-T X.1051.

b) Study and develop a methodology to implement information security management for telecommunications organizations based on the existing standards (ITU-T, ISO/IEC and others).

c) Study and develop a framework/guidelines for the security services, e.g. CDC services including SOC services, MSSs and CIRT services.

d) Study and develop guidelines for lifecycle management for security controls

e) Study and develop guidelines for effective risk management e.g. risk cyber insurance acquisition for risk treatment

f) Study and develop guidelines for management of personally identifiable information.

g) Propose outline of new Recommendations.

h) Assess the outputs of above activities in view of usability for telecommunications facilities and services.

i) Produce draft Recommendations.

j) Maintenance and enhancements of Recommendations in the X.105x-series.

An up-to-date status of work under this Question is contained in the SG 17 work programme at <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

### Relationships

WSIS Action Lines:

C5.

Sustainable Development Goals:

–

Recommendations:

X.800-, X.1000-, X.1100- X.1200- and X.1300- series.

Questions:

ITU-T Qs 1/17, 2/17, 4/17, 6/17, 7/17, 8/17, 10/17, 11/17, 13/17, 14/17, 15/17 and 14/15.

Study Groups:

ITU-D; ITU-R; ITU-T SGs 2, 9, 11, 13, 15, 16 and 20.

Standardization bodies:

Asia Pacific Telecommunity Standardization Programme (ASTAP); European Telecommunications Standards Institute (ETSI); ISO/IEC JTC 1/SC 27; ISO/IEC JTC1 SC40, ISO/TC 68, ISO/TC 215; ISO/TC 307, National Institute of Standards and Technology (NIST); Telecommunication Technology Committee (TTC); Third Generation Partnership Project (3GPP); Forum Incident Response and Security Teams (FIRST).

## Question 4/17 – Cybersecurity and countering spam

(Continuation of Questions 4/17 and 5/17)

### Motivation

The telecommunications landscape is constantly changing, and with it, requirements for associated telecommunication/ICT security. In this cyber environment, threats and attacks to telecommunication/ICT are constantly evolving to be more sophisticated and more targeted and cause a complex range of problems to users, service providers, operators and networks. There is a strong need for developing cybersecurity frameworks and requirements – a set of recommendations including best practices to assist organizations in managing cybersecurity risks.

Cybersecurity frameworks and requirements against threats and attacks consist of a set of components, which should consist of identifying, protecting, detecting, responding, and recovering. Countering cyber-attacks by technical means needs holistic requirements for: mitigating risks, detecting and responding early to incidents, and recovering from their affects; exchanging cybersecurity information such as Cybersecurity Information Exchange techniques (CYBEX) and Structured Threat Information eXpression (STIX); and securing protocols, infrastructures and applications which are used as an integral part of our daily communications.

Artificial intelligence and machine learning are being applied more broadly across industries and applications than ever before. Technical means enabled by artificial intelligence and machine learning should improve the quality and efficiency of the technical activities against threats and attacks. Managed security services (MSS) are services that have been outsourced to a service provider. There are two aspects of managed security services: technical, managerial.

Cybersecurity technologies involve technical supports for managed security services, endpoint detection and response, intrusion prevention/detection, and identification of the source of attackers in order to protect services and personal information including Personally Identifiable Information (PII), and to provide information assurance (IA) among interacting entities.

Cybersecurity information sharing using CYBEX (cybersecurity information exchange framework) techniques and cyber threats intelligence are essential to the protection of telecommunication /ICT infrastructure and to furthering cybersecurity for the telecommunication/ICT providers.

In addition, the aggressive pace of cyber threats evolution requires a review of technical aspects to support cybersecurity procedures, technical policies and frameworks. There is a challenge to achieve a minimum level of harmonization since cybersecurity requires collaboration among all stakeholders.

In the area of cybersecurity challenges, spam has also become a widespread problem causing potential loss of revenue to Internet service providers, telecommunication operators, mobile telecommunication operators and business users around the globe. Furthermore, spam creates problems of information and telecommunication network security while being used as a vehicle for phishing and spreading viruses, worms, spyware and other forms of malware, etc. Therefore, WTSA Resolution 52 instructed the relevant study groups to continue to support ongoing work, in particular in Study Group 17, related to countering spam and accelerate their work on spam in order to address existing and future threats within the remit and expertise of the ITU-T, as appropriate. In addition, it is instructed to continue collaboration with relevant organizations, in order to continue developing, as a matter of urgency, technical Recommendations with a view to exchanging best practices and disseminating information through joint workshops and training sessions, etc., and further instructs Study Group 17 to report regularly to the Telecommunication Standardization Advisory Group on the progress of this resolution.

With the rapid expansion of mobile internet and the convergence of ICT technologies, spam threats become more challenging with new features. The main ingredients of spam have significantly evolved from traditional advertisements and fraud to convergent malicious software such as ransom and targeted attacks. The new generation of spam is also unsolicited and harasses ICT service consumers, but they do even more serious damage than traditional ones. A targeted attack often uses spear phishing, a type of social engineering, to gain access to networks through legitimate means such as email. Ransomware is a type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. Some malwares, especially most ransomwares, can be spread through malicious email attachments and compromised websites. With the evolution of artificial intelligence / machine learning (AI/ML) technology, some communications can be initiated by machines but not humans, such as robocalls, robot chat, automatic text messages and so on. AI/ML algorithms can also make use of personal information more accurately to find target recipients to make large-scale commercial marketing spam or even fraud spam.

With the wide deployment of IMT-2020, Internet of Things and other telecommunication/ICT technologies, spam has also gradually begun to affect the industrial systems.

Countering spam has been recognized as a global problem that requires a multifaceted, comprehensive approach. Study Group 17, as the lead study group on telecommunication security and in supporting the activities of WTSA Resolutions 52, is well-positioned to study the range of potential technical measures to counter spam as it relates to the stability and robustness of the telecommunication network. In addition, technical structure for existing and potential Recommendations on countering spam by technical means has been established to facilitate Recommendation production. Furthermore, new Recommendations should be published to counter new forms of spam.

Recommendations and Supplements under responsibility of this Question as of 3 September 2020: X.1205, X.1206, X.1207, X.1208, X.1209, X.1210, X.1211, X.1212, X.1213, X.1214, X.1215, X.1216, X.1231, X.1232, X.1240, X.1241, X.1242, X.1243, X.1244, X.1245, X.1246, X.1247, X.1248, X.1249, X.1303, X.1303bis, X.1500, X.1500.1, X.1520, X.1521, X.1524, X.1525, X.1526, X.1528, X.1528.1, X.1528.2, X.1528.3, X.1528.4, X.1541, X.1542, X.1544, X.1546, X.1550, X.1570, X.1580, X.1581, X.1582, and Supplements X.Suppl.6, X.Suppl.8, X.Suppl.9, X.Suppl.10, X.Suppl.11, X.Suppl.12, X.Suppl.14, X.Suppl.18, X.Suppl.20, X.Suppl.25 and X.Suppl.29 and Technical Report TR.usm.

Texts under development: X.1246rev, X.1247rev, X.arc-ev, X.fgati (X.1217), X.gcims, X.ics-schema , X.tf-mpc, X.rdmase (X.1218), X.tecwes, X,tfcmms, X.tsfpp, TR.cs-ml and TR.sgfdm,

### Question

Study items to be considered in the context of telecommunication/ICT networks and systems include, but are not limited to:

a) How should telecommunication/ICT providers secure their infrastructure, maintain secure operations and use security assurance mechanisms?

b) What are the security requirements that software, telecommunications protocols, communications systems designers and manufacturers need to consider in the design, development and sharing of best practices in the cyber environment?

c) How should information on vulnerability, weakness and attack measures be shared efficiently to aid in vulnerability life-cycle processes?

d) What requirements and solutions are needed for telecommunication/ICT assurance of composable systems' resilience, security and integrity?

e) What requirements and solutions are needed for telecommunication/ICT accountability, incident response, managed security services, cyber-attack attribution, and threat monitoring and risk communication?

f) What mechanisms are needed for sharing cybersecurity and assurance-related information about cyber-enabled systems, including cloud-based, embedded and composable systems?

g) How can artificial intelligence and machine learning be used to quickly identify and analyse new threats and vulnerabilities?

h) How should telecommunication/ICT providers utilize the threat intelligence to enhance their security activities?

i) How can networks be used to provide critical services, such as use of common alerting protocol, in a secure fashion during national emergencies?

j) What are the set of components of cybersecurity framework that an organization can use to address risks?

k) What are the necessary security guidelines and best practices for identifying, mitigating and reducing impact of cyber threats, including malware, distributed denial of service and social engineering?

l) What kind of technical reports and Recommendations can be developed in support of cybersecurity procedures, technical policies and frameworks?

m) How to understand and identify spam?

n) What are new forms of spam in existing and future networks?

o) What are the serious effects of spam?

p) What are technical factors which contribute to difficulties in identifying the sources of spam?

q) How can new technologies, services and applications, such as instant messaging, social networking, mobile application, Voice Over Long-Term Evolution (VoLTE), and Rich Communication Services (RCS), etc., lead to opportunities to create and spread spam?

r) How can routes, sources and volumes of spam be identified to counter and combat such spam?

s) How can the messaging security be implemented?

t) How can the distribution of malicious software and malware through email be prevented?

u) How can routes, sources and volumes of spam be identified and the amount of investment in facilities and other technical means be estimated to counter and combat such spam?

v) How can a targeted attack using spear phishing be prevented?

w) How can a ransomware distributed through email be prevented?

x) How can AL/ML communication form of spam be identified and prevented?

y) How to protect personal information with the adoption of AI/ML technology to avoid spam message spread?

z) What technical work is already being undertaken within the IETF, 3GPP, GSMA, M3AAWG, in other fora, and by private sector entities to address the problem of spam?

aa) What telecommunication network standardization work, if any, is needed to effectively counter spam as it relates to the stability and robustness of the telecommunication network?

bb) What are the effective and efficient solutions for countering spam?

cc) How are generic and specific requirements developed for information sharing on countering spam?

dd) What are the best practices for countering spam?

### Tasks

Tasks to be considered in the context of telecommunication / ICT networks and systems include, but are not limited to:

a) Collaborate with ITU-T study groups, ETSI, FIRST, IETF, IEEE, ISO/IEC JTC 1, OASIS, OMA, TCG, 3GPP, 3GPP2, and other standardization bodies on cybersecurity.

b) Work on frameworks and Recommendations to address how telecommunication/ICT providers may secure their infrastructure and maintain secure operations and exchange cybersecurity information.

c) Produce a set of Recommendations for providing security solutions for telecommunication/ICT accountability, assurance and incident response and recovery, including technical aspects of managed security services.

d) Study and specify the security techniques and capabilities for service providers to coordinate and exchange information regarding vulnerabilities, platforms, and cyber-attacks.

e) Study and specify cybersecurity framework consisting of a set of components that should consist of identify, protect, detect, respond, and recover.

f) Specify how to use artificial intelligence and machine learning, to quickly identify and analyse new threats and vulnerabilities.

g) Specify how to apply accountability, assurance, and incident response mechanisms in telecommunication/ICT networks.

h) Develop guidelines and techniques to protect personal information and also to protect personally identifiable information (PII) using CYBEX, STIX and TAXII techniques and related security tools.

i) Study and develop a technical guidance to support threats management in terms of identifying source of cyber attackers.

j) Provide assistance to other ITU-T study groups in applying relevant cybersecurity Recommendations for specific security solutions.

k) Develop best practices and guidelines for the sharing of vulnerability information and remedies to aid in vulnerability life-cycle processes.

l) Collaborate with other standards developing organizations (e.g., OASIS to adopt STIX and TAXII into ITU documents).

m) Work on Recommendations and Technical reports on how to address cybersecurity challenges.

n) Act as the lead group in ITU-T on technical means for countering spam, as spam is described by Study Group 2.

o) Identify and examine telecommunication network security risks (at the edges and in the core network) introduced by the constantly changing nature of spam.

p) Identify routes, sources and volumes of spam and estimate the amount of investment in facilities and other technical means to counter and combat such spam.

q) Develop a comprehensive and up-to-date resource list of the existing technical measures for countering spam in telecommunication networks that are in use or under development.

r) Develop new Recommendations for countering existing and emerging forms of spam.

s) Develop a set of technical measures to support messaging security.

t) Develop new Recommendations for preventing malicious software and malware distributed through e-mail.

u) Develop a set of solutions to prevent targeted attacks using spear phishing through e-mail.

v) Develop new Recommendations for preventing ransomware distributed through e-mail.

w) Develop generic and specific requirements for information sharing on countering spam.

x) Determine whether new Recommendations or enhancements to existing Recommendations, including methods to combat delivery of unsolicited email, malware, and other malicious contents, and combat compromised network equipment, such as Botnets, would benefit efforts to effectively counter spam as it relates to the stability and robustness of telecommunication network.

y) Develop a set of solutions or new Recommendations for counting AI/ML communication form spams.

z) Provide regular updates to the Telecommunication Standardization Advisory Group and to the Director of the Telecommunication Standardization Bureau to include in the annual report to Council.

An up-to-date status of work under this Question is contained in the SG 17 work programme at <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>

### Relationships

WSIS Action Lines:

C5.

Sustainable Development Goals:

–

Recommendations:

X-series and others related to security.

Questions:

ITU-T Qs 1/17, 2/17, 3/17, 6/17, 7/17, 8/17, 10/17, 11/17, 13/17, 14/17 and 15/17.

Study Groups:

ITU-D SGs 1 and 2; ITU-T SGs 2, 9, 11, 13, 16 and 20.

Standardization bodies:

European Telecommunications Standards Institute (ETSI); Institute of Electrical and Electronics Engineers (IEEE); Internet Engineering Task Force (IETF); IEC TC 57, IEC TC 292, IEC TC 65/WG10; ISO/IEC JTC 1/SC 27; National Institute of Standards and Technology (NIST); Organization for the Advancement of Structured Information Standards (OASIS); Open Mobile Alliance (OMA); Open Group; Object Management Group (OMG); Third Generation Partnership Project (3GPP); Third Generation Partnership Project 2 (3GPP2); Trusted Computing Group (TCG).

Other bodies:

Anti-Phishing Working Group (APWG); CERT/CC; CIRTs; European Network and Information Security Agency (ENISA); GSM Association (GSMA); Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG); Forum for Incident Response and Security Teams (FIRST); National Institute of Standards and Technology (NIST); Organization for Economic Cooperation and Development (OECD).

## Question 6/17 – Security for telecommunication services and Internet of Things

(Continuation of Question 6/17)

### Motivation

Recommendation ITU-T X.1101 provides the security requirements and framework for multicast communication. Recommendations ITU-T X.1111, X.1112, X.1113 and X.1114 describe the security framework for home network including the device certificate profile, authentication mechanism, and authorization framework. Recommendations ITU-T X.1121, X.1122, X.1123, X.1124, and X.1125 provide a comprehensive specification on security for mobile network. Recommendations ITU-T X.1171, X.1311, and X.1312 specify the privacy framework for mobile NID services, the security framework for USN (ubiquitous sensor network), USN middleware security guideline and security requirements for wireless sensor network routing, respectively. Recommendations ITU-T X.1191, X.1192, X.1193, X.1194, X.1195, X.1196, X.1197 and X.1198 describe a comprehensive set of requirements, mechanisms, and framework for security of IPTV services. Supplements ITU-T X.Suppl.19 and X.Suppl.24 provide security aspects of mobile phones. Recommendation ITU-T X.1331, X.1332 and Supplement ITU-T X.Suppl.26 describes the security aspects of smart grid. Recommendation ITU-T X.1361, X.1362, X.1363, X.1364 and X.1365 provide IoT related security requirements, mechanisms, and frameworks. A continued effort to maintain and enhance these security Recommendations and Supplements to satisfy the needs of new technologies and services is required.

The telecommunication services, networks and IoT refer to the service that allows anyone to access to any desired information in a user-friendly way, anytime and anywhere using any types of device. The telecommunications industry has been experiencing an exponential growth in the area of mobile technology-based telecommunication services. Specifically, security of domain-specific telecommunication services and networks among heterogeneous devices for the application-level technologies such as IoT and smart cities (including Machine to Machine (M2M), RFID, Near Field Communication (NFC) and sensor network), home network, industrial control systems(ex. smart factory), smart grid, embedded subscriber identity module (eSIM), smartphones, and IPTV networks, etc., are crucial for the further development of the industry, network operators and service providers.

Standardization of the best comprehensive security solutions is vital for network operators and service providers that operate in a multi-vendor international telecommunication environment. Due to some specific characteristics of IoT environment (e.g., limited computing power and memory size of the small mobile devices, long lifecycle, customized operating systems and software), providing security and personally identifiable information (PII) protection is an especially challenging task that deserves special attentions and study.

Recommendations and Supplements under responsibility of this Question as of 3 September 2020: X.1101, X.1111, X.1112, X.1113, X.1114, X.1121, X.1122, X.1123, X.1124, X.1125, X.1126, X.1127, X.1171, X.1191, X.1192, X.1193, X.1194, X.1195, X.1196, X.1197, X.1198, X.1311, X.1312, X.1313, X.1314, X.1331, X.1332, X.1361, X.1362, X.1363, X.1364, X.1365, X.1366, X.1367, and Supplements X.Suppl.19, X.Suppl.24 and X.Suppl.26.

Texts under development: X.iotsec-4, X.sc-iot, X.secup-iot (X.1368), X,sg-rat, X.ssp-iot, X.strvms and X.ztd-iot.

### Question

Study items to be considered include, but are not limited to:

a) How should security aspects of telecommunication services and IoT be identified and defined in mobile telecommunication?

b) How should threats behind telecommunication services and IoT be identified and handled?

c) What are the security technologies for supporting telecommunication services and IoT?

d) How should secure interconnectivity in telecommunication services and IoT be kept and maintained?

e) How should security technologies using AI/ML based technologies be studied and developed for telecommunication services and IoT?

f) What security techniques, mechanisms and protocols are needed for new telecommunication services and IoT, especially for new digital content protection services?

g) What are the global security solutions for telecommunication services and IoT (e.g. including services for smart cities, smart grid and ICS (ex. smart factory) which are based on telecommunication/ICT networks)?

h) What are the best practices or guidelines for secure telecommunication services and IoT?

i) What enhancements to existing Recommendations under review or new Recommendations under development should be adopted to reduce impact on climate changes (e.g., energy savings, reduction of greenhouse gas emissions, implementation of monitoring systems) either directly or indirectly in telecommunication/ICT or in other industries?

j) What PII (Personally Identifiable Information) protection and management mechanisms are needed for secure telecommunication services and IoT?

### Tasks

Tasks include, but are not limited to:

a) In collaboration with other ITU-T study groups and standards development organizations, especially with IETF, ISO/IEC JTC 1/SCs 6, 25, 27, 31 and 41, produce a set of Recommendations for providing comprehensive security solutions for secure telecommunication services and IoT.

b) Review existing Recommendations/Standards of ITU-T, ISO/IEC and other standardization bodies in the area of home network, smart grid, smartphone security, IoT and ubiquitous sensor network to identify secure telecommunication services.

c) Study further to define security aspects of telecommunication services and IoT for a multi-vendor international telecommunication environment, and for new services (e.g., those for smart cities, smart grid and ICS (ex. smart factory) which are based on telecommunication/ICT networks).

d) Study and identify security issues and threats in secure telecommunication services and IoT.

e) Study and develop security mechanisms for secure telecommunication services and IoT.

f) Study and develop interconnectivity mechanisms for secure telecommunication services and IoT in a single or multi-vendor telecommunication environment.

g) Study and identify PII protection issues and threats in secure telecommunication services and IoT.

h) Study and develop PII protection and management mechanisms for secure telecommunication services and IoT.

i) Study and develop security technologies utilizing AI/ML based technologies for the secure telecommunication services and IoT.

An up-to-date status of work under this Question is contained in the SG 17 work programme at <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

### Relationships

WSIS Action Lines:

C5.

Sustainable Development Goals:

–

Recommendations:

X-series and others related to security.

Questions:

ITU-T Qs 1/17, 2/17, 3/17, 4/17, 7/17, 8/17, 10/17, 11/17, 13/17, 14/17 and 15/17.

Study Groups:

ITU-R; ITU-T SGs 9, 11, 13, 15, 16 and 20, JCA-IoT and SC&C.

Standardization bodies:

Internet Engineering Task Force (IETF); IEC SEG 6 (Micro Grid), IEC SMB WG3, IEC TCs 57 and 65; ISO/IEC JTC 1/SCs 6, 25, 27, 31 and 41; Open Mobile Alliance (OMA); Third Generation Partnership Project (3GPP), Third Generation Partnership Project 2 (3GPP2).

Other bodies:

Alliance for Telecommunications Industry Solutions (ATIS); China Communications Standards Association (CCSA); European Telecommunications Standards Institute (ETSI); GSM Association (GSMA); M2M Alliance; NFC Forum; National Institute of Standards and Technology (NIST); oneM2M; Telecommunication Technology Committee (TTC); Telecommunications Technology Association (TTA); Universal Plug and Play (UPnP).

## Question 7/17 – Secure application services

(Continuation of Question 7/17)

### Motivation

Recommendations ITU-T X.1141, X.1142, X.1143, X.1144, X.1145, X.1146, X.1147 provide a set of Recommendations on security tokens for authentication/authorization and security architectures for message of network services. Recommendations ITU-T X.1151, X.1152, X.1153, X.1154, X.1155, X.1156, X.1157, X.1158, X.1159 specify guidelines on secure password-based authentication with key exchange and various Trusted Third Party (TTP) services. Recommendations ITU-T X.1161, X.1162, X.1163, and X.1164 specify a comprehensive framework and mechanisms for the security of P2P services. A continued effort to maintain and enhance these security Recommendations to satisfy the needs of emerging technologies and services is required.

The telecommunications industry has been experiencing an exponential growth in TTP (Trusted Third Party) services. Security of telecommunication-based application service including social network service, P2P and TTP service is crucial for the further development of the industry. Secure application protocols play a very critical role for providing secure application service. Standardization of the best comprehensive security solutions is vital for the industry and network operators that operate in a multi-vendor international environment. It is also required to study and develop other types of secure platform, application services such as time stamping services, secure notary services, secure FinTech (open banking, peer-to-peer lending, remittance, mobile wallet, insurance) services, secure OTT (Over The Top) services, and digital twin; use of security assertions as a replacement to the use of certificates in PKI based protocols and PKI application services, etc. Security technologies such as security assertion and access control assertion become very critical in communication networks.

As telecommunication and ICT are developing application services, they are facing two new horizons which need to be studied: applications are generating and processing more and more data, and to support it, artificial intelligence is now required. Secure application services need to be extended to cover the extensive research and market required to study the spectrum of operational and technical aspects of data protection which builds on the existing work on data analytics services.

Regarding Artificial Intelligence, service providers are facing several challenges in particular the selection, onboarding and integration of dozens, if not hundreds, of AI components from open source and industry that they need to package in various form factors (integrated AI applications, AI as more generic platforms, AI as platform as a service, etc.) on various infrastructures (on premise, private cloud, hybrid cloud, public cloud). As when Big Data started, this creates new security interoperability issues, let alone ensuring the confidentiality, integrity, and availability issues for input training data to AI and AI output data. All of this forms a new attack surface for Artificial Intelligence that needs to be studied and developed. Again, it can build on the initial existing work on data analytics services.

Recommendations and Supplements under responsibility of this Question as of 3 September 2020: X.1141, X.1142, X.1143, X.1144, X.1145, X.1146, X.1147, X.1148, X.1149, X.1151, X.1152, X.1153, X.1154, X.1155, X.1156, X.1157, X.1158, X.1159, X.1161, X.1162, X.1163, X.1164, X.1450, X.1451 and Supplements X.Suppl.17, X.Suppl.21 and X.Suppl.22.

Texts under development: X.rdda, X.scpa, X.sec-grp-mov, X.sgos, X,sles, X.smdtsc, X.smsrc, X.tfss (X.1452), X.websec-7 and TR.cta.

### Question

Study items to be considered include, but are not limited to:

a) How should threats behind secure application services be identified and handled?

b) What are the security technologies for providing secure application services?

c) How should secure interconnectivity between application services be kept and maintained?

d) What security techniques or protocols are needed for secure application services?

e) What security techniques or protocols are needed for emerging secure application services, including service platform, FinTech services, OTT services?

f) What are the global security solutions for secure application services and their applications?

g) How to define a strategy for operational and technical data protection for application services?

h) How to define a strategy for protecting Artificial Intelligence attack surface?

### Tasks

Tasks include, but are not limited to:

a) In collaboration with other ITU-T Study Groups and Standards Development Organizations, especially with ISO/IEC JTC 1/SC 27, produce a comprehensive set of Recommendations for providing comprehensive security solutions for application communication services.

b) Review existing Recommendations/Standards of ITU-T and ISO/IEC in the area of secure application services.

c) Study further to define security aspects of secure application services and for emerging new services such as FinTech Services and OTT services.

d) Study and develop security issues and threats in secure application services.

e) Study and develop security mechanisms for secure application services.

f) Study and develop strategies and Recommendations for operational and technical aspects of data protection for application services.

g) Study and develop strategies and Recommendations for protecting Artificial Intelligence attack surface.

An up-to-date status of work under this Question is contained in the SG 17 work programme at <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

### Relationships

WSIS Action Lines:

C5.

Sustainable Development Goals:

–

Recommendations:

X.800 series and others related to security.

Questions:

ITU-T Qs 1/17, 2/17, 3/17, 4/17, 6/17, 8/17, 10/17, 11/17, 14/17, 15/17, 7/13 and 13/17.

Study Groups:

ITU-T SGs 2, 9, 11, 13, 16, and 20.

Standardization bodies:

Internet Engineering Task Force (IETF); European Telecommunications Standards Institute (ETSI); GSM Association (GSMA); ISO/IEC JTC 1/SC 27, ISO/IEC JTC 1/SC 42, ISO/TC 68, ISO/TC 307; Kantara Initiative; Organization for the Advancement of Structured Information Standards (OASIS); Open Mobile Alliance (OMA); World Wide Web Consortium (W3C).

Other bodies:

Council of Europe (COE); European Network and Information Security Agency (ENISA); Fast Identity Online (FIDO) Alliance; International Multilateral Partnership Against Cyber Threats (IMPACT).

## Question 8/17 – Cloud computing and big data infrastructure security

(Continuation of Q8/17)

### Motivation

Cloud computing is a model for enabling service user’s ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services), that can be rapidly provisioned and released with minimal management effort or service provider interaction. The cloud computing model is defined by five essential characteristics (on-demand, delivery over a broad network access, resource pooling, rapid elasticity, self and measured services), five cloud computing service categories, i.e., Software as a Service (SaaS), Communication as a Service (CaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Network as a Service (NaaS), different deployment models (public, private, hybrid…), and flexible extension of service delivery types (core, regional, edge…). The advent of the cloud computing approach as the preferred vehicle for discovering, externalizing, composing, service re-use within workflows, applications, communication enabled applications places new emphasis on the need for security.

Forecasted benefits of cloud computing include flexible and dynamic resource provisioning, and simpler and automated administration of IT infrastructure. Virtualization makes possible to share of nearly unlimited resources, with scalability improvements and massive cost reductions for infrastructure management. The introduction of edge computing enables distribution of cloud capabilities to the edge of the network. This introduces cloud service implementations which have low and deterministic latency and high reliability. However, open systems, shared resources, and inherent interworking of cloud and edge raise many concerns about security, which is perhaps the most important barrier to the adoption of cloud computing. Moving to the cloud implies to shifting from safe, traditional, in-house IT systems to unsafe, “cloudified”, open infrastructures. It thus requires in-depth rethinking of security.

Cloud computing was considered for several years as service-centric IT and controlled by Internet players. However, telecommunication players have an important role to play in the emerging cloud computing market and ecosystem. As cloud services are delivered through telecommunication networks, telecommunication players should guarantee a high assurance level. Strong but flexible security protection will be a key enabler for the whole cloud market and ecosystem. Especially when edge computing provides more local distribution of cloud resources. This leads to more complicated relationships between implementations of edge, regional and core implementations of the cloud.

In addition, the flexible use of rich resources in cloud computing environments will enable new security services that the current premise defences cannot provide (e.g. anti-malware services as a cloud service).

Big Data is considered as the technologies, the set of tools, the data and the analytics used in processing large amount of data. Furthermore, as data grow exponentially and become a key asset of telecommunication/ICT networks, massive datasets are analysed with the support of cloud computing to reveal patterns and relationships that would otherwise remain hidden. The core processes of big data such as data collection, storage, analysis, management and visualization are achieved on the basis of cloud computing, without which big data cannot be rapidly transferred and analysed using traditional technologies (e.g. Big Data as a Service). Thus, there is need to examine what kind of security measures cloud computing can offer in the near future.

Recommendations ITU-T X.1601, X.1602, and X.1631 provide a set of Recommendations on security service for cloud security overview, architecture, and framework, cross-layers cloud security and specific security of network services. Currently there is a strong need for securing cloud computing enabled critical voice, multi-media, identity-based services, information assurance services, identity and data services, and emergency-based services. This Question is intended to develop new Recommendations based on the Focus Group Cloud Technical Report Part 5 for:

– best practices and guidelines development to guide on how to provide security in a cloud computing-based environment

– responsibility clarification, and security requirements and threats definition for the main actors and related roles in the cloud computing ecosystem

– security architecture based on the reference architecture provided by Q18/13

– security management and audit technologies for the trust management.

Question 8/17 will collaborate with related Questions such as 2/17, 3/17, 4/17, 7/17, 10/17 and 11/17 to develop Recommendations on cloud computing security.

Recommendations under responsibility of this Question as of 3 September 2020: X.1601, X.1602, X.1603, X.1606, X.1631, X.1641, X.1642, X.1750 and X.1751.

Texts under development: X.BaaS-sec, X.sgBDIP, X.sgcc, X.sr-cphr, X.sgdc, X.sgmc, X.nssa-cc and TR.fssvs.

### Question

Study items to be considered include, but are not limited to:

a) What new Recommendations or other type of documents should be developed for main actors like service providers, service users and services partners, and other key industry stakeholders to advance the security of the entire cloud computing ecosystem, including cloud computing security, edge computing security, interworking security, etc.?

b) What new Recommendations should be developed for security architecture and security functionalities organization in line with the reference architecture?

c) What new Recommendations should be developed for assurance mechanisms, audit technologies, and associated risks assessment to establish trust among different actors?

d) What new Recommendations should be developed for security solutions, best practices or guidelines to big data platform and infrastructure security?

e) What collaboration is necessary to minimize duplication of efforts with other Questions, study groups, and SDOs?

f) How security as a service should be developed to protect telecommunication/ICT systems?

### Tasks

Tasks include, but are not limited to:

a) Developing Recommendations or other type of documents to advance cloud computing security.

b) Developing Recommendations to identify security requirements and threats to secure cloud computing services based on the general requirements of cloud computing specified by ITU-T Study Group 13.

c) Developing Recommendations to define security architecture and to organize security functions based on the reference architecture specified by ITU-T Study Group 13.

d) Developing Recommendations to define a strong, flexible, and elastic security architecture and implementation for cloud computing systems.

e) Developing Recommendations to identify assurance mechanisms, audit technologies, risk assessment with the objective of achieving trustworthy relationships within the cloud computing ecosystem.

f) Study and develop big data platform and infrastructure security Recommendations aligned with reference architecture specified by ITU-T Study Group 13.

g) Taking charge of all the Study Group 17 activities on cloud computing security and big data platform and infrastructure security.

h) Representing the work of Study Group 17 related to cloud computing security in the Joint Coordination Activity on cloud computing.

An up-to-date status of work under this Question is contained in the SG 17 work programme at <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

### Relationships

WSIS Action Lines:

C5.

Sustainable Development Goals:

–

Recommendations:

Y-series Recommendations on cloud computing

Questions:

ITU-T Qs 1/17, 2/17, 3/17, 4/17, 7/17, 10/17, 11/17 and 15/17.

Study Groups:

ITU-T SGs 2, 13, 16 and 20.

Standardization bodies:

Internet Engineering Task Force (IETF); ISO/IEC JTC 1/SCs 27 and SC 38; Organization for the Advancement of Structured Information Standards (OASIS); and other relevant bodies as identified.

Other bodies:

Cloud Security Alliance (CSA); Distributed Management Task Force (DMTF).

## Question 10/17 – Identity management and telebiometrics architecture and mechanisms

(Continuation of Questions 9/17 and 10/17)

### Motivation

Biometrics is gaining acceptance in applications performing but not limited to identity verification such as e-commerce, tele-medicine, and e-health. Biometric application systems present various challenges related to operational and technical data protection, reliability, and security of biometric data for biosafety and biosecurity applications.

Server-side biometric authentication becomes more complicated and demanding when biometric authentication is adopted in an open network environment. Telecommunication applications (such as telebiometrics) using mobile terminals and Internet services demand authentication methods to provide high security and friendly usage. It is necessary to specify requirements for the usage of telebiometric data in a manner that is safe, secure and with enhanced operational and data protection.

Identity management (IdM) is the management of the life cycle and use (creation, maintenance, utilization, and revocation) of credentials, identifiers, attributes, and patterns by which entities (e.g. service providers, end-user, organizations, network devices, applications, and services) are known with appropriate levels of trust. Depending on the context, multiple identities may exist for a single entity at differing security requirements, and at multiple locations. Depending on the identity model, the control over identities can be centralized or decentralized or a combination of both. In public networks, IdM supports trusted information exchange between authorized entities. The exchange is based on assertion of identities across distributed systems from multiple service providers. The exchange can also be based on various service environments such as cloud and 5G. IdM also improves the protection of private information and based on the trust model can ensure that only authorized information is disseminated.

IdM is a key component of telecommunications/ICT networks, services, and products because it supports establishing and maintaining trusted communications. In addition to performing authentication of an entity’s identity, it also permits authorization of access based on privileges. It also supports the change of privileges when an entity’s role changes delegation, and other identity-based services.

IdM is a critical component in managing network security because it improves assurance for the nomadic, on-demand access to networks and services that end-users expect. Along with other defensive mechanisms, IdM helps to prevent fraud and identity theft and thereby increases users’ confidence that transactions are secure and reliable. As IdM works in a mutual manner, this increased level of trust applies equally to both the end user and service provider.

National/regional specific IdM specifications and solutions will exist and continue to evolve. Setup a foundation upon which harmonize solutions could be implemented is important. In addition to the study of telebiometric, this Question is dedicated to the vision setting and the coordination and organization of the entire range of IdM activities within ITU-T. A top-down approach to the IdM will be used with collaboration with other study groups and other standards development organizations (SDOs). It is recognized that other Questions will be involved in specific aspects of IdM, i.e. protocols, requirements, network device identifiers, etc.

Recommendations and Supplements under responsibility of this Question as of 3 September 2020: X.1080.0, X.1080.1, X.1081, X.1082, X.1083, X.1084, X.1085, X.1086, X.1087, X.1088, X.1089, X.1090, X.1091, X.1092, X.1093, X.1094, X.1250, X.1251, X.1252, X.1253, X.1254, X.1255, X.1256, X.1257, X.1258, X.1275, X.1276, X.1277, X.1278, X.1279, and Supplements X.Suppl.7 and X.Suppl.35.

Texts under development: X.1250rev, X.1252rev, X.b2m, X.gpwd, X.pet\_auth, X.tas, X.tec-idms, and X.upu.

### Question

Study items to be considered include, but are not limited to:

a) How to further enhance or revise the current Recommendations for their wide deployment and usage?

b) What are the requirements for biometrics authentication in a high functionality network?

c) How should security countermeasures be assessed for particular applications of telebiometrics?

d) How should biometric systems and operations be developed in order to be conformant to the security requirements for any application of telebiometrics including cloud computing services?

e) How can identification and authentication of users be improved in the aspects of safety and security by the use of interoperable models in telebiometrics?

f) What mechanisms need to be supported to ensure safe and secure manipulation of biometric data in not only existing but also emerging application of telebiometrics, e.g., e-health, tele-medicine, e-commerce, online-banking, video surveillance?

g) How should biometric systems and operations be developed in order to be conformant to functional requirements for entity authentication of pet animals using telebiometrics?

h) What are the functional concepts for a common identity management (IdM) infrastructure?

i) What is an appropriate IdM model that is independent of network technologies, supports user-centric involvement, cloud based identity, decentralized identity models and supports the secure exchange of IdM information between involved entities (e.g., users, relying parties and identity providers) based on consent and related policies?

j) What are the components of a generic framework and requirements for IdM?

k) What are the specific IdM requirements of service providers?

l) What are the requirements, capabilities, and possible strategies for achieving interoperability between different IdM systems (e.g., identity assurance, inter-working)?

m) What are the issues to consider to support identity on distributed ledger technologies including wallet, decentralized identifiers and verifiable credentials?

n) What are the candidate mechanisms for IdM interoperability to include identifying and defining applicable profiles to minimize interoperability issues?

o) What are the requirements and mechanisms for the protection and disclosure of personally identifiable information (PII)?

p) How can an entity control its relationship when involved in identity-based relationships and interactions?

q) What are the requirements to protect IdM systems from cyber-attacks?

r) What IdM capabilities can be used against cyber-attacks?

s) How should IdM be integrated with advanced security technologies?

t) How can authentication be performed without shared secrets?

u) Can PKI based authentication be performed in an interoperable and secure manner?

v) Can biometric be used as part of strong authentication and trust layer to enable trusted interactions over a network?

w) What are the unique requirements for consumer-based identity management system in terms of identity vetting and account recovery without reliance on passwords?

x) How trust and relationship can be used to enhance account recovery, users’ security and experience when dealing with relying parties?

### Tasks

Tasks include, but are not limited to:

a) Enhance and revise current Recommendations of telebiometric authentication.

b) Review the similarities and differences among the existing telebiometrics Recommendations in ITU-T and standards in ISO/IEC.

c) Study and develop security requirements and guidelines for any application of telebiometrics using architectures and frameworks including the ones developed under Question 2/17.

d) Study and develop requirements for evaluating security and operational and technical data protection techniques for any application of telebiometrics.

e) Study and develop requirements for telebiometric applications in a high functionality network.

f) Study and develop integrated frameworks and requirements of telebiometric applications for cloud computing and data storage environments.

g) Study and develop requirements of telebiometric authentication for trust identity framework.

h) Study and develop requirements for appropriate generic protocols providing safety, security, operational and technical data protection, and consent "for manipulating biometric data" in any application of telebiometrics, e.g., e-health, tele-medicine, e-commerce, online-banking, e-payment, and video surveillance.

i) Study and develop Biology-to-Machine (B2M) protocols for transmitting biological metrics of which interoperate with Machine-to-Machine (M2M) protocols.

j) Study and develop telebiometric applications using bio-signals for applications including but not limited to authentication, identification, and health information monitoring.

k) Study and develop entity authentication services for pet animals based on telebiometrics.

l) Specify an IdM framework that supports discovery, policy and trust model, authentication and authorization, assertions, and credential lifecycle management required for IdM.

m) Define functional IdM architectural concepts to include IdM bridging between networks and among IdM systems, taking into account advanced security technologies.

n) Specify requirements (and propose mechanisms) for identity assurance, and mapping/interworking between different identity assurance methods that might be adopted in various networks. In this context, identity assurance includes identity patterns and reputation.

o) Define interfaces for interoperability of IdM systems.

p) Define requirements (and propose mechanisms) for protection and disclosure of personally identifiable information (PII).

q) Define requirements (and propose mechanisms) to protect IdM systems including how to use IdM capabilities as a means for service providers to coordinate and exchange information regarding cyber-attacks.

r) Maintain and coordinate IdM terminology and definitions living list.

s) Study and define IdM security risks and threats.

t) Study and develop decentralized identity management systems with support to user control of their identities

u) Support of trusted identity management systems that can federate across systems, services, devices, IoT and applications.

v) Support identity management system providing identity management as a service for cloud agents, 5G networks and mobile devices.

w) Specify requirements and propose mechanisms for identity assurance for authentication and federation. Establish criteria for mapping/interworking among different identity assurance methods that might be adopted in various networks. In this context, identity assurance includes identity patterns and reputation.

An up-to-date status of work under this Question is contained in the SG 17 work programme at <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

### Relationships

WSIS Action Lines:

C5.

Sustainable Development Goals:

–

Recommendations:

X- and Y-series

X.200, X.273, X.274, X.509, X.680, X.805 and X.1051.

Questions:

ITU-T Qs 1/17, 2/17, 3/17, 4/17, 6/17, 7/17, 8/17, 11/17, 15/17, 7/13 and 14/15.

Study Groups:

ITU-D SG 1, SG2/2; ITU-R SG7; ITU-T SGs 2, 5, 9, 11, 13, 15, 16 and 20;

Standardization bodies:

IEC/TC 25, IEC/TC 25/JWG 1; Institute of Electrical and Electronics Engineers (IEEE); Internet Engineering Task Force (IETF); ISO/IEC JTC 1/SCs 6, 17, 27 and 37; ISO/TCs 12, 68, 215 and 307; ISO/TC 12/JWG 20; ETSI; OASIS; Kantara Initiative; 3GPP; 3GPP2.

Other bodies:

International Bureau of Weights and Measures (BIPM); International Commission on Radiation Units and Measurements (ICRU); Fast Identity Online (FIDO) Alliance; DID Alliance, International Labour Organization (ILO); World Health Organization (WHO).

## Question 11/17 – Generic technologies (such as Directory, PKI, Formal languages, Object Identifiers) to support secure applications

(Continuation of Questions 11/17 and 12/17)

### Motivation

This Question supports the continued development of a variety of generic technologies that are in wide-spread use in support of secure applications. These include:

– Directory services (X.500 series)

– Public Key Infrastructures (PKI – X.509)

– Secure communication (X.510)

– Privilege Management Infrastructure (PMI – X.509)

– Abstract Syntax Notation One (ASN.1)

– Object Identifiers and their Registration Authorities

– Testing and Test Control Notation version 3 (TTCN-3)

– Maintenance of formal languages:

• Specification and Description Language (SDL)

• Unified Modelling Language (UML) Profile Design

• Message Sequence Chart (MSC)

• User Requirement Notation (URN)

• CHILL, the ITU-T Programming Language

– Maintenance of OSI and ODP.

#### Motivation for the work on directories, PKI, and PMI

The ITU-T X.500-series of Recommendations has a significant impact in the industry. These Recommendations are major components of widely deployed technologies such as Public-Key Infrastructure (PKI) and lightweight directory access protocol (LDAP), and is used in many areas, e.g., financial, medical, and legal. Where high security directory services are required, e.g., in the military area, X.500 is the only answer.

X.500 provides elaborate access control and data privacy protection. It is an open-ended specification adaptable to many different applications. It is extendable to allow future requirements to be met. The widely used LDAP is built on the X.500 Directory model. Recommendation ITU-T X.500 has included capabilities for interworking with LDAP. X.500 and LDAP directory solutions are an important part of identity management (IdM).

X.509 is a significant ITU-T Recommendation. Public-key certificates are widely used.

In addition to being a major part of -e-business, e-banking, e-health, it now also being used other characterized by large networks with machine-to-machine communication and constrained entities e.g., Internet of Things (IoT) and intelligent electric networks (smart grid).

Public-key certificates are also for several IETF specification, e.g. Transport Layer Security (TLS).

Attribute certificates provide a secure method for conveying privileges important for access control. The OASIS SAML specifications are based on X.509 attribute certificates. Attribute certificates are also used in power systems Attribute certificates are in particular useful when privileges are assigned by other authorities than those issuing public-key certificates.

In collaboration with other groups X.509 needs to evolve and to be maintained to reflect and benefit from the experiences obtained within the Public-Key Infrastructure (PKI) area and in the Privilege Management Infrastructure (PMI) area. X.509 needs to be enhanced to cope the new requirements such as Machine-to-Machine communications, smart-grid security, Internet of Things security, quantum safe algorithms and distributed ledger technologies. A Decentralized PKI mechanism using blockchains is under development.

Recommendations under responsibility of this Question as of 3 September 2020: E.104 (in conjunction with SG2), E.115 (in conjunction with SG2), F.500, F.510, F.511, F.515, X.500, X.501, X.509, X.510, X.511, X.518, X.519, X.520, X.521, X.525, X.530 and X.1341.

Texts under development: X.510 Amd.1, X.pki-em.

#### Motivation for the work on ASN.1

Additional Recommendations, where needed, will be developed to accommodate advances in technology and additional requirements from users of the ASN.1 notation, its encoding rules.

ASN.1 has proved to be the notation-of-choice for many ITU-T standardization groups, many of which continue to produce requests for correction of residual ambiguities or lack of clarity.

There is a continuing requirement to provide advice and assistance to other study groups, external standards development organizations (SDOs) and countries on ASN.1.

Recommendations under responsibility of this Question as of 3 September 2020: X.680, X.681, X.682, X.683, X.690, X.691, X.692, X.693, X.694, X.695, X.696, X.697, X.891, X.892, X.893 and X.894.

Texts under development: X.680-690 series-rev, X.894 Cor.2.

#### Motivation for the work on object identifiers and their registration authorities

Object identifiers (OIDs) have proved a very popular namespace based primarily on a tree-structure of hierarchical registration authorities identified by integer value. Its recent extension to International OIDs allowing arcs to be identified by Unicode labels is also in demand for various applications and is likely to produce requirements for further development and extension, and allocations.

There is a continuing requirement to provide advice and assistance to other study groups, external standards development organizations (SDOs) and countries on the management of the OID namespace. It is expected that the need for help and advice will increase with the introduction of international OIDs and the increasing use of Country Registration Authorities by developing countries. There is therefore a continued need for an ITU-T "OID Project" with an appointed project leader to provide such advice and assistance.

Any innovative use of object identifiers is to be developed in conjunction with ITU-T Study Group 2.

Recommendations and Technical Papers under responsibility of this Question as of 3 September 2020: X.660, X.662, X.665, X.666, X.667, X.668, X.669, X.670, X.671, X.672, X.674, X.675, X.676, X.677 and Technical Paper XSTP-OID-ORS.

Texts under development: X.672rev.

#### Motivation for the work on TTCN-3

The Testing and Test Control Notation version 3 (TTCN-3) allows tests for functionality and interoperability of systems to be specified and generic test suites to be written. TTCN-3 is being 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. ITU-T is producing a large number of Recommendations. To achieve interoperability, it is essential that implementations of these Recommendations conform to the Recommendations.

Recommendations under responsibility of this Question as of 3 September 2020: X.292, Z.161, Z.161.1, Z.161.2, Z.161.3, Z.161.4, Z.161.5, X.161.6, Z.161.7, Z.162, Z.163, Z.164, Z.165, Z.165.1, Z.166, Z.167, Z.168, Z.169, Z.170 and Z.171.

Texts under development: None.

#### Motivation for the work on formal language maintenance

No further development is expected on the following formal languages:

– Specification and Description Language (SDL)

– Unified Modelling Language (UML) profile

– Message Sequence Chart (MSC)

– User Requirements Notation (URN)

– CHILL, the ITU-T programming language

But there is a need for on-going maintenance.

Recommendations, Supplements and Implementer’s Guides under responsibility of this Question as of 3 September 2020: Z.100, Z.101, Z.102, Z.103, Z.104, Z.105, Z.106, Z.107, Z.109, Z.110, Z.111, Z.119, Z.120, Z.121, Z.150, Z.151, Z.200, Z.450 and Z.Suppl.1 and Z.Imp100.

#### Motivation for the work on OSI maintenance

The work on the base Recommendations for Open Systems Interconnection (OSI) has been completed. Systems based on OSI Recommendations may be implemented over a relatively long period of time. Operational experience with implemented systems based on these Recommendations may lead to the discovery of technical errors or desirable enhancements to these Recommendations. Therefore, there is a need for on-going maintenance of X-series OSI Recommendations.

Recommendations and Implementer’s Guides under responsibility of this Question as of 3 September 2020: F.400, F.401, F.410, F.415, F.420, F.421, F.423, F.435, F.440, F.471, F.472, X.200, X.207, X.210, X.211, X.212, X.213, X.214, X.215, X.216, X.217, X.217bis, X.218, X.219, X.220, X.222, X.223, X.224, X.225, X.226, X.227, X.227bis, X.228, X.229, X.233, X.234, X.235, X.236, X.237, X.237bis, X.245, X.246, X.247, X.248, X.249, X.255, X.256, X.257, X.260, X.263, X.264, X.273, X.274, X.281, X.282, X.283, X.284, X.287, X.400, X.402, X.404, X.408, X.411, X.412, X.413, X.419, X.420, X.421, X.435, X.440, X.445, X.446, X.460, X.462, X.467, X.481, X.482, X.483, X.484, X.485, X.486, X.487, X.488, X.610, X.612, X.613, X.614, X.622, X.623, X.625, X.630, X.633, X.634, X.637, X.638, X.639, X.641, X.642, X.650, X.851, X.852, X.853, X.860, X.861, X.862, X.863, X.880, X.881, X.882 and X.ImpOSI.

#### Motivation for the work on ODP maintenance

A key aspect of telecommunications systems development is the availability of software to support Open Distributed Processing (ODP). Provision of ODP requires standardization of reference models, architectures, functions, interfaces and languages (ITU-T X.900-series).

Recommendations under responsibility of this Question as of 3 September: X.901, X.902, X.903, X.904, X.906, X.910, X.911, X.920, X.930, X.931, X.950, X.952 and X.960.

### Question

Study items to be considered include, but are not limited to:

#### Study items related to the work on directories, PKI and PMI

In relation to directory services:

a) What new service definitions or modifications in the F-series are required to identify how current capabilities may be used and what new requirements there are on ITU-T X.500?

b) What enhancements to the E-series of Recommendations are necessary to cope with new service requirements?

c) What enhancements are required on the Directory to support new PKI requirements?

d) What new security and privacy requirements are there on directory information?

e) What other encoding rules for ITU-T X.500, such as XML, may be required to further improve the usefulness of ITU-T X.500?

f) What further enhancements are required to public-key and attribute certificates to allow their use in various environments, e.g., resource constrained environments machine-to-machine and large networks?

g) What further enhancements are required to public-key and attribute certificates to increase their usefulness in areas such as biometrics, authentication, access control and electronic commerce?

h) What changes to Recommendation ITU-T X.509 are required to support quantum safe algorithms and distributed leger technologies?

This work will be done in collaboration with ISO/IEC JTC 1/SC 6 in their work on extending ISO/IEC 9594. Cooperation will be maintained with the IETF particularly in the areas of LDAP, and PKI.

#### Study items related to the work on ASN.1

a) What enhancements are required to the Abstract Syntax Notation One (ASN.1) and its associated encoding rules to meet the needs of future applications?

b) What collaboration, beyond current agreements, is required with other bodies producing de jure or de facto standards to ensure that ITU-T work on ASN.1 remains a leader in the area of provision of notations for protocol definition?

This work will be done in collaboration with ISO/IEC JTC 1/SC 6.

#### Study items related to the work on object identifiers and their registration authorities

**a**) **What tutorial activity is needed to support the use of OIDs in a variety of environments?**

**b**) **What additional registration authorities or their procedures are needed to support the work of this and other Questions?**

**c**) **What collaboration, beyond current agreements, is required with other bodies producing de jure or de facto standards to ensure that ITU-T work on OIDs remain a leader for unambiguous naming?**

This work will be done in collaboration with ISO/IEC JTC 1/SC 6.

#### Study items related to the work on TTCN

What enhancements are required to TTCN-3 to meet the needs of future applications?

This work will be done in collaboration with ETSI TC MTS.

#### Maintenance of formal languages

Continue maintenance of Recommendations related to SDL, UML profile, MSC, URN, and CHILL.

#### Maintenance of OSI

Continue maintenance of OSI architecture and individual layer Recommendations to provide any needed enhancements and to resolve any reported defects. Continue maintenance of OSI Message Handling Service and Systems, Reliable Transfer, Remote Operations, CCR, and Transaction Processing to provide any needed enhancements and to resolve any reported defects.

Close collaboration and liaison with other study groups and other international groups implementing OSI is highly desirable to ensure the widest applicability of resulting Recommendations.

This work is to be carried out in collaboration with ISO/IEC JTC 1 and its sub-committees.

#### Maintenance of ODP

Continue maintenance of ODP Recommendations.

Close collaboration and liaison with other study groups and other international groups implementing ODP is highly desirable to ensure the widest applicability of resulting Recommendations.

This work is to be carried out in collaboration with ISO/IEC JTC 1/SC 7/WG 19.

### Tasks

Tasks include, but are not limited to:

#### Tasks related to the work on directories, PKI and PMI

a) Maintain the Directory by progressing Defect Reports and Technical Corrigenda.

b) Identify new directory requirements in support of new and current technologies.

c) Develop the ninth edition of the ITU-T X.500-series of Recommendations.

d) Develop enhancements to ITU-T X.509, X.510 and X.pki-em to support new requirements.

#### Tasks related to the work on ASN.1

a) Provide updated Recommendations for ITU-T X.680- X.690- and X.890-series throughout the study period in response to user needs, producing new editions when appropriate.

b) When there is a need to improve data transfer, assist other Questions in all study groups in the provision of ASN.1 modules equivalent to XML schemas defined in ITU-T Recommendations (existing or under development), particularly in low bandwidth situations.

c) Monitor and assist with the publication process of approved Recommendations | International Standards and Technical Corrigenda.

d) Resolve all Defect Reports and progress Technical Corrigenda as necessary.

e) Ensure that all liaisons related to ASN.1 work are handled in a timely and appropriate manner.

f) Develop any additional tutorials or web pages that are likely to assist users of ASN.1.

#### Tasks related to the work on object identifiers and their registration authorities

a) Provide updated Recommendations for ITU-T X.660-and X.670-series throughout the study period in response to user needs, producing new editions when appropriate.

b) Monitor and assist with the publication process of approved Recommendations | International Standards and Technical Corrigenda.

c) Resolve all Defect Reports and progress Technical Corrigenda as necessary.

d) Ensure that all liaisons related to OID work are handled in a timely and appropriate manner.

e) Develop any additional tutorials or web pages that are likely to assist users of OIDs.

f) Obtain agreement in ISO/IEC JTC 1/SC 6 and SG17 on any additional OID allocations that are considered necessary.

g) Under the responsibility of the OID Project Leader:

* Provide general advice to users of OIDs
* Promote the use of international OIDs within other study groups and external standards development organizations (SDOs)
* Help countries with the establishment and maintenance of national registration authorities for OIDs (including international OIDs).

#### Tasks related to the work on TTCN

a) Maintain Recommendations under responsibility of this Question.

b) Promote the use of TTCN within other study groups and external SDOs.

#### Tasks related to the work on formal language maintenance

Develop corrections or enhancements, as needed, to Recommendations related to SDL, UML profile, MSC, URN, and CHILL. Maintain the SDL Implementers' Guide.

#### Tasks related to the work on OSI maintenance

Develop corrections or enhancements to OSI Recommendations, as needed, based on received contributions and to resolve any reported defects. Maintain the OSI Implementers' Guide.

#### Tasks related to the work on ODP maintenance

Develop corrections or enhancements to ODP Recommendations, as needed, based on received contributions and to resolve any reported defects.

An up-to-date status of work under this Question is contained in the SG 17 work programme at <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

### Relationships

WSIS Action Lines:

C5.

Sustainable Development Goals:

**–**

Recommendations:

H.200-series, H.323, H.350-series, T.120, X.600-X.609 series, X.700-series, X.800-X.849 series, Z-series.

Questions:

All ITU-T Questions related to the above Recommendations and Q14/17 related to Distributed PKI.

Study Groups:

ITU-T SGs 2, 9, 11, 13, 15, 16, 20 and all study groups that use Directory, ASN.1, OIDs, conformance and interoperability testing, or that have need for them.

Standardization bodies:

Internet Engineering Steering Group (IESG); Internet Engineering Task Force (IETF); IEC/TC 57; ISO/IEC JTC 1/SCs 6, 7, 27 and 31, ISO TCs 68, 204; Organization for the Advancement of Structured Information Standards (OASIS); Object Management Group (OMG); World Wide Web Consortium (W3C); European Telecommunications Standards Institute (ETSI) (TC MTS); ISO/IEC JTC 1 and its sub-committees that use the ITU system design languages.

Other bodies:

Universal Postal Union (UPU); SDL Forum Society.

## Question 13/17 – Intelligent transport system security

(Continuation of Question 13/17)

### Motivation

Intelligent Transport System (ITS) including autonomous driving system provides various types of applications in order to increase road safety, decrease the environmental footprint of transport, enhance traffic management and maximize the transport sector’s benefits to public and commercial users.

ITS includes various types of communications in vehicles (e.g., vehicle-to-nomadic device), between vehicles (e.g., vehicle-to-vehicle (V2V)), and between vehicles and fixed locations (e.g., vehicle-to-infrastructure (V2I)), i.e., vehicle-to-everything (V2X) communications. Information and communication technologies (ICT) are used to implement ITS including road transport, rail, water and air transport, including navigation systems.

An automated and assisted driving system consists of various components of systems where perception, decision making, and operation of the automobile are performed by electronics and machinery instead of a human driver, and as introduction of automation into road traffic.

In the ITS including autonomous and assisted driving system environment, vulnerabilities of a vehicle can be propagated to other vehicles since the vehicles are connected to each other. Thus, vulnerabilities of V2X communication systems in a vehicle should be managed and handled in order not to influence a lot of other vehicles.

Electric devices inside a vehicle such as electronic control units (ECUs) and electric toll collection (ETC) devices are becoming more sophisticated. As a result, software modules inside those entities need to be appropriately updated for performance and security improvements.

Recommendation ITU-T X.1373 approved in March 2017 provides the secure software update capability for ITS communication devices. X.1373 is currently under revision.

Standardization of the best comprehensive security solutions is vital for ITS environment. Due to some specific characteristics of the vehicular communications, providing security becomes especially challenging tasks that deserve study.

Recommendations under responsibility of this Question as of 3 September 2020: X.1371, X.1372, X.1373.

Texts under development: X.1373rev, X.edrsec, X.eivnsec, X.evtol-sec, X.fstiscv, X.ipscv, X.itssec-3 (X.1374), X.itssec-4 (X.1375), X.itssec-5, X.mdcv (X.1376), X.rsu-sec and X.srcd.

### Question

Study items to be considered include, but are not limited to:

a) How should security aspects (e.g., security architecture and subsystems) be identified and defined in an ITS and autonomous and assisted driving system environment?

b) How should threats and vulnerabilities in ITS and autonomous and assisted driving system services and networks be identified and handled?

c) What are the security requirements (e.g., those for identification and authentication) for mitigating the threats in an ITS and autonomous and assisted driving system environment?

d) What are security technologies to support ITS services and networks?

e) How should secure interconnectivity between entities in an ITS and autonomous and assisted driving system environment be kept and maintained?

f) What security techniques, mechanisms and protocols are needed for ITS and autonomous and assisted driving system services and networks?

g) What are globally agreeable security solutions for ITS and autonomous and assisted driving system services and networks, which are based on telecommunication/ICT networks?

h) What are best practices or guidelines for ITS and autonomous and assisted driving system security?

i) How AI/ML technologies can be used to provide security and confidence of the ITS and autonomous and assisted driving system?

j) What PII (Personally Identifiable Information) protection and management mechanisms are needed for ITS services?

### Tasks

Tasks include, but are not limited to:

a) Produce a set of Recommendations providing comprehensive security solutions for ITS and autonomous and assisted driving system.

b) Study further to define security aspects of ITS and autonomous and assisted driving system services and networks, which are based on telecommunication/ICT networks.

c) Study and identify security issues and threats in ITS and autonomous and assisted driving system.

d) Study and identify requirements and use cases for specific ITS and autonomous and assisted driving system services and applications.

e) Study and develop security mechanisms, protocols, and technologies for ITS and autonomous and assisted driving system.

f) Study and develop security profiling, hierarchical scheme for authentication and mechanism for specific ITS and autonomous and assisted driving system services and applications.

g) Study and develop applications of efficient encryption and decryption algorithms for fast moving network nodes and dynamically changing network topologies.

h) Study and develop the event data recording technologies in context of ITS and autonomous and assisted driving system.

i) Study and develop secure interconnectivity mechanisms for ITS and autonomous and assisted driving system in a telecommunication environment.

j) Study and identify PII protection issues and threats in ITS and autonomous and assisted driving system.

k) Study and develop PII protection and management mechanisms for ITS and autonomous and assisted driving system.

l) Study and develop secure ITS and autonomous and assisted driving system based on AI/ML technologies.

m) Study and develop an existing draft Recommendation X.1373rev, X.itssec-3, X.itssec-4, X.itssec-5, X.mdcv, X.srcd, X.edrsec, X.eivnsec, X.fstiscv, X.ipscv, X.rsu-sec.

n) Collaborate with the related SDOs to jointly develop Recommendations.

An up-to-date status of work under this Question is contained in the SG 17 work programme at <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

### Relationships

WSIS Action Lines:

C5.

Sustainable Development Goals:

–

Recommendations:

X-series and others related to security.

Questions:

ITU-T Qs 1/17, 2/17, 3/17, 4/17, 6/17, 7/17, 8/17, 10/17, 11/17 and 15/17.

Study Groups and Focus Groups:

ITU-T SGs 11, 13, 16 and 20; ITU-R WP5A; Collaboration on ITS Communication Standards (CITS); ITU-T FG-VM (Vehicular Multimedia).

Standardization bodies:

ISO TCs 22 and 204; ISO/IEC JTC 1/SCs 6 and 27; IETF WG ITS; IEEE 802.11 WG and 1609 WG; SAE International (e.g., Vehicle Cybersecurity Systems Engineering Committee, Connected Vehicles Steering Committee, and DSRC Technical Standard Committee); ETSI TC ITS; W3C Automotive WG.

Other bodies:

GSMA; ATIS; CCSA; TIA; TTA; TTC; UNECE (UN Economic Commission for Europe) Working Party 29 and subsidiary bodies (e.g., Taskforce on cyber security (TFCS)); AGL (Automotive Grade Linux).

## Question 14/17 – Distributed ledger technology (DLT) security

(Continuation of Question 14/17)

### Motivation

Distributed Ledger Technologies (DLT), the most prominent implementation of which is Blockchain, are a new type of secure ledgers that is shared, replicated, and synchronized in a distributed. Data in distributed ledgers is controlled by multiple parties.

As a specific distributed database technology, DLT are inherently resistant to modification of the data - once recorded, the data in a block cannot be altered retroactively. This prominent feature of DLT is well known after the success of its early digital cryptocurrency applications known as Bitcoin.

DLT has become one of disruptive technologies with great potential to change our economy, culture, and society. DLT enables innovative financial/non-financial decentralized applications that eliminate the need for third party intermediaries. DLT will introduce new data management infrastructure that will accelerate a services revolution in industries (for example, banking and finance, government, healthcare, and super logistics) based on telecommunications.

Distributed ledger technologies will have a profound impact for telecom users and industries including telecom service providers.

There is a need for identifying the roles and responsibilities of telecom users, operators, and service providers with regards to security aspects in the DLT environment.

Standardization of the best comprehensive security solutions is vital for DLT that has many use cases for every sector including telecom industry. Due to some specific characteristics of the DLT, providing security becomes an especially challenging task that deserves study.

Recommendations under responsibility of this Question as of 3 September 2020: X.1401, X.1402 and X.1403.

Texts under development: X.dlt-td (X.1400), X.das-mgt, X.sa-dlt (X.1404), X.sc-dlt, X.srip-dlt, X.srscm-dlt, X.sa-dsm, X.ss-dlt, X.stov, X.str-dlt, X.tf-spd-dlt and TR.qs-dlt.

### Question

Study items to be considered include, but are not limited to:

a) How should security aspects (e.g., architecture and subsystems) be identified and defined based on the foundations (terms and definitions, concepts and taxonomy, use cases) in a DLT environment?

b) How should threats and vulnerabilities in applications and services based on DLT be handled?

c) What are the security requirements for mitigating the threats in a DLT environment?

d) What are security technologies to support applications and services based on DLT?

e) How should secure interconnectivity between entities in a DLT environment be kept and maintained?

f) What security techniques, mechanisms and protocols are needed for applications and services based on DLT?

g) What are globally agreeable security solutions for applications and services based on DLT, which are based on telecommunication/ICT networks?

h) What are best practices or guidelines of security for applications and services based on DLT?

i) What PII (Personally Identifiable Information) protection and information security management are needed for applications and services based on DLT?

j) How can DLT be used to support security?

k) How can the DLT security be assessed, evaluated, and assured?

l) What stakeholders should SG17 collaborate with?

### Tasks

Tasks include, but are not limited to:

a) Perform a gap analysis on ongoing security relevant work in other organizations for distributed ledger technologies.

b) Study further to define security aspects of applications and services based on DLT, which are based on telecommunication/ICT networks.

c) Study foundations such as terms and definitions, concepts, and taxonomy, and use cases that are related to security and PII protection in DLT networks.

d) Study and identify security issues and threats in applications and services based on DLT.

e) Study and develop security mechanisms, protocols and technologies for applications and services based on DLT.

f) Study and develop secure interconnectivity mechanisms for applications and services based on DLT.

g) Study and identify PII protection issues and threats in applications and services based on DLT.

h) Study and develop information management system for entities providing applications and services based on DLT.

i) Study and develop guidance on DLT usage to support security.

j) Study and develop guidance for assessment, evaluation, and assurance on DLT security.

k) Produce a set of Recommendations to provide comprehensive security solutions for DLT based applications and services.

An up-to-date status of work under this Question is contained in the SG 17 work programme at <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

### Relationships

WSIS Action Lines:

C5.

Sustainable Development Goals:

–

Recommendations:

X-series and others related to security.

Questions:

ITU-T Qs 1/17, 2/17, 3/17, 4/17, 6/17, 7/17, 8/17, 10/17, 11/17, 13/17 and 15/17.

Study Groups:

ITU-T SGs 5, 11, 13, 16 and 20.

Standardization bodies:

ISO TC 307; ISO/IEC JTC 1/SC 27.

Other bodies:

GSMA, W3C, IEEE; UNECE (UN Economic Commission for Europe); FIGI; ATIS; CCSA; TIA; TTA; TTC.

## Question 15/17 – Security for/by emerging technologies including quantum-based security

(New Question)

### Motivation

SG17 recognizes the dynamic nature of security studies which heavily depend on the both the attacker/defenders’ arms race and the ripple effect from innovations being leveraged by both sides. This results in a cadence of emerging security technologies from which some require global standardization.

As by nature, it is impossible to anticipate what and when, SG17 proactively established and runs an 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.

This incubation mechanism enables SG17 to introduce new work items in an efficient manner in the emerging areas and encourages non-normative texts (Technical Papers and Technical Reports) as a proven best practice to allow SG17 community time to familiarize itself with this new emerging areas and new comers to familiarize themselves with SG17 and ITU-T procedures and environment. In the development of the new work items, sometimes, the nature of the emerging security technology reveals it is closer to an existing Question and this work item can be transferred to maximize the coherency, efficiency and quality of SG17 work.

As well, this incubation mechanism allows the identification of trends in emerging security technologies which are being developed in this Question. Some emerging technologies come from

– the nature of the topic itself is nascent, for example quantum-based security, secure multi-party computation, homomorphism, or potentially identifiable security for robotics, etc.

– the topic is not nascent, but it is the first time they enter global standardization, e.g. malware analysis, data loss prevention, etc.

– operational security architecture gaps that do not fit in any question e.g. security product themselves, heavy integration and composition issues showing emerging new cross-topic solutions, security data schemas, etc.

One of emerging areas identified during incubation mechanism is quantum-based security. The advent of large-scale quantum computers offers potential significant disruptions on conventional telecommunication systems based on ICT as well as, poses significant risks to security.

Indeed, the current cryptography security relies on computationally difficult problems: a discrete logarithmic problem and an integer-factorization problem. They are considered to be difficult to solve in a reasonable time given the current architectures of current computers available today and in the medium term. Yet, public key cryptography using asymmetric keys is a cornerstone of authentication over public networks. As, by its nature, quantum computers can solve integer-factoring and discrete-logarithm problems in a reasonably fast time, they are, by ripple effect, able to break the foundations on which cryptography is currently built on, threatening an existential corner stone of todays’ cyber life and digitalization.

The Quantum Key Distribution (QKD) enables two parties to produce a shared random secret key known only to them which can be used to encrypt and decrypt messages using conventional cryptographic algorithms. QKD had two limits that create network topological and integration issues: a) it is point-to-point (p-t-p) and can only be applied to tow parties, A and B and b) it has distance limitations on terrestrial networks. To overcome these two limitations, the concept of QKD networks has been introduced in the industry consisting of (1) an ensemble of nodes that are linked together through QKD systems working in p-t-p, and (2) a management system that is shared between and embedded in each of the QKD nodes. The purpose of this management system is to distribute secret keys between two or more nodes within the same QKD network that might not be directly linked. Currently, commercial QKD systems are stable and mature enough to start planning for large scale QKD networks. There are several initiatives by companies/institutions to develop QKD networks, however, there is no widely accepted standard for what constitutes a QKD system.

Additionally, random numbers are a fundamental key element in engineering with important applications in cryptography. The inherent randomness at the core of quantum mechanics makes quantum systems a perfect source of entropy. Quantum random number generation is one of the most mature quantum technologies with many alternative generation methods.

In summary, a quantum-based security ensures communication that is not vulnerable to attacks by quantum computers. Implementation of quantum-based security requires several key elements including quantum key distribution and quantum random number generator (QRNG). In addition, the interoperability in the key elements and functionalities for the QKD and the QRNG are important to be widely used in real telecommunication networks.

In turn, there is a strong need for SG17 to study quantum-based security that are resistant to quantum attacks.

Recommendations and Technical Reports under responsibility of this Question as of 3 September 2020: X.1702 and TP.inno, TP.sgstruct, and TR.sec-qkd.

Texts under development: X.cf-QKDN (X.1714), X.sec\_QKDN\_intrq, X.sec-QKDN-km, X.sec-QKDN-ov (X.1710), and X.sec-QKDN-tn, X.rdmase, X.icd-schemas, X.tf-mpc, TR.sgfdm.

### Question

Study items to be considered include, but are not limited to:

a) What are the new emerging security technologies?

b) What are the categories of new emerging security technologies?

c) How to safely develop emerging security technologies?

d) What are the most effective mechanisms for implementing incubation mechanism?

e) What are the impacts and challenges of conventional communications from advent of largescale quantum computers?

f) What are the key elements for building quantum-based security?

g) What is transition strategy for building quantum-based security?

h) How should threats and vulnerabilities in quantum-based security be handled?

i) What are the security requirements for mitigating threats in quantum-based security?

j) What are the security technologies to support quantum-based security?

k) How should secure interconnectivity between entities in quantum-based security be kept and maintained?

l) What security requirements, techniques, mechanisms and protocols are needed for quantum-based security?

m) What are globally agreeable security solutions for quantum-based security, which are based on telecommunication/ICT communications?

n) What are best practices or guidelines of security for quantum-based security?

### Tasks

Tasks include, but are not limited to:

a) Identify new emerging security technologies.

b) Identify new categories of emerging security technologies to firm up Question M strategy.

c) Potentially reallocate NWI to other question should their development makes it clearer the match to an existing Question

d) Incorporate incubation mechanism to address the new emerging areas in ITU-T SG17.

e) Produce a set of technical Recommendations providing comprehensive security solutions to establish quantum-based security.

f) Study to define security aspects of quantum-based security, which is based on telecommunication/ICT infrastructure.

g) Study and identify security issues and threats in quantum-based security.

h) Study and develop security requirements, mechanisms, protocols, and technologies for quantum-based security.

i) Study and develop secure interconnectivity mechanisms for quantum-based security.

j) Study and develop information management system for entities providing quantum-based security.

An up-to-date status of work under this Question is contained in the SG 17 work programme at <https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

### Relationships

WSIS Action Lines:

C5.

Sustainable Development Goals:

–

Recommendations:

X-series and others related to security.

Questions:

ITU-T Qs 1/17, 2/17, 3/17, 4/17, 6/17, 7/17, 8/17, 10/17, 11/17, 13/17, and 14/17.

Study Groups:

ITU-T SGs 2, 3, 5, 9, 11, 12, 13, 15, 16, and 20.

Standardization bodies:

ETSI TC Cyber, ISG-QKD; ISO/IEC JTC 1/SC 27; OASIS; IETF

Other bodies:

GSMA; ATIS; CCSA; TIA; TTA; TTC

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