ITU

ITU-T SG17 work on ITS security – X.1373 and X.itssec-2

Sang-Woo LEE, ETRI

Contents

- Introduction of Q13 in SG17

- Overview of Q13 work items
  - X.1373
  - X.itssec-2

- Future plan

SG17 Structure

- **Q1/17 Telecommunication/ICT security coordination**

- **Working Party 1 “Telecommunication/ICT Security”**
  - Q2/17 Security architecture and framework
  - Q3/17 Telecommunication information security management
  - Q6/17 Security aspects of telecommunication services and networks
  - **Q13/17 Security aspects for Intelligent Transport System**

- **Working Party 2 “Cyberspace security”**
  - Q4/17 Cybersecurity
  - Q5/17 Countering spam by technical means

- **Working Party 3 “Application security”**
  - Q7/17 Secure application services
  - Q8/17 Cloud computing security
  - Q12/17 Formal languages for telecommunication software and testing

- **Working Party 4 “Identity management and authentication”**
  - Q9/17 Telebiometrics
  - Q10/17 Identity management architecture and mechanisms
  - Q11/17 Generic technologies to support secure applications

Q13 in ITU-T SG17

- **Question**

  Study items to be considered include, but are not limited to:

  - How should security aspects (e.g., security architecture and subsystems) be identified and defined in an ITS environment?
  - How should threats and vulnerabilities in ITS services and networks be identified and handled?
  - What are the security requirements (e.g., those for identification and authentication) for mitigating the threats in an ITS environment?
  - What are security technologies to support ITS services and networks?
  - How should secure interconnectivity between entities in an ITS environment be kept and maintained?
  - What security techniques, mechanisms and protocols are needed for ITS services and networks?
  - What are globally agreeable security solutions for ITS services and networks, which are based on telecommunication/ICT networks?
  - What are best practices or guidelines for ITS security?
  - What PII (Personally Identifiable Information) protection and management mechanisms are needed for ITS services?

Q13 in ITU-T SG17

- **Tasks**

  Tasks include, but are not limited to:

  - Produce a set of Recommendations providing comprehensive security solutions for ITS.
  - Study further to define security aspects of ITS services and networks, which are based on telecommunication/ICT networks.
  - Study and identify security issues and threats in ITS.
  - Study and identify requirements and use cases for specific ITS services and applications.
  - Study and develop security mechanisms, protocols and technologies for ITS.
  - Study and develop security profiling, hierarchical scheme for authentication and mechanism for specific ITS services and applications.
  - Study and develop applications of efficient encryption and decryption algorithms for fast moving network nodes and dynamically changing network topologies.
  - Study and develop secure interconnectivity mechanisms for ITS in a telecommunication environment.
  - Study and identify PII protection issues and threats in ITS.
  - Study and develop PII protection and management mechanisms for ITS.
  - Study and develop an existing draft Recommendation X.itssec-2.
  - Collaborate with the related SDOs to jointly develop Recommendations.

Q13 in ITU-T SG17

- **Study Groups:**
  - ITU-T SGs 11, 13, 16 and 20;
  - ITU-R WP5A;
  - Collaboration on ITS Communication Standards (CITS).
- **Standardization bodies:**
  - ISO TCs 22 and 204;
  - ISO/IEC JTC 1/SCs 6, and 27;
  - IETF WG ITS;
  - IEEE 802.11 WG and 1609 WG;
  - SAE International (e.g., Vehicle Cybersecurity Systems Engineering Committee, Connected Vehicles Steering Committee, and DSRC Technical Standard Committee);
  - ETSI TC ITS;
  - W3C Automotive WG.
- **Other bodies:**
  - GSMA;
  - ATIS; CCSA; TIA; TTA; TTC;
  - UNECE (UN Economic Commission for Europe) Working Party 29 and subsidiary bodies (e.g., Taskforce on cyber security (TFCS));
  - AGL (Automotive Grade Linux).

ITS related work items in ITU (30 Nov 2016) (Ref.CITS)

Sector	Work item	Provisional name	Type of work item	Subject/title	Status	Timing	Study Group
ITU-T	HSTP-CITS-Reqs		Technical papers and tutorials	Global ITS communication requirements (Version 1)	Agreed	2014-07-11	Q27/16
ITU-T	Y.2281		Recommendation	Framework of networked vehicle services and applications using NGN	Approved	2011-01-28	Q12/13
ITU-T	P.1100		Recommendation	Narrowband hands-free communication in motor vehicles	Approved	2015-01-13	Q4/12
ITU-T	P.1110		Recommendation	Wideband hands-free communication in motor vehicles	Approved	2015-01-13	Q4/12
ITU-T	P.1140	P.emergency	Recommendation	Speech communication requirements for emergency calls originating from vehicles	Approved	2015-06-29	Q4/12
ITU-T	P.1130	P.VSSR	Recommendation	Subsystem requirements for automotive speech services	Approved	2015-06-29	Q4/12
ITU-T	F.749.1	H.VG-FAM	Recommendation	Functional requirements for vehicle gateways	Approved	2015-11-29	Q27/16
ITU-R	M.1453		Recommendation	Intelligent transport systems - Dedicated short range communications at 5.8 GHz	Approved	Jun-05	SG5
ITU-R	M.1890		Recommendation	Intelligent transport systems - Guidelines and objectives	Approved	Apr-11	SG5
ITU-R	M.1452		Recommendation	Millimetre wave vehicular collision avoidance radars and radiocommunication systems for intelligent transport system applications	Approved	May-12	SG5
ITU-R	M.2057		Recommendation	Systems characteristics of automotive radars operating in the frequency band 76-81 GHz for intelligent transport systems applications	Approved	Feb-14	SG5
ITU-R	M.2322		Report	Systems characteristics and compatibility of automotive radars operating in the frequency band 77.5-78 GHz for sharing studies	Approved	Nov-14	SG5
ITU-R	M.2228		Report	Advanced intelligent transport systems (ITS) radiocommunications	Approved	Jul-15	SG5
ITU-R	M.2084		Recommendation	Radio interface standards of vehicle-to-vehicle and vehicle-to-infrastructure communications for Intelligent Transport System applications	Approved	Sep-15	SG5
ITU-R	R-HDB-49		Handbook	Land Mobile (including Wireless Access) - Volume 4: Intelligent Transport Systems	Published	2006	SG5
ITU-T	X.1373	X.itssec-1	Recommendation	Secure software update capability for Intelligent Transportation System communications devices	Approved	2016	Q6/17

ITS related work items in ITU (30 Nov 2016) (Ref.CITS)

Sector	Work item	Provisional name	Type of work item	Subject/title	Status	Timing	Study Group
ITU-T		F.VGP-REQ	Recommendation	Service and functional requirements of vehicle gateway platforms	Under study	2017	Q27/16
ITU-T		P.carSFS	Recommendation	Super-WideBand (SWB) and FullBand (FB) stereo hands-free communication in motor vehicles	Under study	2017	Q4/12
ITU-T		P.UIA	Recommendation	User interface requirements for automotive applications	Under study	2018	Q4/12
ITU-T		F.AUTO-TAX	Recommendation	Taxonomy for ICT-enabled motor vehicle automated driving systems	Under study	2018	Q27/16
ITU-T		G.V2A	Recommendation	Communications interface between external applications and a Vehicle Gateway Platform	Under study	2017	Q27/16
ITU-T		H.VGP-ARCH	Recommendation	Architecture of vehicle gateway platforms	Under study	2017	Q27/16
ITU-T	X.1373	X.itssec-1	Recommendation	Secure software update capability for Intelligent Transportation System communications devices	Determined	2016	Q6/17
ITU-T		X.itssec-2	Recommendation	Security guidelines for V2X communication systems	Under study	2017	Q6/17
ITU-T		Y.IoT-ITS-framework	Recommendation	Framework of Cooperative Intelligent Transport Systems based on the Internet of Things	Under study	2017	Q2/20
ITU-T		Y.TPS-req	Recommendation	Requirements of transportation safety service including use cases and service scenarios	Under study	2017	Q2/20
ITU-T		Y.TPS-afw	Recommendation	Architectural framework for providing transportation safety service	Under study	2017	Q4/20
ITU-R		M.[ITS-USAGE]	Report	Intelligent transport systems (ITS) usage in ITU Member States	Under study		SG5

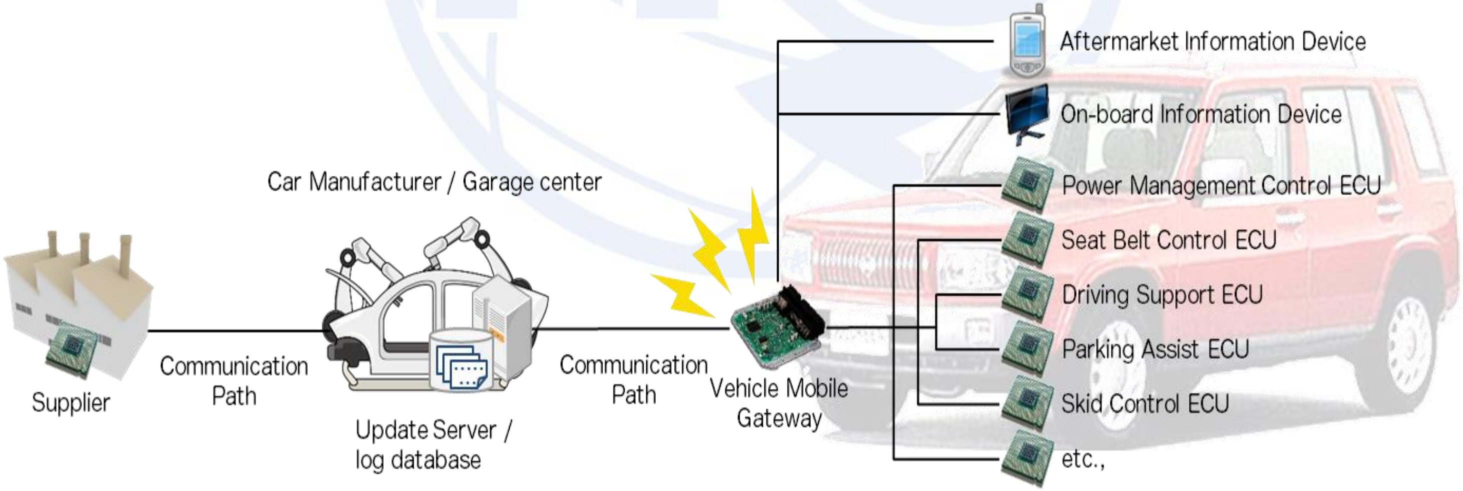
ITS security in ITU-T SG17

- X.1373: **Secure software update** for Intelligent Transportation System communication devices
  - Finalized at SG17 March 2017 meeting

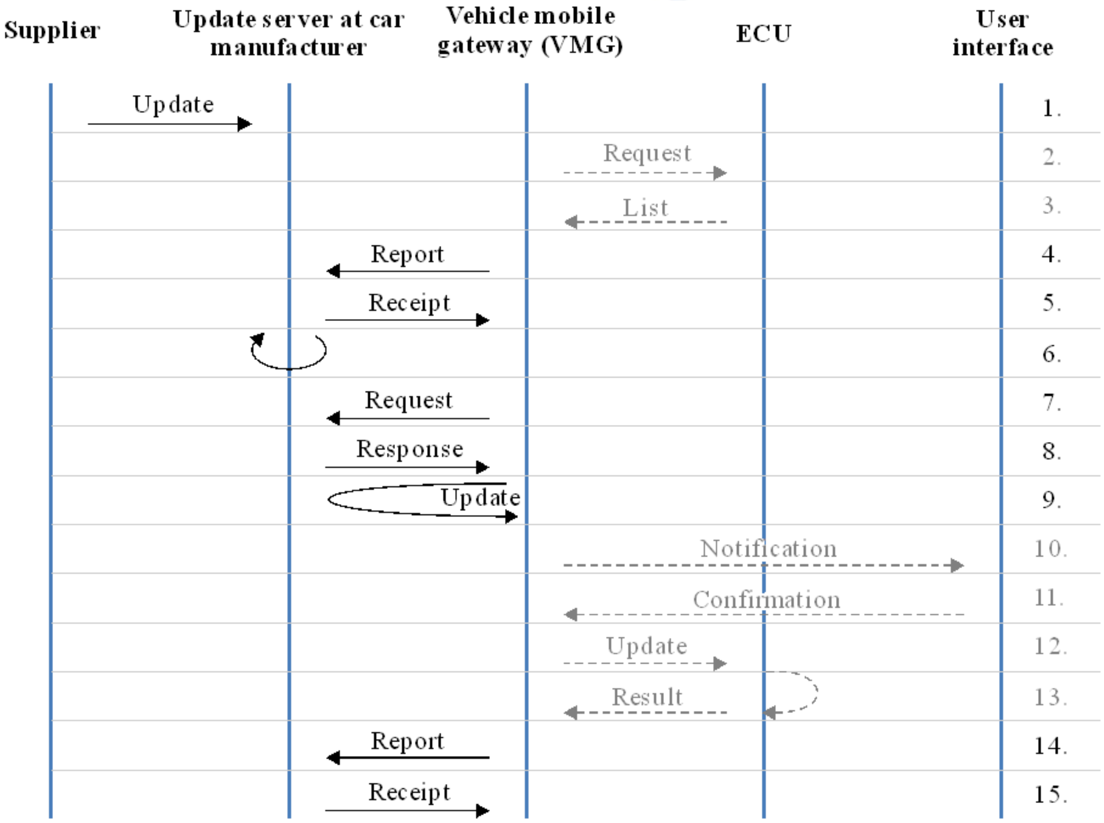
- X.itssec-2 : **Security guidelines for V2X** communication systems
  - ongoing standardization

X.1373(1)

- Scope
  - 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 on vehicles.
- Contents
  - Basic model of software update
  - Threat, risk analysis and security requirement for software update
  - A specification of abstract data format of update software module


Aftermarket Information Device
On-board Information Device
Power Management Control ECU
Seat Belt Control ECU
Driving Support ECU
Parking Assist ECU
Skid Control ECU
etc.,
Car Manufacturer / Garage center
Supplier
Communication Path
Update Server / log database
Communication Path
Vehicle Mobile Gateway

X.1373(2)



<SW updated procedure in X.1373>

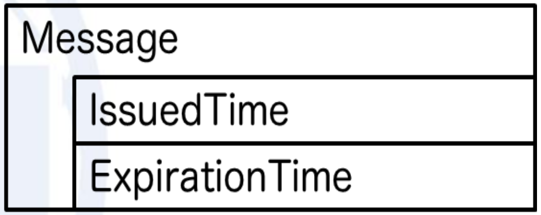
- 15 Steps to update SW
- Mandatory steps between Supplier and Vehicle Mobile Gateway
  - VMG: A module which provides communication between electronic control units (ECUs) in the controller area network (CAN) (in-vehicle buses) and exterior intelligent transportation system (ITS) entities in the external network
- **Optional steps for IVN related messages**
  - Basic model of software update

X.1373(3)

- **XML example** is provided for each type of messages.

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 "request").
	sessionid	Session 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	Trustlevel is determined based on the security capability and safety requirement of the device that generated this message.
	messageid	Message ID is a random GUID associated with an individual message.
IssuedTime	-	Time of generation of this message.
ExpirationTime	-	Expiration time of this message.

<Elements of diagnose (request) message>

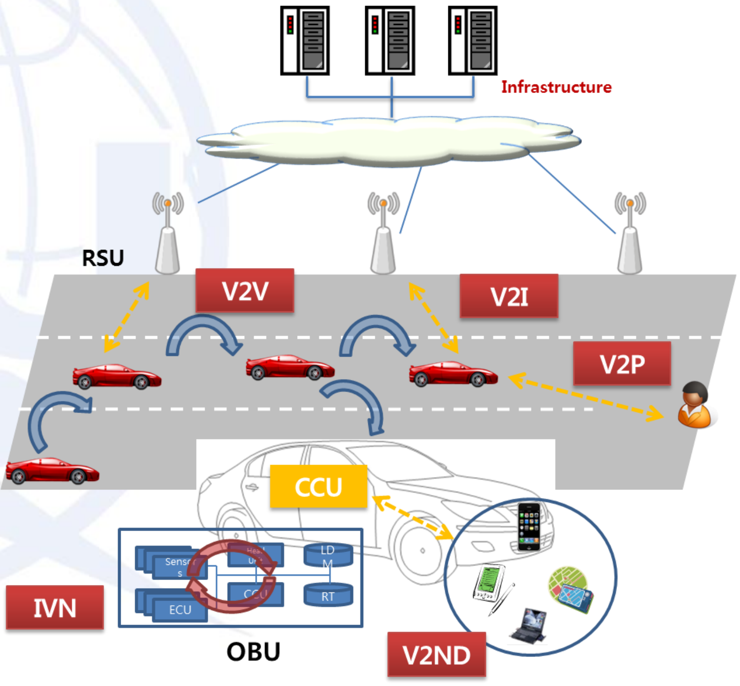


<Structure of diagnose (request) message>

```
<Message protocol="1.0" version="1.0.2" type="diagnose" subtype="request"
sessionid="{7316A97D-8C04-428B-B498-0F51087A1093}"
messageid="{2E255A59-B875-4347-90CA-92326BF45BEF}" trustlevel="3">
  <IssuedTime>1903-07-01T00:00:00Z</IssuedTime>
  <ExpirationTime>1903-07-01T00:00:00Z</ExpirationTime>
</message>
```

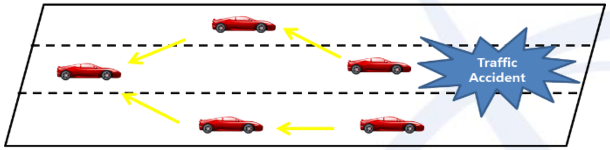
X.itssec-2(Overview)

- Revised draft at SG17 March 2017 meeting
- Scope
  - This Recommendation provides **security guidelines for V2X communication systems**.
- Contents
  - Analysis of threat for V2X communication systems
  - The security requirements for V2X communication systems
  - Use case of V2X communication systems
- V2X
  - V2V(Vehicle to Vehicle)
  - V2I(Vehicle to Infrastructure
  - V2ND(Vehicle to Nomadic Devices)
  - V2P(Vehicle to Pedestrian)

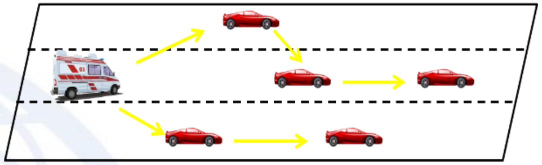


X.itssec-2(V2V/V2I)

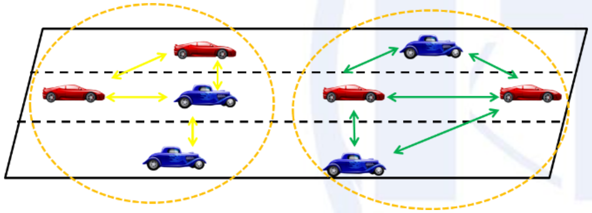
- V2V/V2I communication type



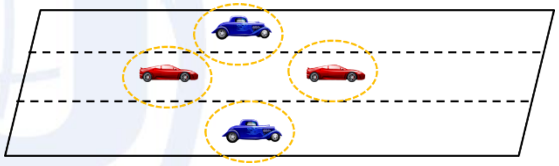
< V2V warning propagation
- warning propagation >



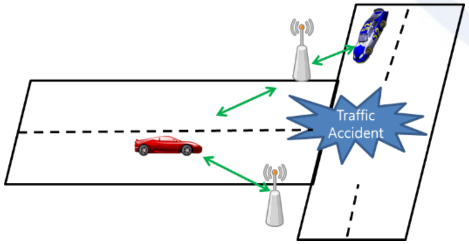
< V2V warning propagation
- warning propagation>



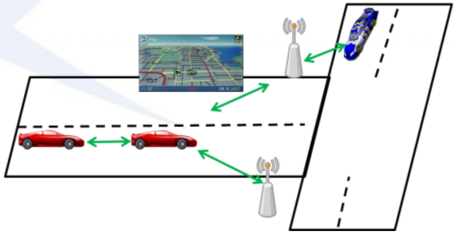
<V2V platoon communication>



< V2V beaconing>



< V2I warning>



< V2V/V2I information exchange>

X.itssec-2(Threat Analysis)

- Threats related to vehicle and RSU authentication

Threat	Description
Routing table and LDM modification attack	Attacker can spoof GPS information of a vehicle and modify the original geospatial information.
Impersonation attack	Attacker can pretend to other entity by stealing other entity's ID information. Attacker can receive a message which is sent to another entity and attacker can send a message which is generated by a specific entity. For example, if attacker can pretend to an emergency vehicle, it can send a message like "I am an emergency vehicle, thus move away on my direction." to other vehicles.
Sybil attack	Sybil attack means that one vehicle simulates multiple vehicles by using multiple vehicle/s IDs.
Attack on infrastructure	Attack on infrastructure is attack when an attacker sends to false malfunction of innocent vehicle. This attack makes CA generate revokes the innocent vehicle.

X.itssec-2(Threat Analysis)

- Threats related to message integrity

Threat	Description
Routing message manipulation attack	A malicious intermediate node modifies the message. Thus, vehicles can be received a forgery information.
Sensor information manipulation	Attacker modifies a physical address of the communication module or manipulates ECU sensor information such as a speed sensor.
Credential manipulation	Sybil attack means that one vehicle simulates multiple vehicles by using multiple vehicle/s IDs.
Attack on infrastructure	Credential manipulation means modifying the vehicle's private key or ID. Attacker can use other vehicle's credential information without authorization

X.itssec-2(Threat Analysis)

- Threats related to confidentiality

Threat	Description
Eavesdropping	Attacker can sniff V2V message nearby vehicles and V2I message of RSUs. Attacker can analyze traffic information by sniffing message.
Replay (Playback attack)	Attacker can intercept V2V message nearby vehicles and V2I message of RSUs. Later, attacker can replay those messages or information for the malicious purpose.

- Threats related to privacy

Threat	Description
Attack on personal information	Attacker can analyse an owner of the vehicle by collecting V2V/V2I messages and track the location of driving route of a particular person.
Pseudonym analysis attack	Attacker can analyse the relation between vehicle ID and pseudonyms and find out that multiple pseudonyms indicate same vehicle.

X.itssec-2(Threat Analysis)

- Threat related to non-repudiation

Threat	Description
Attack on certification database	Attacker can manipulate pseudonym database in the CA. Attacker can modify the relation between long term certificate and short term pseudonym certificate.
Unauthorized access to credential	Attacker can access a private key and certificate without authorization.

- Threats related to availability

Threat	Description
Jamming and DDoS attack on V2V/V2I communication channel	Attacker can send a lot of useless message which is called message flooding. Forwarding only a specific message by a routing node can be categorized into this attack.
DDoS attack on OBU	Attacker can inject malicious code into an OBU and send a message which requires a lot of computation resource. Attacker also sends a lot of message whose size is bigger than storage of the OBU. In particular, frequent software update without authorization can be severe attack.

X.itssec-2(Security Requirements)

Security requirement	Description
Authentication of vehicle and RSU	Attacker can manipulate pseudonym database in the CA. Attacker can modify the relation between long term certificate and short term pseudonym certificate.
Message integrity	Messages sent to or from a vehicle and a RSU should be protected against unauthorized modification and deletion.
Confidentiality	It should not be possible for an unauthorized entity to reveal the messages between vehicles and vehicles and between vehicles and infrastructure.
Privacy protection	It should not be possible for an unauthorized entity to analyse identification of a person through personally-identifiable information such as location or driving route of a particular person within communication messages.
Non-repudiation	It should not be possible for an entity to deny that it has already sent a message. This requirement can be implemented using digital signatures in vehicular communication system.
Availability	It should be possible for an entity to send and receive messages in appropriate latency. For example, forward collision warning message should be transmitted to a incoming vehicle before the vehicle arrives at the accident point. If the warning message cannot deliver to the incoming vehicle because of jamming attack, V2V/V2I safety application can be useless.

X.itssec-2(Security Requirements)

- Security requirements for V2V/V2I communication system in terms of communication type

	V2V warning propagation	V2V platooning communication	V2V beaconing	V2I warning	V2V/V2I Information exchange
Authentication of vehicle and RSU	O	▲	O	O	O
Message integrity	O	O	O	O	O
Confidentiality	-	O	-	-	O
Privacy protection	O	O	O	▲	O
Non-repudiation	O	O	O	O	O
Availability	O	O	O	O	O

O: Required, -: Not required, ▲: partially required

Future plan

– Work items

- Security guidelines on ITS-related technology
  - X.itssec-2 : security guidelines for V2X (on-going)
- Framework or mechanism on ITS-related technology
  - X.1373 : secure software update for ITS(approved)

– Candidate work items

- Security aspects on vehicular fog/edge computing
- Security aspects on intrusion detection for ITS
- Security requirements for vehicle accessible external devices

– Collaboration with other SDOs

- WP29/TFCS_OTA
- ISO TC204