|  |  |  |
| --- | --- | --- |
|  | INTERNATIONAL TELECOMMUNICATION UNION**TELECOMMUNICATIONSTANDARDIZATION SECTOR**STUDY PERIOD 2022-2024 | SCV-TD35 |
| SCV |
| Original: English |
|  | 1/17, All/17 | Virtual, 18 April 2023 |
| **TD****(Ref.: SG17-LS42)** |
| **Source:** | SG17 liaison representative to SCV |
| **Title:** | LS/o on Intended terms and definitions for action at SG17 meeting (21 February - 3 March 2023) [to SCV] |
| **LIAISON STATEMENT** |
| **For action to:** | - |
| **For information to:** | SCV |
| **Approval:** | ITU-T Study Group 17 meeting (Geneva, 2 September 2022) |
| **Deadline:** | - |
| **Contact:** | Paul NajarianSG17 liaison officer to SCV | E-mail: najarianpb@state.gov |

|  |  |
| --- | --- |
| **Abstract:** | SG17 Aug/Sep 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 Feb/Mar 2023 meeting.  |

SG17 Aug/Sep 2022 meeting agreed 11 draft new Recommendations for TAP approval, six draft new Recommendations for TAP determination, four new, one revised and one amended draft Recommendations for AAP consent (and two non-normative texts for SG17 agreement) at next SG17 Feb/Mar 2023 meeting (ref. Annex D of SG17-[R10](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0010)).

The 10 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.5Gsec-message | 2/17 | Security requirements for 5G message service | TAP | [TD869](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-230221-TD-PLEN-0869) | 2023-03 |
|  | X.stie | 4/17 | Structured Threat Information Expression | TAP | [TD808](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-230221-TD-PLEN-0808) | 2023-03 |
|  | X.taeii | 4/17 | Trusted Automated Exchange of Intelligence Informa | TAP | [TD808](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-230221-TD-PLEN-0808) | 2023-03 |
|  | X.sc-iot | 6/17 | Security Controls for Internet of Things (IoT) system | TAP | [TD616](https://www.itu.int/md/T22-SG17-220823-TD-PLEN-0549/en) | 2023-03 |
|  | X.rdda | 7/17 | Requirements for data de-identification assurance | TAP | [TD892](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-230221-TD-PLEN-0892) | 2023-03 |
|  | X.nssa-cc | 8/17 | Requirements of network security situational awareness platform for cloud computing | TAP | [TD595](https://www.itu.int/md/T22-SG17-220823-TD-PLEN-0595/en) | 2023-03 |
|  | X.arc-ev | 4/17 | Functional requirements for a secured process to evaluate technical vulnerabilities | AAP | [TD571](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-220823-TD-PLEN-0571) | 2023-03 |
|  | X.websec-7 | 7/17 | Reference monitor for online analytics services | AAP | [TD877](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-230221-TD-PLEN-0877) | 2023-03 |
|  | X.pki-em | 11/17 | Public-key infrastructure: Establishment and maintenance | AAP | [TD671](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-220823-TD-PLEN-0671) | 2023-03 |
|  | X.srscm-dlt | 14/17 | Security requirements for smart contract management based on distributed ledger technology | AAP | [TD558](https://www.itu.int/md/T22-SG17-220823-TD-PLEN-558/en)R3 | 2023-03 |

SG17 Aug/Sep 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 Feb/Mar 2023 meeting. Annex to this document is produced compiling Section 3.2 of all these **10** draft **new** Recommendations.

**Annex
Compiling of Section 3.2 of 14 draft new Recommendations
for action in SG17 Feb/Mar 2023 meeting**

# X.5Gsec-message, [TD869](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-230221-TD-PLEN-0869)

**3.2.1 5G message centre:** Server providing the 5G messaging service.

**3.2.2 Message as a platform (MaaP):** A platform for third-party application to connect with the 5G message centre.

**3.2.3 5G message user equipment (UE):** A 5G user equipment (UE) whose message app supports both short message service (SMS) and rich communication service (RCS) is called the 5G message UE.

**3.2.4 5G message service:** A 5G messaging service including short message service (SMS) and rich communication service (RCS). 5G messaging service supports messages between persons or between applications and persons, and it also supports various media (e.g. long text, picture, video, audio, file, position, etc.) in the message.

# X.stie, [TD808](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-230221-TD-PLEN-0808)

1. **Boolean Operators**: Boolean Operators are used to combine Comparison Expressions within an Observation Expression.
2. **Comparison Expression**: Comparison Expressions are the basic components of Observation Expressions. They consist of an Object Path and a constant joined by a Comparison Operator (listed in section 9.6.1, Comparison Operators).
3. **Comparison Operators**: Comparison Operators are used within Comparison Expressions to compare an Object Path against a constant or set of constants.
4. **Object Path**: Object Paths define which properties of STIX Cyber-observable Objects (SCO) should be evaluated as part of a Comparison Expression. SCOs and their properties are defined in section 6.
5. **Observation**: Observations represent data about systems or networks that is observed at a particular point in time - for example, information about a file that existed, a process that was observed running, or network traffic that was transmitted between two IPs (internet protocol addresses).
6. **Observation Expression**: Observation Expressions consist of one or more Comparison Expressions joined with Boolean Operators and surrounded by square brackets.
7. **Observation Operators**: Observation Operators are used to combine two Observation Expressions operating on two different Observed Data instances into a single pattern.
8. **Pattern Expression**: A Pattern Expression represents a valid instance of a STIX cyber observable pattern. The most basic Pattern Expression consists of a single Observation Expression containing a single Comparison Expression.
9. **Qualifier**: Qualifiers provide a restriction on the Observations that are considered valid for matching the preceding Observation Expression.
10. **Whitespace**: Any Unicode code point that has WSpace set as a property, for example, line feeds, carriage returns, tabs, and spaces.

# X.taeii, [TD808](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-230221-TD-PLEN-0808)

1. API Root: A logical grouping of TAXII Collections, Channels, and related functionality. (Listed in section 1.6.2.)
2. Channel: A publish-subscribe communications method where messages are exchanged, maintained by a TAXII Server. (Listed in section 1.6.5.)
3. Collection: An interface to a logical repository of a group of CTI objects provided by a TAXII Server. (Listed in section 1.6.4.)
4. Endpoint: An Endpoint consists of a specific URL and HTTP method on a TAXII Server that a TAXII Client can contact in order to engage in a specific type of TAXII exchange. (Listed in sections 1.6.1, 1.6.3, and 3.1.)
5. TAXII Client: A software package that connects to a TAXII Server and supports exchanges of cyber threat information as specified in this document.
6. TAXII Server: A software package that supports exchanges of cyber threat information as specified in this document.

# X.sc-iot, TD616

None.

# X.rdda, TD892

**3.2.1 data de-identification assurance**: Grounds for confidence that a data de-identification process meets a set of security requirements.

# X.nssa-cc, TD595

**3.2.1 Situational awareness (SA):** The perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future.

**3.2.2** **Network Security situational awareness (NSSA):** In a large-scale network environment, it aims to perceive the main elements that cause changes in the network security situation, divide them in time and space dimensions according to certain rules, and use which to assess network security situation, predict the developing trends via statistical analysis, data mining, or artificial intelligence, etc., and present them to users visually.

# X.arc-ev, TD571

**3.2.1 Technical vulnerability:** a vulnerability that could be exploited with using technical measures.

# X.websec-7, TD877

**3.2.1 conceptualization:** It processes some normalization steps to convert unstructured and unmeaning data to structured and meaningful data.

**3.2.2 reference monitor:** It enforces access control policies on subjects, which are various data sources and have the ability to perform operations on objects.

# X.pki-em, TD671

**3.4.1 extractor**: An algorithm that transform a weakly random distribution into an almost uniform distribution-

**3.4.2 brute-force attack**: For cryptographic algorithms it is and exhaustive search of all possible combinations until a workable combination is found.

**3.4.3 crypto agility**: The ability to adapt to more secure cryptographic algorithms without significant changes to system structure.

**3.4.4 cryptographic algorithm:** Well-defined computational procedure that takes variable inputs, often including a cryptographic key, and produces an output.

3.4.5 encryption: The process of converting information or data into a code, especially to prevent unauthorized access.

**3.4.4 fully qualified domain name**: A domain name that specifies its exact location in the tree hierarchy of the domain name system (DNS)

**3.4.5 integer factoring**: Breaking a (large) integer down into prime factors when multiplied equal the original integer.

**3.4.6 key agreement**: A pairwise key-establishment algorithm in which the resulted shared secret is a function of information supplied by both participants.

**3.4.7 key establishment**: The procedure that results in secret keying material shared between communicating entities using either key agreement or key transport.

**3.4.8 key transport**: Secure transfer of a symmetric key to a peer communication partner.

**3.4.9 national trust anchor**: A trust anchor established by a recognized national organization that is considered trustworthy by all entities in the country.

**3.4.10** **nonce**: A value that is used only once within a specified context.

**3.4.11 public-key certificate owner**: An entity that is the subject of a public-key certificate.

**3.4.12 public-key infrastructure (PKI) domain**: A PKI under a single management.

**3.4.12 security strength**: A measure expressed in bits of the expected number of operations of some kind required to crack a cryptographic algorithm.

**3.4.13 semiprime**: An integer being the product of two prime integers.

**3.4.14 signatory**: The entity that digitally signs a document or a message.

**3.4.15 Shor's algorithms**: A quantum algorithm for factoring a (large) integer.

**3.4.16 subject name**: The name supplied in the **subject** component of a public-key certificate, and which is used to reference the entity holding the public-key certificate in question.

**3.4.17 verifier**: The entity that verifies a digital signature.

# X.srscm-dlt, TD558R3

None.

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