|  |  |  |
| --- | --- | --- |
|  | INTERNATIONAL TELECOMMUNICATION UNION**TELECOMMUNICATIONSTANDARDIZATION SECTOR**STUDY PERIOD 2022-2024 | SCV-TD21 |
| SCV |
| Original: English |
| **Question(s):** | 1/17, All/17 | Virtual, 10 November 2022 |
| **TD****(Ref.: SG17-LS21)** |
| **Source:** | ITU-T Study Group 17 |
| **Title:** | LS on Intended terms and definitions for action at SG17 Aug/Sep 2022 |
| **LIAISON STATEMENT** |
| **For action to:** | - |
| **For information to:** | SCV |
| **Approval:** | ITU-T Study Group 17 meeting (Virtual, 20 May 2022) |
| **Deadline:** | - |
| **Contact:** | Paul NajarianSG17 liaison officer to SCV | E-mail: najarianpb@state.gov |

|  |  |
| --- | --- |
| **Abstract:** | SG17 May 2022 meeting entrusted SG17 representative to SCV to send a LS to SCV promptly after this SG17 meeting, compiling all intended terms and definitions for action (consent or determination) at next SG17 Aug/Sep 2022 meeting.  |

SG17 May 2022 meeting agreed (three draft new Recommendations for TAP approval,) 14 draft new (and 12 draft revised) Recommendations for consent or determination (and two non-normative texts for SG17 agreement) at next SG17 Aug/Sep 2022 meeting (ref. Annex D of SG17-[R1](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0001)).

The 14 draft new Recommendations for consent and determination are excerpted and listed in the table below.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | **Work item** | **Q/17** | **Subject / Title** | **Approval process** | **Base text(s)** | **Timing** |
|  | [X.arch-design](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17982) | Q1/17 | Design principles and best practices for security architectures | AAP | [TD3386](http://www.itu.int/md/T17-SG17-200824-TD-PLEN-3386) | 2022-09 |
|  | [X.5Gsec-ecs](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17977) | Q2/17 | Security guideline for IMT-2020 edge computing services | TAP | [TD489](http://www.itu.int/md/T22-SG17-220823-TD-PLEN-0489) (TSB edits TD494) | 2022-09 |
|  | [X.5Gsec-ssl](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18009) | Q2/17 | Guidelines for classifying security capabilities in 5G network slice | TAP | [TD490](http://www.itu.int/md/T22-SG17-220823-TD-PLEN-0490) (TSB edits TD495) | 2022-09 |
|  | [X.sc-iot](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17970) | Q6/17 | Security Controls for Internet of Things (IoT) systems | TAP | [TD4091](http://www.itu.int/md/T17-SG17-210824-TD-PLEN-4091) | 2022-09 |
|  | [X.ztd-iot](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18007) | Q6/17 | Security Methodology for Zero-Touch Deployment in Massive IoT based on Blockchain | TAP | [TD243](http://www.itu.int/md/T22-SG17-220510-TD-PLEN-0243) (TSB edits TD460) | 2022-09 |
|  | [X.sles](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17993) | Q7/17 | Security Measures for Location Enabled Smart Office Services | TAP | [TD295](http://www.itu.int/md/T22-SG17-220510-TD-PLEN-0295) (TSB edits TD459) | 2022-09 |
|  | [X.BaaS-sec (ex TR.BaaS-sec)](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17994) | Q8/17 | Guideline on Blockchain as a service (BaaS) security | TAP | [TD231](http://www.itu.int/md/T22-SG17-220510-TD-PLEN-0231) (TSB edits TD458) | 2022-09 |
|  | [X.sgdc](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17980) | Q8/17 | Security guidelines for distributed cloud | TAP | [TD252](http://www.itu.int/md/T22-SG17-220510-TD-PLEN-0252) (TSB edits TD457) | 2022-09 |
|  | [X.edr-sec (ex X.edrsec)](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17974) | Q13/17 | Security guidelines for cloud-based event data recorders in automotive environment | TAP | [TD461](http://www.itu.int/md/T22-SG17-220823-TD-PLEN-0461) (TSB edits TD467) | 2022-09 |
|  | [X.eivn-sec (ex X.eivnsec)](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17975) | Q13/17 | Security guidelines for the Ethernet-based in-vehicle networks | TAP | [TD462](http://www.itu.int/md/T22-SG17-220823-TD-PLEN-0462) (TSB edits TD468) | 2022-09 |
|  | [X.fstiscv](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17973) | Q13/17 | Guidelines for sharing security threat information on connected vehicles | TAP | [TD464](http://www.itu.int/md/T22-SG17-220823-TD-PLEN-0464) (TSB edits TD470) | 2022-09 |
|  | [X.ipscv](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17983) | Q13/17 | Guidlines for an intrusion prevention systems for connected vehicles | AAP | [TD463](http://www.itu.int/md/T22-SG17-220823-TD-PLEN-0463) (TSB edits TD469) | 2022-09 |
|  | [X.srcd](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17969) | Q13/17 | Security requirements for categorized data in V2X communication | TAP | [TD465](http://www.itu.int/md/T22-SG17-220823-TD-PLEN-0465) (TSB edits TD471) | 2022-09 |
|  | [X.srscm-dlt](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18015) | Q14/17 | Security Requirements for Smart Contract Management based on the distributed ledger technology | AAP | [TD236 (TSB edits TD514](http://www.itu.int/md/T22-SG17-220510-TD-PLEN-0514)) | 2022-09 |

SG17 May 2022 meeting entrusted SG17 representative to SCV to send a LS to SCV promptly, compiling all intended terms and definitions for action (consent or determination) at next SG17 Aug/Sep 2022 meeting. Annex to this document is produced compiling Section 3.2 of all these **14** draft **new** Recommendations.

**Annex
Compiling of Section 3.2 of 14 draft new Recommendations
for action in SG17 Aug/Sep 2022 meeting**

# X.arch-design, TD3386

**3.2.1 criteria:** a principle or standard by which something may be judged or decided

**3.2.2 design:** a specification for the construction of a system (hardware or software or both)

**3.2.3 design criteria:** a criteria that applies to a given design

# [X.5Gsec-ecs](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17977), [TD49](http://www.itu.int/md/T22-SG17-220823-TD-PLEN-0489)4

**3.2.1 IMT-2020 edge computing service:** A service provided via the IMT-2020 system which enables a service to be hosted close to the user equipment's access point, so as to achieve an efficient service delivery through the reduced end-to-end latency and load on the transport network.

**3.2.2 IMT-2020 system**: 3GPP system consisting of the IMT-2020 access network (AN), IMT-2020 core network and user equipment (UE).

# [X.5Gsec-ssl](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18009), TD495

None.

# X.sc-iot, TD4091

None.

# X.ztd-iot, TD460

**3.2.1** **zero-touch deployment:** A bootstrapping methodology enabling devices to securely obtain bootstrapping identity with no installer action beyond physical placement and connecting network and power cables.

**3.2.2** **massive IoT:** A large number of Internet of things (IoT) devices (usually from thousands to millions).

**3.2.3** **identifiable information**: Any information that can be used to identify a device to which such information relates, or b) is or might be directly or indirectly linked to a device.

# X.sles, TD459

**3.2.1 Smart office service**: A service combining multiple smart applications (e.g., smart parking, smart water, smart retail store, etc.) that aim to serve and support the office business, improve the quality of an official business, the efficiency of management, and create a suitable office environment for people.

# X.BaaS-sec, TD458

**3.2.1 51% attack:** An attack in which attackers control enough blockchain nodes or enough computational resources to revoke or rewrite the distributed ledger system ledger by controlling the generation of blocks.

**3.2.2 network partition**: A network connection scenario where the network is divided into more than one disconnected part.

# X.sgdc, TD457

None

# X.edr-sec, TD467

**3.2.1 cloud interface**: A gateway of the cloud system, which is an interface for communications between a cloud system and vehicles, users, third parties.

**3.2.2 general manager**: The component of a cloud system that governs the basic procedures of storing, and retrieving EDR / DSSAD data, and verifies basic requirements of request from a user, third party, or vehicle.

**3.2.3 neutral server**: The independent server from the vehicle manufacturers that can provide anonymized or Vehicle Identifiable Information (VII-removed EDR / DSSAD data.

**3.2.4 rule / policy manager**: The component of a cloud system that updates the rule / policy, which is a part of a general manager.

**3.2.5 storage coordinator**: The component of a cloud system that separates EDR / DSSAD data and VII to store and retrieve the data in the cloud storage with a predetermined policy.

# X.eivn-sec, TD468

**3.2.1 electrical and electronic architecture (E/E architecture)**: A coupled, two-plane vehicular architecture, consisting of: 1) an electrical energy or power distribution network plane; and 2) an information processing and communication network architectural plane.

NOTE – A third tag is sometimes added to E/E to indicate the vehicular propulsion technology, i.e., E3;the third E indicates an electric vehicle.

**3.2.2 vehicle border gateway**: A vehicle gateway positioned at the border of and in vehicle internal network domain(s) and vehicle external network domain(s). Consequently, all vehicle-to-everything (V2X) communication traffic is routed via such a vehicle gateway type.

NOTE 1 – The term vehicle gatewayalso covers this meaning, and might therefore be sufficient for in-vehicle network (IVN) architectures with only a single vehicle gateway deployed. However, IVNs can also use vehicle gateways for internal interconnection and interworking purposes only. Such network contexts can lead to the need to differentiate between gateway types in a more detailed manner.

NOTE 2 – The specific interworking functions as supported by a particular *gateway* type are often expressed by an extended gateway name, indicating, for example, the location in a network hierarchy (such as access or core network level), the border or interconnection type of inter-networking (such as security domains), specific network interfaces or communication technologies.

NOTE 3 – A communication control unit is understood as a technical component that belongs to the category of vehicle border gateway (functions).

NOTE 4 –V2X communication covers all traffic types, e.g. that from telematic, ITS or diagnostic services.

**3.2.3 zone-oriented electrical and electronic architecture**: An electrical and electronic (E/E)architecture grouping in-vehicle components (Note 1) such as sensors, actuators and compute nodes, by their location (Note 2) in network subdomains. Each subdomain, a so-called zone (Note 3), has a distinguished zone-related vehicle compute node (known as a zone controller in automotive applications), connected to all intra-subdomains in-vehicle components. Zone controllers of each zone again are interconnected with a superior high-performance in-vehicle compute node. Thus, there is a resulting processing hierarchy between zones and the overall in-vehicle network (IVN) domain, from the perspective of distributed computing architecture.

NOTE 1 – Scoping on the computing and networking components in context of IVNs.

NOTE 2 – “Location” is understood as the network location at the physical or virtual IVN topological level.

NOTE 3 – The notion of zone here is primarily related to the concept of network domains in the context of E/E architectures. Such a zone does not necessarily include the concept of security zone, trusted zone or demilitarized zone as used in other security-related ITU-T Recommendations (like e.g., [b-ITU-T Y.2770].

# X.fstiscv, TD470

None.

# X.ipscv, TD469

**3.2.1 external component**: A software application, firmware or appliance that operates outside a vehicle for in-vehicle intrusion detection and prevention, including:

* external switch controller;
* intrusion detection algorithm and configurations;
* intrusion detection system and database storage for storing detection results;
* infrastructure to maintain vehicle-to-infrastructure communications when connected vehicles are moving.

**3.2.2 flow entry**: A record describing a flow and a corresponding instruction (e.g., forward to a port, forward to external switch controller, modify and forward, drop), priority, timeout, packet counter and byte counter.

**3.2.3 flow table**: A set of flow entries.

**3.2.4 programmable switch**: A managed switch that handles incoming packets by referring them to a built-in flow table.

**3.2.5 switch**: a software application, firmware or appliance that dynamically interconnects physical links to form a connection for information transfer.

**3.2.6 switch controller**: An external component that monitors and manages flow entries for programmable switches.

# X.srcd, TD471

None

# X.srscm-dlt, TD236

**3.2.1 operating environment**: The execution container of the smart contract.

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