|  |  |  |
| --- | --- | --- |
| Title: ITU logo | INTERNATIONAL TELECOMMUNICATION UNION**TELECOMMUNICATIONSTANDARDIZATION SECTOR**STUDY PERIOD 2017-2020 | TSAG-R16 |
| **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 11 |
| **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 11 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 5](#_Toc62037167)

[2 Wording of Questions 7](#_Toc62037168)

[A Question 1/11 – Signalling and protocol architectures for telecommunication networks and guidelines for implementations 7](#_Toc62037169)

[A.1 Motivation 7](#_Toc62037170)

[A.2 Question 7](#_Toc62037171)

[A.3 Tasks 8](#_Toc62037172)

[A.4 Relationships 8](#_Toc62037173)

[B Question 2/11 – Signalling requirements and protocols for services and applications in telecommunication environments 10](#_Toc62037174)

[B.1 Motivation 10](#_Toc62037175)

[B.2 Question 10](#_Toc62037176)

[B.3 Tasks 10](#_Toc62037177)

[B.4 Relationships 11](#_Toc62037178)

[C Question 3/11 – Signalling requirements and protocols for emergency telecommunications 12](#_Toc62037179)

[C.1 Motivation 12](#_Toc62037180)

[C.2 Question 12](#_Toc62037181)

[C.3 Tasks 12](#_Toc62037182)

[C.4 Relationships 13](#_Toc62037183)

[D Question 4/11 – Protocols for control, management and orchestration of network resources 15](#_Toc62037184)

[D.1 Motivation 15](#_Toc62037185)

[D.2 Question 15](#_Toc62037186)

[D.3 Tasks 16](#_Toc62037187)

[D.4 Relationships 17](#_Toc62037188)

[E Question 5/11 – Signalling requirements and protocols for border network gateway in the context of network virtualization and intelligentization 18](#_Toc62037189)

[E.1 Motivation 18](#_Toc62037190)

[E.2 Question 18](#_Toc62037191)

[E.3 Tasks 19](#_Toc62037192)

[E.4 Relationships 20](#_Toc62037193)

[F Question 6/11 – Protocols supporting control and management technologies for IMT-2020 network and beyond 21](#_Toc62037194)

[F.1 Motivation 21](#_Toc62037195)

[F.2 Question 21](#_Toc62037196)

[F.3 Tasks 21](#_Toc62037197)

[F.4 Relationships 22](#_Toc62037198)

[G Question 7/11 – Signalling requirements and protocols for network attachment and edge computing for future networks, IMT-2020 network and beyond 23](#_Toc62037199)

[G.1 Motivation 23](#_Toc62037200)

[G.2 Question 23](#_Toc62037201)

[G.3 Tasks 23](#_Toc62037202)

[G.4 Relationships 24](#_Toc62037203)

[H Question 8/11 – Protocols supporting distributed content networking, information centric network (ICN) technologies for future networks, IMT-2020 network and beyond 25](#_Toc62037204)

[H.1 Motivation 25](#_Toc62037205)

[H.2 Question 25](#_Toc62037206)

[H.3 Tasks 26](#_Toc62037207)

[H.4 Relationships 26](#_Toc62037208)

[I Question 12/11 – Testing of internet of things, its applications and identification systems 28](#_Toc62037209)

[I.1 Motivation 28](#_Toc62037210)

[I.2 Question 28](#_Toc62037211)

[I.3 Tasks 29](#_Toc62037212)

[I.4 Relationships 30](#_Toc62037213)

[J Question 13/11 – Monitoring parameters for protocols used in emerging networks, including cloud/edge computing and software-defined networking/network function virtualization (SDN/NFV) 31](#_Toc62037214)

[J.1 Motivation 31](#_Toc62037215)

[J.2 Question 31](#_Toc62037216)

[J.3 Tasks 31](#_Toc62037217)

[J.4 Relationships 32](#_Toc62037218)

[K Question 14/11 – Testing of cloud, SDN and NFV 33](#_Toc62037219)

[K.1 Motivation 33](#_Toc62037220)

[K.2 Question 33](#_Toc62037221)

[K.3 Tasks 33](#_Toc62037222)

[K.4 Relationships 34](#_Toc62037223)

[L Question 15/11 – Combating counterfeit and stolen telecommunication/ICT devices 35](#_Toc62037224)

[L.1 Motivation 35](#_Toc62037225)

[L.2 Question 35](#_Toc62037226)

[L.3 Tasks 36](#_Toc62037227)

[L.4 Relationships 37](#_Toc62037228)

[M Question 16/11 – Test specifications for protocols, networks and services for emerging technologies, including benchmark testing 39](#_Toc62037229)

[M.1 Motivation 39](#_Toc62037230)

[M.2 Question 40](#_Toc62037231)

[M.3 Tasks 40](#_Toc62037232)

[M.4 Relationships 41](#_Toc62037233)

[N Question 17/11 – Combating counterfeit or tampered telecommunication/ICT software 43](#_Toc62037234)

[N.1 Motivation 43](#_Toc62037235)

[N.2 Question 44](#_Toc62037236)

[N.3 Tasks 44](#_Toc62037237)

[N.4 Relationships 45](#_Toc62037238)

# 1 Introduction

This document contains the clean text of the Questions agreed by Study Group 11 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 9/11, 10/11 and Question 11/11 were merged into Question 16/11 and new Question 17/11 was created, as indicated in Table 1.

Table 1 – Map of in-force SG11 Questions (endorsed, left) to the previous ones (right)

| New number | Current Question title | Status | Previous number | Previous Question title |
| --- | --- | --- | --- | --- |
| 1/11 | Signalling and protocol architectures for telecommunication networks and guidelines for implementations | Continued | 1/11 | Signalling and protocol architectures in emerging telecommunication environments and guidelines for implementations |
| 2/11 | Signalling requirements and protocols for services and applications in telecommunication environments | Continued | 2/11 | Signalling requirements and protocols for services and applications in emerging telecommunication environments |
| 3/11 | Signalling requirements and protocols for emergency telecommunications | Continued | 3/11 | Signalling requirements and protocols for emergency telecommunications |
| 4/11 | Protocols for control, management and orchestration of network resources | Continued | 4/11 | Protocols for control, management and orchestration of network resources |
| 5/11 | Signalling requirements and protocols for border network gateway in the context of network virtualization and intelligentization | Continued | 5/11 | Protocols and procedures supporting services provided by broadband network gateways |
| 6/11 | Protocols supporting control and management technologies for IMT-2020 network and beyond | Continued | 6/11 | Protocols supporting control and management technologies for IMT-2020 |
| 7/11 | Signalling requirements and protocols for network attachment and edge computing for future networks, IMT-2020 network and beyond | Continued | 7/11 | Signalling requirements and protocols for network attachment including mobility and resource management for future networks and IMT-2020 |
| 8/11 | Protocols supporting distributed content networking, information centric network (ICN) technologies for future networks, IMT-2020 network and beyond | Continued | 8/11 | Protocols supporting distributed content networking and information centric network (ICN) for future networks and IMT-2020, including end-to-end multi-party communications |
| 12/11 | Testing of internet of things, its applications and identification systems | Continued | 12/11 | Testing of internet of things, its applications and identification systems |
| 13/11 | Monitoring parameters for protocols used in emerging networks, including cloud/edge computing and software-defined networking/network function virtualization (SDN/NFV) | Continued | 13/11 | Monitoring parameters for protocols used in emerging networks, including cloud computing and software-defined networking/network function virtualization (SDN/NFV) |
| 14/11 | Testing of cloud, SDN and NFV | Continued | 14/11 | Cloud interoperability testing |
| 15/11 | Combating counterfeit and stolen telecommunication/ICT devices | Continued | 15/11 | Combating counterfeit and stolen ICT equipment |
| 16/11 | Test specifications for protocols, networks and services for emerging technologies, including benchmark testing | Continuation of Q9/11, Q10/11 and Q11/11 | 9/11 | Service and networks benchmark testing, remote testing including Internet related performance measurements |
| 10/11 | Testing of emerging IMT-2020 technologies |
| 11/11 | Protocols and networks test specifications; frameworks and methodologies |
| 17/11 | Combating counterfeit or tampered telecommunication/ICT software | New | – | – |

# 2 Wording of Questions

## A Question 1/11 – Signalling and protocol architectures for telecommunication networks and guidelines for implementations

(Continuation of Question 1/11)

### A.1 Motivation

The desire to support services within networks and supported by networks has resulted in a number of architectural solutions being worked on in numerous standardization bodies and forums. A standardized architectural model for a control signalling with regard to the voice and video over LTE based networks (VoLTE/ViLTE), network virtualization, cloud computing, ML/AI, Distributed Ledger Technology, QKDN and related technologies and other emerging telecommunication/ICT technologies which might be applied in IMT-2020, IMT-2020 network and beyond is needed.

A standard reference model for the control plane is required to identify a set of interfaces which provide interoperability between telecommunication networks, between equipment from different suppliers, between the cloud computing networks, between the virtualized and the physical networks and between networks evolve in different phases such as IMT-2020 network and beyond.

As ITU‑T has developed the standards for existing public networks, including services and control protocols, this Question plans to develop the signalling and protocol architectures for telecommunication networks with emerging technologies including ML/AI, Distributed Ledger Technology, QKDN and related technologies and so on. Furthermore, this Question will study the enhancements to the signalling and control architecture to support the distributed ENUM signalling system.

Cooperation with the ITU‑T study groups and with other standards development organizations (SDOs) is required to gather any relevant information from these organizations and take an important role to coordinate them to achieve the global interoperability.

In addition, ongoing studies and results achieved by various international standardization bodies have led to the emergence of different solutions to address convergence and interoperability due to the evolution of protocols in packet-based networks. For this reason, ITU Member States, particularly those in developing countries, have expressed the needs for assistance in understanding network and service deployment strategies and scenarios by developing Guidelines on signalling protocols implementations for networks and services.

This Question will maintain the previous Technical Reports and Guidelines on implementation of signalling and protocols developed to support developing countries. In addition, it will maintain Recommendations in force for which the Question is responsible, e.g. ITU-T Q.3030, Q.3040, Q.3050, Q.3051 and Q.3052.

### A.2 Question

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

– What enhancements to the signalling and control architecture are required to model the control plane for telecommunication networks with emerging technologies such as ML/AI, Distributed Ledger Technology, QKDN and related technologies and the technologies applied in IMT-2020 network and beyond, taking into account new services and new applications and all types of wireline and wireless public access networks over which these services may be delivered?

– What enhancements to the signalling and control architecture are required to support the distributed ENUM signalling system?

– What enhancements to the signalling and control architecture are required to support VoLTE/ViLTE and IMT-2020 services including eMBB, mMTC and uRLLC, and other new value-added services?

– What enhancements to the signalling and control architecture are required to assure security of signalling and control, and to support services and/or applications of public interest such as emergency call handling, number portability, privacy, etc.?

– What activity is needed to prepare common Guidelines by the ITU‑T and ITU‑D Sectors, containing different aspects related to network and service deployment strategies and scenarios to support the implementation of signalling protocols in networks and services?

– What coordination mechanisms are needed in regards of the signalling and protocol development for emerging telecommunication networks in cooperation with the ITU‑T study groups and with other standards development organizations (SDOs)?

### A.3 Tasks

Tasks include, but are not limited to:

– determine the requirements that the generic, access-technology-independent telecommunication network signalling control protocol architecture is intended to support. It is anticipated that these requirements will need to be periodically refined to reflecting the evolution of telecommunications and computer communication technologies taking into consideration the signalling control protocol architectures available from ITU‑T and other SDOs;

– identify modifications and enhancements to the signalling control protocol architecture that will enable the architecture to meet the requirements of the emerging network architecture (including IMT2020, IMT-2020 network and beyond, etc.);

– study the signalling and control architecture to model the control plane for telecommunication networks with emerging technologies such as ML/AI, Distributed Ledger Technology, QKDN and related technologies and the technologies applied in IMT-2020 network and beyond;

– identify enhancements to the signalling control protocol architecture to support the distributed ENUM signalling system;

– identify enhancements to the signalling control protocol architecture in support of the telecommunication networks evolving to future networks;

– identify a set of interfaces for which interoperability and interworking between different network equipment is desirable and for which detailed signalling requirements need to be studied and control protocols need to be standardized;

– study and prepare common Guidelines containing different aspects related to network and service deployment strategies and scenarios to support the implementation of signalling protocols in networks and services, especially to support developing countries;

– ensure communication and cooperation amongst study groups and forums related to signalling and protocol development for emerging networks.

An up-to-date status of work under this Question is contained in the SG11 work programme (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>).

### A.4 Relationships

Recommendations:

– Y.2012, Y.3015, Y.3510, Y.3104

Questions:

– All Questions of SG11, especially Questions related to signalling architectures and protocols

Study Groups:

– SG2 on ENUM aspects

– SG13 on architecture of the existing and emerging networks

– SG15 on transport

– SG16 on multimedia services and coding

– SG17 on security framework

– SG20 on IoT and its applications

– ITU‑D SG1 and SG2

Other bodies:

– ATIS

– Broadband Forum

– CCSA

– ETSI

– IETF

– IEEE

– W3C

WSIS action lines:

– C2, C11

Sustainable Development Goals:

– 9

## B Question 2/11 – Signalling requirements and protocols for services and applications in telecommunication environments

(Continuation of Question 2/11)

### B.1 Motivation

With the ever-increasing number of services and applications, demand has been continuously increasing to enhance the capabilities of telecommunication networks. Also, technologies, including cloud computing big data, DLT and Machine Learning/Artificial Intelligence, QKDN and related technologies and other emerging telecommunication/ICT technologies will promote new signalling protocols to enable interconnection and proper communication in IMT-2020 network and beyond. These emerging technologies, as well as the evolution of existing ones, will certainly impact on the signalling and protocol standardization.

One of the objectives of telecommunication network’s evolution is to support, in a secure fashion, wide range of services, from legacy telephony and intelligent services to innovative services, encompassing audio, data, video broadcast and conversational services, streaming services, interactive games, mobile payment/banking, third party applications, etc.

### B.2 Question

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

– What are the suitable signalling protocols for implementation of different services and applications in emerging telecommunication environment?

– What new signalling requirements and protocols need to be developed to support services in telecommunication networks evolving to IMT-2020 network and beyond?

– What new signalling requirements and protocols need to be developed to support emerging telecommunication/ICT technologies services and applications?

– What kind of emerging technologies, including QKDN and related technologies enabled architecture and mechanisms are required to guarantee signalling and control security, including signalling system number 7 (SS7) and emerging signalling systems?

– What signalling requirements and protocols need to be developed to support real-time communications and messaging services?

– What new signalling requirements and protocols need to be developed to support telecommunications services management?

– What new signalling requirements and protocols are required to support services and/or applications of public interest, such as mobile payment/banking, crypto currency, multimedia emergency communications, privacy, number portability, etc.?

### B.3 Tasks

Tasks include, but are not limited to:

– develop signalling requirements and protocols to implement different services and applications in telecommunication environment;

– develop signalling requirements and protocols to support future services in telecommunication networks evolving to IMT-2020 network and beyond;

– develop signalling requirements and protocols to support emerging technologies enabled services and applications;

– develop signalling requirements and protocols to support real-time communications and messaging services;

– develop signalling network’s security based on emerging technologies including QKDN and related technologies;

– develop signalling requirements and protocols to support telecommunications services management;

– develop specifications for interworking between new and existing signalling and protocols;

– develop signalling requirements and protocols for public interest;

– enhance existing signalling protocols based on identified needs.

An up-to-date status of work under this Question is contained in the SG11 work programme (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>).

### B.4 Relationships

Recommendations:

– Q.600-series, Q.700-series, Q.900-series, Q.1900-series, Q.2700-series, Q.2900-series, Q.3400-series, Q.3500-series and Q.3600-series

Questions:

– All Questions of SG11

Study Groups:

– SG2 on network management aspects and emergency communications

– SG13 on service requirements, architecture, cloud computing and mobility aspects

– SG15 on smart grid

– SG16 on multimedia services and applications

– SG17 on security aspects

– SG20 on IoT and its applications

Other bodies:

– ARIB

– ATIS

– Broadband Forum

– CCSA

– ETSI

– IETF

– IEEE

– TIA

– TTA

– TTC

WSIS action lines:

– C2, C5, C11

Sustainable Development Goals:

– 9

## C Question 3/11 – Signalling requirements and protocols for emergency telecommunications

(Continuation of Question 3/11)

### C.1 Motivation

In the emerging network environment, impacts of new emerging technologies, capabilities, and application services (e.g. IMT-2020 network and beyond, terrestrial and satellite network convergence, video and voice over LTE (VoLTE/ViLTE), machine to-machine (M2M) communication, Internet of things (IoT), Distributed Ledger Technology, Machine Learning/Artificial Intelligence, QKDN and related technologies) on emergency telecommunications, including emergency telecommunication service (ETS), will need to be studied. In addition, it is needed to be studied how some of the emerging technologies and application services can be leveraged for the benefit of emergency telecommunications.

There is also a need to continue development of emergency telecommunications applications, e.g. voice, video, data signalling requirements and protocol enhancements.

The Question is responsible to ensuring the maintenance of existing ETS capabilities in SG11 Supplements and Recommendations, e.g. Q.931, Q.761, Q.762, Q.763, Q.764, Q.1902.1, Q.1902.3, Q.1902.4, Q.1950, Q.2630.3, Q.2931, Q-series Supplement 47, Q-series Supplement 49 for ETS specific information, Q-series Supplement 53, Q-series Supplement 57, Q-series Supplement 61, Q series Supplement 62, Q-series Supplement 63, Q-series Supplement 68, Q-series Supplement 69 and Q-series Supplement 70.

The Question will liaise with regional SDOs dealing with emergency telecommunications or capabilities required for their implementation. For example, 3GPP developments with respect to priority communications; IETF technical solution developments of congestion control techniques, all of which facilitate the implementations of priority communications for emergency telecommunication users; IEEE developments with respect to IEEE 802.11-series which apply to emergency telecommunication users.

### C.2 Question

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

– What signalling requirements and protocol enhancements need to be defined in support of emergency telecommunications and disaster relief in IMT-2020 network and beyond?

– What signalling requirements and protocol need to be defined in support of emergency telecommunications and disaster relief for terrestrial and satellite network convergence?

– What Recommendations must be created in response to these requirements because the work is not covered by other SG Questions?

– What changes should be proposed to the overall plans maintained by the respective lead study groups, to provide for new capabilities, to provide better realization of capabilities already being standardized, or to remove obsolete content?

### C.3 Tasks

Tasks include, but are not limited to:

– analyse emergency telecommunication capabilities to which priority has been assigned by their respective lead study group to determine the specific study tasks that must be added to the work plans of individual SG Questions;

– ensure that the necessary communications take place at the technical level between the Questions of the study group, so that their work of realization of emergency telecommunication capabilities is effective, consistent, and complete;

– ensure that the necessary communications take place at the technical level between the Questions of the study group, Questions of other study groups, and other groups defining standards relating to emergency telecommunications, as identified by the plans maintained by the respective lead study groups;

– review capabilities associated with ETS and disaster relief specified in Recommendations within the area of responsibility of the study group, to ensure that they are still relevant and effective;

– contribute to the development and maintenance of the plans which are the responsibility of the respective lead study groups for emergency telecommunications, including the proposal of new content when this seems appropriate;

– create Supplements and Recommendations defining signalling requirements and protocols in support of emergency telecommunications and disaster relief in IMT-2020 network and beyond;

– create Supplements and Recommendations defining signalling requirements and protocols in support of emergency telecommunications and disaster relief for terrestrial and satellite network convergence.

An up-to-date status of work under this Question is contained in the SG11 work programme (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>).

### C.4 Relationships

Recommendations:

– The work that the Question oversees operates within the framework defined by Recommendation ITU‑T Y.1271 and Recommendation ITU‑T Y.2205

Questions:

– All Questions of SG11

Study Groups:

The Question will relate to the following Study Groups, especially with Questions specifically related to emergency telecommunications:

– ITU‑T SG2

– ITU‑T SG9

– ITU‑T SG13

– ITU‑T SG16

– ITU‑T SG17

– ITU‑T SG20

Other bodies:

– ARIB

– ATIS

– IETF

– IEEE

– ETSI

– TIA

– TTA

– TTC

WSIS action lines:

– C2, C5

Sustainable Development Goals:

– 9, 11, 13, 16

## D Question 4/11 – Protocols for control, management and orchestration of network resources

(Continuation of Questions 4/11)

### D.1 Motivation

ITU‑T SG11 Q4 has developed a series of data models, signalling requirements and protocols related Recommendations on control, management and orchestration of bearer network resources. It is expected that the standardization on the above aspect continues, including but not limited to Software-Defined Networking (SDN), Network Function Virtualization (NFV), cloud computing networking, network slicing, IMT-2020 network and beyond, network virtualization, IPv6 transition, future networks (FN), and expands to new ITU-T study area, such as Artificial Intelligence/Machine Learning (AI/ML) and big data driven networking, Distributed Ledger Technology, distributed cloud, Multi-access Edge Computing (MEC), computing power networking, and other emerging IT supporting bearer network technologies.

The behaviour of the traffic which is generated by more and more new services, such as the service enabled by SDN, NFV, cloud computing networking, and other emerging IT supporting bearer network technologies, is very different from the traffic generated by the traditional NGN services. Accordingly, the architecture to control such new traffic may become more complicated. Bearer network signalling requirements are closely related to network resource control mechanisms and protocols.

Recommendations in force for which the Question is responsible: Q.1970, Q.1990, Q.2630, Q.2761-2764, Q.2920, Q.2931 and Q.2932.1, Q.3150/Y.1416, Q.3151/Y.1417, Q.3300, Q.3301.1, Q.3302.1, Q.3303.0, Q.3303.1, Q.3303.2, Q.3303.3, Q.3304.1, Q.3304.2, Q.Suppl.51, Q.Suppl.67, Q.3316, Q.3405, Q.3716, Q.3718, Q.3740, Q.3741.

### D.2 Question

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

– What data models, signalling requirements and protocols are required for control, management, and orchestration of network resources involving new types of transport protocols and transport networks (e.g. cloud computing networking, smart grid, FN, SDN, NFV, network virtualization, network slicing, MEC and IMT-2020 network and beyond)?

– What data models, signalling requirements and protocols are required for big data and AI/ML driven networking?

– What data models, signalling requirements and protocols are required for networking telemetry?

– What data models, signalling requirements and protocols are required for Distributed Ledger Technology supported networking?

– What data models, signalling requirements and protocols are required for cloud and distributed cloud networking?

– What data models, signalling requirements and protocols are required for computing power networking?

– What new Recommendations are required to support bearer and resource control for new application areas such as unicast/multicast flows for IPTV service, home networking, and mobility?

– What new Recommendations are required to support handover control for mobility?

– What new Recommendations are required to support security of bearer and resource control and signalling?

– What new functional architecture and protocol enhancements are required to support bearer and resource control for services and applications of public interest, such as emergency call handling and disaster relief?

– What new Recommendations are required to support signalling of quality of service (QoS) information, traffic management?

– What enhancements to existing Recommendations are required to provide energy savings directly or indirectly and efficient resource utilization in information and communication technologies or in other industries?

– What enhancements to new Recommendations are required to provide such energy savings and efficient resource utilization?

– What new services can be identified for which the introduction of IPv6 is a necessary precondition?

– What new protocol procedures are required to implement the services identified above?

– What new Recommendations on information model and data model are required to collaborate with emerging open source communities?

### D.3 Tasks

Tasks include, but are not limited to:

– develop data models, signalling requirements and protocols for new bearer services to support traffic of new applications based on future network architectures, including SDN, NFV, network virtualization, MEC, network slicing, cloud and distributed cloud networking, IMT-2020 network and beyond, etc.;

– develop data models, signalling requirements and protocols for big data and AI/ML driven networking;

– develop data models, signalling requirements and protocols for networking telemetry;

– Develop data models, signalling requirements and protocols for cloud and distributed cloud networking;

– develop data models, signalling requirements and protocols for Distributed Ledger Technology supported networking, including Decentralized Trustworthy Network Infrastructure (DNI);

– develop data models, signalling requirements and protocols for computing power networking;

– develop signalling requirements and protocols for admission control coordination;

– develop signalling requirements and protocols for bearer and resource control and traffic management supporting unicast/multicast flows for IPTV service;

– develop signalling requirements and protocols for QoS signalling and traffic management;

– develop signalling requirements and protocols for bearer and resource control supporting home networking;

– develop signalling requirements and protocols to support handover for seamless session mobility;

– develop signalling requirements and protocols for interaction among bearer and resource control domains;

– develop specifications of interfaces to adjacent layers with relevant ITU‑T SG Questions/groups;

– enhance the existing bearer and resource control and signalling related Recommendations;

– study and develop Recommendations to identify requirements for service dependent bearer control and signalling related mechanisms;

– identify services for which new protocol procedures are required for the transition to IPv6;

– develop new protocol procedures for services identified above;

– develop informational model and data model based signalling requirements and protocols for further implementation using open source.

An up-to-date status of work under this Question is contained in the SG11 work programme (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>).

### D.4 Relationships

Recommendations:

– H.248, Q.1950, Y.1541, Y.1221, Y.2111, I.555, Q.1970, Q.1990, Q.263x-series, Q.29xx-series, Y.2121, Y.3300, Y.35xx-series, Q.37xx-series, Q.33xx-series, Q.34xx-series

Questions:

– All Questions of SG11

Study Groups:

– SG15 on transport and ASON technologies, especially on transport network architectures and management and control of transport systems and equipment

– SG16 on multimedia and AI aspects

– SG17 on security aspects

– SG13 on SDN, NFV, cloud and distributed cloud networking, network virtualization, network slicing, MEC, big data driven networking, AI/ML driven networking, IMT‑2020 network and beyond

Other bodies:

– 3GPP

– ETSI

– IEEE

– IETF

– TIA

– Linux Foundation Edge

– Linux Foundation Networking (LFN)

– Linux Foundation Hyperledger

– OpenStack

– Open Network Operating System

WSIS action lines:

– C2, C11

Sustainable Development Goals:

– 9

## E Question 5/11 – Signalling requirements and protocols for border network gateway in the context of network virtualization and intelligentization

(Continuation of Question 5/11)

### E.1 Motivation

As the anchor of user access network and service provision, the device form and the deployment of service functions for border network gateway (BNG) are constantly evolving with new technologies such as SDN, NFV, cloud computing, Internet of Things and artificial intelligence, especially with the network architecture evolving toward virtualization, openness and intelligentization. Therefore, in order to adapt to the network architecture evolution, new service requirements, interfaces and signalling protocols for border network gateway need to be defined to support the multi-services, as well as BNG's capabilities need to be enhanced to provide better QoS, reliability and security for bearing multi-services.

When introducing the software-defined networking (SDN), network function virtualization (NFV) and network intelligence technology into access network, it is required to define new interfaces for open network capabilities, define new protocol to control underlay physical transfer devices, define new protocol interactive process to communicate between controller and transfer devices, define new protocols and procedures to improve reliability, resource utilization and flexibly distribute user's policies among the multiple BNGs. Also new protocol procedures are required to enable the rapid provisioning of services over customer IP networks, the services to the customer through multiple border network gateways and the open networking value added service (VAS).

With the introduction of the emerging technologies, the carrier’s network architecture is also gradually evolving. The border network gateway is required to have the capabilities to bearer multi-service, and implement functions such as a fixed network (e.g. BRAS), a mobile network (e.g. PDN Gateway), an IoT service gateway, and Space-terrestrial network gateway, etc. The BNG’s functions can be implemented by loading virtual network functions (VNFs) onto the virtualized telecom-cloud infrastructure. It is necessary to study the functional requirements of the border network gateway according to the different scenarios, the user access control, the service distribution and provision process, the signalling protocol and QoS guarantee mechanism for flexible resource scheduling when different forwarding performance requirements and security features are needed.

In addition, in order to realize the network automation operation and efficient and flexible scheduling of the network resources, artificial intelligence technology is introduced into the network. It is required to acquire the real-time network status data of the whole network from the key network elements (e.g. BNG) to achieve intelligent control decision to provide users with higher QoS guarantee. The data model, the data interaction process, and the signalling protocol need to be defined, so that the AI decision entity can acquire the real-time network status data, and deliver the optimized policy to the network elements (e.g. BNG) to implement efficient bearing the user services.

### E.2 Question

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

– What new protocols and procedures need to be specified to enable rapid provisioning of services over customer IP networks adopting emerging technologies (e.g. SDN/NFV, cloud computing, IoT, AI, MEC, etc.)?

– What new protocols and procedures need to be specified to enable services and policies to the customer through broadband network gateways adopting emerging technologies?

– What new protocols and procedures need to be specified to enable computing power network among multiple border network gateways?

– What new interfaces, protocols and functions need to be implemented for border network gateway to support emerging technologies?

– What new interfaces, protocols and functions need to be implemented for border network gateway to support the convergence of multiple access network technologies (including. fixed access, mobile access, IoT access and space access, etc.)?

– What new mechanisms, protocols and procedures need to be specified to distribute user's policies to control user's access and ensure user's QoS?

– What new protocols and procedures need to be specified to enable open networking value added service (VAS)?

– What new protocols and procedures need to be specified in border network gateway for bearing multi-services?

– What new protocols and procedures need to be specified to enable the AI-assisted network management and resource orchestration among multiple border network gateways?

– What new data model, protocol and interaction process to be specified to enable the AI decision entities acquiring the real-time status data from border network gateways?

### E.3 Tasks

Tasks include, but are not limited to:

– develop service descriptions for the services, which are not described in other SDOs, and define terms as needed;

– develop new protocols and procedures to enable rapid provisioning of services over customer IP networks;

– develop new protocols and procedures to enable service to the customer through border network gateways adopting emerging technologies;

– develop new protocol and procedures to enable computing power network among multiple border network gateways;

– develop new requirements, protocols and functions for border network gateway to support emerging technologies (e.g. SDN/NFV, cloud computing, IoT, AI, MEC, etc.);

– develop new requirements, protocols and functions for border network gateway to support the convergence of multiple access network technologies (including fixed access, mobile access, IoT access and space access, etc.);

– develop new protocols and procedures for border network gateway to improve network resource utilization by intelligent network control;

– develop new protocols and procedures to enable the management and distribution of user's policies by SDN technologies;

– develop new protocols and procedures to enable open networking value added service (VAS);

– develop new protocols and procedures for bearing multi‑services on BNG;

– development of methodology for security testing and test specification for security testing of protocol procedures relating to services provided by broadband network gateways;

– develop new protocol and procedures to enable the AI-assisted network management and resource orchestration among multiple border network gateways.

An up-to-date status of work under this Question is contained in the SG11 work programme (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>).

### E.4 Relationships

Recommendations:

– Q, Y and H-series

Questions:

– A/11, B/11 and D/11 on policy control

– C/11, G/11 and M/11

Study Groups:

– ITU‑T SG13 and other Study Groups working on NGN, FNs, IMT-2020 and broadband network gateways

– ITU-T SG20

Other bodies:

– Broadband Forum

– IETF

– ETSI

Open Source:

– ONAP

WSIS action lines:

– C2

Sustainable Development Goals:

– 9

## F Question 6/11 – Protocols supporting control and management technologies for IMT-2020 network and beyond

(Continuation of Question 6/11)

### F.1 Motivation

ITU‑T SG11 Q6/11 has developed several protocols for control and management technologies such as orchestration, network slicing, network capability exposure, identification and network management of heterogeneous network environments to realize IMT-2020 network.

Artificial Intelligence (AI) application in network for enabling network automation and intelligence are important topics these days. How AI and big data technologies are leveraged to support intelligent control and management for IMT-2020 network and beyond should be specified and provided urgently to meet the market requirements. Especially, protocols to support intelligent control for IMT-2020 network and beyond, enhanced mechanisms such as low latency, low jitter and packet loss, guaranteed bandwidth, very large scale network, flexible connectivity and topology, resources assignment and sharing, and network slicing should be developed with high priority. With specific requirements from vertical industries, user plane management should be enhanced to optimize the user path and meet industry needs.

Also, protocols on common management system for accommodating both fixed and mobile networks are other important issues that have to be resolved in the future.

### F.2 Question

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

– What protocols and mechanisms need to be defined in response to gap analyses developed by relevant SDOs?

– What protocols and mechanisms need to be defined in support of service scenarios, requirements, capabilities, and architecture for IMT-2020 network and beyond provided by relevant ITU-T SGs and other SDOs?

– What protocols and mechanisms need to be defined for the key technologies to realize IMT-2020 network and beyond including intelligent control for transport network, orchestration, network slicing, user plane optimization, network capability exposure, identification, device authentication, fixed/mobile convergence, network management of heterogeneous network environments, etc.?

– How emerging technologies including AI, big data, and QKDN and related technologies are leveraged in the control and management protocols for IMT-2020 network and beyond?

– What protocols and mechanisms should be defined to realize high performance with features like ultra-low latency and high reliability for IMT-2020 network and beyond?

– What protocols and mechanisms should be defined to realize improvements and enhancements to service-based interface for IMT-2020 in order to improve efficiency, flexibility and intelligence?

– How to utilize and guide the open source software, in collaboration with relevant bodies, related to key technologies of IMT-2020 network and beyond to implement the developed Recommendations?

### F.3 Tasks

Tasks include, but are not limited to:

– develop Recommendations on protocols, including mechanisms, to control IMT-2020 network and beyond with enhanced features, supporting very large-scale network, flexible connectivity and topology, fixed/mobile convergence, user plane optimization, etc.;

– develop Recommendations on protocols, including mechanisms, to support IMT-2020 network and beyond by using technologies such as network slicing, resource virtualization, orchestration, AI and big data, QKDN and related technologies, etc.;

– develop Recommendations on protocols, including mechanisms, for other key technologies of IMT-2020 network and beyond including identification, device authentication, and network capability exposure, etc.;

– develop Recommendations on protocols, including mechanisms, for common management system for IMT-2020 network and beyond;

– develop Recommendations on protocols, including mechanisms, for IMT-2020 network to realize high performance with features like ultra-low latency and high reliability;

– develop Recommendations on protocols for IMT-2020 network and beyond, to realize improvements and enhancements to service-based interface in order to improve efficiency, flexibility and intelligence;

– develop Supplement, Technical Report, Guidelines on the best practices and implementations of protocols and mechanisms, for IMT-2020 network and beyond, including open source software, in collaboration with relevant bodies.

An up-to-date status of work under this Question is contained in the SG11 work programme (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>).

### F.4 Relationships

Recommendations:

– Y-series and Q-series

Questions:

– D/11, G/11, H/11, K/11

Study Groups:

– ITU-T Study Group 2

– ITU-T Study Group 13

– ITU-T Study Group 15

– Other SGs involved with IMT-2020 studies

Other bodies:

– ITU-R

– ETSI

– IETF

– IEEE

– 3GPP

**WSIS action lines:**

– C2, C5

**Sustainable Development Goals:**

– 9, 17

## G Question 7/11 – Signalling requirements and protocols for network attachment and edge computing for future networks, IMT-2020 network and beyond

(Continuation of Question 7/11)

### G.1 Motivation

ITU‑T has conducted studies on signalling requirements and protocols for future networks. Edge computing which is required for AI, big data, autonomous drive and robots are hot topics since IMT-2020 has been firstly commercialized in these days.

The future networks and the IMT-2020 will involve a wide range of services (e.g. multimedia, sensing, AI, big data, mobility, robots, etc.) including convergence aspects, based on its high computing power and capability in edge networks for heterogeneous networks (e.g. IMT-2020, LTE, 3G, WLAN, BLE, LPWA, etc.) and multiple devices (e.g. smart phone, tablet, laptop, sensors, CCTV etc.) and cloud computing environment (e.g. edge cloud, public cloud etc.) of different capabilities in dynamic combination for collaboration. This is the so called "Edge Computing", and signalling protocols are expected to bridge the source and the device to realize it. Those will involve federated authentication and configuration for dynamic media handover, per-session allocation of IP addresses and terminal configuration, network access authorization checking, in-session modification of service connectivity, attachment control, resource allocation for edge computing.

In addition, IMT-2020 increases the data packet traffic speed by up to ten times than 4G, whereas edge computing reduces transaction latency by locating computing capability in IMT-2020 network, closer to the end mobile users. In this perspective, cloud-based computing capability is also important to provide ultra-low latency-based data transaction for low latency and high throughput required services (e.g. VR/AR, Streaming Media, Industrial 4.0, Robots, IoT etc.). These procedures will have to be designed to take into account various emerging services such as AR/VR, Streaming Gaming, AI, Bigdata, Autonomous Driving, Robots, etc.

Maximizing service versatility and device capability also requires the maximization of resource utilization and awareness-based control. Accordingly, the core aspects of future networks, such as virtualization and software-defined networking (SDN), intelligent edge computing (IEC), multi-access edge computing (MEC), Cloud Services for access network must be considered.

### G.2 Question

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

– What new and revised Recommendations are required to handle the revisions of NACF signalling protocol requirements?

– What new Recommendations are required to specify signalling requirements and protocols to support attachment and edge computing services (AI, Bigdata, mobility, edge cloud, etc.) for multi-device/interface/connection services?

– What associated mechanisms are required with attachment and edge computing signalling to assure security for multi-device/interface/connection services?

– What control mechanisms are required with attachment and edge computing signalling to support the mobility management and virtual resource management?

– What functional architecture and entities are required for network attachment and edge computing to support future networks and IMT-2020 network, including SDN, NFV, IEC and MEC in access network?

– What functional architecture and entities are required to support multi-interface streaming services focusing on its access attachment signalling and protocols?

### G.3 Tasks

Tasks include, but are not limited to:

– maintain existing Recommendations which are under study in this Question;

– develop signalling requirements and protocols to support revisions of network attachment and edge computing protocol requirements;

– develop signalling requirements and protocols to support attachment and edge computing procedures for multi-devices, multi-connections, and multi-interfaces for future networks (e.g., SDN, NFV) and IMT-2020 network and beyond;

– develop signalling requirements and protocols to support mobility and resource management functions in both access and core networks;

– develop signalling requirements and protocols to support diverse and efficient traffic classification and steering schemes based on MEC enabled device (e.g. SDK, IEC, MEC enabled layer etc.), Core Network (e.g. network slicing, APN etc.) and edged equipment management (e.g. edge cloud computing etc.) for low latency guaranteed IMT-2020 network and beyond;

– develop signalling requirements and protocols to support mobility management and service/application migration over edge computing and edge cloud enabled environment including computation allocation, mobility-aware resource allocation and fault tolerance support for nearest edge traffic routing in future networks, IMT-2020 network and beyond.

An up-to-date status of work under this Question is contained in the SG11 work programme (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>).

### G.4 Relationships

Recommendations:

– Y-series Recommendations on requirements and architecture of FNs and IMT-2020 network and beyond

– Q-series Recommendations on signalling requirements, protocols, measurement and testing

Questions:

– Questions A/11, B/11, D/11, M/11, F/11

Study Groups:

– SG13 on requirement and architecture, mobility management and virtualization of resources of future networks and IMT-2020 network and beyond

– SG16 on multimedia services over multi-device/interface/connection environments

– SG20 on M2M and IoT services and protocols

– SG17 on security and identity management

Other bodies:

– ISO/IEC JTC1/WG7

– IETF

– OMA

– ETSI

WSIS action lines:

– C2

Sustainable Development Goals:

– 9

## H Question 8/11 – Protocols supporting distributed content networking, information centric network (ICN) technologies for future networks, IMT-2020 network and beyond

(Continuation of Question 8/11)

### H.1 Motivation

Emerging multimedia services and applications require various functions and facilities. One of the key features of multimedia applications with multi-party communication capability is end-to-end multicast transport functions. Based on this motivation, a set of ITU-T Recommendations have been developed on frameworks and protocols for group management and end-to-end multicast communications over IP multicast as well as non-IP multicast network environments. As a result of collaboration work with ISO/IEC JTC 1/SC 6, common text standards have been developed for multi-party communications and include ITU-T X.606-series | ISO/IEC 14476-series, ITU-T X.607-series | ISO/IEC 14476-series, ITU-T X.608-series | ISO/IEC 14476-series, ITU-T X.602 | ISO/IEC 16513, ITU-T X.603-series | ISO/IEC 16512-series, ITU-T X.604-series | ISO/IEC 24793-series, ITU-T X.605 | ISO/IEC 13252. These Recommendations will need to be continuously maintained and may be updated if further requirements from the market arise.

Various distributed and conversational multimedia services, such as IPTV, Digital signage, VoD, telepresence, personal broadcasting service, multimedia streaming and other emerging contents delivery services require efficient communications capability over various network environments and need to support enhanced contents such as AR/VR, UHD (4K, 8K). Distributed service networking protocols based on peer-to-peer (P2P) technology can be one of the useful solutions for supporting new emerging applications which require high performance and scalable communications capability. SG11 has been developing Recommendations on signalling architecture and protocols for managed P2P (MP2P) communications, which can be applied to end-to-end multimedia communications including video streaming and content distribution services. Standards development of protocols for hybrid P2P (HP2P) communications which consist of mesh-based P2P network and tree-based P2P network has also started and will be continued. HP2P communication protocols will provide efficient and flexible information distribution capabilities for IoT related services and Distributed Ledger Technology services. The set of Recommendations to be developed will provide solutions and guidelines for vendors and providers who want to implement and deploy distribution and delivery services for various types of content using P2P technologies.

Information centric network (ICN) has been and continues to be studied in many SDOs and notably in the Information Centric Research Group of IETF. Consideration is given to ICN technologies integrated into the existing Internet through Overlay deployments (ICN over IP), Underlay deployments (ICN islands within IP), or ICN in Virtualized IP infrastructure. These approaches are described in RFC 8763. Protocols and mechanisms for content discovery, distribution and delivery based on information centric network (ICN) technology in overlay, underlay and virtualised IP deployments will constitute very important emerging issues to support related requirement and capabilities of IMT-2020 network and beyond.

Recommendations under responsibility of this Question include: X.601, X.602, X.603, X.603.1, X.603.2, X.604, X.604.1, X.604.2, X.605, X.606, X.606.1, X.607, X.607.1, X.608 and X.608.1, X.609, X.609.1, X.609.2, X.609.3, X.609.4, X.609.5, X.609.6, X.609.7, X.609.8, X.609.9, X.609.10, Q.4100-Q.4139 (for protocols and signalling for P2P communications).

### H.2 Question

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

– What maintenance or enhancements to existing Recommendations need to be developed in response to new market requirements?

– What Recommendations need to be developed to provide protocols for content discovery, distribution and delivery to support requirements and functional architectures of legacy and FNs, IMT-2020 network and beyond?

– What Recommendations need to be developed to provide protocols for content discovery, distribution and delivery based on ICN technology in overlay, underlay and IP virtualisation deployments which are taken into account in FNs, IMT-2020 network and beyond?

– What protocols and mechanisms need to be developed to support managed and hybrid peer-to-peer communications?

– What mechanisms and key technologies need to be defined to realize application defined and network aware?

– What layer 4 interfaces and parameters need to be defined toward upper and lower layer, respectively?

### H.3 Tasks

Tasks include, but are not limited to:

– Maintain and enhance Recommendations X.60x-series, including common text standards for multi-party communications in collaboration with ISO/IEC JTC 1/SC 6 in response to new market requirements;

– Develop Recommendations on protocols to support contents discovery, distribution and delivery issues for legacy network, FNs, IMT-2020 network and beyond;

– Develop Recommendations on protocols to support contents discovery, distribution and delivery issues based on information centric network (ICN) technology in overlay, underlay and IP virtualisation deployments which are taken into account in IMT-2020 network and beyond;

– Develop Recommendations on protocols and mechanisms to support managed and hybrid peer-to-peer communications;

– Develop Recommendations on protocols to support end-to-end multi-party, multimedia communications including personal broadcasting services and applications.

An up-to-date status of work under this Question is contained in the SG11 work programme (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?Q=8/11>).

### H.4 Relationships

Recommendations:

– X-series Recommendations on multi-party, multimedia communications

– Y-series Recommendations and Supplements on IPTV, content delivery, DSN, FNs and IMT-2020 network and beyond

– H-series Recommendations on multimedia services and applications

– Q-series Recommendations on signalling, protocols, measurements and test specifications related to the scope of Question

Questions:

– All Questions of SG11

Study Groups:

– ITU‑T SG13 on FNs, and IMT-2020 network and beyond

– ITU‑T SG16 on multimedia services and applications

– ITU‑T SG17 on related security issues

Other bodies:

– ISO/IEC JTC 1/SC 6

– IETF, ICNRG

WSIS action lines:

– C2

Sustainable Development Goals:

– 9

## I Question 12/11 – Testing of internet of things, its applications and identification systems

(Continuation of Question 12/11)

### I.1 Motivation

In a broad perspective, the Internet of things (IoT) can be perceived as a vision with technological and societal implications. From the perspective of technical standardization, IoT can be viewed as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies. Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst maintaining the required privacy. The concepts of u1-society, u-network, u-city and others have been formulated in support of the worldwide perspective for IoT applications, services and technologies which may be enabled by radio frequency identification (RFID), ubiquitous sensor network (USN), machine-oriented communication (MOC), machine-to-machine (M2M) communication, smart device communication (SDC), Cloud-enabled IoT services (CIS), where RFID has been taken into account by ISO/IEC JTC 1/SC 31, sensor network technologies by ISO/IEC JTC 1/WG 7, USN by ITU‑T SG20, MOC by ITU-T SG13, M2M by ITU‑T and ETSI, SDC by TIA, CIS by ETSI, OGC, and W3C.

NOTE 1 – "u" stands for "ubiquitous" which has been interpreted as a capability for any services at anytime and anywhere through any devices.

All these keywords have some similar use cases and imply some identical functions but consider some different technology views. The IoT may be seen as an umbrella for all these technology keywords.

Since the IoT has such broad concept and may be associated with various enabling technologies, interoperability issues shall be considered.

In general, IoT discovers various new types of connectivity which may be used in different customer-oriented applications (e.g. flying ubiquitous sensor networks (FUSN), IoT-based augmented reality (AR) and so on).

Also, taking into account the secure authentication mechanism used by IoT-based technologies and IoT identity, IoT may be considered as one of the tools to be used for combating counterfeiting.

Bearing in mind all the above, the testing of the IoT technologies/applications are becoming more important today, especially in terms of interoperability of the IoT devices and trust of the used IoT systems.

In addition to traditional IoT applications, it is advisable to consider testing in areas in which the largest implementation of IoT-devices is observed:

– Smart Sustainable Cities;

– Wearable devices;

– Industrial Internet of things (IIoT);

– Network-based driving assistance for autonomous vehicles;

– Flying networks based on Unmanned Aerial Vehicles.

As a rule, in each of these areas there are different scenarios for connecting IoT-devices to the Internet, cloud platforms and remote services. In this regard, the consideration of issues of testing procedures of IoT-devices seems to be very relevant.

### I.2 Question

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

– What types of tests are needed for IoT network elements?

– How to test the security of IoT-device taking into account their parameters (e.g. performance, memory size, communication channel etc.)?

– What test suites need to be developed for testing IoT identification/authentication procedures?

– How to test IoT technical solutions to be used for combating counterfeiting?

– What new Recommendations need to be developed in order to provide mechanisms to test the IoT applications, including the security and privacy aspects?

– What new Recommendations need to be developed in order to provide mechanisms to test the interoperability, capability, and security of IoT identification systems?

– What are the testing scenarios to be used for testing wearable devices?

– What are the testing scenarios to be used for testing Industrial IoT (IIoT) system and devices?

– What test suites need to be developed for testing methodology and/or mechanism (procedures) for testing the technologies and protocols for IoT and IIoT based on prediction analytics?

– What new Recommendations need to be developed in order to provide the interoperability, compatibility, and security of IoT devices to be used in Smart Sustainable City?

– What testing procedures need to be developed for IoT-based technologies and protocols for network-based driving assistance to be used in autonomous vehicles?

### I.3 Tasks

Tasks include, but are not limited to:

– develop the test suites to be used for testing IoT network elements;

– develop the methodology for security testing and test specification related to security testing of IoT;

– develop test suites for testing IoT identification/authentication procedures;

– develop test suites for testing IoT technical solutions to be used for combating counterfeiting;

– develop the methodology and/or mechanism for testing the IoT applications, including the security and privacy aspects;

– develop the methodology and/or mechanism for testing the interoperability, capability, and security of IoT identification systems;

– develop the methodology and/or mechanism for testing the wearable devices;

– develop the methodology and/or mechanism for testing the Industrial Internet of Things and IIoT applications;

– develop the methodology and/or mechanism for testing the technologies and protocols for IoT and IIoT based on prediction analytics;

– develop the methodology and/or mechanism for testing the IoT-based technologies and protocols to be used in Smart Sustainable City;

– develop the methodology and/or mechanism for testing the IoT-based technologies and protocols for network-based driving assistance to be used in autonomous vehicles.

An up-to-date status of work under this Question is contained in the SG11 work programme (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>).

### I.4 Relationships

Recommendations:

– Q, Y, H, I, M and F-series

Questions:

– L/11; M/11

Study Groups:

– ITU‑T SG2

– ITU-T SG5

– ITU‑T SG13

– ITU‑T SG16

– ITU‑T SG17

– ITU‑T SG20

Other bodies:

– ETSI especially TC cyber

– IEEE

– IETF

– ISO/IEC JTC 1 (especially ISO/IEC JTC 1 TC27, JTC1 WG 7, ISO/IEC JTC 1/SC 6, ISO/IEC JTC 1/SC 31, ISO/IEC JTC 1/WG 10)

– OGC

– TIA

– W3C

WSIS action lines:

– C5

Sustainable Development Goals:

– 9

## J Question 13/11 – Monitoring parameters for protocols used in emerging networks, including cloud/edge computing and software-defined networking/network function virtualization (SDN/NFV)

(Continuation of Question 13/11)

### J.1 Motivation

The following emerging networks have been identified and developed: future networks (FNs), Internet of things (IoT), VoLTE/ViLTE-based networks, IMT-2020, etc. In order to reduce investment and operating costs, software defined networking (SDN) as well as network function virtualization (NFV) have been deployed in emerging networks to achieve the separation of control and service, control and bearer, hardware and software.

Cloud computing and edge computing is also becoming the infrastructure of the cyber world. In this new emerging environment, operators and end-users should have capabilities in place to monitor whether the infrastructure they are using can support applications and services.

As AI technology becomes more and more mature, it is applied to the network, such as intelligent decision-making and intelligent prediction for operators and Internet enterprises. The selection of monitoring parameters in intelligent decision-making model or intelligent prediction model has great influence on the efficiency of the network and users’ experience lastly.

Standardization of monitoring system parameters for emerging networks, including cloud computing, will give operators, administrations and end-users monitoring information that is compatible and comparable across network operators, service providers and end-users. Moreover, it could be useful to help resolve points of disagreement.

### J.2 Question

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

– What is the minimum parameter set, which need to be used to assess network performance?

– What is the minimum parameter set, which need to be used for monitoring cloud computing and edge computing?

– What is the minimum parameter set, which need to be used for monitoring NFV and SDN?

– What is the minimum parameter set, which need to be used for monitoring emerging networks, applications and services?

– What kind of parameters need to be used for monitoring security issues?

– What kind of parameters need to be used for AI technology in emerging networks, applications and services?

– What is the minimum parameter set, which need to be used for monitoring intelligent networks, applications and services?

### J.3 Tasks

Tasks include, but are not limited to:

– develop a minimum parameter set and a methodology for its measurement, which need to be used to assess network performance;

– develop a minimum parameter set and a methodology for its measurement, which need to be used to assess cloud computing and edge computing;

– develop a minimum parameter set and a methodology for its measurement, which need to be used to assess NFV and SDN;

– develop a minimum parameter set and a methodology for its measurement, which need to be used to assess emerging networks, applications and services;

– study what kind of parameters need to be used for monitoring security issues;

– study what kind of parameters need to be used for AI technology in emerging networks, applications and services;

– study what kind of parameters need to be used intelligent networks, applications and services.

An up-to-date status of work under this Question is contained in the SG11 work programme (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>).

### J.4 Relationships

Recommendations:

– ITU‑T Q, Y, H, I, M, F and P-series

Questions:

– A/11, B/11, D/11, G/11, M/11, I/11 and K/11

Study Groups:

– ITU‑T SG3 on policy and regulatory issues

– ITU‑T SG12 on QoS/QoE issues

– ITU‑T SG13 on FNs, SDN/NFV, cloud computing and emerging networks architecture

– ITU‑T SG16 on multimedia services and applications

– ITU‑T SG17 on security issues

– ITU‑T SG20 on IoT and its applications

Other bodies:

– ETSI

– IEEE

– IETF

WSIS action lines:

– C2, C5

Sustainable Development Goals:

– 9

## K Question 14/11 – Testing of cloud, SDN and NFV

(Continuation of Question 14/11)

### K.1 Motivation

Cloud computing is a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand. Software-defined networking is a set of technologies that enables to directly program, orchestrate, control and manage network resources, which facilitates the design, delivery and operation of network services in a dynamic and scalable manner. Network functions virtualization refers to principle of separating network functions from the hardware they run on by using virtual hardware abstraction.

Cloud, SDN and NFV are emerging technologies that are widely used in a variety of scenarios. The conformance, interoperability, and benchmark testing of cloud, SDN and NFV are very important study topics.

In the context of cloud/SDN/NFV, conformance testing is testing to verify that an implementation of cloud/SDN/NFV is compliant with a developed standard, such as a functional requirement standard or a protocol specification. Interoperability testing is testing to assess the ability of entities involved in cloud/SDN/NFV to interact with each other as expected. Benchmark testing is testing used to measure implementation of cloud/SDN/NFV, from the performance aspect.

In addition, more and more services are implemented by using cloud, SDN and NFV technologies, such as SD-WAN. The testing of services based on cloud, SDN and NFV are needed to be considered.

Cooperation with ITU-T SG13 (the lead SG on cloud) on testing of cloud is necessary. Cloud related testing activities will start after terminology and architecture are identified by SG13.

### K.2 Question

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

– What are the requirements for conformance, interoperability and benchmark testing of cloud, SDN and NFV?

– What kind of test suites are needed for testing of cloud, SDN and NFV, including conformance, interoperability and benchmark aspect?

– How to establish automated testing system for cloud, SDN and NFV to improve testing efficiency?

– What kind of test suites are needed for testing of services implemented by cloud, SDN and NFV?

– What collaboration is necessary to minimize duplication of efforts with other SDOs?

– What collaboration is necessary to utilize open source community?

### K.3 Tasks

Tasks include, but are not limited to:

– identify conformance, interoperability and benchmark testing requirements for cloud, SDN and NFV;

– develop test suites for conformance, interoperability and benchmark testing of cloud, SDN and NFV;

– develop methodology and framework for automated testing of cloud, SDN and NFV;

– develop test suites for testing of services implemented by cloud, SDN and NFV;

– provide necessary collaboration with external SDOs, consortia and forums and open source communities;

– maintain and enhance the Recommendations for which the Question is responsible.

An up-to-date status of work under this Question is contained in the SG11 work programme (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>).

### K.4 Relationships

Recommendations:

– Q, Y, H, I, M and F-series (especially Cloud computing and testing related Recommendations)

Questions:

– All Questions of SG11

Study Groups:

– SG2 on Operational aspects

– SG12 on QoS/QoE

– SG13 on future network architecture and cloud computing

– SG15 on Transport, Access and Home

– SG16 on multimedia services and applications

– SG17 on security

Other bodies:

– ISO/IEC JTC 1 (especially ISO/IEC JTC 1 SC 38)

– IETF

– ETSI NFV ISG

– IEEE

– OASIS

– NIST

– TM Forum

– ONF

WSIS action lines:

– C2, C5, C11

Sustainable Development Goals:

– 9

## L Question 15/11 – Combating counterfeit and stolen telecommunication/ICT devices

(Continuation of Question 15/11)

### L.1 Motivation

The work of this Question was mainly focused on the development of Recommendations and Technical Reports on combating counterfeit telecommunication/ICT device. The growing usage of telecommunication/ICT device in people’s daily lives in recent years resulted in increased problems related to the sale, circulation and use of counterfeit device in most markets as well as their adverse consequences for manufacturers, users and governments.

A considerable number of telecommunication/ICT device have been found to be counterfeit and have created concerns about national security, performance, quality of service delivery and revenue losses for all stakeholders. This has led to calls by ITU Member States, particularly those in developing countries to address the issue, especially the negative effects and to study any positive impact of measures taken.

In addition, the demand for services, resulting in the increased production and availability of telecommunication/ICT device has also seen the rise of stolen device. Some of these devices are returned to the market after they have been tampered with and their identity modified, hence bypassing identity blacklisting solutions implemented by Governments and mobile network operators. Consequently, most countries around the world are not only engaged in combating counterfeit telecommunication/ICT device, but also have put in place measures against theft of telecommunication/ICT device and some of them to tackle stolen device with modified identities from reactivating on networks and to effectively manage the situation.

SG11 approved Recommendation ITU-T Q.5050 “Framework for solutions to combat counterfeit ICT devices”, Recommendation ITU-T Q.5051 “Framework for combating the use of stolen mobile devices” and started a number of new work items.

Within ITU and around the world, there have been debates as to whether or not conformance and interoperability testing could be one of the solutions to combat counterfeit ICT devices. ITU Resolution 188 (Rev. Dubai, 2018) of the Plenipotentiary Conference, aware that tampering with telecommunication/ICT devices may diminish the effectiveness of solutions adopted by the countries to address counterfeiting, invites Member States to take all necessary measures to combat counterfeit telecommunication/ICT devices. Any unique and persistent identifiers could allow the recognition of genuine products. Additionally, special attention should be given to consider the potential growth of counterfeit IoT devices and the concern this may pose.

Moreover, ITU Resolution 189 (Rev. Dubai, 2018) of the Plenipotentiary Conference, on the combat of mobile devices theft, resolves to explore and encourage the development of ways and means to continue to combat and deter mobile device theft, and invites Member States to adopt the necessary actions to prevent, discover and control tampering and replication of mobile ICT device identifiers, and prevent devices with tampered/replicated identifiers from accessing mobile networks.

This Question intends to explore relevant possibilities to combat stolen and counterfeit telecommunication/ICT devices and, in particular, its relations to products supply chain identity management, traceability, security, privacy and trust of people and networks. Cooperation among ITU‑T study groups, between ITU-T and ITU-D as well as with external bodies outside the ITU (in particular with SDOs), will be required to gather a complete information and understanding on the subject including the organization of seminar/workshops in collaboration with stakeholders. Coordination among relevant organizations is also necessary to fulfil these tasks.

This Question will maintain the ITU-T Q.5050-Q.5069 and ITU-T TR-CF.

### L.2 Question

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

– What Technical Reports are needed to raise awareness of the problem of counterfeiting of ICT device and the dangers they pose?

– Can conformity and interoperability testing and assessment schemes be used to combat counterfeit telecommunication/ICT device?

– What technologies may be used as a tool for combating counterfeit, tampered and stolen telecommunication/ICT device?

– What identity management frameworks are appropriate to combat counterfeit and stolen telecommunication/ICT device with their identity modified?

– What new categories of telecommunication/ICT devices must be considered for counterfeit and what appropriate unique device identifier should be considered for each category?

– What kind of Recommendations, Supplements, Technical Reports and Guidelines should be developed to combat and provide solutions to address ICT counterfeiting, tampering, modification and/or duplication of unique device identifiers?

– What kind of Recommendations, Supplements, Technical Reports and Guidelines should be developed to assist ITU Members, in cooperation with ITU-D Sector, on combating counterfeit and mitigate the use of stolen ICT device?

– What ITU Recommendations, Supplements, Technical Reports and Guidelines are required to secure the supply chain management (from manufacturing, importation, distribution and marketing) to enhance traceability, security, privacy and trust of people, products and networks?

– What ITU Recommendations, Supplements, Technical Reports and Guidelines are appropriate to combat counterfeit IoT devices and the concerns this may pose?

– In this field, what should be taken into account to provide energy savings, directly or indirectly, in ICTs or in other industries?

### L.3 Tasks

Tasks include, but are not limited to:

– develop Recommendations, Supplements, Technical Reports and Guidelines to assist ITU Members, in cooperation with ITU-D Sector, on combating counterfeit telecommunication/ICT device and the concerns they may pose;

– develop Recommendations, Supplements, Technical Reports and Guidelines to assist ITU Members, in cooperation with ITU-D Sector, on combating counterfeit IoT devices;

– develop Recommendations, Supplements, Technical reports and Guidelines to address the problem of stolen telecommunication/ICT device and to assist the Member States, in cooperation with ITU-D Sector, in deploying solutions to mitigate the use of stolen device;

– develop Recommendations, Supplements, Technical Reports and Guidelines to identify new categories of telecommunication/ICT devices that may benefit from combatting counterfeit, and what device identifier should be considered for each category;

– study appropriate solutions, including identity management frameworks, to combat counterfeit and stolen telecommunication/ICT device with tampered or duplicated unique identifiers;

– study relevant technologies that can be used as a tool for combating counterfeit, tampered and stolen telecommunication/ICT device and the dangers they pose;

– organise workshops and events across ITU regions in cooperation with the ITU-D Sector to promote the work of ITU-T in this field and involve stakeholders;

– study possible conformity and interoperability testing (C&I) solutions to combat counterfeiting and tampering of telecommunication/ICT device, taking into account the activities of the ITU-T CASC;

– study results achieved by various international standardization bodies and develop technical specifications to feed the standardization work of the Question.

An up-to-date status of work under this Question is contained in the SG11 work programme (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>).

### L.4 Relationships

Resolutions:

– Resolution 188 of the Plenipotentiary Conference (Rev. Dubai, 2018) “Combating counterfeit telecommunication/information and communication technology devices”;

– Resolution 189 of the Plenipotentiary Conference (Rev. Dubai, 2018) “Assisting Member States to combat and deter mobile device theft”;

– Resolution 79 of the WTDC (Rev. Buenos Aires, 2017) “The role of telecommunications/information and communication technologies in combating and dealing with counterfeit telecommunication/information and communication devices”;

– Resolution 76 of the WTSA (Rev. Hammamet, 2016) “Studies related to conformance and interoperability testing, assistance to developing countries, and a possible future ITU Mark programme”;

– Resolution 96 of the WTSA (Rev. Hammamet, 2016) “ITU Telecommunication Standardization Sector studies for combating counterfeit telecommunication/information and communication technology devices”;

– Resolution 97 of the WTSA (Rev. Hammamet, 2016) “Combating mobile telecommunication device theft”.

Recommendations:

– ITU-T X.1255, ITU-T X.660, ITU-T Q.5050, ITU-T Q.5051

Questions:

– All Questions of SG11, especially Questions relating to control, signalling architectures, protocols, conformance and interoperability testing

Study Groups:

– ITU‑T SG2

– ITU-T SG3

– ITU-T SG5

– ITU‑T SG12

– ITU-T SG13

– ITU‑T SG17

– ITU‑T SG20

– ITU‑D SG1 and SG2

Other bodies:

– ETSI

– IEC

– IEEE

– IETF

– ISO/IEC JTC 1

WSIS action lines:

– C2, C5, C11

Sustainable Development Goals:

– 9

## M Question 16/11 – Test specifications for protocols, networks and services for emerging technologies, including benchmark testing

(Continuation of Question 9/11, 10/11 and 11/11)

### M.1 Motivation

WTSA Resolution 76 – Studies related to conformance and interoperability testing, assistance to developing countries, and a possible future ITU Mark programme – resolves that ITU-T Study Group 11 coordinates the sector’s activities related to the ITU Conformance and Interoperability (C&I) programme across all study groups and reviews the Recommendations in the C&I business plan for the long term implementation of the C&I programme.

ITU T is producing a large number of Recommendations. To achieve interoperability and conformity, one of the important aspects of the ITU C&I Programme concerns the development and maintenance of testing frameworks and methodologies.

It is essential that conformance and interoperability testing methodologies used by all study groups engaged in testing are aligned and consistent with each other. To achieve interoperability on a global scale, the ITU-T Recommendations must be developed and maintained with conformance and interoperability in mind according to the relevant methodology.

The objective of conformance testing is to determine how completely and correctly the requirements stated in the Recommendation have been met by the implementation. On the contrary, in interoperability testing, the objective is to determine if two or more implementations of the same Recommendation communicate and correctly exchange information with each other. It is generally assumed that the conformity of an implementation has been tested prior to perform an interoperability testing assessment.

The recent trends (such as IMT-2020, IoT technologies) may lead to many changes with regards to the extant network architecture that will require higher network performance. This in turn would impact on the specifications of the terminal unit as in CPE, Mobile Units, and Phones etc.

Most of the telecom operators are implementing various emerging technologies and migrate from circuit-switched to the packet-switched networks, trying to provide their services using “all over IP” concept. As a result, operators face some issues which are in general related to the compatibility and interoperability of the used ICT equipment and the interconnection of IP-based networks (e.g. 4G, IMT-2020), which, among others, will be used for roaming/nomadic services. For example, providing voice and video over LTE (VoLTE/ViLTE) roaming services pose some challenges to the operators due to the lack of agreed roaming procedures among stakeholders, various available VoLTE/ViLTE implementation scenarios and other not standardized issues (e.g. ENUM, emergency call, etc.). The conformance and interoperability testing of network-network interfaces (NNI) against ITU-T Recommendations may help operators to be sure that their VoLTE/ViLTE solutions are ready for interconnection. This interconnection approach may be also used for future packet-based networks, e.g. IMT-2020 network and beyond.

In general, benchmarking is a common approach used for the measurement and testing of signalling parameters against the performance design objectives, which should help to provide the end to end service delivery and ensure network reliability.

Benchmarking in the case of IMT-2020 is not limited only to the transport layer and includes performance, quality and reliability of virtual platforms.

The issues of finding the values of network performance and productivity for services with required quality of service (QoS) is an important question for operators and their users.

For example, the Internet-related performance measurement systems, which are publicly available on the Internet, do not provide reliable and comparable measurements. Beyond the lack of standardized metrics for Internet speed in ITU-T Recommendations, the obtained test results, which can be achieved by an existing testing method, may vary from the results achieved by other methods. Obviously, the testing results depend on the network segments which are used during e2e connection. Particularly, it is not possible to guarantee that the e2e connection is based on the telecom operator’s network only and does not include other network segments which may belong to other operators.

The development of a unified approach to Internet-related performance measurement is important for all ICT stakeholders.

Also, this standardized approach will support the development of the *“Framework for ICT service delivery with the guaranteed QoS and requested bitrate on fixed & mobile data networks, for development of efficient economic mechanisms and models of interaction in the "operator-provider-user" chain”*.

NOTE − The network performance QoS/QoE, including the networks and services KPIs, parameters and requirements, are defined by ITU‑T SG12 and related SDOs. This Question is responsible for Q.3900-Q.4099-series (testing for next generation networks), Q.1912.x-series, X.290-series (except X.292), X.Suppl.4, X.Suppl.5 and Z.500-series.

### M.2 Question

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

– What is the testing methodology for testing emerging technologies?

– What are the existing ITU-T Recommendations which include test suites?

– What is the architecture of the testbed or testing facilities to be used for testing emerging technologies?

– Which technologies that are being developed for the ICT market require conformity and interoperability testing (taking into account market needs)?

– What kind of test suites are needed for testing interconnection of IP-based networks (e.g. 4G, IMT-2020 network and beyond)?

– What kind of equipment could be benchmark tested?

– What kind of test procedures could be used for benchmark testing?

– What type of traffic could be simulated for benchmark testing?

– What design objectives need to be benchmark tested?

– What test procedures for standardized network parameters, including those defined in the framework of Internet related performance measurements (ITU-T Q.3960), such as e2e bit rate within and outside the fixed and mobile operator’s network (that is between users of the operator’s network and a particular Internet resource), need to be developed?

– How parameters/technologies/services may be tested remotely?

– What procedures need to be developed to implement remote testing?

– What is the network architecture to be used for remote testing?

– What is the methodology for testing IMT-2020 mobile devices?

– What is the methodology for testing services which require ultra-low latency?

### M.3 Tasks

Tasks include, but are not limited to:

– study the testing methodology for testing emerging technologies;

– identify the existing ITU-T Recommendations which include test suites;

– identify the architecture of the testbed or testing facilities to be used for testing emerging technologies;

– identify market driven ICT technologies, which require conformity and interoperability testing;

– develop test suites to be used for testing interconnection of IP-based networks (e.g. 4G, IMT-2020 network and beyond);

– determine the types of equipment, which could be benchmark tested;

– develop the test procedures for benchmark testing;

– identify the type of traffic to be simulated for benchmark testing;

– define the design objectives that need to be benchmark tested;

– develop test procedures for standardized network parameters, including those defined in the framework of Internet-related performance measurements (ITU-T Q.3960), such as e2e bit rate within and outside the fixed and mobile operator’s network (that is between users of the operator’s network and a particular Internet resource);

– determine the parameters/technologies/services which may be tested remotely;

– develop the procedures needed to implement remote testing;

– Specify the network architecture to be used for remote testing;

– develop a methodology (guide) that would extend current experiences and testing approaches to IMT-2020;

– determine the methodology for testing IMT-2020 devices;

– determine the methodology for testing services which require ultra-low latency.

An up-to-date status of work under this Question is contained in the SG11 work programme (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>).

### M.4 Relationships

Recommendations:

– Q, Y, H, G, E, I, M, P, X, Z and F-series

Questions:

– All ITU-T SG11 Questions

Study Groups:

– ITU‑T SG13 on future networks (e.g. SDN, NFV), cloud computing, IMT-2020, machine learning

– ITU‑T SG15 on core and access technologies

– ITU‑T SG16 on multimedia services, applications and e-health

– ITU-T SG17 on testing languages, including TTCN-3

– All other ITU-T SGs that are involved with C&I, IMT-2020 network and beyond, machine learning activities

– ITU‑D SG1 and ITU-D SG2 on remote test centres

– ITU‑T SG3 on policy issues

– ITU‑T SG12 on parameters and requirements of QoS

Other bodies:

– ETSI (especially ETSI TC INT and ETSI TC NTECH)

– IETF

– IEEE

WSIS action lines:

– C5, C6

Sustainable Development Goals:

– 9

## N Question 17/11 – Combating counterfeit or tampered telecommunication/ICT software

(New Question)

### N.1 Motivation

ITU Resolution 188 (Rev. Dubai, 2018) of the Plenipotentiary Conference, recognizing the adverse impact of counterfeit telecommunication/ICT devices on governments, manufacturers, vendors and consumers and aware that tampering with telecommunication/ICT devices may diminish the effectiveness of solutions adopted by the countries to address counterfeiting, invites Member States to take all necessary measures to combat counterfeit telecommunication/ICT devices.

At the same time, Resolution 96 (Hammamet, 2016) of World Telecommunication Standardization Assembly, recognizes that counterfeit and tampered telecommunication/ICT devices negatively impact on security and privacy for users and impose adverse impact on governments, manufacturers, vendors, operators and consumers such as the loss of revenues, erosion of brand value/intellectual property rights and reputation and network disruptions.

Moreover, ITU Resolution 189 (Rev. Dubai, 2018) of the Plenipotentiary Conference, on the combat of mobile devices theft, recognizing that device theft can have a negative impact on users' data and on their sense of security and confidence in the use of information and communication technologies (ICTs), resolves to explore and encourage the development of ways and means to continue to combat and deter mobile device theft, and invites Member States to adopt the necessary actions to prevent, discover and control tampering and replication of mobile ICT device identifiers.

Resolution 97 (Hammamet, 2016) of World Telecommunication Standardization Assembly, recognizes that the theft of user-owned mobile devices may lead to the criminal use of telecommunication/ICT services and applications, resulting in economic losses for the lawful owner and user; indicates the necessity to identify existing and future technological measures, both software and hardware, to mitigate the consequences of the use of stolen mobile devices.

ITU-T SG11 received contributions from ITU Member State and from Sector members that led to the approval of Recommendation ITU-T Q.5050 “Framework for solutions to combat counterfeit ICT devices” and Recommendation ITU-T Q.5051 “Framework for Combating the use of Stolen Mobile Devices”. In addition, a number of new work items were agreed.

At the same time, some contributions suggested the need to address some new scenarios, such as:

(i) The tampering with stolen mobile device software in order to achieve unauthorized access to the user data with consequent impacts.

(ii) Counterfeit/tampered network devices (such as routers or switches) that has backdoors access to the user network, allowing data theft and consequent revenue loss.

(iii) Counterfeit/tampered Paid TV receivers with tampered software that allow unauthorized access to the content provider data by non-subscribers.

There is no simple solution for this topic, since in general the telecommunication/ICT user is unaware of the vulnerabilities that are included on counterfeit devices or can be present with the counterfeit or tampered ICT software. Therefore, is critical to raise the awareness of all stakeholders regarding this topic.

Therefore, this Question intends to explore appropriate possibilities to combat counterfeit or tampered ICT software. Cooperation among ITU‑T study groups, between ITU-T and ITU-D as well as with external bodies outside the ITU (in particular with SDOs), will be required to gather a complete information and understanding on the subject including the organization of seminar/workshops in collaboration with stakeholders. Coordination among relevant organizations is also necessary to fulfil these tasks.

### N.2 Question

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

– What are the adverse impacts to the stakeholders due to the use of counterfeit telecommunications/ICT devices or devices with tampered or counterfeit software, and consequent data misappropriation?

– What kind of adverse impacts could counterfeit telecommunication/ICT and or regular devices with tampered telecommunication/ICT software impose on telecommunication/ICT stakeholders (such as the user and service provider), in particular with regard to data misappropriation?

– What Technical Reports and Guidelines are needed to raise awareness of the problem of telecommunication/ICT software tampering, telecommunication/ICT data misappropriation and the concerns they pose?

– What kind of Recommendations, Supplements, Technical Reports and Guidelines should be developed to assist ITU Members, in cooperation with ITU-D Sector, on combating counterfeit or tampered telecommunication/ICT software, theft misappropriation and the concerns they pose?

– What kind of Recommendations, Technical Reports and Guidelines should be developed to mitigate ICT data misappropriation, in special the user data contained on ICT devices and content delivered by ICT service providers?

– What technologies and solutions may be used for combating counterfeit or tampered telecommunications/ICT software and its adverse impacts?

– Can conformity assessment schemes be used to combat counterfeit or tampered ICT software?

### N.3 Tasks

Tasks include, but are not limited to:

– study the adverse impacts to the stakeholders due to the use of counterfeit telecommunications/ICT devices or devices with tampered or counterfeit software, and consequent data misappropriation;

– study relevant and appropriate technologies and solutions that can be used to combat counterfeit or tampered ICT software, consequent data misappropriation and other adverse impacts;

– develop Recommendations, Supplements, Technical Reports and Guidelines to assist ITU Members, in cooperation with ITU-D Sector, on combating counterfeit or tampered ICT software and data misappropriation and its adverse impacts;

– organize workshops and events across ITU regions, in cooperation with the ITU-D Sector, to promote the work of ITU-T in this field and involve stakeholders;

– study possible conformity assessment schemes to combat counterfeit or tampered ICT software and data misappropriation, taking into account the activities of the ITU-T CASC;

– study results achieved by various international standardization bodies and develop technical specifications to feed the standardization work of the Question.

An up-to-date status of work under this Question is contained in the SG11 work programme (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=11>).

### N.4 Relationships

Resolutions:

– Resolution 188 of the Plenipotentiary Conference (Rev. Dubai, 2018) “Combating counterfeit telecommunication/information and communication technology devices”;

– Resolution 189 of the Plenipotentiary Conference (Rev. Dubai, 2018) “Assisting Member States to combat and deter mobile device theft”;

– Resolution 96 of the WTSA (Rev. Hammamet, 2016) “ITU Telecommunication Standardization Sector studies for combating counterfeit telecommunication/information and communication technology devices”;

– Resolution 97 of the WTSA (Rev. Hammamet, 2016) “Combating mobile telecommunication device theft”.

Recommendations:

– ITU-T X.1127, ITU-T Q.5050, ITU-T Q.5051

Questions:

– All Questions of SG11, especially Questions relating to control, signalling architectures, protocols, conformance and interoperability testing, combating counterfeit and stolen ICT

Study Groups:

– ITU‑T SG2

– ITU-T SG3

– ITU‑T SG9

– ITU-T SG13

– ITU-T SG16

– ITU‑T SG17

– ITU‑T SG20

– ITU‑D SG1 and SG2

Other bodies:

– ETSI

– IEC

– IEEE

– IETF

– ISO/IEC JTC 1

WSIS action lines:

– C2, C5, C9, C11

Sustainable Development Goals:

– 9

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