|  |  |  |
| --- | --- | --- |
| The International Teleocmmunication Union - Connecting the World. | **International telecommunication union****Telecommunication Standardization Bureau** |  |
|  | Geneva, 28 March 2023 |
| **Ref:** | **TSB Circular 79**SG17/XY | **To:**- Administrations of Member States of the Union**Copy to:**- ITU-T Sector Members;- ITU-T Associates of Study Group 17;- ITU Academia- The Chairman and Vice-Chairmen of ITU-T Study Group 17;- The Director of the Telecommunication Development Bureau;- The Director of the Radiocommunication Bureau |
| **Tel:** | +41 22 730 6206 |
| **Fax:****E-mail:** | +41 22 730 5853tsbsg17@itu.int |
| **Subject:** | **Member State consultation on Determined draft new Recommendations** **ITU‑T X.1333 Cor.1, X.1353 (X.ztd-iot), X.1471 (X.websec-7), X.1645 (X.nssa-cc), X.1771 (X.rdda), and X.1817 (X.5Gsec-message) proposed for approval at the meeting of ITU-T Study Group 17, Goyang, Korea, 29 August – 8 September 2023** |

Dear Sir/Madam,

1 ITU-T Study Group 17 (Security) intends to apply the Traditional Approval Procedure as described in Section 9 of WTSA Resolution 1 (Rev. Geneva, 2022) for the approval of the above-mentioned draft Recommendations at its next meeting in Korea, 29 August – 8 September 2023. The agenda and all relevant information concerning the ITU-T Study Group 17 meeting will be available in Collective letter [5/17](https://www.itu.int/md/T22-SG17-COL-0005/en).

2 The titles, summaries and locations of the draft ITU-T Recommendations proposed for approval can be found in **Annex 1**.

TSB NOTE 1 – Except for draft new Recommendation X.1817 (X.5Gsec-message), no ITU-T A.5 justifications have been submitted for the other determined texts.

TSB NOTE 2 – As of the date of this Circular, no IPR statement had been received by TSB for any of these determined texts. For up-to-date information, members are invited to consult the IPR database at [www.itu.int/ipr/](http://www.itu.int/ipr/).

3 This Circular initiates the formal consultation with ITU Member States on whether these texts may be considered for approval at the upcoming meeting, in accordance with clause 9.4 of Resolution 1. Member States are kindly requested to complete and return the form in **Annex 2** by 2359 hours UTC on **16 August 2023.**

4 If 70% or more of the replies from Member States support consideration for approval, one Plenary session will be devoted to apply the approval procedure. Member States that do not assign authority to proceed should inform the Director of TSB of the reasons for this opinion and indicate the possible changes that would enable the work to progress.

Yours faithfully,

Seizo Onoe
Director of the Telecommunication
Standardization Bureau

**Annexes:** 2

Annex 1

Summary and location of Determined draft new Recommendations
ITU T X.1333 Cor.1, X.1353 (X.ztd-iot), X.1471 (X.websec-7), X.1645 (X.nssa-cc), X.1771 (X.rdda), and X.1817 (X.5Gsec-message)

# Draft Corrigendum 1 to Recommendation ITU-T X.1333 [[R34](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0034)]

Security guidelines for use of remote access tools in Internet-connected control systems

# Draft new Recommendation X.1353 (X.ztd-iot), [[R35](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0035)]

Security methodology for zero-touch deployment in massive IoT based on blockchain

## Summary

Massive Internet of Things (mIoT) is a significant application of future communication networks. With diverse use cases anticipated in mIoT, it is difficult for manufacturers to pre-install their manufactured IoT devices with mobile-operator-specific and/or service-specific information (e.g., identities and keys), since manufacturers may not know where their devices will eventually be deployed and activated. The current approach relies on customers’ manual configuration which is acceptable for small-scale IoT applications. However, for mIoT devices, the aforementioned approach is unacceptable due to the fact that manual configuration is time consuming, cost-ineffective and cumbersome. Thus, automatic credential provisioning without user involvement, known as "zero-touch" is needed for mIoT.

This Recommendation provides a security methodology for designing a decentralized identity management system to support the zero-touch deployment of future mIoT. Zero-touch deployment will enable IoT devices to automatically find their mobile network operator and their service provider, automatically obtain credentials from them and automatically connect to the network and the service. This will greatly facilitate the future deployment of mIoT devices for verticals. The content of this Recommendation covers the security architecture, the security considerations and the related security procedures (such as device attestations, authentication, and credential provisioning) which are needed for building such a zero-touch mIoT deployment platform.

# Draft new Recommendation X.1471 (X.websec-7) [[R36](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0036)]

Reference Monitor for Online Analytics Services

## Summary

Big data analysis service is based on the undefined unstructured data including user behaviour, purchase, payment, location and consuming of various internet contents. It can provide new insights not previously discovered and predicts future states. However, some un-authorized data can be used maliciously in the analysis process.

This Recommendation describes a reference monitor for big data analytics and operations to detect an un-authorized data use. The Recommendation analyses security threats and challenges in the big data analytics, and describes security considerations that could mitigate these threats and address security challenges with access control mechanisms. A reference monitor methodology based on access control is provided for determining which of these security capabilities are required for mitigating security threats and addressing security challenges for big data analytics.

# Draft new Recommendation X.1645 (X.nssa-cc) [[R38](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0038)]

Requirements of network security situational awareness platform for cloud computing

## Summary

Network security situational awareness (NSSA) is derived from “situational awareness”. It usually includes four processes: data acquisition, security situation analysis, security situation assessment and security situational tendency projection, and generally has the following capabilities: 1) the capability of detection and persistent monitoring various attack threats, abnormal behaviour and their scope of influence; 2) the capability of data mining, threat analysis, and the traceability of abnormal behaviour; 3) the capability of security prediction and early warning; 4) the capability of visualization of security situation.

For cloud computing service providers, NSSA platform plays an important role in improving cloud computing's security protection, the ability to detect security breaches or anomalous behaviours, security decision-making and emergency response ability, and even it can help improve the early warning mechanism for cloud computing.

This recommendation will first introduce the concept and development of network security situational awareness, analyze the advantages of NSSA coping with the security challenges of cloud computing, then aim to document the requirements for network security situational awareness platform for cloud computing.

# Draft new Recommendation X.1771 (X.rdda) [[R37](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0037)]

Requirements for data de-identification assurance

## Summary

De-identified data incurs the risk of re-identifying individuals. So, it is important to assess the threat that de-identified data is used to identify individuals through re-identification methods. De-identification methods, which can be used for re-identification risk assessment, may be selected accordingly based on the following considerations:

* Data risk assessment: Data composition, data distribution, possession of other data,
* Data use environment risk assessment: Confidence level of data recipient, impact during re-identification, inadvertent re-identification,
* Using and managing de-identification data: Security measures for de-identification data, monitoring of re-identification possibilities, compliance with de-identification data provision or consignment contracts.

This Recommendation defines data de-identification assurance. It also provides a set of requirements for managing data de-identification assurance, including data risk assessment, risk assessment of the data use environment, and using and managing de-identified data.

# Draft new Recommendation X.1817 (X.5Gsec-message) [[R33](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0033)]

Security requirements for 5G messaging service

## Summary

This Recommendation provides the security requirements for 5G messaging service, including use security requirements, management security requirements and control security requirements for 5G messaging service.

Annex 2

Subject: Member State response to TSB Circular 79:
Consultation on Determined draft new Recommendations ITU T X.1333 Cor.1, X.1353 (X.ztd-iot), X.1471 (X.websec-7), X.1645 (X.nssa-cc), X.1771 (X.rdda), and X.1817 (X.5Gsec-message)

|  |  |  |  |
| --- | --- | --- | --- |
| **To**: | Director of the Telecommunication Standardization Bureau,International Telecommunication UnionPlace des NationsCH 1211 Geneva 20, Switzerland | **From**: | [Name][Official role/title][Address] |
| **Fax**:**E-mail**: | +41-22-730-5853tsbdir@itu.int  | **Fax**:**E-mail**: |  |
|  |  | **Date**: | [Place,] [Date] |

Dear Sir/Madam,

With respect to the Member State consultation on the Determined draft text(s) listed in TSB Circular 79, I would like to advise you of the opinion of this Administration, which is set out in the table below.

|  | **Select one of the two boxes** |
| --- | --- |
| **Draft Corrigendum 1 to Recommendation ITU-T X.1333**  | [ ]  **assigns authority** to SG17 to consider this text for approval (in which case, select one of the two options ⃝):⃝ No comments or suggested changes⃝ Comments and suggested changes are attached |
| [ ]  **does not assign authority** to SG17 to consider this text for approval (reasons for this opinion and an outline of possible changes that would enable the work to progress are attached) |
| **Draft new Recommendation ITU-T X.1353(X.ztd-iot)** | [ ]  **assigns authority** to SG17 to consider this text for approval (in which case, select one of the two options ⃝):⃝ No comments or suggested changes⃝ Comments and suggested changes are attached |
| [ ]  **does not assign authority** to SG17 to consider this text for approval (reasons for this opinion and an outline of possible changes that would enable the work to progress are attached) |
| **Draft new Recommendation ITU-T X.1471 (X.websec-7)** | [ ]  **assigns authority** to SG17 to consider this text for approval (in which case, select one of the two options ⃝):⃝ No comments or suggested changes⃝ Comments and suggested changes are attached |
| [ ]  **does not assign authority** to SG17 to consider this text for approval (reasons for this opinion and an outline of possible changes that would enable the work to progress are attached) |
| **Draft new Recommendation ITU-T X.1645 (X.nssa-cc)** | [ ]  **assigns authority** to SG17 to consider this text for approval (in which case, select one of the two options ⃝):⃝ No comments or suggested changes⃝ Comments and suggested changes are attached |
| [ ]  **does not assign authority** to SG17 to consider this text for approval (reasons for this opinion and an outline of possible changes that would enable the work to progress are attached) |
| **Draft new Recommendation ITU-T X.1771 (X.rdda)** | [ ]  **assigns authority** to SG17 to consider this text for approval (in which case, select one of the two options ⃝):⃝ No comments or suggested changes⃝ Comments and suggested changes are attached |
| [ ]  **does not assign authority** to SG17 to consider this text for approval (reasons for this opinion and an outline of possible changes that would enable the work to progress are attached) |
| **Draft new Recommendation ITU-T X.1817 (X.5Gsec-message)** | [ ]  **assigns authority** to SG17 to consider this text for approval (in which case, select one of the two options ⃝):⃝ No comments or suggested changes⃝ Comments and suggested changes are attached |
| [ ]  **does not assign authority** to SG17 to consider this text for approval (reasons for this opinion and an outline of possible changes that would enable the work to progress are attached) |

Yours faithfully,

[Name]

[Official role/title]

Administration of [Member State]

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