

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1374

(10/2020)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Secure applications and services (2) – Intelligent
transportation system (ITS) security

**Security requirements for external interfaces
and devices with vehicle access capability**

Recommendation ITU-T X.1374



International
Telecommunication
Union
Documents

Document Sharing Hub

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
5G SECURITY	X.1800–X.1819

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1374

Security requirements for external interfaces and devices with vehicle access capability

Summary

Recommendation ITU-T X.1374 analyses security threats to connected vehicles in two parts: threats against interfaces which are used to communicate between a vehicle and its external devices, and threats against external devices which communicate with the vehicle. Recommendation ITU-T X.1374 specifies security requirements for such external interfaces and external devices with vehicle access capability in telecommunication network environments to address identified threats depending on types of access interfaces. Interfaces and external devices with vehicle access capability include the remote keyless entry (RKE) system with smart key, diagnostic tools and wireless dongles using on-board diagnostic II (OBD-II) port, telematics control units with wireless communication devices and so on.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1374	2020-10-29	17	11.1002/1000/14446

Keywords

Electric vehicle charging system security, external interfaces, ITS security, on-board diagnostics-II, vehicle-accessible device.

* To access the Recommendation, type the URL <http://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID. For example, <http://handle.itu.int/11.1002/1000/11830-en>.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2021

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

		Page
1	Scope	1
2	References.....	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation.....	2
5	Conventions	2
4	Abbreviations and acronyms	2
6	External interfaces and devices with vehicle access capability to a vehicle	4
7	Security threats on external interfaces and devices	5
	7.1 General	5
	7.2 Threats to confidentiality.....	6
8	General security requirements for external interfaces and external devices	7
	8.1 Hardware-assisted security	7
	8.2 Secure communication	8
	8.3 Secure functions	8
	8.4 Protection against hardware tampering	10
9	Security requirements for external devices with wireless communication capability..	10
	9.1 Bluetooth interface	10
	9.2 Cellular interface	11
	9.3 Wi-Fi interface.....	11
10	Security requirements for external devices of remote key-less entry.....	12
	10.1 Reverse engineering prevention	12
	10.2 Secure communication	12
	10.3 Secure key registration procedure	13
11	Security requirements for external devices of charging systems in an EV	13
12	Use cases of security measures for external devices and interfaces in a vehicle	13
	12.1 Use case 1: Smart key and external interface	13
	12.2 Use case 2: Charging device and external interface	14
	12.3 Use case 3: Wireless communication device and external interface	15
	12.4 Use case 4: External devices connected to OBD-II port and external interface	16
	Appendix I – Information on Bluetooth specification	17
	Appendix II – Information on cellular communication specification.....	18
	Bibliography.....	19

Recommendation ITU-T X.1374

Security requirements for external interfaces and devices with vehicle access capability

1 Scope

This Recommendation analyses security threats to connected vehicles in two parts: threats against interfaces which are used to communicate between a vehicle and its external devices, and threats against external devices which communicate with the vehicle. This Recommendation specifies security requirements for such external interfaces and external devices with vehicle access capability in telecommunication network environments to address identified threats depending on the types of access interfaces.

Interfaces and external devices with vehicle access capability include the remote keyless entry (RKE) system with smart key, diagnostic tools and wireless dongles using on-board diagnostic II (OBD-II) port, telematics control units with wireless communication devices and so on.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1371] Recommendation ITU-T X.1371 (2020), *Security threats to connected vehicles*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 authentication [b-ITU-T X.1252]: A process used to achieve sufficient confidence in the binding between the entity and the presented identity.

3.1.2 availability [b-ITU-T X.800]: The property of being accessible and useable upon demand by an authorized entity.

3.1.3 confidentiality [b-ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

3.1.4 data integrity [b-ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

3.1.5 plug and charge (PnC) [b-ISO 15118-1]: Identification mode where the customer just has to plug their vehicle into electric vehicle supply equipment and all aspects of charging are automatically taken care of with no further intervention from the driver.

3.1.6 threat [b-ISO/IEC 27000]: A potential cause of an unwanted incident, which may result in harm to a system or organization.

3.1.7 electric vehicle (EV) [b-ISO 15118-1]: All road vehicles, including plug-in hybrid electric vehicles (PHEVs) that derive all or part of their energy from on-board rechargeable energy storage systems (RESS).

3.1.8 electric vehicle supply equipment (EVSE) [b-ISO 15118-1]: Conductors, including the phase(s), neutral and protective earth conductors, the electric vehicle (EV) couplers, attached plugs, and all other accessories, devices, power outlets or apparatuses installed specifically for the purpose of delivering energy from the premises wiring to the EV and allowing communication between them as necessary.

3.1.9 electric vehicle communication controller (EVCC) [b-ISO 15118-1]: Embedded system, within the vehicle, that implements the communication between the vehicle and the supply equipment communication controller (SECC) in order to support specific functions.

3.1.10 supply equipment communication controller (SECC) [b-ISO 15118-1]: Conductors, including the phase(s), neutral and protective earth conductors, the electric vehicle (EV) couplers, attached plugs, and all other accessories, devices, power outlets or apparatuses installed specifically for the purpose of delivering energy from the premises wiring to the EV and allowing communication between them as necessary.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 external device: An independent device located outside the vehicle and is connected to the vehicle via the external interface (see clause 3.2.2).

3.2.2 external interface: A communication interface to provide connectivities between diverse external devices (see clause 3.2.1) and the internal systems of a vehicle.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AES	Advanced Encryption Algorithm
ASM	Application Software Module
ASW	Application Software
BR/EDR	Basic Rate / Enhanced Data Rate
BSW	Basic Software
CAN	Controller Area Network
CIA	Confidentiality, Integrity and Availability
CMAC	Cipher-based Message Authentication Code
CPU	Central Processing Unit
DoS	Denial of Service
DTC	Diagnostic Trouble Code
ECU	Electronic Control Unit
EV	Electric Vehicle
EVCC	Electric Vehicle Communication Controller
EVSE	Electric Vehicle Supply Equipment
JTAG	UMTS Joint Test Action Group

HSM	Hardware Security Module
LE	Low Energy
LF	Low Frequency
LTE	Long-Term Evolution
MAC	Message Authentication Code
ODB-II	On-Board Diagnostic-II
OEM	Original Equipment Manufacturer
PHEV	Plug-in Hybrid Electric Vehicle
PII	Personally Identifiable Information
PKE	Passive Keyless Entry
PKI	Public Key Infrastructure
PLC	Power Line Communication
PnC	Plug and Charge
RESS	Rechargeable Energy Storage System
RF	Radio Frequency
RKE	Remote Keyless Entry
RNG	Random Number Generator
SECC	Supply Equipment Communication Controller
SHA	Secure Hash Algorithm
SSID	Service Set Identifier
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TCU	Telematics Control Unit
UART	Universal Asynchronous Receiver/Transmitter
UMTS	Universal Mobile Telecommunication System
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup

5 Conventions

This Recommendation uses the following conventions:

The keywords "**should**" and '**required**' indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keyword '**can**' indicate an optional requirement which is permissible, without implying any sense of being recommended.

The keywords "**should not**" indicates a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.