

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1373

(03/2017)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

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

Secure software update capability for intelligent transportation system communication devices

Recommendation ITU-T X.1373

ITU-T

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	
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	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	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
PKI related Recommendations	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1379
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

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

Recommendation ITU-T X.1373

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 those electric devices need to be appropriately updated for the purpose of bug fixing, and for performance and security improvements to avoid accidents.

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

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1373	2017-03-30	17	11.1002/1000/13197

Keywords

Communication devices, denial of service attack, DoS, embedded system, hardware security module, HSM, intelligent transportation system, ITS, malware, privacy, risk analysis, vehicle-to-vehicle, V2V, vehicle-to-infrastructure, V2I, vehicle-to-X (vehicle/infrastructure) (V2X), wireless communications.

* 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 2017

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
4	Abbreviations and acronyms	2
5	Conventions	3
6	Basic model of remote software update.....	3
	6.1 Modules of ITS environment for software update	3
	6.2 Model of software update procedure	4
7	Specification of secure software update procedure	6
	7.1 General message format with security functions.....	6
	7.2 Protocol definition and data format	7
	Appendix I – Methodology on risk analysis	22
	I.1 Methodology on risk analysis based on [b-JASO TP15002]	22
	I.2 Data verification using MAC algorithms	29
	Appendix II – Threats, security requirements and security controls	30
	II.1 Definition of target of evaluation	30
	II.2 Identification of major threats	32
	II.3 Security Requirements in TOE.....	35
	II.4 Security controls	38
	Bibliography.....	40

Recommendation ITU-T X.1373

Secure software update capability for intelligent transportation system communication devices

1 Scope

In the context of updates of software modules in the electric devices of vehicles in the intelligent transportation system (ITS) communication environment, this Recommendation aims to provide a procedure of secure software updating for ITS communication devices for the application layer in order to prevent threats such as tampering of and malicious intrusion to communication devices in vehicles. This includes a basic model of software update, security controls for software update and a specification of abstract data format of update software module.

The procedure related to in-vehicle communication is the out of scope of this Recommendation. For reference, the procedure used in-vehicle in this Recommendation is informative.

The procedure is intended to be applied to communication devices on ITS vehicles under vehicle-to-infrastructure (V2I) communication by means of the Internet and/or ITS dedicated networks. The procedure provides a technical guideline without compliance requirements and can be practically utilized by car manufactures and ITS-related industries as a set of secure procedures and security controls.

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.509] | Recommendation ITU-T X.509 (2012) ISO/IEC 9594-8:2014, <i>Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.</i> |
| [ITU-T X.1521] | Recommendation ITU-T X.1521 (2011), <i>Common vulnerability scoring system.</i> |
| [ISO/IEC 15408-1] | ISO/IEC 15408:2009, <i>Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.</i> |
| [ISO/IEC 27000] | ISO/IEC 27000:2014, <i>Information technology – Security techniques – Information security management systems – Overview and vocabulary.</i> |

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 threat [ISO/IEC 27000]: Potential cause of an unwanted incident, which may result in harm to a system or organization.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 risk score: A score that a risk analysis method calculates for each threat.

3.2.2 vehicle mobile gateway (VMG): A module which provides communication between electronic control units (ECUs) in the controller area network (CAN) (in-vehicle buses) and exterior intelligent transportation system (ITS) entities in the external network.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CA	Certification Authority
CAN	Controller Area Network
CD	Compact Disc
CRSS	CVSS based Risk Scoring System
CVSS	Common Vulnerability Scoring System
DoS	Denial of Service
DVD	Digital Versatile Disc
ECU	Electronic Control Unit
ETC	Electronic Toll Collection
FT	Fault Tree
GPS	Global Positioning System
GUID	Global User ID
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ID	Identifier
IT	Information Technology
ITS	Intelligent Transportation System
LIN	Local Interconnect Network
MAC	Message Authentication Code
MOST	Media Oriented Systems Transport
OBD	On-board diagnostics
OEM	Original Equipment Manufacturer
PC	Personal Computer
RPM	Revolutions per Minute
RSS	Risk Scoring System
SD	Secure Digital
SHA	Secure Hash Algorithm
SSL	Secure Socket Layer

TLS	Transport Layer Security
TOE	Target of Evaluation
TPM	Trusted Platform Module
TV	Television
UI	User Interface
URL	Uniform Resource Locator
USB	Universal Serial Bus
Usvr	Update server
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-X (vehicle/infrastructure)
VMG	Vehicle Mobile Gateway
Wi-Fi	Wireless-Fidelity
XML	Extended Mark-up Language

5 Conventions

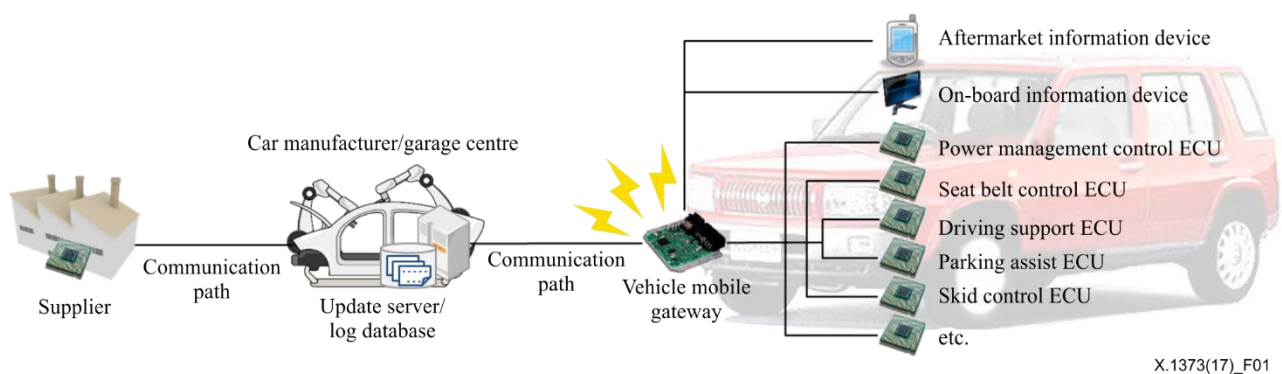
None.

6 Basic model of remote software update

For considerations of a practical security architecture, this clause introduces a basic model of conventional architecture of software update, where a definition of principal modules and typical software update processes are provided.

6.1 Modules of ITS environment for software update

Figure 1 provides a view of principal modules around a vehicle for a remote software update in the ITS communication environment. The principal modules are information devices, electronic control units (ECUs), and vehicle mobile gateway (VMG) on a vehicle, update server (Usvr) and log database of car manufacturer and supplier. The procedure related to in-vehicle communication (e.g., between ECUs and vehicle mobile gateway) is out of the scope of this Recommendation. Modules used for in-vehicle communication (such as "User Interface" and "ECUs") are described below in an informative manner.



X.1373(17)_F01

Figure 1 – Principal modules around a vehicle

6.1.1 User interface (informative)

The user interface (UI) is generally an on-board or an aftermarket information device with display and input devices on a vehicle. Such an information device is directly connected to other devices on a vehicle (e.g., VMG or ECU (see clause 6.1.2)) so that it can obtain and indicate various status information of the vehicle such as speed, revolutions per minute (RPM), fuel level, and so on. Particularly, in this Recommendation, a user interface is used to notify car drivers of the necessity for updates.

6.1.2 Electronic control unit (ECU) (informative)

ECU is a generic term for computers which control various kinds of devices in a vehicle. In the earliest years of ECU, its main functions were controls of ignition timing, injection, idling adjustment and limiter of engine in order to improve fuel efficiency and reduce gas emissions. According to the computerization of the vehicle, ECU has expanded its applications to various kinds of functions such as power management, seat belt control, driving support, parking assist, skid control, automatic transmission, etc. In recent years, the number of ECUs within a vehicle increased from 50 to 100, and the importance of ECUs for safety control and communication is especially growing. However, since the development of ECU involves sophisticated software implementations, the recent increase of ECUs in vehicles imposes a heavy burden on car manufacturers.

6.1.3 Vehicle mobile gateway

A vehicle mobile gateway is a module assigned for facing to "Update Server" (in clause 6.1.4) in order for the vehicle to conduct software update. Software update process located in vehicle is out of the scope in this Recommendation. VMG can be a conceptual entity which is practically implemented with a set of multiple components. For example, the connection management entity (a.k.a. "central gateway", "Head unit", "communication head unit" or "Vehicle Gateway (VG)") can be used for the role of VMG in this context, and any devices can also be used for the software update. A cellular network (mobile network) and a fixed network via wireless are applied as a communication path between vehicle mobile gateway and exterior ITS entities.

6.1.4 Update server and log database

An update server is located at car manufacturers or garage centres to gather status information of software modules from vehicles and to distribute software update modules to the vehicles. Likewise, in most recent networked computers such as personal computers (PCs) and smart phones, one of the important functions of the update server is to entirely manage and control software on vehicles. In order to automatically manage such software status of each vehicle, the update server should work with a log database which stores such software status information of the vehicle as evidence. Note that an update server can be deployed not only at a car manufacturer but also at a supplier or third party.

6.1.5 Supplier

A vehicle is an assembly of thousands of automotive parts that are provided by automotive suppliers. On-board communication devices and ECUs are provided by those suppliers and assembled by car manufacturers while considering dependencies among the various devices. Therefore, and in general, update modules for on-board communication devices are not produced beforehand by a car manufacturer but by a corresponding supplier. The provided update modules are distributed from a car manufacturer to vehicles after careful testing and evaluation at the car manufacturer.

6.2 Model of software update procedure

6.2.1 General update procedure

Figure 2 shows a typical model of software update procedure which is initiated by the vehicle mobile gateway by checking the existence of updates. Since in-vehicle communication is out of the scope of

this Recommendation, the steps related to in-vehicle communications in Figure 2 are just informative examples to be referred for practical implementation of secure update procedure.

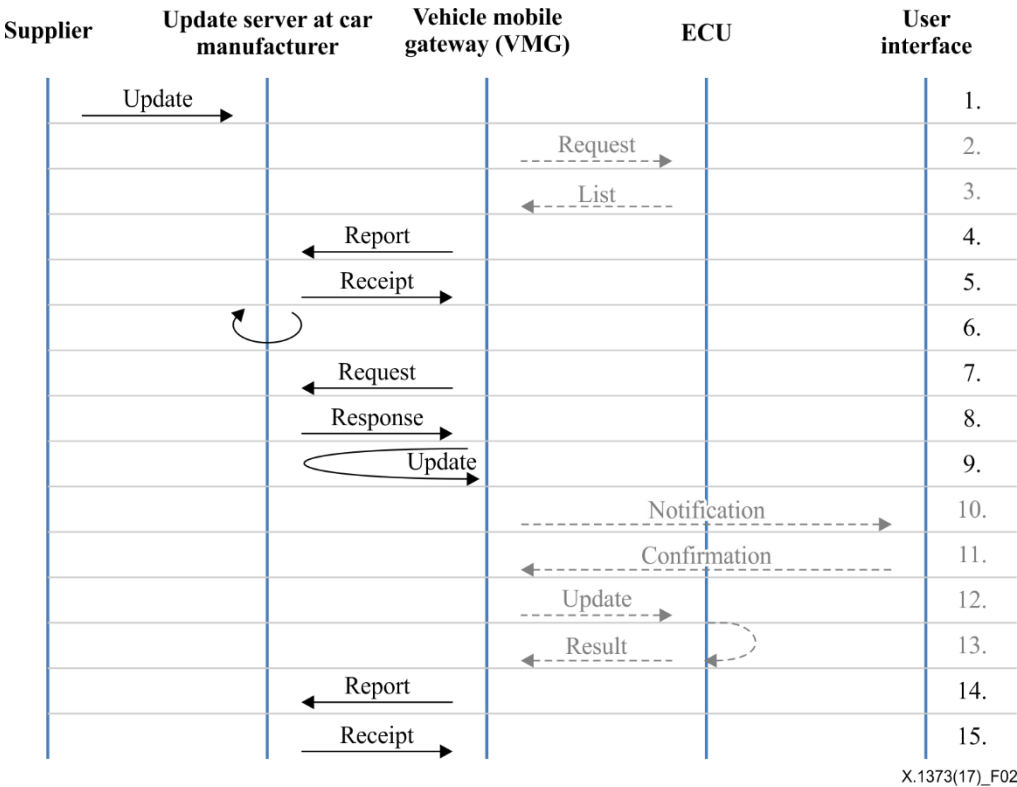


Figure 2 – Model of software update process

Steps for the update procedure are described as follows, where steps 2, 3 and 10 to13 (shown in italics) are informative in nature:

- 1) At the first step of the process, an update module is provided by an automotive component supplier, which occurs asynchronously with the following steps.
- 2) *As the initiation of the update procedure starts, a vehicle mobile gateway requests ECUs to submit their software list.*
- 3) *An ECU checks its software status, generates a list of software modules and reports it to VMG.*
- 4) VMG submits the collected list to the update server to check whether any update for the vehicle exists.
- 5) The update server sends back a receipt of the submitted list to VMG.
- 6) According to the list, the update server inspects the status of the installed software of the vehicle and determines the necessary software updates for the ECUs.
- 7) Since this inspection may take a long time, VMG periodically checks the necessity of the updates for the vehicle.
- 8) If there is any update, the update server sends an access uniform resource locators (URLs) for the updates; otherwise, it sends back only an acknowledgement message.
- 9) If there is any update for the vehicle, VMG connects to the update server to download the update modules for the vehicle.
- 10) *Before applying the updates to ECUs, VMG notifies the driver to confirm the application of the updates.*
- 11) *The driver confirms and accepts to apply the updates.*

- 12) *VMG delivers the update files to the corresponding ECUs and requests them to apply the updates (see clause 6.2.3).*
- 13) *Each ECU applies the update and reports the application result to the vehicle mobile gateway.*
- 14) *The vehicle mobile gateway submits a report of application results to the update server.*
- 15) *Finally, the update server sends back a receipt of the update information. If the application of the update has failed or some remaining update is found, the update server retries the procedure from steps 6 to 14 until the application has succeeded (see clause 6.2.2).*

6.2.2 Consideration for unbounded retries

According to the retry-until-succeed description mentioned in step 15, note that in some cases the procedure will never succeed, and eventually the description can cause the VMG to retry an unbounded number of times. To avoid this, the number of retries should be bounded by a number 'N' which can be determined based on the policy for the update procedure. How to define the policy for the update is out of the scope in this Recommendation.

6.2.3 Consideration for resource constraints

As for the practical application of the update software in a vehicle (in informative step 12 in clause 6.2.1), there are modules in the vehicle that do not mount enough memory resource for caching a whole update module at one time. For those modules, the stream updating technology is required by means of streaming fragmented data.

In general, for any modules in a vehicle, whatever the update system, the constraints of finite resources of devices such as memory, storage and network throughput should be carefully taken into account.

7 Specification of secure software update procedure

This clause specifies a practical procedure and its application message formats between update server and vehicle (VMG) for software update with security functions. Note that this Recommendation does not specify functions of message confidentiality. The confidentiality can be provided by lower layer protocols (e.g., hypertext transfer protocol secure (HTTPS) and secure tunnelling protocol, etc.).

The procedure needs to take into account the diversity of security capabilities among vehicles. Therefore, in this Recommendation, vehicles with asymmetric crypto algorithm apply the digital signature method (clause 7.1.1), while vehicles without asymmetric crypto algorithm apply the message authentication code (MAC) method (clause 7.1.2) for secure message exchange.

7.1 General message format with security functions

This clause introduces a general message format with security functions including authentication method of message sender and verification of the integrity of a message. In terms of integrity and authenticity technique, the digital signature method with the public key algorithm and/or message authentication code with shared key algorithm can be applied. In the secure software update procedure, every message should be constructed in one of the security methods as follows.

7.1.1 Digital signature method

As one implementation method, the digital signature based on [ITU-T X.509] can be applied for authentication of entities and verification of message integrity among vehicles with asymmetric crypto capability by hardware security module (HSM) (e.g., TPM).

7.1.2 MAC method

Since the shared key algorithm requires less processing load than the public key algorithm, the shared key algorithm is suitable for devices with a low processing capacity. However, in the shared key algorithm, the sender and receiver use the same key, thus a large number of devices use the same key. This operation requires the update of keys in all devices in the system once the shared key is leaked. Besides, since the shared key itself does not provide authenticity of the sender, each message needs to contain a device ID of the sender, which presupposes that the ID in the device is not improperly manipulated.

7.2 Protocol definition and data format

The application data format is dedicated to deliver messages only regarding software update, which is enclosed in the general message format described in the previous clause. This clause firstly defines message types applied in the software update procedure, and secondly it introduces specifications of the message types. The examples of messages are provided with an extended mark-up language (XML) format for information.

7.2.1 Protocol overview

Based on the model of software update procedure described in clause 6, the messages are categorized into several types according to their objectives, as depicted in Figure 3. Procedures of in-vehicle communication are out of the scope in this Recommendation and are described with grey fonts in Figure 3.

NOTE – Procedure of in-vehicle communication can be found in [b-ISO 14229] and [b-ISO 13440].

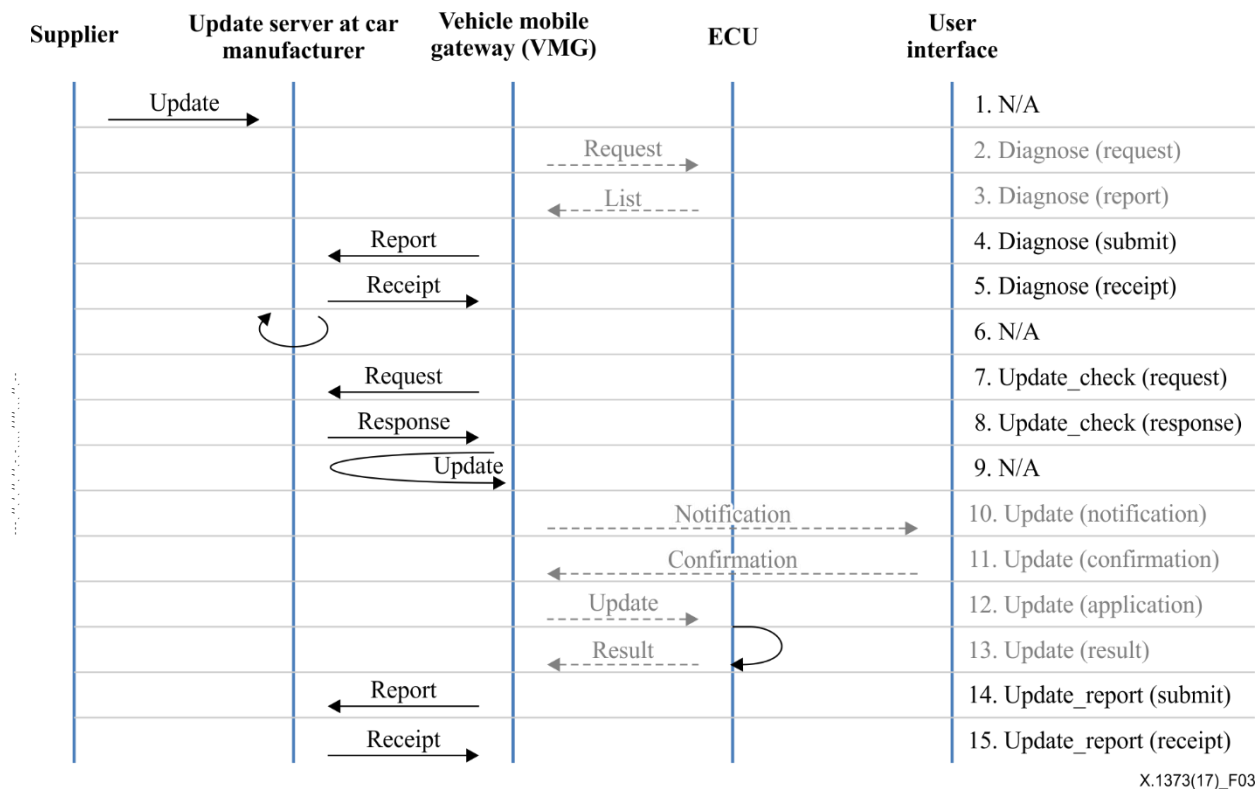


Figure 3 – Definition of message types

In steps 2, 3, 4 and 5, since the purpose of the messages are request and report of diagnoses of the software status of each ECU, the messages are categorized as "diagnose". In the same manner, the messages in steps 7 and 8 are categorized as "update_check". Steps 10, 11, 12 and 13 are "update", which are messages to confirm and apply the updates. Finally, the results of the updates are submitted

by "update_report" messages in steps 14 and 15. The types, subtypes and codes of the messages are shown in Table 1.

Table 1 – Message types

Type	Subtype	From	To	Purpose
diagnose	<i>request</i>	VMG	ECU	<i>Request of diagnose of software status</i>
	<i>report</i>	ECU	VMG	<i>Result of diagnose including software status</i>
	submit	VMG	Usvr	Report of results of ECUs in a vehicle
	receipt	Usvr	VMG	Receipt for submit of diagnose report
update_check	request	VMG	Usvr	Request of update module
	response	Usvr	VMG	Update module provided
update	<i>notification</i>	VMG	UI	<i>Notification message to introduce update for the driver</i>
	<i>confirmation</i>	UI	VMG	<i>Confirmation message from the driver to apply update</i>
	<i>application</i>	VMG	ECU	<i>Request message including update module</i>
	<i>result</i>	ECU	VMG	<i>Result of application of the update module</i>
update_report	submit	VMG	Usvr	Report of application of the update
	receipt	Usvr	VMG	Receipt of the report
* Usvr: Update server * UI: User interface				

NOTE – In Table 1 grey font italics is used to indicate elements that are outside the scope of this Recommendation, and are provided just for information.

7.2.2 Diagnose messages

With the purpose of determining the necessary update modules for a vehicle, diagnose messages are used between an update server and VMG to upload software information from vehicles to the update server.

7.2.2.1 Diagnose (submit) message

After collecting the diagnose results from the vehicle, VMG submits a list of software information to the update server in the manufacture (or garage). The diagnose (submit) message includes the identity of the vehicle (vid) and a list of software information that is extracted from diagnose (report) messages.

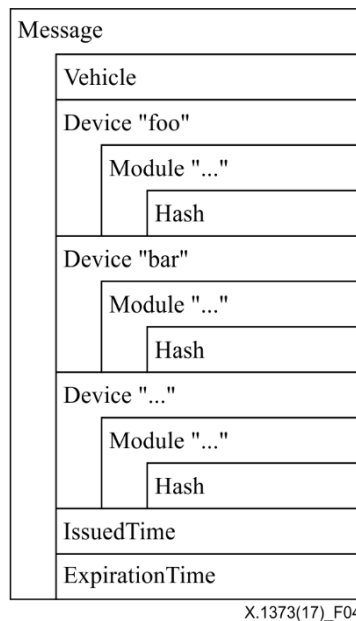


Figure 4 – Structure of diagnose (submit) message

Table 2 – Elements of diagnose (submit) message

Element	Attribute in element	Description
Message	–	Container of the message.
	protocol	Always '1.0'.
	version	The version number of the message sender.
	type	Message type (always "diagnose").
	subtype	Message subtype (always "submit").
	sessionid	Session identifier (ID) is a random global user ID (GUID) associated with the diagnose session. An identical session ID is applied to a set of diagnose request, report, submit and receipt messages.
	trustlevel	Trust level is determined based on the security capability and safety requirement of the device that generated this message.
	ownerid	Owner ID provided by a car manufacturer/supplier.
	messageid	Message ID is a random GUID associated with an individual message.
Vehicle	–	Container of vehicle information. It contains multiple module elements.
	name	Name of the vehicle, if any.
	model	Model name of the vehicle provided by the car manufacturer.
	modelid	Model name of the vehicle.
	vehicleid	Vehicle ID defined by a car manufacturer/supplier.
	locale	Locale information of the vehicle.
Device	–	Container of device information. It contains multiple module elements.
	name	Name of the device, if any.
	type	Type name of the device, such as "Power management ECU", "Seat belt control ECU", etc.
	model	Model name of the device.