|  |  |
| --- | --- |
| World Telecommunication Standardization Assembly (WTSA-20)Geneva, 1-9 March 2022 |  |
|  |  |
|  |  |
| PLENARY MEETING | Document 22-E |
|  | December 2021 |
|  | Original: English |
|  |
| **ITU-T Study Group 20** |
| Internet of things (IoT) and smart cities and communities (SC&C) |
| REPORT OF ITU-T SG20 TO THE WORLD TELECOMMUNICATION STANDARDIZATION ASSEMBLY (WTSA-20), Part II: QUESTIONS PROPOSED FOR STUDY DURING THE NEXT STUDY PERIOD (2022-2024) |

|  |  |
| --- | --- |
| **Abstract:** | This contribution contains the text of ITU-T Study Group 20 Questions proposed for approval by the Assembly for the next study period. |
| **Contact:** | Mr Nasser Saleh Al MarzouqiChairman ITU-T SG20UAE | Tel: +971 2 777 2468Fax: +971 2 777 2122E-mail: nasser.almarzouqi@tdra.gov.ae  |

Note by the TSB:

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

Part I: **Document 21** – General

Part II: **Document 22** – Questions proposed for study during the study period 2022-2024

**1 List of 7 Questions proposed by Study Group 20**

| Question number | Question title | Status |
| --- | --- | --- |
| A/20 | Interoperability and interworking of IoT and SC&C applications and services | Continuation of Question 1/20 and part of Questions 2/20, 3/20 and 4/20 |
| B/20 | Requirements, capabilities and architectural frameworks across verticals enhanced by emerging digital technologies | Continuation of Question 2/20 and part of Question 4/20 |
| C/20 | IoT and SC&C architectures, protocols and QoS/QoE | Continuation of part of Question 3/20 |
| D/20 | Data analytics, sharing, processing and management, including big data aspects, of IoT and SC&C | New study items and continuation of part of Questions 1/20 and 4/20 |
| E/20 | Study of emerging digital technologies, terminology and definitions | Continuation of Question 5/20 |
| F/20 | Security, privacy, trust and identification for IoT and SC&C | Continuation of Question 6/20 and part of Questions 1/20 and 4/20 |
| G/20 | Evaluation and assessment of Smart Sustainable Cities and Communities | Continuation of Question 7/20 |

**2 Wording of Questions**

The proposed text of the Questions is provided in the remaining part of this document.

QUESTION A/20

**Interoperability and interworking of IoT and SC&C applications and services**

(Continuation of Question 1/20 and part of Questions 2/20, 3/20 and 4/20)

**A.1 Motivation**

The population living in urban areas of the world has grown rapidly and 68% of the world’s population is expected to live in urban areas by 2050. This rapid urbanization brings risks of social instability, failure of critical infrastructure, water crises and the spread of infectious disease.

Cities and communities (including villages and towns) need to increase the efficiency in which they operate and use their resources to response to the challenges posed by this rapid urbanization.

The efficiency improvements can be achieved by interconnecting individual systems within cities and communities such as water, electricity, waste management and transportation and sharing the data from various silos within cities.

Due to many citizens moving to other cities frequently, the interoperability between cities is also important.

**A.2 Questions**

This Question addresses use cases, requirements, architectures and data sets and format to support interworking and provide interoperability between IoT and SC&C applications and services not only within but also between cities and communities.

Study items include, but are not limited to:

– What are the use cases for interworking between IoT and SC&C applications and services?

– What are the requirements and architectures to support interworking and provide interoperability of IoT and SC&C applications and services?

– How to provide data interoperability and semantic interoperability?

**A.3 Tasks**

Tasks include, but are not limited to:

– Developing Recommendations, Supplements, Reports, Guidelines, etc. as appropriate on:

• use cases for interworking of IoT and SC&C applications and services in different verticals;

• interworking and interoperability requirements and architectures;

• middleware and platforms for interworking and interoperability;

• data sets and formats to enable data interoperability and semantic interoperability among various verticals; and

• implementation, deployment, operation and maintenance with respect to the above tasks.

– Providing the necessary collaboration for joint activities in this field within ITU and between ITU-T and other relevant SDOs, consortia and forums.

An up-to-date status of work under this Question is contained in the SG20 work programme
(<https://www.itu.int/ITU-T/workprog/wp_search.aspx?q=1/20>).

**A.4 Relationships**

**WSIS Action Lines:**

– C2, C3, C5, C6, C7, C8, C10

**Sustainable Development Goals:**

– 11

**Recommendations:**

– Y.4000-series including Y.4100/Y.2066, Y.4111/Y.2076, Y.4113, Y.4114, Y.4200, Y.4201, Y.4401/Y.2068, Y.4461, Y.4552/Y.2078

**Questions:**

– All ITU-T SG20 Questions

**Study groups:**

– ITU-T (e. g. considering their lead study group role), ITU-D and ITU-R Study Groups as appropriate

– This Question will coordinate with ITU-T SG13 on big data relevant aspects.

**Other bodies:**

– 3GPP

– ETSI

– IEC/SyC smart cities

– IETF

– ISO/IEC JTC 1/SC 41, ISO/IEC JTC 1/WG 11

– ISO/TC 268

– Joint IEC-ISO-ITU Smart Cities Task Force

– oneM2M

– W3C

QUESTION B/20

**Requirements, capabilities and architectural frameworks across verticals enhanced by emerging digital technologies**

(Continuation of Question 2/20 and part of Question 4/20)

**B.1** **Motivation**

With the ever-increasing number of Internet of Things (IoT) services and applications, it is needed to study the requirements, capabilities and architectural frameworks for IoT and Smart Cities and Communities (SC&C). Emerging IoT and SC&C services and applications are placing more and more requirements on networks and the provisioning of new services, resulting in the need to make networks more and more intelligent with the provisioning of new capabilities.

One essential objective is the maximization of the usage of common capabilities and architectural frameworks in order to provide support to a broad range of IoT and SC&C services and applications in different verticals, in cost efficient, multi-vendor and easily deployable ways over converged infrastructures.

In the IoT there is an increasing integration and convergence of Information and Communication Technologies (ICTs) and emerging digital technologies, including but not limited to, edge computing, artificial intelligence/machine learning (AI/ML), blockchain, digital twin, data processing and analytics, orchestration and automation technologies, emerging networking technologies, with advanced sensing and actuation technologies. These technologies are making available a large set of advanced capabilities for the support of IoT and SC&C services and applications, which need to be integrated in terms of architectural frameworks, from both common (not vertical dependent) and vertical specific viewpoints.

It is also needed to make the effective linkage between the IoT and SC&C standards and the practical aspects of implementation, deployment, operation and maintenance, in order to assess the opportunities and benefits of using these standards in concrete application scenarios.

**B.2 Questions**

This Question addresses the common and specific requirements, capabilities and architectural frameworks enhanced by emerging technologies across verticals.

On the basis of use cases and related ecosystem aspects, the requirements, capabilities and architectural frameworks enhanced by emerging technologies for the support of IoT and SC&C services and applications will be specified from both common (not vertical dependent) and vertical specific viewpoints.

Study items include, but are not limited to:

– What are the use cases for IoT and SC&C applications and services across different verticals?

– What are the requirements, capabilities and architectural frameworks needed for the support of emerging services and applications for IoT and SC&C across different verticals?

– With which standards development organizations (SDOs) collaboration would be necessary to maximize synergies and harmonize existing standards?

**B.3 Tasks**

Tasks include, but are not limited to:

– Developing Recommendations, Reports, Roadmaps, Guidelines etc. as appropriate for the support of emerging services and applications for IoT and SC&C, covering:

• use cases of IoT and SC&C services and applications across different verticals;

• ecosystem aspects taking into account business models and use cases;

• common and specific requirements, capabilities and architectural frameworks enhanced by emerging technologies across different verticals; and

• related implementation, deployment, operation and maintenance, as well as Proof of Concepts, for IoT and SC&C with respect to the above tasks.

– Providing the necessary collaboration for joint activities in this field within ITU and between ITU-T and other relevant SDOs, consortia and forums.

An up-to-date status of work under this Question is contained in the SG20 work programme (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?q=2/20>).

**B.4 Relationships**

**WSIS Action Lines:**

– C2, C3, C5, C6, C7, C8, C10

**Sustainable Development Goals:**

– 9, 10 and 11

**Recommendations:**

– Y.4000-series including Y.4000/Y.2060, Y.4003, Y.4100/Y.2066, Y.4101/Y.2067, Y.4102/Y.2074, Y.4103/F.748.0, Y.4105/Y.2221, Y.4108/Y.2213, Y.4109/Y.2061, Y.4110/Y.2065, Y.4111/Y.2076, Y.4112/Y.2077, Y.4113, Y.4116, Y.4117, Y.4118, Y.4119, Y.4120, Y.4121, Y.4201, Y.4203, Y.4204, Y.4207, Y.4208, Y.4250/Y.2222, Y.4401/Y.2068, Y.4408/Y.2075, Y.4457, Y.4464, Y.4552/Y.2078, Y.4702, Y.Suppl.53, Y.Suppl.56 to Y-series

**Questions:**

– All Questions of ITU-T SG20

**Study Groups:**

– ITU-T (e.g. considering their lead study group role), ITU-D and ITU-R Study Groups as appropriate

**Other bodies:**

– IETF

– Open Mobile Alliance (OMA)

– Open Geospatial Consortium (OGC)

– IEEE

– ATIS

– ETSI TC Smart M2M

– CCSA TC10

– oneM2M

– ISO/IEC JTC 1/SC41, ISO/IEC JTC 1/WG11

– Joint IEC-ISO-ITU Smart Cities Task Force

– GSMA

– 3GPP/3GPP2

– W3C

– Organization for the Advancement of Structured Information Standards (OASIS)

– Object Management Group (OMG)

– Industrial Internet Consortium (IIC)

– Alliance of Industrial Internet (AII)

– Alliance for IoT Innovation (AIOTI)

– Open Connectivity Foundation (OCF)

– 5G Alliances (e.g., 5G AA, 5G ACIA, etc.)

QUESTION C/20

**IoT and SC&C architectures, protocols and QoS/QoE**

(Continuation of part of Question 3/20)

**C.1 Motivation**

As the Internet of Things (IoT) establishes its position as an underlying mechanism for various applications, special attention is being paid to how advanced information and communication technology (ICT) systems are designed based on IoT and related conceptual architectures including network requirements and protocols. Given the rich features of IoT, highly capable ICT systems meeting vertical industry demands can be realized by supplementary development based on IoT architectures. This is a promising way in terms of efficiency and time to market.

To support this approach, the IoT and SC&C architectures, their functionalities, interfaces, protocols, data models, intelligent management mechanisms, control mechanisms, connectivity technologies, APIs, and Quality of Experience/Service (QoE/QoS) have to be studied, also building on existing Recommendations, including ITU-T Y.4000/Y.2060.

**C.2 Questions**

This Question addresses architectures, including their functionalities, interfaces, protocols, data models, intelligent management mechanisms, control mechanisms, connectivity technologies, APIs, and Quality of Experience/Service (QoE/QoS) of IoT and Smart Sustainable Cities and Communities (SSC&C), which needed to construct architectural frameworks to interact with services and applications, as well as different networks and systems.

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

– What new and revised Recommendations are required to realize IoT and SC&C architectures?

– What technologies including networks, interfaces, functions, management mechanisms, as well as protocols are required for the architecture of IoT and SC&C?

– What functionalities of the ICT technologies, signalling and control architectures are required to support services and/or applications of IoT and SC&C?

– What enhancements to existing connectivity, interfaces, functions, management mechanisms and protocols are required to support machine-to-machine (M2M) communication services and/or applications of IoT and SC&C?

– What performance requirements of connectivity technologies are required to support services and/or applications of IoT and SC&C?

– What are the mechanisms for achieving QoS/QoE and measurement principles required for IoT and SC&C?

– Collaboration with which standards development organizations (SDOs) would be necessary to maximize synergies and harmonize existing standards?

**C.3 Tasks**

Tasks include, but are not limited to:

– Developing Recommendations, Reports, Guidelines, etc. as appropriate on:

• conducting studies on general reference models on IoT and vertical industry needs

• developing frameworks to identify the basic architectural compositions and views on IoT and SC&C. These will be based on the architectural requirements derived from the industry needs;

• identifying entities, their functions, and reference points required to provide support to IoT applications and services;

• determining the requirements that the connectivity and protocols are intended to support. It is anticipated that these requirements will need to be periodically refined to reflect the evolution of IoT related technologies taking into consideration the connectivity, management mechanisms (including device management) and protocols available from ITU-T and other SDOs;

• developing modifications and enhancements to the signalling requirements, connectivity technologies, management mechanisms (including device management) and protocols that will enable them to meet the requirements and architecture of IoT and SC&C;

• identifying performance requirements of connectivity technologies that will enable them to meet the IoT and SC&C requirements;

• developing mechanisms for achieving QoS and its measurement principles required for IoT and SC&C;

• identifying interfaces for which interoperability between different IoT network elements is desirable and for which detailed requirements need to be studied and protocols need to be standardized;

• defining interworking with legacy systems;

• developing intelligence control related technologies that will provide support to IoT applications and services for various verticals and systems;

• identifying mechanisms for achieving architectural interoperability for IoT and SC&C.

– Providing the necessary collaboration for joint activities in this field within ITU and between ITU and SDOs, consortia and forum.

An up-to-date status of work under this Question is contained in the SG20 work programme (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?q=3/20>).

**C.4 Relationships**

**WSIS Action Lines:**

– C2, C3, C5, C6, C7, C8, C10

**Sustainable Development Goals:**

– 9 and 11

**Recommendations:**

– Y.4000-series

**Questions:**

– All ITU-T SG20 Questions

**Study Groups:**

– ITU-T (e.g. considering their lead study group role), ITU-D and ITU-R Study Groups as appropriate

– IoT signalling and protocols will be developed in collaboration with ITU-T SG11

**Other bodies:**

– ATIS

– IETF

– ETSI

– oneM2M

– ISO/IEC JTC 1/ WG10

– Joint IEC-ISO-ITU Smart Cities Task Force

– 3GPP/3GPP2

– IEEE

– W3C

– OCF

QUESTION D/20

**Data analytics, sharing, processing and management, including big data aspects, of IoT and SC&C**

(New study items and continuation of part of Questions 1/20 and 4/20)

**D.1 Motivation**

There is an increasing demand for connected cities with pervasive embedded devices to improve quality of Internet of Things (IoT) and Smart Cities and Communities (SC&C) services. The evolution of IoT technology with interconnected things conceives a “smart environment” with an autonomous information infrastructure, diverse data sources and more than 50 billion devices within the IoT and SC&C ecosystem.

While traditional information databases and analytics architectures and infrastructures remain essential, with the growing data management demands, specific capabilities and capacities are required to be able to handle diverse and complex data streams from different sources. This data needs to be processed and managed properly to maximize its value in a secure and policy compliant manner, while complementing it with other information sources.

It is important to note that any imperfections within the Data Processing and Management (DPM) framework can adversely affect the quality of services, pose risks associated with security and could hinder the overall urban planning and decision-making process.

In light of the above, IoT and SC&C environments increasingly require defined and comprehensive DPM frameworks and guidelines which incorporate reasonable measures to achieve a layered, data-centric paradigm. Data driven services and applications will be enabled by data analytics incorporated into the data ecosystem using emerging technologies (e.g., blockchain, artificial intelligence, digital twin, etc.) to support IoT and SC&C. Therefore, the Question will identify and study characteristics of emerging DPM systems considering big data aspects of IoT and SC&C.

Implementing feasible DPM guidelines and standards can make the collection, storage and retrieval of large amounts of data fast and cost-effective while addressing data complexities and governance.

Taking into account the data ecosystem that affects various stakeholders, this Question will develop a series of Recommendations on effective DPM, data analytics and sharing for IoT and SC&C.

**D.2 Questions**

This Question focuses on DPM, data analytics and sharing including big data aspects for IoT and SC&C.

Study items include, but are not limited to:

– analysis of existing technologies, platforms, guidelines and standards for DPM in support of the mandate of SG20;

– architectural frameworks for the future of data driven ecosystems and their applications with DPM and big data;

– data analytics and data sharing issues with the development of efficient and scalable DPM approaches;

– the role of emerging technologies (e.g., blockchain, artificial intelligence and digital twin, etc.) to support DPM;

– governance, security and privacy concerns within DPM frameworks;

– trusted data and data quality in DPM frameworks including digital identification and certification; and

– collaboration with standards development organizations (SDOs) to maximize synergies and harmonize existing standards related to this field work.

**D.3 Tasks**

Tasks include, but are not limited to:

– Developing Recommendations, Supplements, Reports, Guidelines, etc. as appropriate for DPM for IoT and SC&C, covering:

• methodology for DPM concept building based on use cases, requirements analysis;

• data value chain, data lifecycle, capabilities and functional architectures to support DPM including big data aspects for IoT and SC&C;

• data analytics and data sharing to support data-driven intelligent services and applications for IoT and SC&C;

• tools, mechanisms and standardized interfaces for data analytics and data sharing;

• DPM, data analytics and sharing with support of emerging technologies (e.g., blockchain, artificial intelligence and digital twin, etc.) in IoT and SC&C;

• governance, security, privacy protection and risk management for IoT and SC&C;

• trusted data and data quality management for IoT and SC&C.

– Providing the necessary collaboration for joint activities in this field within ITU and between ITU-T and other relevant SDOs, consortia and forums.

An up-to-date status of work under this Question is contained in the SG20 work programme
(<https://www.itu.int/ITU-T/workprog/wp_search.aspx?q=4/20>).

**D.4 Relationships**

**WSIS Action Lines:**

– C2, C3, C5, C6, C7, C8, C10, C11

**Sustainable Development Goals:**

– 9, 10 and 11

**Recommendations:**

– Y.4000-series on IoT and smart cities & communities

– Y.4000-series on Data Processing and Management (including ITU-T FG-DPM deliverables)

**Questions:**

– All ITU-T SG20 Questions

**Study Groups:**

– ITU-T (e.g., considering their lead study group role), ITU-D and ITU-R Study Groups as appropriate

– This Question will coordinate with ITU-T SG13 on big data relevant aspects.

**Other bodies:**

– 3GPP

– 5G Alliances (e.g., 5G AA, 5G ACIA, etc.)

– BDVA

– BSI

– ETSI

– GSMA

– IEEE

– IETF

– ISO/IEC JTC 1

– Joint IEC-ISO-ITU Smart Cities Task Force

– OASC

– OCF

– OMA

– oneM2M

– OSG

– W3C

QUESTION E/20

**Study of emerging digital technologies, terminology and definitions**

(Continuation of Question 5/20)

**E.1 Motivation**

The Internet of Things (IoT) has the potential to change the lifestyle of the people and the way they interact with the surroundings, especially in smart cities and communities (SC&C). In this regard, it is important to explore the emerging technologies and trends that will contribute to that change. It is expected that IoT will have a significant impact on key infrastructural elements pertaining to cities, including the transportation, health and energy sectors, quality of life (QoL) and environment, as well as on society and the economy as a whole. Due to its ubiquitous nature, the IoT is in direct interaction with all application domains and all countries, with a direct impact on the achievement of the Sustainable Development Goals.

To facilitate discussions and to have a common background of relevant issues, the terminologies relating to IoT and SC&C need to be coordinated and unified. It would also be appropriate to identify, research, and analyse emerging digital technologies that are relevant for IoT and/or SC&C standardization. This Question intends to serve as a bridge with the research community and where appropriate to facilitate and accelerate transfer of emerging technologies to standardization. This Question will focus on topics that are not yet addressed by the other Questions.

**E.2 Questions**

This Question is tasked to capture and develop definitions, to contribute to a common terminology for IoT and SC&C. This Question can also contribute to research solutions for interoperability across different technologies, taking into account both end-user, regulatory and market needs. Considering the rapid evolution of the IoT domain, this Question can also contribute to the identification and discussion of relevant research and technological developments in this area, to bring the most relevant topics to the attention of the ITU-T Study Group 20 (SG20) and/or to the corresponding Questions. Considering the fast evolution of IoT technologies and shorter time to market, this question is expected to serve as a facilitator with the research and innovation community in order to identify emerging technologies requiring standardization for the global market and the industry.

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

– What are the terms, definitions, abbreviations, letter symbols and schematic symbols used for IoT and SC&C?

– What are the emerging research and technologies related to IoT and/or SC&C that are relevant for standardization?

– How can IoT technologies contribute to implement the Sustainable Development Goals (SDGs)?

– What are the impacts of introducing IoT on human activities and how can the corresponding constraints be addressed?

– How can end-user experience with IoT be enhanced?

– How can IoT comply with regulatory requirements and how can IoT systems and components communicate information on their legal compliance with each other in a standardized manner?

– How will IoT change the business models and the market environment?

– Collaboration with which standards development organizations (SDOs) would be necessary to maximize synergies and harmonize existing standards?

– How to engage with the IoT community at large, including its various stakeholders for supporting global standardization and interoperability?

**E.3 Tasks**

Tasks include, but are not limited to:

– Developing Recommendations, Reports, Guidelines, etc. as appropriate on:

• developing, maintaining and enhancing the Recommendations on terminology related to IoT and SC&C;

• maintaining and enhancing the Study Group 20 Recommendations;

• development in collaboration with other SG20 Questions, of frameworks and roadmaps, for the harmonized and coordinated development of Internet of things (IoT), including M2M communications and ubiquitous sensor networks in ITU-T;

• cooperating with ITU-D and ITU-R Study Groups and other regional and international standards development organizations (SDOs), academia and industry forums;

• developing guidelines, methodologies and best practices related to IoT and SC&C to support the achievement of the Sustainable Development Goals (SDGs) and to prevent a digital gap with developing countries;

• developing guidelines, methodologies and best practices related to IoT to support legal compliance of IoT systems and solutions in a standardized and interoperable manner;

• identifying emerging technologies and relevant research work on IoT and SC&C that are relevant for standardization;

• liaising and fostering cooperation with academia, research and innovation community, as well as with other SDOs and industry forums including small and medium enterprises (SMEs) on IoT and SC&C;

• identifying in coordination with other SG20 Questions, new work areas linked to IoT and SC&C, and collaborating with relevant ITU-T SGs and other SDOs and forums, to initiate studies on those identified work areas.

– Providing the necessary collaboration for joint activities in this field within ITU and between ITU-T and other relevant SDOs, consortia and forums.

An up-to-date status of work under this Question is contained in the SG20 work programme (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?q=5/20>).

**E.4 Relationships**

**WSIS Action Lines:**

– C1, C6, C11

**Sustainable Development Goals:**

– 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 and 17

**Recommendations:**

– Y.4050/Y.2069

**Questions:**

– All ITU-T SG20 Questions

**Study Groups:**

– ITU-T (e.g., considering their lead study group role), ITU-D and ITU-R Study Groups as appropriate

– TSAG Rapporteur Group on Standardization Strategy (RG-SS)

– ITU Standardization Committee for Vocabulary

**Other bodies:**

– IEC

– ISO

– Joint IEC-ISO-ITU Smart Cities Task Force

– IEEE

– IETF

– IPv6 Forum

– IoT Forum

– IoT Lab

QUESTION F/20

**Security, privacy, trust, and identification for IoT and SC&C**

(Continuation of Question 6/20 and part of Questions 1/20 and 4/20)

**F.1 Motivation**

Towards the information society, there are increases in cyber-attacks, cybercrime, and loss of credit or trust. The ICT infrastructure will evolve to provide converged services and applications by accommodating many Internet of Things (IoT) sensors and IoT-related systems. Additionally, the world is experiencing an evolution of Smart Cities. Many stakeholders from various industries are involved in future converged and intelligent services to be deployed using ICT infrastructure. This heterogeneous environment, while it promises great advances in the way the services and applications are provisioned, and in the way systems are managed, administered, and maintained, yet comes with a very wide range of sector-specific risks and threat vectors. Implications for security, privacy[[1]](#footnote-2) and the overall trust of use, adoption, and proliferation of IoT, and smart city devices, systems, services, applications, and platforms could hinder its overall market development. Therefore, it is important that security and privacy concerns are taken into account throughout the design process of products and systems to be used in IoT implementations commonly known as privacy by design and security by design, which emphasize that protection be built into information technologies, business practices, systems, processes, physical design, and networked infrastructure.

The satisfaction of security and privacy requirements plays a fundamental role in the IoT environment and SC&C. Such requirements include data confidentiality and authentication, access control within the IoT network, availability, data integrity, privacy and trust among users and things, and non-repudiation.

Some security measures may not always be directly applied to IoT technologies. Moreover, the high number of interconnected devices raises scalability issues when applying security techniques; therefore, flexible infrastructures are needed, to deal with security threats in such environments. ICT infrastructures should be reliable, safe, confidential, and trustworthy. Therefore, security, privacy and trust provisioning for IoT is one of the outstanding standardization issues of the ITU-T SG20.

On the other hand, various identification technologies have always been regarded as an important enabling technology for IoT implementation. Both physical devices (such as tagged items and products, sensing devices) and virtual entities (such as computational processes, software) could be, or already are, assigned identifiers, in order to be identified and distinguished. It is important for each thing to be addressable, and identifiable in order to tackle, inter alia, privacy, security, trust, and network reachability issues in IoT deployments.

Taking into account the variety of devices, systems, services and applications within IoT and SC&C domains, it is essential to develop trustworthiness models that ensure all physical and virtual things involved are trusted enough to be part of IoT and SC&C environment. Such models should be integrated within IoT and SC&C architectures while defining the set of rules to ensure implementation of trusted IoT systems. The security and trustworthiness architectures should be substantial part of any E2E architectures developed for IoT and SC&C verticals and use-case.

In addition, the adoption of new technologies such as block-chain, big data, quantum computing, machine learning and artificial intelligence (AI) can play important role in developing advanced cost-effective measures and mechanisms to create such trustworthy environment within IoT and SC&C domains.

All above requirement need to be carefully analysed for various IoT verticals and use-cases that may require specific additional demands due to its nature and underlying standards used for IoT and SC&C devices, systems, applications, protocols, platforms, and services.

**F.2 Questions**

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

– What are the possible threats against the compromise of authenticity, confidentiality, integrity, non-repudiation, and availability of IoT and SC&C devices, systems, applications, protocols, platforms, and services?

– What is needed to mitigate and counteract the risks and threats identified in IoT and SC&C systems, and services?

– What are the identification systems capable of fulfilling the requirements of IoT and SC&C including security, privacy and trust?

– What are the requirements and mechanisms for protecting, and preventing disclosure of things' information?

– How can authentication technologies work with identification systems?

– How can security measures be applied in IoT devices to protect identity, privacy, and security of the system, given that the device's environment and resources may be constrained?

– What technical measures are needed to support the protection of privacy in SC&C applications, services, and platforms? How can trust be maintained and supported for the use of such systems?

– What measures can be taken to prevent compromise and protect the integrity and privacy of IoT systems, applications, platforms, and services?

– How to create trustworthiness in IoT & SC&C devices, systems, applications, protocols, platforms, and services?

– How to ensure security, privacy and trustworthiness in data related to IoT & SC&C as well as the relevant data planforms?

– How can block-chain based technologies and mechanisms support security and trustworthiness in IoT & SC&C?

– How to use machine learning and artificial intelligence (AI) technologies for supporting secured interoperability and trustworthiness in IoT & SC&C?

– How can quantum technologies support security and trustworthiness in IoT & SC&C?

– How to apply big data techniques for enhancing security and trustworthiness in IoT & SC&C?

– How Public Key Infrastructure can enhance authentication mechanisms and communication trustworthiness in IoT and SC&C

– What measures can be developed or used to assist with availability and portability of the data in IoT and SC&C platforms, systems, and services?

– What options or measures are available for identification of IoT objects, including non-IP based and non-web-based objects in a heterogeneous IoT system, for SC&C?

– What are identification systems and mechanisms that can be used to support IoT and SC&C?

– How can identification mechanisms support interoperability in IoT and SC&C and mitigate risks?

– How to ensure security and trustworthiness in the interactions through Application Programming Interfaces (API)?

– What options and mechanisms may be used for registering and managing IoT identifiers when appropriate?

– What are the appropriate technical measures needed for identity discovery?

– Which standards development organizations (SDOs), consortia and forums would it be necessary to collaborate with to maximize synergies and harmonize existing standards?

**F.3 Tasks**

Tasks include, but are not limited to:

– Developing Recommendations, Reports, Guidelines, etc. as appropriate on:

• authenticity, confidentiality, integrity, non‑repudiation, and availability of IoT devices, systems, applications, protocols, platforms, and services;

• security and trust provisioning in IoT both at the ICT infrastructure and future heterogeneous converged service environments;

• security and trust provisioning in IoT services and applications for converged environments among stakeholders of different industries;

• requirements to mitigate the risks and threats identified in IoT and SC&C systems and services;

• utilizing security constructs in IoT systems to protect identity, privacy, and security of the system;

• technical measures to prevent compromise, and protect the integrity and privacy of IoT systems, applications, platforms, and services;

• technical measures needed to support the protection of privacy in SC&C applications, services, and platforms;

• identifying the potential risks associated with the different management, administration, maintenance, and service provisioning in SC&C;

• how to mitigate risks associated with the different management, administration, maintenance, and service provisioning in SC&C;

• supporting availability and portability of the data in IoT and SC&C platforms, systems, and services;

• the use of naming, addressing, and identification in IoT and SC&C deployments;

• identity discovery and identity management in IoT and SC&C;

• methodologies to create trustworthiness in IoT & SC&C devices, systems, applications, protocols, platforms, and services;

• security and trustworthiness in using Application Programming Interfaces (API);

• block-chain based technologies and mechanisms to support security and trustworthiness in IoT & SC&C;

• machine learning and artificial intelligence (AI) technologies for supporting secured interoperability and trustworthiness in IoT & SC&C;

• quantum computing mechanisms to support security and trustworthiness in IoT & SC&C;

• big data techniques for enhancing security and trustworthiness in IoT & SC&C;

• security architectures for IoT and SC&C;

• security, privacy and trustworthiness of Data and relevant platforms in IoT and SC&C.

– Providing the necessary collaboration for joint activities in this field within ITU and between ITU-T and SDOs, consortia and forums.

An up-to-date status of work under this Question is contained in the SG20 work programme (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?q=6/20>).

**F.4 Relationships**

**WSIS Action Lines:**

– C5

**Sustainable Development Goals:**

– 11 and 17

**Recommendations:**

– Y.4000-series and other Recommendations related to security, privacy, trust and identification

**Questions:**

– All Questions of ITU-T SG20

**Study Groups:**

– ITU-T (e.g., considering their lead study group role), ITU-D and ITU-R Study Groups as appropriate

– This Question will collaborate with ITU-T SG2 and ITU-T SG17 on identification aspects of IoT as per the mandate of each study group.

– This Question will collaborate with ITU-T SG17 on security, privacy and trust issues relating to IoT and SC&C as per the mandate of each study group.

**Other bodies:**

– ETSI

– ENISA

– AIOTI

– IEEE

– 3GPP

– W3C

– ISO/IEC JCT 1

– Joint IEC-ISO-ITU Smart Cities Task Force

– IETF

– OASIS

– oneM2M

QUESTION G/20

**Evaluation and assessment of Smart Sustainable Cities and Communities**

(Continuation of Question Q7/20)

**G.1 Motivation**

Comprehensive strategies to implement smart sustainable cities and communities (SSC&C) are emerging around the globe integrating information and communication technologies (ICTs) into all aspects of city planning and operation. In this context, ICTs, especially the Internet of Things (IoT) and other emerging technologies improve the efficiency of a city's functions by making use of pertinent information from different domains through appropriate data analytics. This allows municipalities, communities and citizens to make better-informed decisions, and to more effectively integrate city services and cooperation across different sectors.

At this stage, it is important to be able to assess the impact and measure the performance of various SC&C ventures. One such approach for measurement is provided by key performance indicators (KPIs) that facilitate the monitoring of the progress achieved in support of SC&C transitions, including IoT implementation in specific sectors such as environment, safety, transportation, health, education, and utilities.

It is desirable that cities can quantify and also qualitatively assess their achievement according to their goals. Therefore, by utilizing these indicators, cities as well as their stakeholders can also objectively assess the extent to which they may be perceived as smarter and more sustainable cities.

**G.2 Questions**

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

– General principles that could be used to establish methodologies to assess the use of ICT as well as the impact of ICT on city smartness and sustainability.

– Smart Sustainable Cities Index for worldwide use across countries and regions.

– Usefulness of different methodologies (measurement, statistics sampling, case studies, best practices, etc.) with respect to different countries and regions.

– Best methods for collecting reliable data, accounting for the evolution of that data over time.

– How to assess the achievement of the sustainable development goals (SDGs) in a smart city?

– How to measure and evaluate a city's specific performance and e/smart services with respect to defined sector (or vertical) indicators such as open data indicators, e-health indicators, utilities indicators, etc.

– How to assess city resilience and robustness?

– Collaboration with which standards development organizations (SDOs) would be necessary to maximize synergies and harmonize existing standards?

**G.3 Tasks**

Tasks include, but are not limited to:

– Developing Recommendations, Reports, Guidelines, etc. as appropriate on:

• providing guidance and structured methods to cities for helping prioritize initiatives and also for assessing the maturity of smart and sustainable cities;

• developing methodologies for assessment of city SDGs, considering general principles and criteria for evaluating ICT impact;

• identifying methods for collecting and calculating reliable data to feed into the assessment model;

• developing methodologies and frameworks for measuring and evaluating a city's specific performance and e/smart services with respect to defined sector indicators;

• developing methodologies and frameworks for assessing smart and sustainable city resilience and robustness;

• reporting on the Global Smart Sustainable Cities Index;

• reporting a city's performance to help cities to reach SDGs.

– Providing the necessary collaboration for joint activities in this field within ITU and between ITU-T and SDOs, UN agencies, consortia and forums.

An up-to-date status of work under this Question is contained in the SG20 work programme (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?q=7/20>).

**G.4 Relationships**

**WSIS Action Lines:**

– C2, C3, C6, C7, C8, C10, C11

**Sustainable Development Goals:**

– 3, 6, 7, 9, 11 and 13

**Recommendations:**

– All the pertinent Y.4000 series Recommendations and Y supplements

**Questions:**

– All Questions of ITU-T SG20

**Study Groups:**

– ITU-T, ITU-D and ITU-R Study Groups as appropriate

**Other bodies:**

– IETF

– Open Mobile Alliance (OMA)

– Open Geospatial Consortium (OGC)

– IEEE

– ATIS

– ETSI TC Smart M2M

– CCSA TC10

– oneM2M

– ISO/IEC JTC 1/SC41, ISO/IEC JTC 1/WG11

– Joint IEC-ISO-ITU Smart Cities Task Force

– GSMA

– 3GPP/3GPP2

– W3C

– Organization for the Advancement of Structured Information Standards (OASIS)

– Object Management Group (OMG)

– Industrial Internet Consortium (IIC)

– Alliance of Industrial Internet (AII)

– Alliance for IoT Innovation (AIOTI)

– Open Connectivity Foundation (OCF)

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

1. Consistent with WTSA Resolution 2 (Hammamet, 2016) [↑](#footnote-ref-2)