|  |  |  |
| --- | --- | --- |
| The International Teleocmmunication Union - Connecting the World. | **International telecommunication union****Telecommunication Standardization Bureau** |  |
|  | Geneva, 28 September 2022 |
| **Ref:** | **TSB Circular 42**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.1353 (X.ztd-iot), X.1380 (X.edr-sec), X.1381 (X.eivn-sec), X.1382 (X.fstsicv), X1383 (X.srcd), X.1410 (X.sa-dsm), X.1411 (X.BaaS-sec), X.1454 (X.sles), X.1644 (X.sgdc), X.1815 (X.5Gsec-ecs), and X.1816 (X.5Gsec-ssl), for approval at the plenary meeting of ITU-T Study Group 17 (Geneva, 21 February – 3 March 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 Geneva, 21 February – 3 March 2023. The agenda and all relevant information concerning the ITU-T Study Group 17 meeting will be available in Collective letter [3/17](https://www.itu.int/md/T22-SG17-COL-0003/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 draft X.1382 (X.fstsicv),X.1815 (X.5Gsec-ecs), and X.1816 (X.5Gsec-ssl), no ITU-T A.5 justification document has been prepared for other determined draft texts.

TSB NOTE 2 – As of the date of this Circular, no IPR statement had been received by TSB regarding any of these draft 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 **9 February 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,

Chaesub Lee
Director of the Telecommunication
Standardization Bureau

**Annexes:** 2

Annex 1

Summary and location of Determined draft new Recommendations
ITU-T X.1353 (X.ztd-iot), X.1380 (X.edr-sec), X.1381 (X.eivn-sec), X.1382 (X.fstsicv), X1383 (X.srcd), X.1410 (X.sa-dsm), X.1411 (X.BaaS-sec), X.1454 (X.sles), X.1644 (X.sgdc), X.1815 (X.5Gsec-ecs), and X.1816 (X.5Gsec-ssl)

# Draft new Recommendation ITU-T X.1353 (X.ztd-iot) [[R18](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0018)]

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.1380 (X.edr-sec) [[R22](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0022)]

Security guidelines for cloud-based data recorders in automotive environments

## Summary

Event data recorders (EDRs) are one of the most important components installed in automotive road vehicles to record vehicle status, vehicle movements and user inputs during crashes. By analyzing the event data, the cause of a crash can be understood and eventually, used to improve safety in automotive environments. A data storage system for automated driving is also an important component to record data that will give a clear picture of the interactions between the driver and the automated driving system. Conventional event data recorders, however, record and manage the whole data locally and in this way, the data could come under threat of loss and destruction.

Cloud computing is being considered as an enabler of network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand. Industries such as the aviation industry are already attempting to apply cloud services to event data recording systems to increase safety in the aviation environment. According to the current trend of connectivity among vehicles, EDRs and the data storage systems for automated driving will be implemented to increase their overall safety. However, they have various vulnerabilities in the process of collecting, transferring, storing, managing, and using the recorded data according to the distinctive characteristics of the automotive environment. Therefore, it is necessary to study these vulnerabilities, security requirements, and use cases for cloud-based data recorders in automotive environments.

This Recommendation provides security guidelines for cloud-based data recorders in automotive environments. It describes threats, vulnerabilities, security requirements, and use cases for cloud-based data recorders in automotive environments.

# Draft new Recommendation X.1381 (X.eivn-sec) [[R23](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0023)]

Security guidelines for Ethernet-based in-vehicle networks

## Summary

This Recommendation provides security guidelines for Ethernet-based in-vehicle networks (IVNs). The current trend in electrical and electronic (E/E) architecture is to integrate the Ethernet with legacy IVNs such as the controller area network (CAN), local interconnect network (LIN), media-oriented systems transport (MOST) and FlexRay. In the past, the Ethernet was considered only as a connection between vehicles with external environments. Standard protocols that enable Internet protocol-based connections over the Ethernet (e.g., diagnostic communication over Internet protocol or universal measurement and calibration protocol) have been used to enable communications between the external environment and vehicles. These use cases generally do not need to meet stringent real-time constraints. However, in-vehicle applications using Ethernet communication require characteristics that include high time sensitivity and reliability.

Current developments in in-vehicle communication technologies require increased bandwidth in the network. Compared to the Ethernet, legacy IVNs are insufficient to meet the bandwidth requirements of current in-vehicle applications. Therefore, now and in the future, Ethernet-based IVNs are a major part of E/E architecture.

However, countermeasures known from common computer networks cannot be suitable for an automotive application because they were not designed with regard to automotive requirements and capabilities.

To address this demand, this Recommendation provides security guidelines for automotive Ethernet technology. This Recommendation includes a reference model of automotive Ethernet and analysis of threat and vulnerability for Ethernet-based IVNs. In addition, this Recommendation provides security requirements and use cases of Ethernet-based IVNs.

# Draft new Recommendation X.1382 (X.fstsicv) [[R24](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0024)]

Guidelines for sharing security threat information on connected vehicles

## Summary

Connected vehicles are facing increasingly prominent network security issues along with their rapid development. Security threat information of connected vehicles, which plays an integral role in securing connected vehicles, is any information that can help an organization identify, assess, monitor, and respond to a connected vehicle. Organizations that share threat information for connected vehicles can improve their own security postures and those of other organizations.

This Recommendation provides guidance on the principles, rules, methodology and procedures of sharing security information for connected vehicles. It also provides a brief description of the different scopes, roles and effectiveness of the various organizations while they engage in the lifecycle of security threat information sharing.

This Recommendation is intended to help organizations stay in touch with the connected vehicles sharing community and to contribute threat information which would support the practices of connected vehicles safety protection. Overall, this Recommendation aims to enhance security threat information sharing and mitigate the potential impact of cybersecurity attacks on connected vehicles.

This determined draft text includes normative references that require an ITU-T A.5 justification, which can be found in SG17-[TD510](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-220823-TD-PLEN-0510).

# Draft new Recommendation X.1383 (X.srcd) [[R25](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0025)]

Security requirements for categorized data in vehicle-to-everything (V2X) communication

## Summary

Data security is one of the most important considerations for vehicle-to-everything (V2X) communication. However, in a resource constrained environment such as in-vehicle communication, data protection consumes a lot of resources since cryptographic functions are required.

This Recommendation categorizes the data used in V2X communication into several types such as object attribute data, vehicle status data, environmental perception data, vehicle control data, application service data and user personal data, and assigns three security levels for the categorized data types. Based on these categorized data types and assigned data security levels, this Recommendation provides security requirements for categorized data in V2X communication.

# Draft new Recommendation X.1410 (X.sa-dsm) [[R26](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0026)]

Security architecture for data-sharing management based on distributed ledger technology

## Summary

Distributed ledger technologies (DLTs) provide innovative solutions that are transforming industries and changing the way governments, institutions, and businesses operate. Their decentralization and tamper-proof features enable DLTs to provide a solution for securely replicating, sharing, and synchronizing data across a distributed computer network. Current approaches for sharing business data and personally identifiable information (PII) data with companies and digital platforms have led to privacy vulnerabilities from hacks or poor data management. Adopting DLT or blockchain in data-sharing management allows individuals or companies to maintain more direct control over their own confidential information. In the DLT-based solution, only non-PII data, e.g., hashed data values, is stored in the on-chain while the PII data about a data owner is stored in the off-chain. A DLT-based solution provides a way that improves the traceability, verifiability and changeability of status of data.

This Recommendation specifies a security architecture of data-sharing management based on distributed ledger technologies (DLTs). Based on this architecture, this Recommendation specifies the interfaces between the functional entities and the procedures of data-sharing management based on DLT.

# Draft new Recommendation X.1411 (X.BaaS-sec) [[R20](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0020)]

Guideline on blockchain as a service (BaaS) security

## Summary

Blockchain as a service (BaaS) has become mainstream in blockchain development due to its promising capabilities and the extensive support it has received from the industry, especially top cloud providers. BaaS provides the fundamental service and resources for blockchain applications, however, it faces security challenges arising from both blockchain core technologies and cloud platforms. Guidance on Baas security is thus of great importance and a necessity.

This Recommendation provides generic security guidelines for blockchain as a service (BaaS). The security threats and vulnerabilities of BaaS are first analysed and then the security measures of BaaS are provided. The Recommendation also addresses security requirements and provides guidelines for all the activities in the construction, operation and use of BaaS.

# Draft new Recommendation X.1454 (X.sles) [[R19](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0019)]

Security measures for location enabled smart office services

## Summary

The smart office services combining multiple smart applications aim to improve the quality of official businesses and enhance efficiency management. Since information and communication technologies (ICTs) serve as the basis for technologies in smart office services, the telecommunication operator plays an important role among the stakeholders in smart office services.

Typical smart office services include smart parking, smart driving, smart retail shop, smart office, smart meeting room management, smart water, smart energy consumption management, etc. Among these typical smart office services, the location data provided by the operator is one of the key elements in most smart office service implementations.

In order to ensure the security of location enabled smart office services, security threats and relevant security requirements specific to location enabled services need to be analyzed and the overall security measures established.

This Recommendation analyzes the typical application scenarios of location enabled smart office services, specifies their security threats and requirements and establishes security measures for the operator and key stakeholders in a smart office to safeguard location enabled services.

# Draft new Recommendation X.1644 (X.sgdc) [[R21](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0021)]

Security Guidelines for distributed cloud

## Summary

This Recommendation analyses security threats and challenges on distributed cloud and proposes security guidelines against threats to distributed cloud, which includes the security guidelines for core cloud, regional cloud and edge cloud.

# Draft new Recommendation X.1815 (X.5Gsec-ecs) [[R16](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0016)]

Security guidelines and requirements for IMT-2020 edge computing services

## Summary

The IMT-2020 network will enable a variety of services, including enhanced mobile broadband (eMBB) services, massive machine type communications (mMTC) based services and ultrareliable low latency communications (URLLC) based services, on an infrastructure of network and computing resources. In line with the key features and the requirements identified for the IMT-2020 network, it is required to be more efficient, personalized, intelligent, reliable and flexible.

To support the typical services in the IMT-2020 network, especially eMBB services and URLLC based services, edge computing is acknowledged to be one of the key technologies for meeting the demanding key performance indicators (KPIs) of the IMT-2020 network, especially as far as low latency and bandwidth efficiency are concerned.

Edge computing enables the operator and the third party service provider to deploy the services close to the user's access point, thus achieving high-efficiency service delivery through reduced end-to-end latency and load on the transport network.

In order to ensure the security of edge computing service deployment and application, the security threats and relevant security requirements specific to edge computing service need to be analysed and the overall security framework need to be established.

This draft Recommendation analyses the deployment scheme and typical application scenarios of edge computing services, specifies the security threats and requirements specific to edge computing services in IMT-2020 and thus establishes security capabilities for the operator to safeguard its applications.

This determined draft text includes normative references that require an ITU-T A.5 justification, which can be found in SG17-[TD605](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-220823-TD-PLEN-0605).

# Draft new Recommendation X.1816 (X.5Gsec-ssl) [[R17](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0017)]

Guidelines and requirements for classifying security capabilities in IMT-2020 network slice

## Summary

The definition of basic network slicing technology functions and processes has laid a solid foundation for the first wave of IMT-2020 deployment and commercial use of network slicing services. As an end-to-end logical network that is customized on demand, slicing can provide differentiation security capabilities.

First, the IMT-2020 network slicing provides the supporting security measures for the differentiated network implementation. Second, the IMT-2020 network supports some optional security measures at the slice level. Some security measures can also provide multiple security options and operators may own different security resources which may bring different degrees of security guarantee or non-security performance.

Slice customers also have specific security requirements and may request customized network slices with different security protection levels from slice operators. There exist some challenges for both slice customers and slice operators in choosing the security capabilities of their slices such as management cost and definition inconsistency, etc.

This Recommendation provides a description of differentiated IMT-2020 network slice security capabilities and guidance in classifying these security capabilities to aid the IMT-2020 ecosystem in selecting network slice security capabilities.

This determined draft text includes normative references that require an ITU-T A.5 justification, which can be found in SG17-[TD552](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-220823-TD-PLEN-0552).

Annex 2

Subject: Member State response to TSB Circular 42:
Consultation on Determined draft new Recommendations ITU-T X.1353 (X.ztd-iot), X.1380 (X.erd-sec) and X.1381 (X.eivn-sec), X.1382 (X.fstsicv), X1383 (X.srcd), X.1410 (X.sa-dsm), X.1411 (X.BaaS-sec), X.1454 (X.sles), X.1644 (X.sgdc), X.1815 (X.5Gsec-ecs), X.1816 (X.5Gsec-ssl)

|  |  |  |  |
| --- | --- | --- | --- |
| **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 42, 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.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.1380 (X.edr-sec)** | [ ]  **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.1381 (X.eivn-sec)** | [ ]  **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.1382 (X.fstsicv)** | [ ]  **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.1383 (X.srcd)** | [ ]  **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.1410 (X.sa-dsm)** | [ ]  **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.1411 (X.BaaS-sec)** | [ ]  **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.1454 (X.sles)** | [ ]  **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.1644 (X.sgdc)** | [ ]  **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.1815 (X.5Gsec-ecs)** | [ ]  **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.1816 (X.5Gsec-ssl)** | [ ]  **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]

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