|  |  |  |
| --- | --- | --- |
| The International Teleocmmunication Union - Connecting the World. | **International telecommunication union****Telecommunication Standardization Bureau** |  |
|  | Geneva, 11 October 2023 |
| **Ref:** | **TSB Circular 142**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 Recommendations** **ITU T X.1150 (X.saf-dfs), X.1221 (X.stie), X.1222 (X.taeii), X.1280 (X.oob-sa), X.1281 (X.osia), Amendment 1 to X.1352, revised X1373, and X1818 (X.5Gsec-ctrl), proposed for approval at the meeting of ITU-T Study Group 17, 20 February – 1 March 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 meeting in Geneva, 20 February – 1 March 2024. The agenda and all relevant information concerning the ITU-T Study Group 17 meeting will be available in Collective letter [6/17](https://www.itu.int/md/T22-SG17-COL-0006/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.1221 (X.stie), X.1222 (X.taeii), 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 **8 February 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 Recommendations
ITU T X.1150 (X.saf-dfs), X.1221 (X.stie), X.1222 (X.taeii), X.1280 (X.oob-sa), X.1281 (X.osia), Amendment 1 to X.1352, revised X1373, and X1818 (X.5Gsec-ctrl)

# Draft new Recommendation ITU-T X.1150 (X.saf-dfs) [[R50](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0050)]

Security assurance framework for digital financial services

## Summary

Digital financial service (DFS) involves a complex ecosystem with the participation of different stakeholders such as banks, DFS providers, mobile network operators (MNOs), DFS platform providers, regulators, agents, merchants, payment service providers, device manufacturers, application developers, token service providers, original equipment manufacturers (OEMs), and clients. The interconnectedness of these entities and reliance on several parties in the ecosystem extends the security boundaries beyond the DFS provider to customers, network providers, mobile phone manufacturer, and other third-party providers in the ecosystem.

A DFS security assurance framework provides an overview of the security threats and vulnerabilities facing the applicable DFS stakeholders. Regulators including telecom authorities, banking, and payment regulators could also make use of the DFS security assurance framework to establish security baselines for the DFS providers as well.

The framework, when implemented, would complement established risk and information security management practices of the stakeholders involved in the DFS ecosystem. For example, the security controls in this Recommendation can be included as part of the information and communication technology (ICT) security programme of the DFS provider.

This Recommendation describes a DFS security assurance framework which provides a systematic security risk management process to assess threats and vulnerabilities and identifies appropriate security controls to be implemented by the DFS stakeholders. Threats related to merchants, payment service providers and other financial services organizations and the specific mitigations for addressing the threats that they face are out of scope for this Recommendation.

The DFS security assurance framework consists of the following components:

a) A security risk management process based on [b-ISO/IEC 27005].

b) Assessment of threats and vulnerabilities to the underlying infrastructure of the mobile network operator and DFS provider, DFS applications, services, network operations and third-party providers involved in the ecosystem for DFS delivery.

c) Mitigation strategies based on the outcome of (b) above. The mitigation measures identify 119 security controls for security threats which are outlined in clause 13 of this Recommendation.

# Draft new Recommendation X.1221 (X.stie), [[R47](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0047)]

Structured Threat Information eXpression (STIX)

## Summary

This Recommendation defines Structured Threat Information Expression (STIX), a language used to express data objects and exchange cyber threat intelligence, along with a JSON serialization format. STIX does not rely on any specific transport mechanism. This Recommendation is technically equivalent and compatible with the published OASIS standard STIX 2.1 [b-STIX v2.1].

# Draft new Recommendation X.1222 (X.taeii) [[R48](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0048)]

Trusted Automated eXchange of Intelligence Information (TAXII)

## Summary

This Recommendation is an application layer protocol for the communication of cyber threat information in a simple and scalable manner. This specification defines the TAXII REST application programming interface (API) and its resources, along with requirements for TAXII Client and Server implementations. TAXII is a set of methods for sharing and communicating data objects relevant to the exchange of cyber threat intelligence. This Recommendation is technically equivalent and compatible with the published OASIS Standard TAXII Version 2.1 [b-TAXII v2.1].

# Draft new Recommendation X.1280 (X.oob-sa) [[R51](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0051)]

Framework for out-of-band server authentication using mobile devices

## Summary

In the authentication technology standards, the verifier impersonation resistance is considered as a requirement of the highest level of authentication assurance. However, existing authentication technologies focus on user authentication so there is a limitation that cannot verify service providers explicitly.

This Recommendation provides a framework for out-of-band server authentication using mobile devices, which resolves the vulnerability of verifier impersonation and the limitation of user terminal dependency of the existing authenticators. It allows a user to provide user authentication information after verifying the service provider explicitly and independently in the user authentication process on any user terminals.

# Draft new Recommendation X.1281 (X.osia) [[R52](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0052)]

APIs for interoperability of identity management systems

## Summary

This Recommendation describes a set of standardized application program interfaces (APIs) needed to connect the multiple building blocks of an identity management solution.

# Draft new Amendment 1 to Recommendation X.1352 [[R49](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0049)]

Security requirements for Internet of things devices and gateways

## Summary

Recommendation ITU-T X.1352 establishes detailed requirements for five security dimensions applicable to Internet of things (IoT) device and gateway: authentication; cryptography; data security; device platform security; and physical security, based on the IoT reference model specified in Recommendation ITU‑T Y.4100 and the IoT security framework in Recommendation ITU-T X.1361.

The authentication dimension includes user authentication, secure use of authentication credentials and device authentication. The cryptography dimension includes the use of secure cryptography, secure key management and secure random number generation. The data security dimension includes secure transmission and storage, information flow control, secure session management and personally identifiable information (PII) management. The device platform security dimension includes five elements: software security; secure update; security management; logging; and timestamp. Likewise, the physical security dimension includes a secure physical interface and tamper-proofing.

# Draft revised Recommendation X.1373 [[R53](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0053)]

Secure software update capability for intelligent transportation system communication devices

## Summary

As Intelligent Transportation System (ITS) technologies improve, it has become common for vehicles to communicate with other entities such as other vehicles, Vehicle-to-Vehicle (V2V) and Vehicle-to Infrastructure (V2I) communications. Electric devices inside a vehicle such as Electronic Control Units (ECUs), Electronic Toll Collections (ETCs) and car navigation systems are becoming more sophisticated. As a result, software modules inside these electric devices need to be appropriately updated for the purposes of bug fixing and performance and security improvements, to avoid accidents.

In order to fulfil the above requirements, Recommendation ITU-T X.1373 provides secure software update procedures between a software update server and vehicles with appropriate security controls including in-vehicle communication messages. This Recommendation can be utilized by car manufacturers and ITS-related industries as a set of standard capabilities for best practice.

# Draft new Recommendation X.1818 (X.5Gsec-ctrl) [[R46](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0046)]

Security controls for operation and maintenance of IMT-2020/5G network systems

## Summary

This Recommendation provides comprehensive guidance on securing the IMT-2020 (aka 5G) system during operation and maintenance phases in practice. The described security threats and recommended security controls are the result of a threat analysis.

The focus of this Recommendation is the 5G Standalone (5G SA) system as well as the virtual infrastructure and associated management systems that are expected to form the foundation for 5G deployments. Furthermore, consideration has been given not only to technology, but also people and process aspects affecting the security of 5G services. Recommended security controls are described at a high-level and reference established standards and best practices where relevant.

Annex 2

Subject: Member State response to TSB Circular 142:
Consultation on Determined draft Recommendations ITU T X.1150 (X.saf-dfs), X.1221 (X.stie), X.1222 (X.taeii), X.1280 (X.oob-sa), X.1281 (X.osia), Amendment 1 to X.1352, revised X1373, and X1818 (X.5Gsec-ctrl)

|  |  |  |  |
| --- | --- | --- | --- |
| **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 142, 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.1150(X.saf-dfs)** | [ ]  **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.1221(X.stie)** | [ ]  **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.1222 (X.taeii)** | [ ]  **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.1280 (X.oob-sa)** | [ ]  **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.1281 (X.osia)** | [ ]  **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 Amendment to Recommendation ITU-T X.1352**  | [ ]  **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 revised Recommendation ITU-T X.1373** | [ ]  **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.1818 (X.5Gsec-ctrl)** | [ ]  **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]

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