International Telecommunication Union

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

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/.

Table of Contents

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.

6 External interfaces and devices with vehicle access capability to a vehicle

Benefiting from information and communication technologies, recent vehicles have various external interfaces to provide connectivities between diverse external devices and internal systems of the vehicle for the purpose of diagnosing the vehicle status, remote communication service, remote entry service, electric charging, over-the-air updates and so on. The external interface refers to the communication interface to provide connectivities between diverse external devices and the internal systems of a vehicle. The external device is an independent device located outside the vehicle and is connected to the vehicle via the external interface. Figure 1 shows an overview of various external devices, external interfaces and internal systems of a vehicle.

The external interfaces used to communicate between the external devices and internal system of vehicle are as follows:

- OBD-II port: Represents a port in the vehicle used for the vehicle's self-diagnostic and reporting capability
- Telematics control unit (TCU): Represents the integrated use of communications and information technology to transmit, store and receive information from telecommunications devices to remote objects over a network
- External interface of remote keyless entry (RKE) and passive keyless entry (PKE): Represents an automotive security system that remotely controls the opening and closing of the door in a vehicle without using a conventional mechanical key. A standard RKE device requires the driver to hold the device and push a button to lock or unlock the vehicle. A PKE however is an automotive security system that operates automatically without the driver's additional action. For example, when the driver is in proximity to the vehicle, the PKE unlocks the door. When the user walks away or touches the door of the vehicle on exit, and the PKE locks the door. The PKE device can operate while stored in the user's pocket or bag.
- Charging interface on a vehicle: Represents an automotive charging system for an electric vehicle (EV) that has physical and data link layers on high-level communication, based on wired and wireless communication technology.

Through the above external interfaces, the following external devices have access to a vehicle:

- Scanning tool: an electronic tool used to interface with, diagnose and reprogram vehicle control modules.
- Wireless dongle: a small piece of hardware that connects to another device to provide additional functionality using wireless communication.
- Wireless communication-enabled device: any type of device supporting various wireless communication technologies such as smartphones, tablets, laptops, etc.
- Smart key: a vehicle key used for unlocking the door and starting the engine based on the RKE system.
- EV supply equipment (EVSE): an installed equipment specifically for the purpose of delivering energy from the premises wiring to the EV and allowing communication between them as necessary.

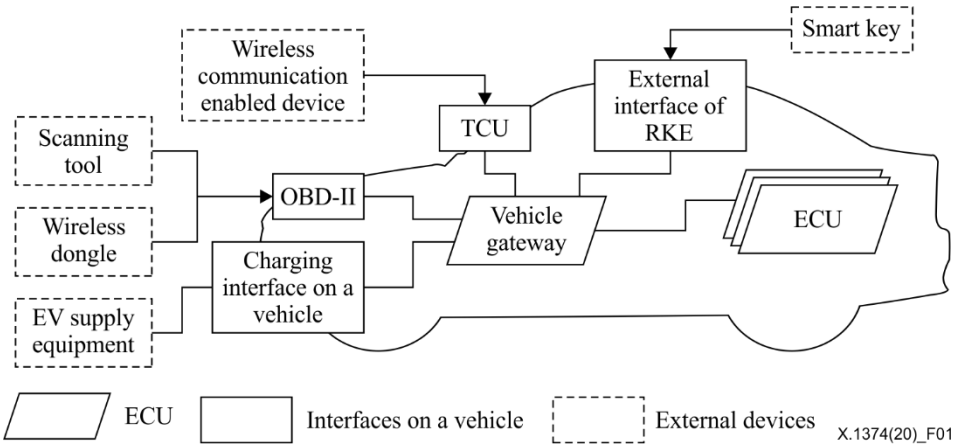

Figure 1 – Overview of vehicle external interfaces and external devices

The relations between external devices and interfaces, and corresponding use cases are listed in Table 1.

Table 1 – List of external devices and interfaces

External devices	External interfaces	Connection type	Use case
Scanning tool	OBD-II	Wired	Scanning tool can diagnose internal systems of a vehicle through OBD-II
Wireless dongle	OBD-II	Wireless	A wireless dongle, such as Bluetooth dongle, Wi-Fi dongle and Long-Term Evolution (LTE) dongle, enables OBD-II port to have a wireless communication capability to be connected with wireless communication enabled devices
Wireless communication-enabled device	TCU	Wireless	Wireless communication enabled devices, such as a tablet, mobile phone or laptop, can access to the internal systems of a vehicle through TCU
Smart key	External interface of RKE/PKE	Wireless	Smart key transmits a message to an external interface of RKE/PKE to open or close the door
EV supply equipment	Charging interface on a vehicle	Wired and Wireless	For EV charging, essential data such as billing information and vehicle identification information is transmitted between EV supply equipment and charging system in a vehicle

7 Security threats on external interfaces and devices

7.1 General

General security threats related to external interfaces are specified in [ITU-T X.1371] especially in clauses 7.1.2 (*Threats to vehicles regarding their communication channels*) and 7.1.5 (*Threats to vehicles regarding their external connectivity and connections*).

In addition, the following threats which are caused by external interfaces and devices with weak security are specified for extended confidentiality, integrity and availability (CIA). Extended CIA in this Recommendation means CIA with non-repudiation and authenticity added.

7.2 Threats to confidentiality

− Eavesdropping

Sensitive information such as the location of a vehicle, payment information, personally identifiable information (PII) can be used in the service application between external devices and a vehicle. An attacker can acquire confidential information by eavesdropping on the communication between the external device and the vehicle. In particular, in the case of software updates thorough an OBD-II port or telematics control unit, the software and/or firmware can be sniffed by an attacker. Then, the attacker analyses the software and modifies it to make his own malicious software.

7.3 Threats to integrity

− Code injection to a vehicle

An attacker who wants to compromise a target electronic control unit (ECU) in a vehicle injects tampered software binary into the communication stream. After the attacker compromises the target ECU, a malicious command can be sent to the target ECU.

− Message manipulation

Manipulation of a message may be the easiest way to hack a target vehicle. For example, attackers get some data or code and modify just one bit or byte. It causes an unintended action or results on the target vehicle. In the case of a charging system in an EV, payment information can be manipulated.

− Replay attack

An attacker can replay controller area network (CAN) data packets acquired through sniffing. In particular, the replay attack is fatal in an RKE system. If an attacker can obtain a remote key packet, he can open and start the target vehicle by just replaying it.

− Maintenance record manipulation

The diagnostic devices are used to maintain a vehicle. The diagnostic device first diagnoses the vehicle and then transmits diagnostic data or maintenance data to a central server which is operated by the vehicle original equipment manufacturer (OEM), or a third party. If the external devices are compromised, information of the vehicle such as maintenance history, accident record, mileage of the vehicle, etc. can be manipulated.

7.4 Threats to availability

− Denial of service (DoS)

As for other industries, there are many types of DoS attacks on the vehicle. The simplest method of DoS attack is by injecting a large amount of data packets into the CAN of a vehicle. Another example of a DoS attack is called a 'CAN bus off attack' using CAN protocol characteristics. It causes a target ECU to turn to a bus-off state and eventually it performs its original functionality.

7.5 Threats to non-repudiation

− Exposure of credential or a private key of an external device

Most of the connected-car services adopt a security access mechanism between the vehicle and external devices based on public key infrastructure (PKI). If an attacker hacks external devices and acquires certificates and private keys of external devices, the security access mechanism in the vehicle is no longer valid.

7.6 Threats to authenticity

− Impersonation attack

If an external device is compromised, it can pretend to be an authorized external device to a vehicle. The compromised device can then receive and send a message which is only allowed for the authorized external devices.

For example, an external device that is originally used for simple diagnostics such as a read and delete diagnostic trouble code (DTC) can actuate some of the safety-related functions such as controlling a steering wheel or shutting off the fuel valve.

– Session hijacking

There is diverse and important information in communication between external devices and a vehicle (e.g., charging information, location information, vehicle identity information, and actuation command data). An attacker can bypass authentication through session hijacking and acquire confidential information.

7.7 Threats to accountability

− Modification or deletion of log information

Log information such as authentication attempts and configuration changes is stored in the diagnostic device. This information can be used to analyse a security incident. An attacker can modify or delete log information to hide his malicious behaviour.

7.8 Threats to authorization

− Unauthorized access to personal-sensitive information in a vehicle

Recently vehicles tend to provide a lot of convenience services such as location sharing, remote actuation, in-vehicle payment and healthcare services. These trends make a vehicle or a vehicle OEM save personal-sensitive information in the vehicle. These personally identifiable information (PII) data can be accessed or used through external devices which are authorized by the vehicle OEM or service provider. If there is no appropriate authorization mechanism, personal-sensitive information can be misused or exposed.

8 General security requirements for external interfaces and external devices

8.1 Hardware-assisted security

External devices and external interfaces should be equipped with hardware-assisted security. Hardware-assited security is the root of trust in various security features. This hardware is a dedicated module specifically designed for cryptographic processing with/without a hardware accelerating feature and storing and managing cryptographic keys inside a hardened, tamper-resistant device. The hardware security module (HSM) could be one example of this hardware. Hardware-assisted security should include the following components:

− Secure central processing unit (CPU)

− Secure storage

− Crypto hardware acceleration

8.1.1 Secure CPU

Secure CPU is a dedicated CPU for hardware-assisted security that controls secure storage and cryptographic operation. Secure CPU does not load application core and performs operations independently. In addition, the secure CPU can control registers and interrupts for sending and receiving data with application core.

8.1.2 Secure storage

Secure storage is a storage space for securely storing keys, message authentication codes (MAC) and certificates or user-defined important information. Secure storage is located inside hardware-assisted security and is used exclusively by a secure CPU. Therefore application core cannot access secure storage.

8.1.3 Crypto hardware acceleration

Cryptographic operation is a costly operation for computing resources. Therefore, there is a limit to performing the computing with only software in a limited embedded environment such as a vehicle. To improve this, crypto hardware acceleration should be used to overcome this limitation. Hardware-assisted security provides a random number generator (RNG), hash, symmetric/asymmetric algorithms, and interfaces to support them. The hardware acceleration can be used to improve the cryptographic operation speed.

8.2 Secure communication

External devices and external interfaces with wireless communication capabilities are required to be ported or updated based on latest version of standards and to be certified by a certificate authority. For example as of September 2020 for a Bluetooth communication featured device, it should be equipped with Bluetooth version 5 and certified by Bluetooth SIG (Special Interest Group).

In the case of wireless communication between the external interface and external devices, confidentiality and integrity are required because wireless communication is highly vulnerable to eavesdropping and malicious modification.

8.3 Secure functions

Security access, secure flash, secure boot and secure debug are four essential functions required for external devices and external interfaces.

8.3.1 Security access

Security access can guarantee the authentication of the external device to access to internal sub-systems of a vehicle. For example, any diagnostic tool should be authenticated based on a certificate issued by vehicle OEM or supplier in order to access the internal ECUs. In this case the encryption algorithms developed by Ron Rivest, Adi Shamir and Leonard Adleman – RSA2048 and SHA-2 can be used for this security feature. Only critical functions which can damage the internal systems and result in threats to vehicle's safety such as re-programming, actuation, etc., should be considered in this security access. Figure 2 shows the security access function for OBD-II.

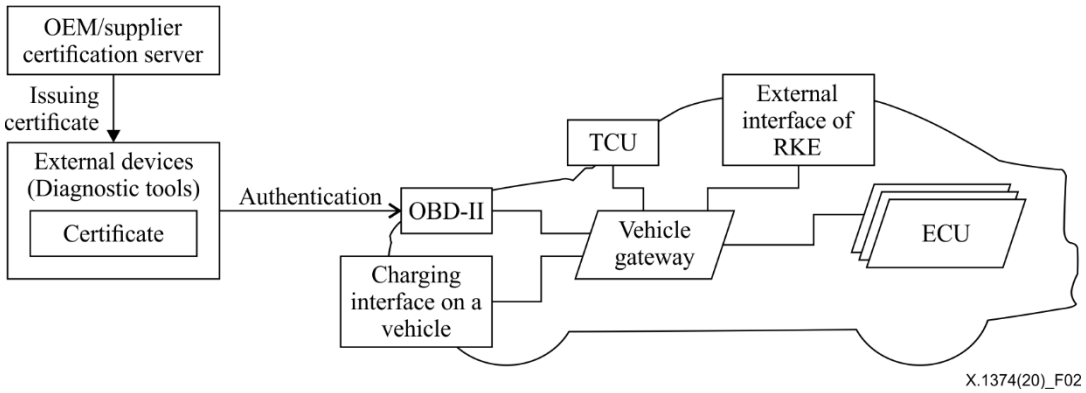

Figure 2 – Security access for OBD-II

8.3.2 Secure flash

Secure flashing can guarantee the integrity of reprogramming software and result in blocking malicious reprogramming. Downloaded software should be verified using a digital signature before flashing hardware in the external device. An asymmetric key algorithm should be used for verification of a digital signature of software. Figure 3 shows the secure flash function.

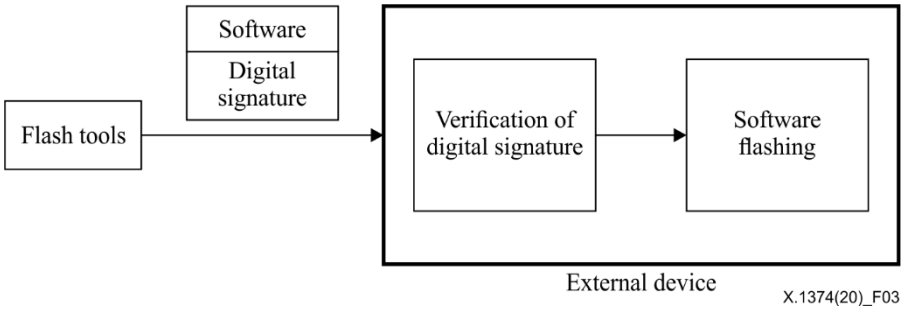

Figure 3 – Secure flash

8.3.3 Secure boot

Secure booting can guarantee the integrity of software in the external devices. While it loads software on memory in the booting sequence, a lower entity should certify the integrity of the upper entity's software sequentially. The root of trust verifies the integrity of basic software (BSW) first, and then the BSW verifies the integrity of application software (ASW) [b-AUTOSAR-055]. Figure 4 shows the secure boot function.

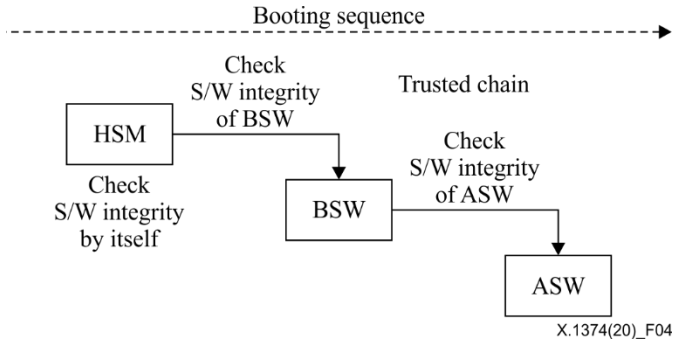

Figure 4 – Secure boot

8.3.4 Secure debug

Secure debug can guarantee control using a debugger such as a universal asynchronous receiver/transmitter (UART)/JTAG (UMTS Joint Test Action Group) to debug dedicated hardware for security. A host of that hardware should provide control of permission for debugging the core part in itself. Figure 5 shows the secure debug function.

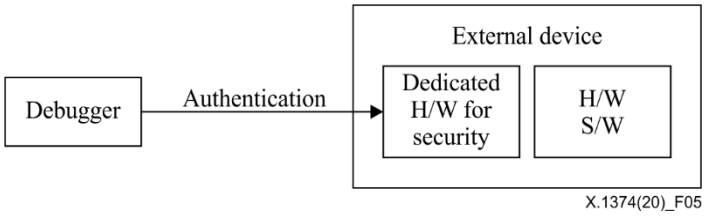

Figure 5 – Secure debug

8.4 Protection against hardware tampering

To carry out reverse engineering, in most cases, opening or modifying a device is needed. To protect from reverse engineering, devices should be designed so that attackers must spend a lot of resources to open or modify devices. Additional protection systems, such as tamper-resistance or tamper-response can be applied.

− Tamper-resistance

An external device should be designed so that it is difficult to open. (e.g., one-way screws, epoxy encapsulation, sealed housings)

− Tamper-response

An external device should actively respond to casing access to prevent internal contents from being read. (e.g., Zeroize critical memory, shutdown/disable/destroy the device, enable logging features)

9 Security requirements for external devices with wireless communication capability

Security patches and secure reprogramming should be implemented.

Security patches for reported vulnerabilities in all software used (including OS) should be installed before testing for mass-production.

For a Linux OS or Android OS based device, it should check new OS updates and security updates regularly to protect against known vulnerabilities.

To protect against malicious software, the requirements listed below for a secure reprogramming function should be implemented:

− All versions of the software should be managed.

− Software version downgrades should not be allowed.

− Software reprogramming should be allowed with authorized persons or tools.

− Integrity of software should be guaranteed.

− The entire process of software reprogramming should be configured as a single transaction.

There are three kinds of wireless communication methods (Bluetooth, cellular and Wi-Fi) for an external device to access a telematics control unit (TCU).

9.1 Bluetooth interface

External devices using a Bluetooth interface should include the requirements presented in clauses 9.1.1 to 9.1.3.

9.1.1 Bluetooth basic rate / enhanced data rate (BR/EDR)

For Bluetooth basic rate / enhanced data rate (BR/EDR), the newest version should be implemented. If not, proper Bluetooth secure connection mode should be considered. For example, in the case of Bluetooth v2.1, devices should operate in a security mode higher than or equal to security mode 3. Security mode 3 is the link level-enforced security mode, in which a Bluetooth device initiates security procedures before the physical link is fully established. Bluetooth devices operating in security mode 3 mandate authentication and encryption for all connections to and from the devices.

When security mode 4 is used, level 3 or higher level of security for Bluetooth services should be used.

9.1.2 Bluetooth low energy (LE)

For Bluetooth LE, secure key exchange, data confidentiality and integrity should be guaranteed. For example, security mode 1 with level 3 should be used.

LE security mode 1 has multiple levels associated with encryption. Level 3 requires authenticated pairing with encryption. Because security mode 1 level 3 requires authenticated pairing and encryption, it is considered the most secure mode and level.

9.1.3 Unused service and profile

Bluetooth is widely used for various services such as audio streaming, video streaming, remote control, and so on. If a device has unused services and profiles, they can cause unexpected results and an attacker can use those vulnerabilities. Therefore, unused services and profiles should be removed or disabled.

9.2 Cellular interface

External devices using a cellular interface should include the requirements presented in clauses 9.2.1 and 9.2.2.

9.2.1 Secure communication

External devices using a cellular interface should guarantee a secure authentication procedure, data confidentiality and integrity.

Requirements shown below concern usages of an LTE cellular and 3G interface as examples.

For a LTE cellular interface, the following security algorithms should be supported:

- 128-evolved packet system encryption algorithm 2 (EEA2) or 128-evolved packet system encryption algorithm3 (EEA3) for data confidentiality
- Evolved packet system integrity algorithm 2 (EIA2) or evolved packet system integrity algorithm 3 (EIA3) for data integrity

For a 3G cellular interface, the following security algorithms should be supported:

Universal mobile telecommunication system (UMTS) encryption algorithm 1 (UEA1) + UMTS integrity algorithm 2 (UIA2) or UMTS encryption algorithm 2 (UEA2) + UMTS integrity algorithm 2 (UIA2) or data confidentiality and integrity.

9.2.2 Application layer security

Additional transport or application layer security should be applied to a cellular interface. All connections between external devices and vehicles should be used for additional security to guarantee authenticity, confidentiality, and integrity of any data transmitted through the cellular interface.

9.3 Wi-Fi interface

External devices using a Wi-Fi interface should include the requirements presented in clauses 9.3.1 to 9.3.3.

9.3.1 Security protocol

An external device using a Wi-Fi interface should use the latest security protocol with a secure password. Some of the security protocols have known security vulnerabilities. Also if there is an unnecessary management protocol in an external device, it may cause other vulnerabilities. However, not all security protocols are secure. Therefore, wireless communication devices should use the latest security protocols instead of legacy protocols that are no longer secure. Examples of insecure protocols and unnecessary management protocols are wired equivalent privacy (WEP), Wi-Fi protected access (WPA), Wi-Fi protected setup (WPS) and temporal key integrity protocol (TKIP).

9.3.2 SSID and password

For the Wi-Fi interface, a unique and non-obvious service set identifier (SSID) should be used. Rainbow tables with hash values for common SSIDs and passwords are readily available on the Internet. Using different SSIDs significantly increases the complexity of attack through the Wi-Fi interface.

Passwords should not include information about the device. Also, there should be guidance indicating that the password needs to be changed periodically.

9.3.3 Connection range management

If Wi-Fi has an unnecessarily wide range, it allows an attacker to remain distant from the target vehicle. For this reason, the effective connection range (distance) of a Wi-Fi interface should be restricted by adjusting the minimum allowable connection speed. Connection speed needs to be set in accordance with the desired connection range

10 Security requirements for external devices of remote key-less entry

Many recently mass-produced vehicles contain RKE systems. These consist of a smart key (key fob) for a driver and designated electronic control unit (ECU) for a vehicle. The smart key can be one of the attack points to the vehicle. Because most of vehicle OEM set low cost to smart keys, limited security technology can be applied.

There are three different features that external devices in the RKE system should include:

- Reverse engineering prevention.
- Secure communication.
- Secure key registration procedure.

10.1 Reverse engineering prevention

Because of the low cost, hardware-assisted security can rarely be applied to the smart key. Instead a kind of mechanism for preventing reverse engineering should be required.

10.1.1 Key extraction prevention

Most RKE systems use mutual authentication using cryptographic keys. Those keys should be encrypted for storing. Also, a debug interface and a diagnosis interface (e.g., UMTS Joint Test Action Group – JTAG) should be removed.

10.1.2 One time programmable

A smart key should be designed as one time programmable in order to prevent modifying of the smart key function. If the smart key can be updated via wired or wireless, it should only be allowed with adequate authorization and integrity checks.

10.2 Secure communication

Most of the RKE systems include simple communication procedures because of the low cost of the system and limitations of reaction time. To ensure secure communication, mutual authentication and replay attack prevention should be applied.

10.2.1 Mutual authentication and channel encryption

When an RKE system is in operation, both a smart key and a designated ECU on the vehicle require verification of the reliability of each other. For this, the smart key and the RKE system should include adequate mutual authentication protocols including challenge-response protocol. It

generally employs a cryptographic nonce as the challenge to ensure that every challenge-response sequence is unique.

10.2.2 Replay attack prevention

Recently, there have been some cases of smart key hacking by replaying a smart key radio signal. To prevent these replay attacks, a cryptographic nonce should be implemented. A cryptographic nonce is an arbitrary number that can be used just once. Generally a nonce also includes a timestamp to ensure it is fresh and has not been reused. To generate the nonce, a true random generator or pseudo-random generator should be required.

10.2.3 Limitation of radio signal intensity

The power level of the radio signal directly relates to connection or system operating range. An attacker can get the radio signal without authorization by radio signal range expansion, known as 'Mafia attack'. An unnecessarily high power level would allow an attacker who is more distant from the target vehicle to view and possibly inject a malicious packet. For this reason, the power level of the radio signals should be limited to use.

10.3 Secure key registration procedure

There are three different features that should be considered for a secure key registration procedure:

- Authentication through a user, vehicle OEM, vehicle, ECU, smart-key.
- Secure communication channel (confidentiality, integrity).
- User (driver, owner) verification.

11 Security requirements for external devices of charging systems in an EV

External devices connected through the charging system including wired and wireless port is required to use transport layer security (TLS) on all communications used in the charging system. This establishes an authenticated and encrypted (ensures integrity protection and confidentiality protection) channel between the EV and the external devices. TLS allows for unilateral or mutual authentication. Also, the communicated message is encrypted using a symmetric-key encryption algorithm allowing the message not to be eavesdropped and both EV and external devices to be certain that the opponent is indeed identical throughout the session of service in order to prevent session hijacking.

Plug and charge (PnC) is a technology that can charge and pay for an electric vehicle without the driver's intervention. The only action required by the driver is to plug the charging cable into the EV. Once the charging cable is plugged in, the EV will automatically identify itself to the charging station and be authorized to receive energy for recharging its battery and payment will be made without additional payment methods such as credit card, and so on.

The payment method for charging the EV should be safe against possible attacks that may occur in public networks such as sniffing, replay attack, etc. Security measures such as encryption, authentication, and digital signature can be used to protect payment methods from attacks.

The payment information which is related to the location of the EV should not be revealed to unauthorized parties in order to protect the driver's location information.

12 Use cases of security measures for external devices and interfaces in a vehicle

12.1 Use case 1: Smart key and external interface

A smart key can open or close the vehicle door through wireless communication with the RKE/PKE system. Smart key and RKE/PKE systems communicate by radio frequency (RF). The attacker

captures the RF signal transmitted from the smart key using a device with full-duplex RF capabilities and retransmits it.

The sequence number, timestamp and nonce can be used to ensure the freshness of communication data between the smart key and the RKE/PKE system. Figure 6 shows replay attack prevention to prevent a replay attack. The first way to prevent a replay attack is to add a nonce to the communication data. Nonce means a random value created by hardware-assisted security (e.g., a HSM). The second way is to add a timestamp to the communication data. The smart key adds a timestamp to the communication data using a predefined time zone and time precision. The RKE/PKE system determines whether the time stamp included in the message is within an acceptable time slot. An important point when using timestamp is time synchronization between the smart key and the RKE/PKE system. Additional mechanisms may be required for time synchronization. The third way is to add a sequence number to the communication data. The smart key and RKE/PKE system increase the sequence number by a predetermined size and add it to the communication data. If the sequence number is smaller than or equal to the previously received data, the RKE/PKE system determines as a replay attack.

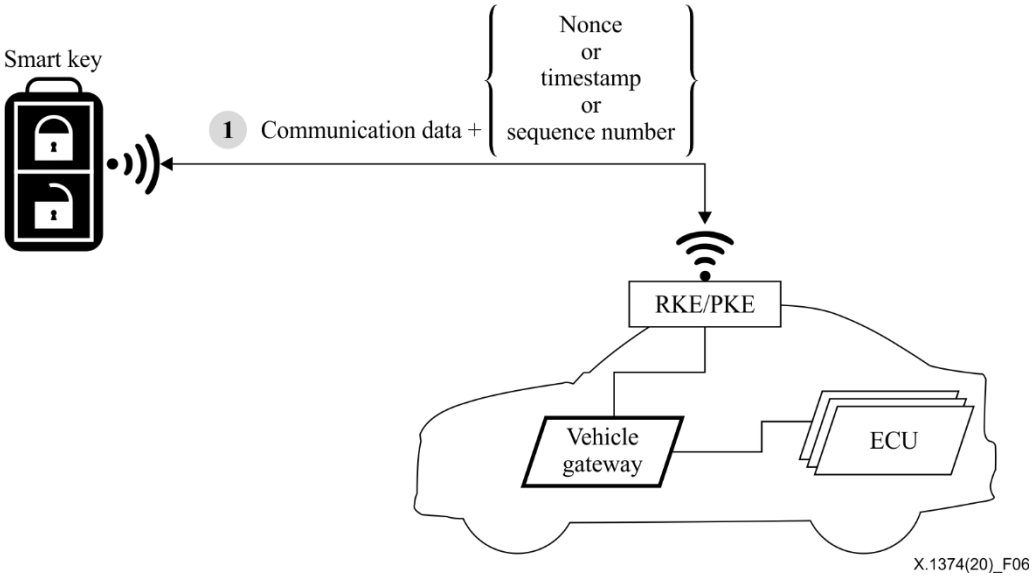

Figure 6 – Replay attack prevention

In order to prevent a replay attack from the perspective of defence in depth, not only the freshness of the communication data but also the confidentiality of the communication data is important.

12.2 Use case 2: Charging device and external interface

The charging device means a charging station that supplies power to an electric vehicle. The EV is connected to an EVSE for charging and the EVSE is connected to both the EV and the external Internet to exchange information. EV and EVSE have controllers for communication which are named EVCC and SECC. The connection between EVCC and SECC may use power line communication (PLC) or wireless communication. TLS should be applied for secure communication between EVCC and SECC. When TLS is applied, a secure channel is established between EVCC and SECC. This channel ensures the confidentiality and integrity of all messages between EVCC and SECC. The first step in creating a secure channel is EVCC and SECC exchanging cipher suites. Cipher suite includes key exchange algorithms, digital signature algorithm, symmetric key encryption algorithm, and message authentication code algorithm. Figure 7 shows the TLS handshaking process between EVCC and SECC.

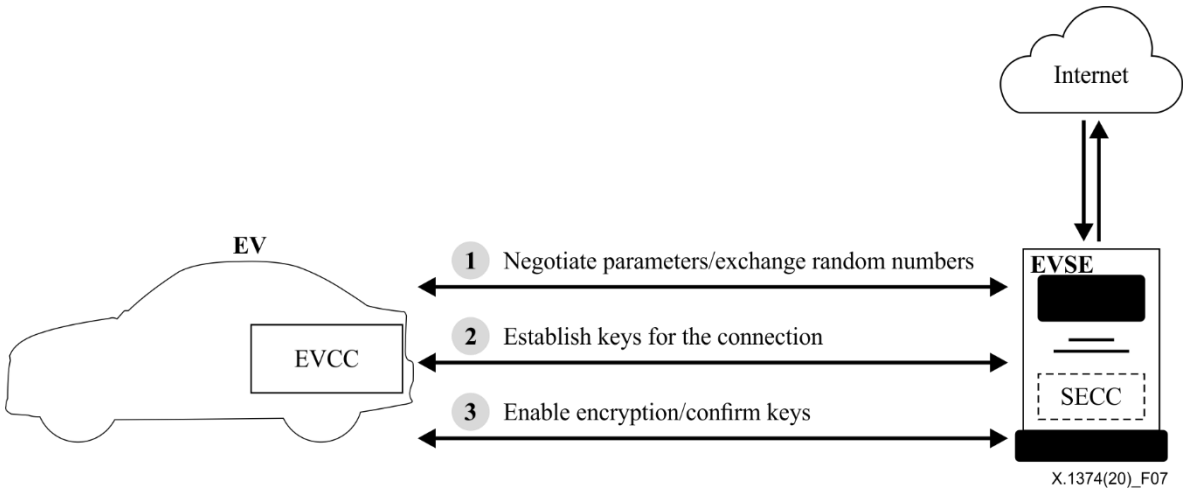

Figure 7 – TLS handshaking process between EVCC and SECC

12.3 Use case 3: Wireless communication device and external interface

The wireless communication device is connected to the vehicle's TCU interface through communication protocols such as Wi-Fi, cellular, and Bluetooth. This connection allows vehicle owners to use text messages, telephones and additional infotainment features in the vehicle. In general, the security protocol supported by the communication protocol can be used to connect the wireless communication device to the TCU. Wireless communication devices should use the latest security protocols instead of legacy protocols that are no longer secure.

Wireless communication devices should periodically check for software updates. Software updates can mitigate security vulnerabilities discovered during the operation.

In the case of Wi-Fi, ensuring the Wi-Fi access password's complexity is as important as using a secure protocol. The password of the Wi-Fi connection must be combined with two or more characters of different types to respond to an attacker's brute force attack. It should not contain consecutive characters, and there should be no dependency on the device. Figure 8 shows Wi-Fi security.

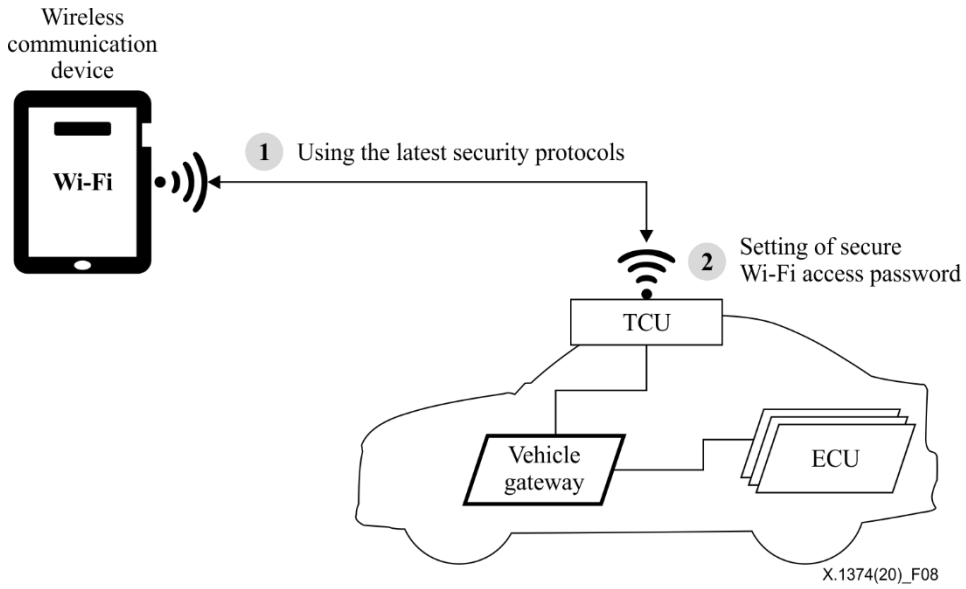

Figure 8 – Wi-Fi security

12.4 Use case 4: External devices connected to OBD-II port and external interface

As modern vehicles have become increasingly electronic, software is becoming a key element of vehicles. Problems occurring in vehicles can be checked through software, even problems caused by the software itself. It is not necessary to physically investigate the vehicle when it comes to knowing the situation inside the vehicle or fixing problems caused by software. The OBD-II port connects a diagnostic device or dongle to diagnose vehicles and modify the software.

A diagnostic device can check the status of the ECU or update it. In it is not mandatory to apply security measures when a diagnostic device communicates with a vehicle. However, most vehicle manufacturers recommend to use it with the security access as shown in Figure 9.

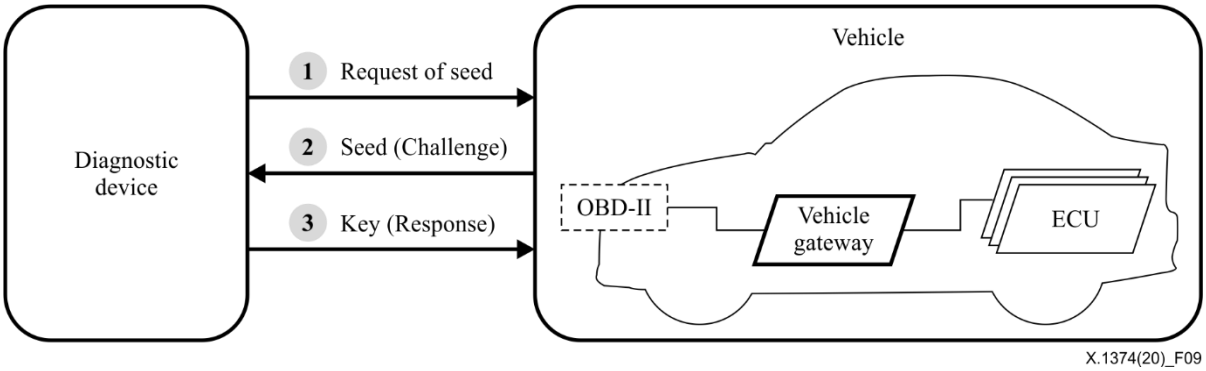

Figure 9 – Security access

The security access performs authentication based on a challenge-response method. When a diagnostic device is plugged into the vehicle, it sends a request seed message, which will be used to generate a response. When the request is received, the vehicle generates a random number as a seed and a challenge, and sends it as a reply to the diagnostic device. If the diagnostic device receives the seed, both of the diagnostic device and the vehicle have the same seed at the same time. The diagnostic device calculates the key as a response using the pre-defined calculation methods which the vehicle also has, and then sends it to the vehicle. The key can be verified by the vehicle with the same seed and key calculation methods [b-ITU-T X.1124].

In the case of firmware updates or other behaviours which can have significant impact, authentication through certificates which are issued by the vehicle manufacturers themselves may also be enforced in addition to security access.

When it comes to dongles, they are mainly used to know the status inside the vehicle. They can be provided by insurance companies or purchased from the automotive aftermarket. Dongles communicate with the dedicated smartphone application to communicate the situation inside the vehicle. However, several studies have reported cases of attacks through the dongle. Therefore, it is necessary to block the control commands received through the dongle from an unauthorized devices.

Appendix I

Information on Bluetooth specification

(This appendix does not form an integral part of this Recommendation.)

Bluetooth is a short-range wireless communication industry standard for digital communication devices. The standard is being developed by the Bluetooth SIG (Bluetooth Special Interest Group). Bluetooth is divided into Classic (BR/EDR) and Bluetooth with low energy (LE), and has different security functions. Bluetooth 4.0 BR/EDR uses E0 algorithm for data encryption, and Bluetooth 4.0 LE uses AES-CCM. The E0 algorithm is a stream cipher used in the Bluetooth protocol. It generates a series of pseudo-random numbers and uses the XOR operator to generate the ciphertext. Bluetooth 4.0 BR/EDR is no longer secure due to algorithmic issues. Therefore Bluetooth 4.1 BR/EDR uses AES-CCM for data encryption. Table I.1 shows the differences in security protocols by the Bluetooth version. See the Bluetooth technical documentation for details.

Table I.1 – Comparison of Bluetooth security protocols

	Basic rate/Enhanced data rate (BR/EDR)	**Bluetooth with low energy (LE)**
4.0 (2009)	**Secure simple pairing (SSP)** Pairing: HMAC-SHA-256, P-192 ECDH, four association models (JW/NC/PK/OOB) Authentication: E1 Encryption: E0 Message integrity: none (just CRC)	**LE legacy pairing** Pairing: Broken homebrew key exchange, AES, three association models (JW/PK/OOB) Encryption: AES-CCM Message integrity: AES-CCM
4.1 (2013)	**Secure connections** Pairing: HMAC-SHA-256, P-256 ECDH Authentication: HMAC-SHA256 Encryption: AES-CCM Message Integrity: AES-CCM	**LE privacy 1.1 (reconnection address obsolete)**
4.2 (2015)	no change	**LE secure connections** Pairing: P-256 ECDH, AES-CMAC, four association models (JW/NC/PK/OOB) Authentication: AES-CCM Encryption: AES-CCM Message integrity: AES-CCM LE privacy 1.2 (RPA resolution now already in controller)
5 (2016)	no change	LE channel selection algorithm #2
5.1 (2019)	no change	Indoor location stuff

Appendix II

Information on cellular communication specification

(This appendix does not form an integral part of this Recommendation.)

This appendix provides an overview of the security features used in 3rd generation mobile cellular communication and 4th generation mobile cellular communication. Universal mobile telecommunications system (UMTS), a 3rd generation mobile cellular communication system, is a system for GSM standards-based networks and was developed by the 3rd Generation Partnership Project (3GPP). Long-term evolution (LTE), a fourth-generation mobile cellular communication system based on GSM/EDGE and UMTS/HSPA technology, was developed by 3GPP.

Table II.1 shows the security function groups of UMTS and LTE. See the UMTS or LTE technical documentation for details.

Table II.1 – Five security function groups of UMTS and LTE

Function groups	Short description
Network access security	ensures that mobile users have secure access to network services and mobile network is secured against attacks via the (radio) access link.
Network domain security	ensures that mobile backhaul nodes to securely exchange signalling data and user data at the mobile backhaul networks and protects against attacks on wireline link.
User domain security	secures access to mobile stations.
Application domain security	allows applications on user and network side to securely exchange data.
Visibility and configurability of security	allows user to get information about enabled security features and provision of services. Present-day LTE network operators use a wide range of security mechanisms in each domain.

Bibliography

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.1124] Recommendation ITU-T X.1124 (2007), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.

[b-ISO/IEC 18014-2] ISO/IEC 18014-2:2009, *Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens*.

[b-ISO 15118-1] ISO 15118-1:2019, *Road vehicles – Vehicle to grid communication interface – Part 1: General information and use-case definition*.

[b-ISO/IEC 27000] ISO/IEC 27000:2016, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-AUTOSAR-055] AUTOSAR *Glossary FO Release 1.1.0* (2017).

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2021