|  |  |  |
| --- | --- | --- |
| The International Teleocmmunication Union - Connecting the World. | **International telecommunication union****Telecommunication Standardization Bureau** |  |
|  | Geneva, 23 April 224 |
| **Ref:** | **TSB Circular 195**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 Chair and Vice-Chair 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.1237 (X.tsfpp), X.1283 (X.gpwd), X.1353 (X.ztd-iot), X.1354 (X.sc-iot), X.1384 (X.itssec-5), X.1471 (X.websec-7), X.1819 (X.5Gsec-netec) and X.1820 (X.5Gsec-srocvs) proposed for approval at the meeting of ITU-T Study Group 17, Geneva, 2-6 September 2024** |

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 physical meeting, Geneva, 2-6 September 2024. The agenda and all relevant information concerning the ITU-T Study Group 17 meeting will be available in Collective letter [8/17](https://www.itu.int/md/T22-SG17-COL-0008/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 Recommendations X.1820 (X.5Gsec-srocvs), 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 **21 August 2024.**

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.1237 (X.tsfpp), X.1283 (X.gpwd), X.1353 (X.ztd-iot), X.1354 (X.sc-iot), X.1384 (X.itssec-5), X.1471 (X.websec-7), X.1819 (X.5Gsec-netec), X.1820 (X.5Gsec-srocvs)

# Draft new Recommendation ITU-T X.1237 (X.tsfpp) [[R62](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0062)]

Security requirements for personally identifiable information protection while countering mobile messaging spam

## Summary

Nowadays, driven by commercial interests (advertising), spam content is infiltrating every media to reach us. Operators, software developers and other organizations explore various sorts of technologies, platforms, services and apps to counter spam. However, if personally identifiable information (PII) protection is not taken into account in the design and implementation of these approaches, their functionality and effectiveness might be impaired.

This Recommendation takes PII protection into account in the design and implementation of mobile messaging anti-spam solutions. It provides an overview of mobile messaging anti-spam processes and proposes security requirements for countering mobile messaging spam. Entity functions and processing procedures are also introduced.

# Draft new Recommendation ITU-T X.1283 (X.gpwd) [[R66](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0066)]

Threat Analysis and guidelines for securing password and password-less authentication solutions

## Summary

The security community is making a large movement to replace password authentication with alternative solutions that are known as password-less authentication. Unfortunately, many of the proposed password-less solutions suffer from the same limitation as current password solutions. These solutions are vulnerable to man-in-the-middle and phishing attacks among others.

Recommendation ITU-T X.1283 (X.gpwd) performs security and threat analysis of authentication solutions that are based on the use of shared secrets. It takes a close look into security risks associated with password systems and emerging password-less solutions.

This Recommendation performs threat analysis, develops guidelines and best practices for the protection of users and accounts based on these methods. This work can be used by those adopters to support legacy solutions as they migrate to stronger authentication methods based on PKI (e.g., ITU-T X.1277 and ITU-T X.1278).

# Draft new Recommendation ITU-T X.1353 (X.ztd-iot) [[R63](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0063)]

Blockchain-based Security Methodology for Zero-Touch Deployment of Massive IoT

## 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., identifiers and keys), since manufacturers may not know where and how 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’s involvement, known as "zero-touch" is needed for mIoT.

This Recommendation provides a security methodology for designing a decentralized credential management system to support the zero-touch deployment of future mIoT based on the blockchain technology. This is one feasible and promising approach to achieve the zero-touch deployment for future massive-IoT. Zero-touch deployment will enable IoT devices to obtain credentials automatically from their mobile network operator and their service provider, and thus automatically connect to the network and the service. This will greatly facilitate the future deployment of mIoT devices for verticals. This Recommendation covers security architecture, security considerations and related security procedures (such as device attestations, authentication, and credential provisioning), which are essential for building such a zero-touch deployment platform for mIoT.

# Draft new Recommendation ITU-T X.1354 (X.sc-iot) [[R64](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0064)]

Security controls for IoT systems

## Summary

Recommendation ITU-T X.1354 (X.sc-iot) provides practical security guidelines for three stakeholders, namely providers, developers and users of services, in Internet of things (IoT) systems, whose concept, risks and security controls are also described.

IoT systems present particular challenges for information security because they are highly distributed and involve a large number of diverse entities. This implies that there is a very large attack surface and a significant challenge for an information security management system to apply and maintain appropriate security controls across the whole system.

# Draft new Recommendation ITU-T X.1384 (X.itssec-5) [[R67](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0067)]

Security requirements and guidelines for vehicular edge computing

## Summary

ITU-T Recommendation X.1384 (ex X.itssec-5) provides security requirements and guidelines for vehicular edge computing (VEC). VEC refers to a computing paradigm that deploys processing capability at network edge to distribute computing resources in a core cloud in ITS environments. VEC also provides more localized storage and application services to road users, thereby making it possible to achieve lower latency delays, faster response times, location awareness, high availability, and quality of service for streaming real-time applications, since the data processing is conducted closer to the vehicle.

VEC faces many security challenges and issues since it requires a faster service response time to end users. This Recommendation analyses threats and vulnerabilities identified of VEC and provides security requirements for VEC. Further, it also provides use cases for VEC services.

# Draft new Recommendation ITU-T X.1471 (X.websec-7) [[R65](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0065)]

Reference monitor for online analytics services

## Summary

# Big data analysis service is based on 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 big data analytics and describes security requirements that could mitigate these threats and address security challenges with access control mechanisms. A reference monitor methodology based on access control is provided to determine what security capabilities are required for mitigating security threats and addressing security challenges for big data analytics.

# Draft new Recommendation ITU-T X.1819 (X.5Gsec-netec) [[R60](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0060)]

Security capabilities of network layer for IMT-2020/5G edge computing

## Summary

Edge computing for IMT-2020/5G network (5G EC) will play a key role in low latency services and traffic offload services in next generations of IMT networks. Several prominent factors could increase the complexity and enlarge the security risks to the network layer that supports 5G EC and even bring new security challenges to network security operation. These factors include flexible network architectures of IMT-2020/5G, variable deployment positions of EC, various application scenarios, different types of customers’ private networks and access networks, etc. The boundaries between the telecommunication networks and the private networks would be more ambiguous, and the exposure surface would be expanded. Therefore, security requirements and measures of the network layer including telecommunication networks and private networks should be specified.

# Draft new Recommendation ITU-T X.1820 (X.5Gsec-srocvs) [[R61](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0061)]

Security Requirements for the Operation of IMT-2020/5G Core Network to Support Vertical Services

## Summary

With the development of the IMT-2020/5G system, vertical services have become key scenarios for IMT-2020/5G. In vertical services for smart factories and smart cities that use an IMT-2020/5G network, many user devices use vertical services with massive machine-type communications and ultra-reliable low-latency communications (URLLC).

To support vertical use cases which require URLLC, some IMT-2020/5G core network functions might be deployed at local sites that are closer to vertical users, while other IMT-2020/5G core network functions are still deployed at a central site. Compared with the IMT-2020/5G core network deployed as a whole, the IMT-2020/5G core network operating in such deployment may face specific security threats.

In order to ensure the security of the operation of the IMT-2020/5G core network to support vertical services, specific security threats need to be analysed and relevant security requirements need to be specified.

This Recommendation analyses data security threats, network security threats and physical security threats specific to the operation of the IMT-2020/5G core network deployed at both a central site and local sites to support vertical services, and specifies the relevant security requirements.

This determined draft text includes normative references that require an ITU-T A.5 justification, which can be found in SG17-[TD1739](https://www.itu.int/md/T22-SG17-240220-TD-PLEN-1739/en).

Annex 2

Subject: Member State response to TSB Circular 195:
Consultation on Determined draft new Recommendations ITU-T X.1237 (X.tsfpp), X.1283 (X.gpwd), X.1353 (X.ztd-iot), X.1354 (X.sc-iot), X.1384 (X.itssec-5), X.1471 (X.websec-7), X.1819 (X.5Gsec-netec), X.1820 (X.5Gsec-srocvs)

|  |  |  |  |
| --- | --- | --- | --- |
| **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 195, 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 new Recommendation ITU-T X.1237 (X.tsfpp)** | [ ]  **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.1283 (X.gpwd)** | [ ]  **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.1354(X.sc-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.1384 (X.itssec-5)** | [ ]  **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.1819 (X.5Gsec-netec)** | [ ]  **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.1820 (X.5Gsec-srocvs)** | [ ]  **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]

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