



SURFACE VEHICLE STANDARD

J3217™

JUN2022

Issued

2022-06

V2X-Based Fee Collection

RATIONALE

This document defines profiles for V2X electronic fee collection—including the concept of operations, reference system architecture, user needs, system functional and performance requirements, and ASN.1 entities such as messages and related data frames and elements—to enable V2X-based tolling and other financial transactions.

TABLE OF CONTENTS

1.	SCOPE	4
2.	REFERENCES	4
2.1	Applicable Documents	4
2.1.1	SAE Publications	4
2.1.2	IEEE Publications	4
2.1.3	ISO Publications	4
2.1.4	Other Publications	4
3.	DEFINITIONS	5
4.	ABBREVIATIONS	5
5.	CONCEPT OF OPERATIONS	7
5.1	Current Situation and Problem Statement (Informative)	7
5.1.1	Relationship to ARC-IT	8
5.2	Reference Architecture	8
5.2.1	Business Architecture	8
5.2.2	Reference Architecture	9
5.3	Architectural Needs	10
5.3.1	Infrastructure-Based Tolling	10
5.4	Features	11
5.4.1	Toll Charger Features	11
5.4.2	Toll Service Provider Features	11
5.4.3	Toll Service User Features	12
5.5	Security	13
5.5.1	Data Integrity	13
5.5.2	Authentication	13
5.5.3	Authorization	13
5.5.4	Non-Repudiation	13
5.5.5	Data Confidentiality	14
5.5.6	Physical Security	14
5.6	Operational Scenarios	14
5.6.1	Toll Point Use Case: Toll Point Crossing	14
5.6.2	Tolling Point Use Case: Entry and Exit Based Charging	15

SAE Executive Standards Committee Rules provide that: "This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

SAE reviews each technical report at least every five years at which time it may be revised, reaffirmed, stabilized, or cancelled. SAE invites your written comments and suggestions.

Copyright © 2022 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of SAE.

TO PLACE A DOCUMENT ORDER: Tel: 877-606-7323 (inside USA and Canada)
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
http://www.sae.org

SAE WEB ADDRESS:

Full document details: SAE J3217_202206

For more information on this standard, visit
https://www.sae.org/standards/content/J3217_202206/

Documents

Document Sharing Hub

6.	REQUIREMENTS	16
6.1	Architectural Requirements	16
6.1.1	OBE	16
6.1.2	RSE	16
6.2	Data Exchange Requirements	17
6.2.1	Toll Advertisement	17
6.2.2	Toll Usage	21
6.2.3	TUMack Message	23
6.3	Security Requirements	23
6.3.1	Interface Between RSE and OBE	23
6.3.2	Hardware Tamper Prevention	23
6.3.3	OBE Private Key Generation	24
6.3.4	Certificate Change	24
6.3.5	Certificate Revocation List (CRL)	24
6.3.6	1609.2 Message Validity	24
6.3.7	Trust Management Information	24
7.	SYSTEM DESIGN	24
7.1	Dialogs (Message Exchanges)	24
7.1.1	Infrastructure-Based Tolling	24
7.2	Security	25
7.2.1	TAM and TUMack Security Profile	25
7.2.2	TUM Security Profile	27
8.	ASN.1 ENTITIES	29
8.1	Message Modules	29
8.1.1	Toll Advertisement Message (TAM)	29
8.1.2	Toll Usage Message (TUM)	34
8.1.3	TUMack Message	37
9.	NOTES	38
9.1	Revision Indicator	38
APPENDIX A	ENFORCEMENT OVERVIEW (INFORMATIVE)	39
APPENDIX B	WSA AND WSMP REQUIREMENTS (NORMATIVE)	40
APPENDIX C	LOWER LAYER INTERFACE CONFIGURATION (NORMATIVE)	42
APPENDIX D	SERVICE-SPECIFIC PERMISSIONS	43
APPENDIX E	SAE J2735 EDITING INSTRUCTIONS (INFORMATIVE)	44
APPENDIX F	SAMPLE MESSAGES (INFORMATIVE)	45
Figure 1	Illustration of roles in EFC	8
Figure 2	Reference technical architecture	9
Figure 3	Infrastructure-based tolling architecture	10
Figure 4	Toll point use case example	14
Figure 5	Toll point (generalized)	15
Figure 6	Closed network/road segment charging example	15
Figure 7	Toll point maps and map use	21
Figure 8	Infrastructure-based tolling data exchange dialog	25
Figure 9	TAM structure	30
Figure 10	TUM message structure	34
Figure 11	TUMack message structure	37
Table 1	Toll advertisement message (TAM) contents summary	18
Table 2	Toll charges tables	20

Table 3	Use of GenericLane	21
Table 4	Toll usage message (TUM) contents summary	22
Table 5	Toll usage data (TumData) contents summary.....	22
Table 6	TUMack contents summary	23

1. SCOPE

The scope of this document is the concept of operations including reference system architecture, the user needs, the system functional and performance requirements, the messages, the corresponding data frames and elements, and other related functionality to enable V2X-based fee collection and other financial transactions.

2. REFERENCES

2.1 Applicable Documents

The following publications form a part of this specification to the extent specified herein. Unless otherwise indicated, the latest issue of SAE publications shall apply.

2.1.1 SAE Publications

Available from SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 877-606-7323 (inside USA and Canada) or +1 724-776-4970 (outside USA), www.sae.org.

SAE J2945	Dedicated Short Range Communication (DSRC) Systems Engineering Process Guidance for SAE J2945/X Documents and Common Design Concepts
SAE J2945/1	On-Board System Requirements for V2V Safety Communications
SAE J2945/5	Service-Specific Permissions and Security Guidelines for Connected Vehicle Applications
SAE J3161	LTE Vehicle-to-Everything (LTE-V2X) Deployment Profiles and Radio Parameters for Single Radio Channel Multi-Service Coexistence
SAE J3161/1	On-Board System Requirements for LTE-V2X V2V Safety Communications

2.1.2 IEEE Publications

Available from IEEE Operations Center, 445 and 501 Hoes Lane, Piscataway, NJ 08854-4141, Tel: 732-981-0060, www.ieee.org.

IEEE Std 1609.2	IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages (as amended by IEEE Std 1609.2a™-2017 and IEEE Std 1609.2b™-2019)
IEEE Std 1609.3	IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services

2.1.3 ISO Publications

Copies of these documents are available online at <http://webstore.ansi.org/>.

ISO 17573-1	Electronic Fee Collection - System Architecture for Vehicle-Related Tolling - Part 1: Reference Model
ISO 17573-3	Electronic Fee Collection - System Architecture for Vehicle-Related Tolling - Part 3: Data Dictionary ASN.1 file: https://standards.iso.org/iso/ts/17573/-3/ed-1/en/ISO17573-3(2021)EfcDataDictionary.asn
ISO 12855	Electronic Fee Collection - Information Exchange Between Service Provision and Toll Charging (Second Edition 2015-12-15)

2.1.4 Other Publications

RTCM 10403.3	Differential GNSS (Global Navigation Satellite Systems) Services - Version 3 + Amendment 1 (April 28, 2020) - A more efficient alternative to RTCM 10402.3
--------------	--

3. DEFINITIONS

3.1 ROADSIDE EQUIPMENT

Equipment located along the road, ether fixed or mobile.

3.2 ON-BOARD EQUIPMENT

All required equipment on-board a vehicle for performing required EFC functions and communication services.

3.3 CHARGER

The entity that levies the fee.

3.4 SERVICE PROVIDER

The entity providing EFC services and the on board equipment.

4. ABBREVIATIONS

The additional abbreviations and acronyms cited below are terms related to this standard (and of the other companion volumes and guides), unless specifically cited otherwise.

3GPP	Third Generation Partnership Project
CRL	Certificate Revocation List
DSRC	Dedicated Short Range Communications
EFC	Electronic Fee Collection
ETC	Electronic Toll Collection
E-UTRA	Evolved Universal Mobile Telecommunications System (UMTS) Terrestrial Radio Access
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HARQ	Hybrid Automatic Repeat Request
HOT	High-Occupancy Toll (Lane)
HOV	High-Occupancy Vehicle (Lane)
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers
ITS	Intelligent Transportation Systems
LOS	Line of Sight
LPN	License Plate Number
LPR	License Plate Recognition

LTE	Long Term Evolution
MAC	Medium Access Control
MAP	SAE J2735 Map Data Message
MCS	Modulation and Coding Scheme
MHz	Megahertz
MSM4	Multiple Signal Message (Type 4)
NTCIP	National Transportation Communications for ITS Protocols
OBE	On-Board Unit
OBE	On-Board Equipment
OEM	Original Equipment Manufacturer
OTA	Over the Air
PC5	ProSe Communications 5
PDU	Protocol Data Unit
PER	Packet Error Ratio
PHY	Physical Layer
PICS	Protocol Implementation Conformance Statement
PII	Personal Identifiable Information
PPPP	ProSe per Packet Priority
PSID	Provider Service ID
RAN	Radio Access Network
RSE	Roadside Unit
RSE	Roadside Equipment
RTCM	Radio Technical Commission for Maritime Services
SCMS	Security Credential Management System
SDO	Standards Developing Organizations or Standards Development Organization
SPDU	Session Protocol Data Unit
SSP	Service-Specific Permissions
TAM	Toll Advertisement Message
TUM	Toll Usage Message
TUMack	Toll Usage Message Acknowledgement

Tx	Transmit
UTC	Universal Coordinated Time
Uu	UMTS Air Interface
V2X	Vehicle-to-Everything Equipped Object
WAVE	Wireless Access in Vehicular Environments
WSA	WAVE Service Advertisement
WSM	WAVE Short Message
WSMP	WAVE Short Message Protocol

5. CONCEPT OF OPERATIONS

The following sections describe the V2X fee collection concept of operations and features necessary to implement the system. Note that participation in a V2X fee collection system is optional, and this document assumes the user has already chosen to participate in the system. As such, this document does not address opt in or opt out features.

5.1 Current Situation and Problem Statement (Informative)

V2X-based fee collection is widely applied for purposes such as:

- Construction, operation, and maintenance of road transport infrastructure such as pavement, bridges, etc.
- Influencing and managing the traffic flow (e.g., congestion charging).

Charging for the use of roadways can be performed effectively using electronic fee collection (EFC). EFC is an intelligent transportation system (ITS) service that allows users to pay fees electronically, with the aim to limit delays, congestion, and environmental impact.

The geographic area where road tolls are applied is called the toll domain. The toll domain may encompass a road network, a specific section of road (e.g., a bridge, a tunnel or a ferry connection), or a specific area offering a service (e.g., a parking lot).

The set of rules governing the collection of toll in a toll domain is called a toll regime. A toll regime can be of the following types/subtypes:

- Road segment pricing: A fee is charged for driving on specific segments of roads. This includes casts where payment is required at each toll point.
- Closed network pricing: A fee is charged for driving on a road network and depends only on the points where the vehicle enters and leaves the network.
- Object pricing: A fee is charged for the use of road transportation objects (e.g., tunnel, ferries, passes, parking).

The focus of this document is on infrastructure-based tolling using V2X communications. Infrastructure-based EFC systems use an access technology that enables localized communications between the OBE and the RSE to collect charging data “on the spot.” A suitable access technology is required to support the exchange of data between OBE and RSE, and the localization of the OBE. Infrastructure-based EFC systems are one solution suited to implement road segment-based tolling and pricing.

The interoperability of EFC systems is an important aspect to enable drivers to make use of the EFC service using a single contract and OBE across multiple toll domains.

The recent development of standards for V2X (notably V2I) communication has brought new technologies into play that could be very well used for a new generation of electronic fee collection systems. This could bring benefits in terms of re-use of ITS equipment being deployed in vehicles in future, while keeping the solid foundation of the existing EFC standards and best practices.

5.1.1 Relationship to ARC-IT

The Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) classifies electronic toll collection as traffic management, and electronic toll collection is described in service package TM10. This document is consistent with the architecture described therein (refer to <https://www.arc-it.net/html/servicepackages/sp109.html#tab-3>).

5.2 Reference Architecture

5.2.1 Business Architecture

ISO 17573 uses the enterprise viewpoint concepts to define an EFC architecture in terms of actors, roles, and policies. The well-established role model defined in ISO 17573 is summarized in [Figure 1](#). Note that these are the business interactions, not data exchange interfaces.

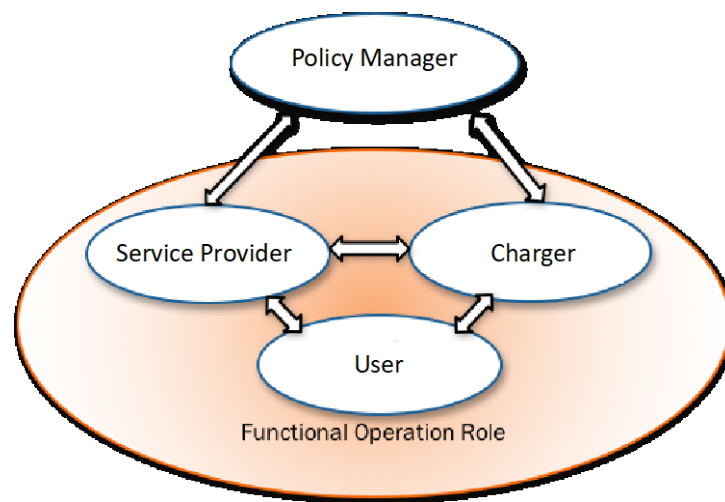


Figure 1 - Illustration of roles in EFC

The charger levies toll for the use of vehicles in a toll domain. It defines the toll regime and operates the toll system, including the interface between OBE and RSE.

The service provider provides toll services to users across one or more chargers. It is responsible for providing the basic artifacts, mechanisms, organization structures, and information transfer tools needed to run an EFC system.

The user of the service is a customer of a service provider, i.e., one liable for toll, owner of the vehicle, fleet operator, or driver, depending on the context. Implementations of toll systems in various domains commonly refer to this role as driver, user, or customer.

Policy manager: A specific role is identified to manage a toll charging environment, i.e., defining and maintaining a set of rules that, taken together, defines the policy of a given regime or of the overall toll charging environment. In the ISO 17573 business architecture, this is referred to as interoperability manager.

A detailed description of the roles and their responsibilities can be found in ISO 17573-1 clause 6.

5.2.2 Reference Architecture

The complete technical architecture for infrastructure-based system is defined in ISO 12855. [Figure 2](#) provides an overview of the architectural elements and identifies a relevant subset of the interfaces and data flows between them. While the charger and service provider are included in the architecture for context, the scope of requirements in this document is the interface between RSE and OBE. The features described in the EFC system are also related to the service provider and charger, and those features are satisfied with the data exchanged between RSE and OBE.

For a further description, refer to ISO 12855.

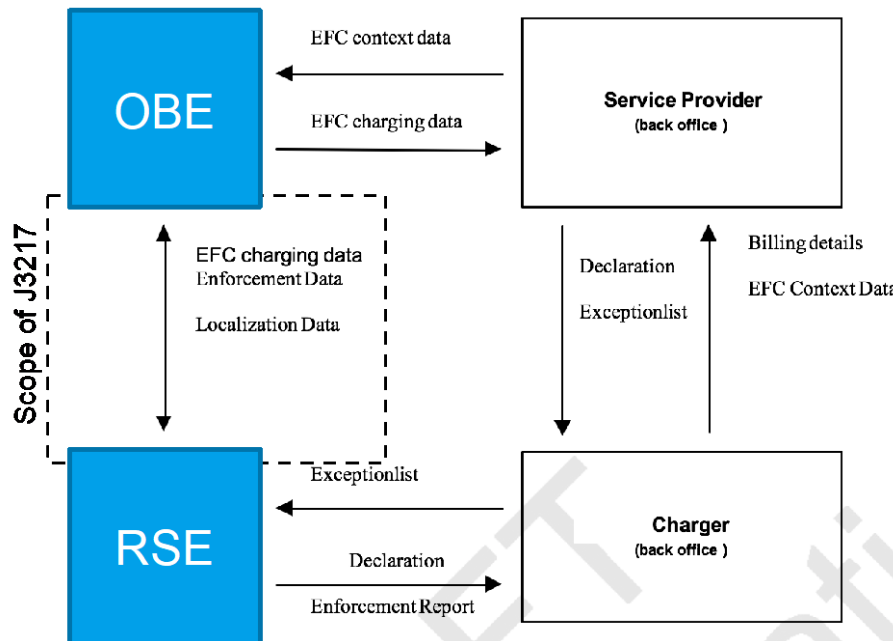


Figure 2 - Reference technical architecture

The main architectural elements are:

- The (service provider's) front end (top left box in [Figure 2](#)), equipment where road tolling information and usage data are stored, collected and processed.
- OBE, equipment on-board a vehicle for performing electronic fee collection (EFC) functions and communication services. The OBE is issued by and part of the toll service provider.
- The (charger's) RSE, equipment located along the road to enable localized communication with OBEs.
- The service provider back-office, central equipment which processes data for/from the charger and which manages the front ends.
- The charger back-office, central equipment which processes data for/from the service provider and which manages the RSEs.

The main interfaces in the architecture are those that “open up” the system and make it interoperable:

- The back office interface between service provider and charger for the exchange of all necessary data. This interface is outside the scope of this document.
- The OBE to RSE interface for the exchange of data for local charging, enforcement data (e.g., license plate number), and localization purposes (see [7.1.1](#)).

The following interfaces are regarded as system internal and not relevant for interoperability between a charger and various service providers:

- The interface between the service provider's front end and the back office.
- The interface between the charger's RSE and the charger's back office.

5.3 Architectural Needs

This section describes the architecture needs for infrastructure-based tolling enabled by V2X-based fee collection, hereon referred to as tolling. Three messages are defined here that are used to complete the toll transaction:

1. Toll advertisement message (TAM): Used to provide the toll point data to the OBE, which may include charges/payment fees. This message is sent from the RSE to OBE to provide information on the toll zone geometry and toll charges. The information is referred to as the toll charging data.
2. Toll usage message (TUM): Used to initiate a toll transaction by the OBE. This message is sent from the OBE to RSE and contains the information necessary for the toll to be charged to the appropriate user, which enables payment of the fee. TUM also carries data used to support enforcement systems.
3. Toll usage message acknowledgement (TUMack): Indicates to the OBE that the RSE has received the TUM. This message is sent from the RSE to OBE and confirms that the RSE at a specific toll point has received and verified the signature of the TUM. The message does not indicate successful payment (payment receipts are provided separately to by service provider to the toll user, which is outside the scope of this document).

A security credential management system (SCMS) provides certificates to the the OBE and RSE for the purpose of securing the tolling data.

5.3.1 Infrastructure-Based Tolling

5.3.1.1 System Architecture

The system architecture is shown in [Figure 3](#), where the toll transaction is conducted via RSE. The interface between the RSE and OBE uses the WAVE service advertisement containing the TAM in the application data field, as defined in IEEE 1609.3. The WSA that contains the tolling data is signed using a certificate containing the WSA PSID. WSMs that carry the TUM and TUMack are exchanged between RSE and OBE using a V2X communications interface.

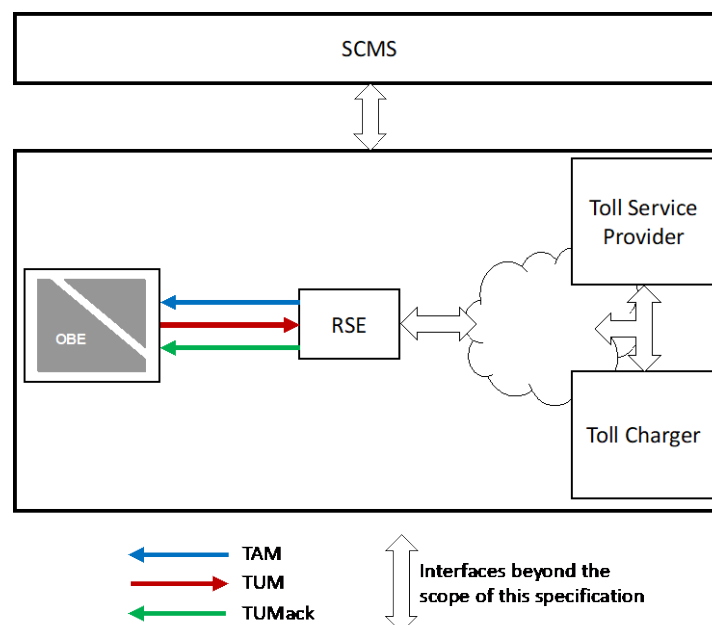


Figure 3 - Infrastructure-based tolling architecture



5.4 Features

This section defines the user needs for electronic fee collection (tolling) features using V2X communications. Note that some of the features described in this section may reflect legal or contractual obligations, depending on local regulations, and service provider or charger requirements.

5.4.1 Toll Charger Features

5.4.1.1 Provide Payment Information

The charger needs to provide general payment information about the toll road (toll domain, applicable tariffs) to users. This information is provided to the OBE in the toll advertisement message.

5.4.1.2 Report Billing Details

The charger needs to provide billing details to the service provider. This information is needed to substantiate successive payment claims to the service provider.

5.4.1.3 Deny/Allow List

The charger needs to receive deny/allow lists of users for which the service provider denies/accepts responsibility. This information may be used for the enforcement of users.

While the interface that supports deny/allow lists is outside the scope of this document, the lists may be partially compiled based on information received in a TUM. Note that the certificate revocation list (CRL) provided by the SCMS is not the same as the deny list (see [6.3.5](#)).

5.4.1.4 Receive User Details

The charger needs to receive information about the contractual status of users (i.e., vehicles identified by the LPN) with a specific service provider. This information may be used to match enforcement detections with the toll declarations from the service provider, to generate billing details and/or to trigger the enforcement process. This includes accurate information of the toll transaction time of the toll user. While the interface between service provider back office and charger back office is outside the scope of this specification, the toll usage message facilitates this feature.

5.4.1.5 Receive Transaction Data and Produce Toll Declaration

The charger needs to locally receive toll transaction information from the OBE (including user identification and vehicle information such as number of occupants, number of axles, and vehicle type) related to the use of a specific tolling service in order to produce toll declarations. The toll usage message facilitates this feature.

5.4.1.6 Provide Toll Payment Status

The charger needs to inform the service provider in a timely manner about the toll payment status (paid, not paid, amount due) related to the use of the toll road. While the interface between service provider back office and charger back office is outside the scope of this specification, the toll usage message facilitates this feature.

5.4.2 Toll Service Provider Features

5.4.2.1 Provide General Toll Payment Information

The service provider needs to provide general toll service information (service fees, applicable chargers, applicable tariffs) to users. The toll advertisement message facilitates this feature.

5.4.2.2 Provide Deny/Allow Lists

The service provider needs to provide deny/allow lists of users for which it denies/accepts responsibility.

5.4.2.3 Receive Billing Details

The service provider needs to receive billing details¹. This information is needed to provide user-specific toll payment information and to validate successive payment claims from the charger. While the interface between service provider back office and charger back office is outside the scope of this specification, the toll usage message facilitates this feature.

5.4.2.4 Provide Toll Payment Status

The service provider needs to inform the user in a timely manner (on a human financial scale) about the toll payment status (toll paid, toll not paid, amount paid) related to the use of the transport service. While the interface between service provider back office and toll user back office is outside the scope of this specification, the toll usage message facilitates this feature.

5.4.2.5 Provide User-Specific Toll Payment Information

The service provider needs to provide user-specific toll service information (service fee, total amount per period, single usage amount, applied tariffs, etc.) and invoices to users. The toll advertisement message facilitates this feature.

5.4.2.6 Change Operational Status

The service provider needs to be able to change the operational status (ON, OFF, contact service provider) of the EFC service. This allows the service provider to limit its responsibility in case the contract with the user has been ended. The interface between service provider back office and charger back office is outside the scope of this specification.

5.4.2.7 Protect Toll User Personally Identifiable Information (PII)

The service provider needs to provide adequate protection of the toll user PII. Toll user PII will not be shared without explicit consent of the toll user. The service provider may use data retention policies to manage how long toll user PII is retained.

5.4.2.8 Provide Detailed Timing of the Toll Point Crossing

The service provider needs to provide accurate information to the toll user of the toll transaction time with a resolution of 1 ms. The toll usage message facilitates this feature and contains the time and position at which the message was generated, which can be compared with the time the RSE receives the message. Note that the data is collected in the toll zone, and the TUM is transmitted when the OBE exits the toll zone.

5.4.2.9 Provide Transaction Data

The service provider needs to locally provide toll transaction information to the charger (charging data including user identification and vehicle information) related to the use of a specific tolling service. While the interface between service provider back office and charger back office is outside the scope of this specification, the toll usage message facilitates this feature.

5.4.3 Toll Service User Features

5.4.3.1 Get General Toll Payment Information

The user needs to be informed about general toll service conditions (applicable infrastructure, applicable tariff) and toll service conditions (service fees, applicable chargers, applicable tariffs). This information may be used by the user to decide whether to use the toll service, to decide at which time/day to use the tolled infrastructure, to decide which type of vehicle to use, and/or to decide about the needed vehicle occupancy. The toll advertisement message supports this feature.

¹ A billing detail may represent an elementary usage of a transport service (e.g., the toll for the single usage of a road section) or several usages of a transport service within a given period of time (a day, a week, a month, etc.), or several elementary usages of a transport service within a given journey.

5.4.3.2 Check Operational Status

The user needs to be able to check the operational status of the EFC service before the start and after the end of a trip. This information may be used by the user to decide whether to use the tolled infrastructure and/or whether to use an alternative payment method or a belated payment method. The interface between service provider and toll user is outside the scope of this specification.

5.4.3.3 Check Toll Payment Parameters

The user needs to be able to check and modify the dynamic vehicle-related parameters that influence the toll payment such as the presence of a towed trailer or occupancy information. The interface between service provider and toll user is outside the scope of this specification.

5.4.3.4 Get Toll Payment Status

The user needs to be informed in a timely manner (on a human financial scale) about the toll payment status (toll paid, toll not paid, amount paid) related to the use of the transport service. This information may be used by the user to make use of belated payment methods and to avoid fines. In systems with barriers, this information may be used by the driver to decide whether to proceed through the lane or to stop in front of the barrier. While the interface between charger and toll user is outside the scope of this specification, the toll advertisement message and TUMack support this feature.

5.4.3.5 Get Lane Status

The user needs to receive the status of a lane (open, closed) that depends on the status of toll payment, e.g., the status of a lane at a toll plaza with barriers or the status of an HOT/HOV lane. The toll advertisement message supports this feature.

5.4.3.6 Check Toll Payment Information

The user needs to be able to check specific toll payment information (status, total amount per period, single usage amount, applied tariffs, etc.) and the related invoices. While the interface between service provider and toll user is outside the scope of this specification, the toll advertisement message and TUMack support this feature.

5.5 Security

The interface between the RSE and OBE is secured using techniques defined in IEEE 1609.2. This includes message signing/encryption and certificates. In order to receive certificates, OBE and RSE need to have access to a security credential management system (SCMS).

5.5.1 Data Integrity

The system needs to ensure messages transmitted by the OBE were not modified in transit over the V2X interface.

5.5.2 Authentication

The system needs to verify messages transmitted by the OBE are sent by a valid sender.

5.5.3 Authorization

The system needs to ensure the OBE (vehicle) is authorized to act in the role it claims (e.g., police or non-agency vehicle). Some vehicles may be exempt from tolls or have special toll rates. This is enabled by the service-specific permissions (SSP) design.

The RSE is authorized to act in charger role (send TAM and TUMack).

5.5.4 Non-Repudiation

The system needs to ensure that the sender/OBE cannot deny that it sent the information.

5.5.5 Data Confidentiality

The system needs to ensure protection of personally identifiable information sent by the OBE.

5.5.6 Physical Security

The OBE and RSE need to provide tamper proof or tamper evident levels of physical protection.

5.6 Operational Scenarios

This section describes two use cases in terms of toll points. A number of use cases based on these simple constructs can be readily imagined. For example, this document supports features such as managed lanes, congestion pricing, and other dynamic pricing and roadway management approaches.

5.6.1 Toll Point Use Case: Toll Point Crossing

This use case a vehicle crosses a toll point where a fee is applied at a toll point crossing. This type of toll point can also be applied to managed lanes scenarios, where subsets of lanes may have different or no fees. This is illustrated in [Figure 4](#) and more generally in [Figure 5](#) where a toll is paid whenever the gantry (virtual or not) is passed.

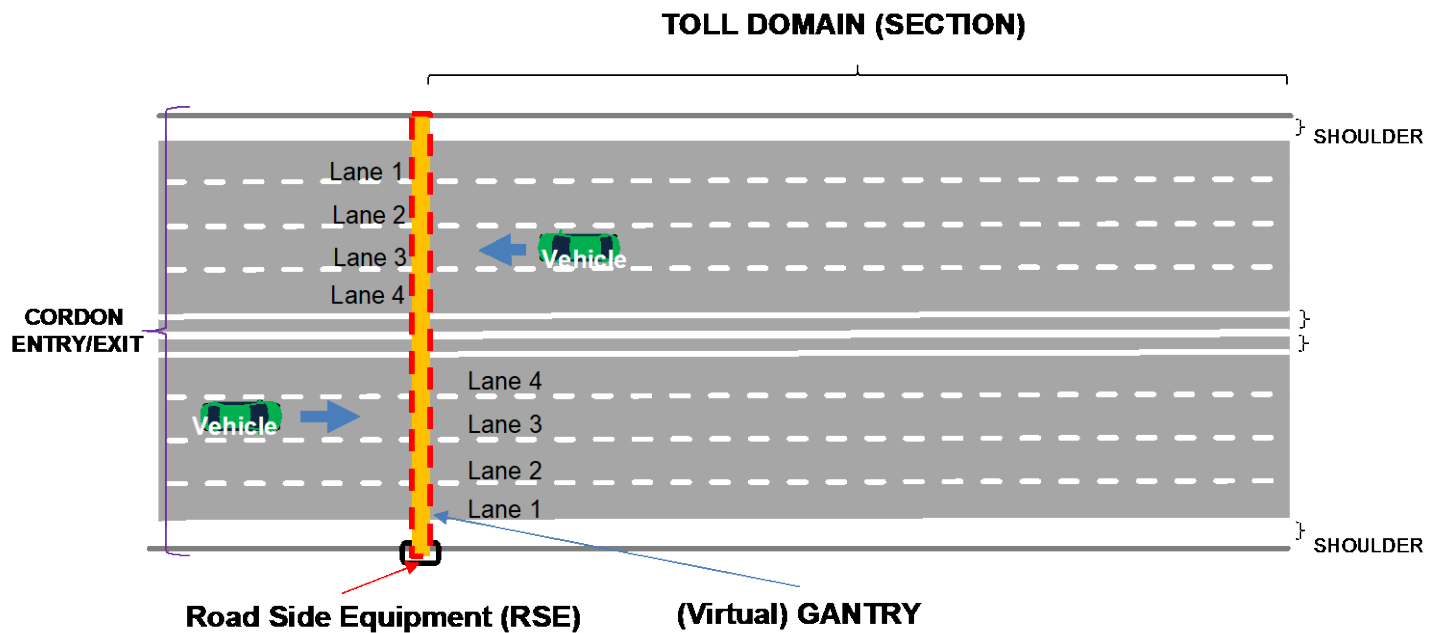


Figure 4 - Toll point use case example

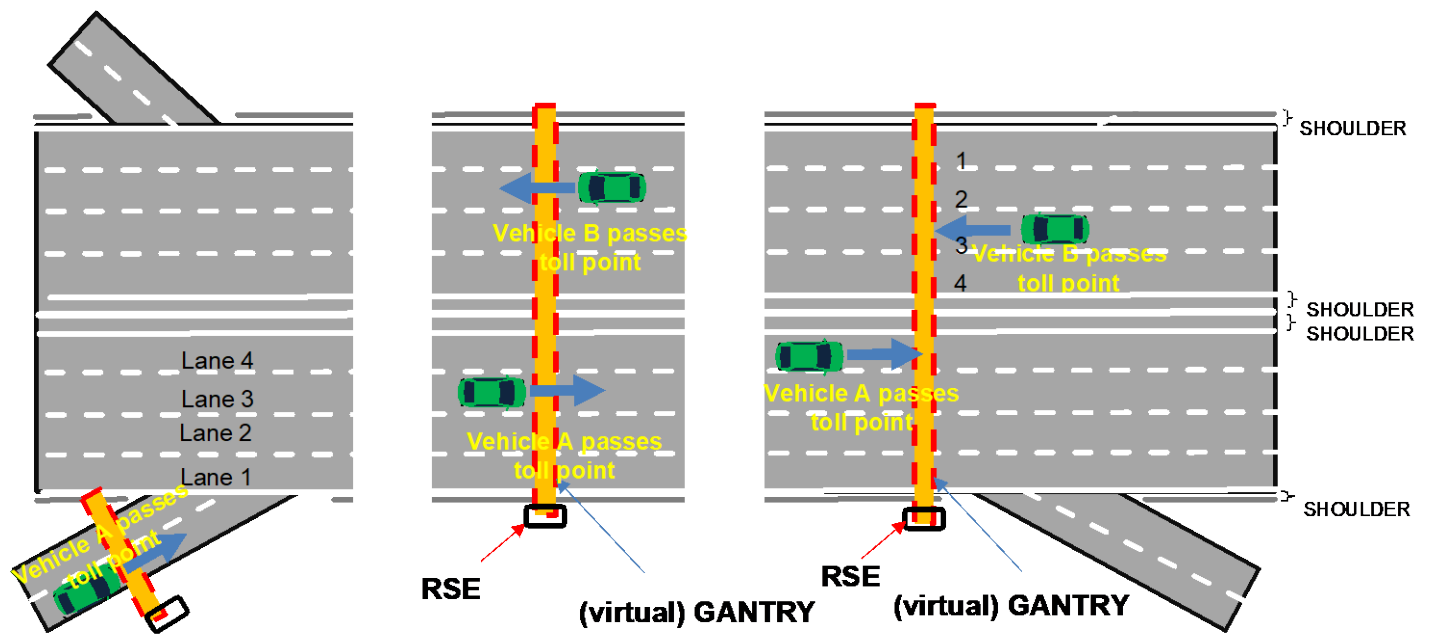


Figure 5 - Toll point (generalized)

5.6.2 Tolling Point Use Case: Entry and Exit Based Charging

This type of charging supports closed networks of roads or roads with charges based on the length of the segment traveled on a toll road. In this case the charge is applied based on the entry and exit points. Different classes of vehicles, or vehicles with more axles/weight, may have different fees. Charges may change with time, and this type of use case can also cover trip-building scenarios where the toll is applied after road use. A subset of this use case also includes charging for time between entry and exit.

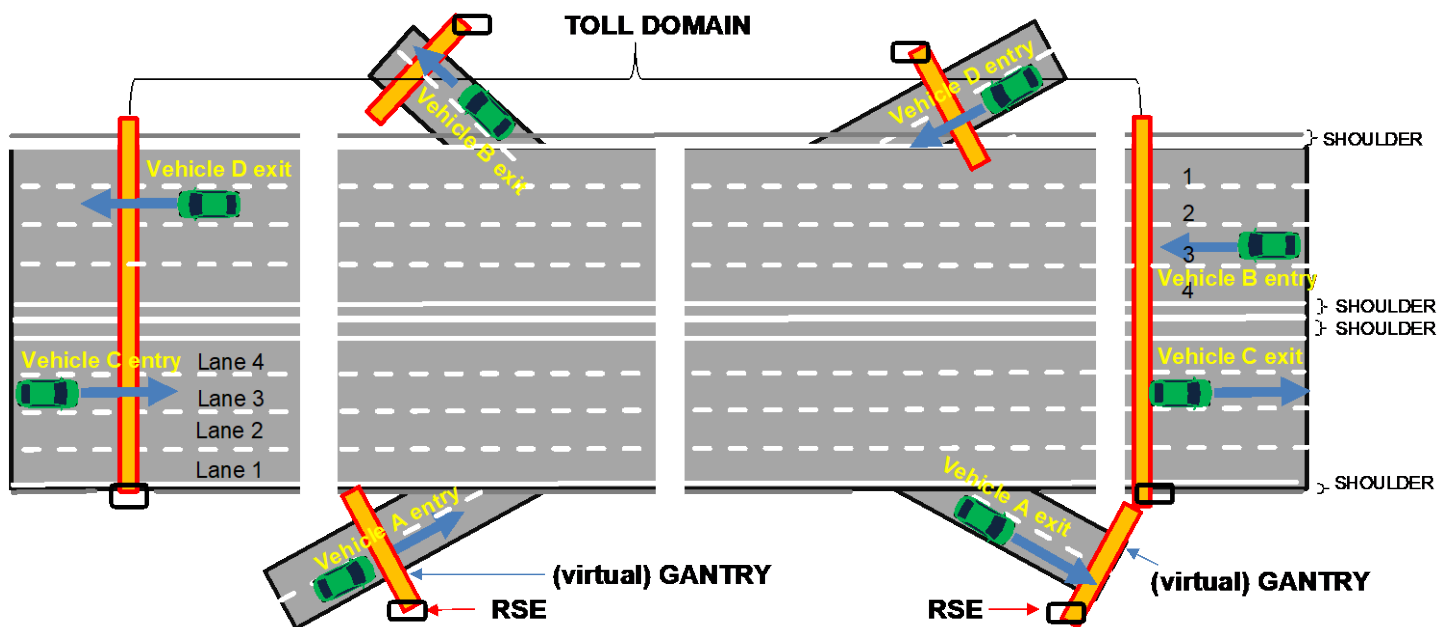


Figure 6 - Closed network/road segment charging example

6. REQUIREMENTS

6.1 Architectural Requirements

6.1.1 OBE

6.1.1.1 Communications Interface

The communications interface used for exchange of TAM, TUM, and TUMack messages shall be 3GPP PC5 mode 4 (refer to SAE J3161) or DSRC (refer to SAE J2945). The TAMs are encapsulated in a WSA per IEEE 1609.3, and the TUM and TUMack are encapsulated in WAVE short messages per IEEE 1609.3.

6.1.1.1.1 RF Performance Requirements

6.1.1.1.1.1 Minimum Transmitter RF Performance and Signal Strength

The communications interface, including antennas, shall conform to the minimum TX RF performance and signal strength requirements in SAE J3161/1 section 6.4.1, Table 14.

6.1.1.1.1.2 Receiver Sensitivity

The communications interface shall conform to the receiver sensitivity requirements specified in SAE J3161/1 section 6.4.2. For payload sizes greater than 367 octets and up to 1400 octets, the receiver sensitivity shall be at least -91 dBm.

6.1.1.2 Positioning and Timing

The OBE shall conform to the timing and positioning requirements in sections 6.2.4, 6.3.6.4, and 6.3.6.5 of SAE J2945/1. The position reference of the vehicle is as defined in SAE J2945/1, adjusted to the position of the front most point of the vehicle in along the line bisecting the longitudinal direction. For trucks and vehicles with trailers, only the pulling vehicle is included in the position reference (the trailer is not part of the position reference).

6.1.2 RSE

6.1.2.1 Communications Interface

The communications interface used for exchange of TAM, TUM, and TUMack messages shall be 3GPP PC5 mode 4 or DSRC. These messages are encapsulated in WAVE short messages per IEEE 1609.3.

6.1.2.1.1 Range and RF Performance Requirements

6.1.2.1.1.1 Minimum Transmitter Signal Strength

In order to support the necessary range in any environment, RSE installations shall be capable of a transmitter signal strength of up to 23 dBm or maximum allowed by regulatory limits, whichever is lower. Transmitter signal strength is the sum of conducted transmit power as measured at the antenna connector of the RSE in dBm and antenna gain in dBi in the direction of OBE at horizon minus cable and connector losses in dB.

NOTE: The goal of this requirement is that the OBE receives a TAM at least 500 m prior to entering the corresponding toll zone.

6.1.2.1.1.2 Receiver Sensitivity

The effective isotropic sensitivity (EIS) of the communications interface shall be at least -91 dBm in the direction of OBE at horizon for payload sizes of up to 367 octets. In a single antenna system, EIS equals the sum of receiver sensitivity, cable, and connector losses in dB minus antenna gain in dBi.

6.1.2.2 Positioning Corrections

The RSE shall broadcast SAE J2735 RTCM corrections messages. These can be locally generated or provided by a nearby reference station or virtual reference system. The SAE J2735 RTCM corrections message shall include the following RTCM messages:

- a. Station location message number 1005 and/or 1006; 1006 is preferred, but 1005 is used if 1006 is not available.
- b. The GNSS antenna and receiver location message 1033 (per the RTCM recommendation).
- c. The system parameter message 1013.
- d. The GPS MSM4 message 1074.
- e. If available, one or more of the following MSM4 messages: 1084 (GLONASS), 1094 (Galileo), and 1124 (BeiDou).

NOTE: In the U.S., GLONASS is the most commonly supported GNSS beyond GPS, so sending messages 1074 and 1084 is recommended. A transmission interval on once every 1 to 2 seconds is recommended.

NOTE: Sending RTCM corrections may not be necessary in all environments. RTCM is useful in environments where there is RF clutter and may be necessary for the OBE to achieve the necessary positioning accuracy in those environments. Vehicles may also use alternative means of obtaining high precision position.

6.1.2.3 Timing

The RSE shall use UTC as its time reference. This facilitates synchronization with enforcement systems (see [Appendix A](#)).

6.1.2.3.1 Time Reference

The RSE shall be able to provide a UTC time reference to other systems at the toll point using network time protocol (NTP). (The RSE already has an integrated GNSS.) This feature supports synchronization with enforcement systems if no other time source is available.

6.2 Data Exchange Requirements

6.2.1 Toll Advertisement

The toll advertisement message (TAM) shall be used to provide toll payment information to the OBE. The TAM contains a geographical description of the toll point, including the road geometry of the approach and toll zone, and information necessary to pay the corresponding toll. It is typically transmitted 1 to 2 times per second.

6.2.1.1 Use of WAVE Service Advertisement

The TAM shall be carried in the application data service information segment segment of the IEEE 1609.3 WAVE service advertisement (WSA). The WSA containing the TAM advertises only the PSID reserved for tolling (0p80-0F); no other PSIDs can be advertised by the same WSA (only one service info segment is present in the WSA). If a TAM exceeds 1400 bytes, it is segmented across multiple WSA.

The WSA also includes the V2X radio interface information that the OBE must use, as indicated by the channelinfo segment of the WSA.

NOTE: This limitation of only including the PSID for tolling in a WSA ensures performance and security of the EFC transaction (the certificates issued to the charger are EFC application specific). If the road operator desires to offer other services, it may send separate WSAs to advertise those services.

6.2.1.2 TAM Contents

The contents and use of fields within the TAM are described in [Table 1](#) and subsequent subsections. See [Table 1](#) for the formal ASN.1 definitions of the messages.

Table 1 - Toll advertisement message (TAM) contents summary

Data Object (ASN.1 Entity)	Description	Type	Source
TollChargesTable			This document
tollTypeCharge	Four types of toll charge tables are supported: Point-based: used for cordon-based tolling. Lane-based: used for cordon-based tolling that has per-lane, per-vehicle type rates. Entry/exit-based. Time-based.	Choice	This document
pointCharges	Used for road segment/cordon-based tolling. Charges can be based on vehicle type, weight or number of axles. Special charges (e.g., HOV or electric vehicle charges) are also supported.	Sequence	This document
chargesTable	Contains the fee information based on type of vehicle (FHWA classes 1 through 13), number of axles (up to ten or more), or weight (up to ten buckets of weight classes up to 80000 pounds). Special charges are also supported (up to HOV 5+ or clean air). See Table 2 and the TAM ASN.1 representation for further details.	Choice	This document
perLaneCharges	Used for cordon-based tolling that supports lane-based fee structures, e.g., for supporting managed lanes.	Sequence	This document
laneID	Lane ID of the lane associated with the fee. Up to 64 lanes are supported. The rightmost lane in the direction of travel for any toll point map is always laneID 1, and for example if there are four lanes the leftmost lane is laneID 4.	Integer (0-255)	SAE J2735
chargesTable	Contains the fee information based on type of vehicle (FHWA classes 1 through 13), number of axles (up to ten or more), or weight (up to ten buckets of weight classes up to 80000 pounds). Special charges are also supported (up to HOV 5+ or clean air). See Table 2 and the TAM ASN.1 representation for further details.	Choice	This document
closedNetworkCharges	Used for closed network.	Choice	This document
entryChargesTable exitInfo exitNumber exitLetter tollPointID chargesTable	Exit number and letter. Exit number. Exit letter. Upon entering a closed network, the table of prices per exit can be provided within the TAM. ID of the exit toll point. Contains the fee information based on type of vehicle (FHWA classes 1 through 13), number of axles (up to ten or more), or weight (up to ten buckets of weight classes up to 80000 pounds or more). Special charges are also supported (up to HOV 5+ or clean air). See Table 2 and the TAM ASN.1 representation for further details.	Sequence Integer (1-999) Integer (65-90) Integer (1-2048)	This document
exitChargesTable entryInfo chargesTable	TollPointID of the entry point. Upon exiting a closed network, the table of prices per entry can be provided within the TAM. The vehicle uses the toll point ID corresponding to its network entry to determine the toll owed upon exit. If there is a price discrepancy between the TAM on entry and the TAM on exit, the OBE pays the lower of the two prices. Contains the fee information based on type of vehicle (FHWA classes 1 through 13), number of axles (up to ten or more), or weight (up to ten buckets of weight classes up to 80000 pounds or more). Special charges are also supported (up to HOV 5+ or clean air). See Table 2 and the TAM ASN.1 representation for further details.	Sequence Integer (0-2048)	This document
timeBasedCharges	Used for fees based on elapsed time.	Sequence	This document
maxTime	Max time that will be charged for 24 hours.	Integer (1-1440)	This document

Data Object (ASN.1 Entity)	Description	Type	Source
chargesTable	Contains the fee information (per minute) based on type of vehicle (FHWA classes 1 through 13), number of axles (up to ten or more), or weight (up to ten buckets of weight classes up to 80000 pounds or more). Special charges are also supported (up to HOV 5+ or clean air). See Table 2 and the TAM ASN.1 representation for further details.		This document
TollAdvertisementInfo		Sequence	This document
tamSequenceNum	MsgCount: This is incremented only when the TAM contents or any contents of any linked TAMs change. In the case of multiple linked TAMs, all linked TAMs use the same sequence number. The next value after 127 is 0.	Integer (0-127)	SAE J2735
totalTams	Up to ten TAMs can be linked together to manage message size. If a set of TAMs is used to provide the fee information at a single toll point, the TollAdvertisementInfo data is sent in the first of those TAMs.	Integer (1-10)	This document
tamNum	Up to ten TAMs can be linked together. This field identifies each TAM in the set.	Integer (1-10)	This document
tollChargerInfo	Information used to identify the toll charger.	Sequence	This document
tollChargerID	ID of the toll charger.	Object identifier	This document
tollPointID	ID of the toll point.	Integer (1-2048)	This document. Same structure as ISO 17573-3
DescriptiveName	Text string (optional).	IA5String (1-63)	SAE J2735
timeStamp	DDateTime: the time the TAM was generated. A TAM may be signed and stored for repeated periodic transmission by RSE.	Sequence	SAE J2735
tumInstructions maxNumOfLocationTimeStamps locTimeStampRate	Number of location and timestamp pairs to be collected while in the toll zone. The vehicle includes as many position and timestamp pairs as possible within the toll zone, up to the number indicated by this field. Determines the rate in Hz at which location and time stamps are collected. 1 = once per second, 10 = ten times per second.	Sequence Integer (1-5) Integer (1-10)	This document
tollPointMap	Map of the approach lanes and toll zone lanes.	Sequence	This document
revisionNum	Revision number of the tollPointMap. The next value after 10 is 1. This field is typically used by the OBE to determine if it has the latest revision of the map.	Integer (1-10)	This document
referencePoint	Position3D: the reference point (latitude, longitude, and elevation) basis for the lane nodes in a toll point map.	Sequence	SAE J2735
speedLimit	RegulatorySpeedLimit: The speed limit at the toll point. Refer to SAE J2735 for details.	Sequence	SAE J2735
laneWidth	LaneWidth: The nominal lane width in centimeters of the lanes approaching the toll point.	Integer (1-32767)	SAE J2735
approachLanesMap	A sequence of up to 64 instances of GenericLane (one for each lane in the approach map).	Sequence	This document, SAE J2735
tollZoneLanesMap	A sequence of up to 64 instances of GenericLane (one for each lane in the toll zone map).	Sequence	This document, SAE J2735
tumPublicKey	The 256-bit public key used to encrypt the TumData.	Octet string (32)	This document
ackPolicy	The parameters used for TUM retries.	Sequence	This document
timeout	The time to wait (in milliseconds) for a TUMack after sending a TUM. If a TUMack is not received within the timeout, the OBE retries sending the TUM.	Integer (100-10000)	This document
numOfRetries	The max number of retries for sending a TUM. After the numOfRetries + 1 attempts, the OBE stops attempting to send the TUM.	Integer (1-5)	This document
lastTollPtDataReq	This field, if included and set to ON, indicates that the last toll transaction information (toll point info and transaction time) is requested to be included in the TUM.	Boolean	This document

6.2.1.2.1 Toll Charges (Fee)

The structures for toll charges are described in [Table 2](#). A fee is associated with each entry in the a ChargesTable, whether it be based on the vehicle class/type, weight or number of axles. Special charges for HOV and clean air vehicles are also supported.

Each fee is based on the currency associated with the countryCode included in the TAM. A fee can be up to 200000 units, and the units are hundredths of the currency. For example, in the U.S., a fee of 225 would be \$2.25 USD (two dollars and twenty-five cents).

Table 2 - Toll charges tables

Data Object (ASN.1 Entity)	Description	Type	Source
ChargesTable	Fee table (vehicle type, axle, or weight based).	Choice	This document.
vehTypeBased	VehTypeChargesTable: Used to indicate the charge based on the type of vehicle (FHWA classes 1-13, or HOV or clean air). If a fee is not included for a specific class of vehicle, the fee for the next highest class of vehicle in the charges table applies. SpecialCharges indicates fee for HOV, clean air or other operator-defined vehicle classifications. For example, operator-defined categories can be used for vehicle size or shape-based fee structures, or for exempting agency-owned and emergency vehicles. If this fee structure is included, it overrides any applicable FHWA vehicle class-based fee. OperatorDefined supports up to 16 categories of charges defined by the toll operator.	Sequence	This document and ISO 17573-3. See the TAM ASN.1 representation for details.
numAxlesBased	AxlesChargesTable: Used to indicate fees for vehicles with two or fewer, or three or more axles. Fees for vehicles with up to ten or more axles are supported. For example, there can be three entries in the charges table, one for two axles, one for three axles, and one for six axles. In this case, a vehicle with two or fewer axles pays the two-axle fee; a vehicle with three, four, or five axles pays the three-axle fee; and a vehicle with six or more axles pays the six-axle fee. Note that AxlesChargesTable can also include total weight.	Sequence	This document and ISO 17573-3. See the TAM ASN.1 representation for details.
weightBased	WeightCharges: Supports both total weight and per axle weight charges. Total weight is the entire vehicle train. Units are also specified in this entity (pound or kilograms).	Choice	This document and ISO 17573-3. See the TAM ASN.1 representation for details.

6.2.1.2.2 Toll Point Maps

A toll point map is associated with each toll point. For lanes approaching a toll zone, ApproachLanesMap is sent in the TAM. For the lanes within the actual toll zone, TollZoneLanesMap is sent in the TAM. Approach lanes connect to one or more toll zone lanes, and the direction of travel is from the approach lanes toward the toll zone lanes. Both of these maps use a sequence of up to 64 instances of GenericLane. Note that approach lanes may connect to one or more toll zone lanes.

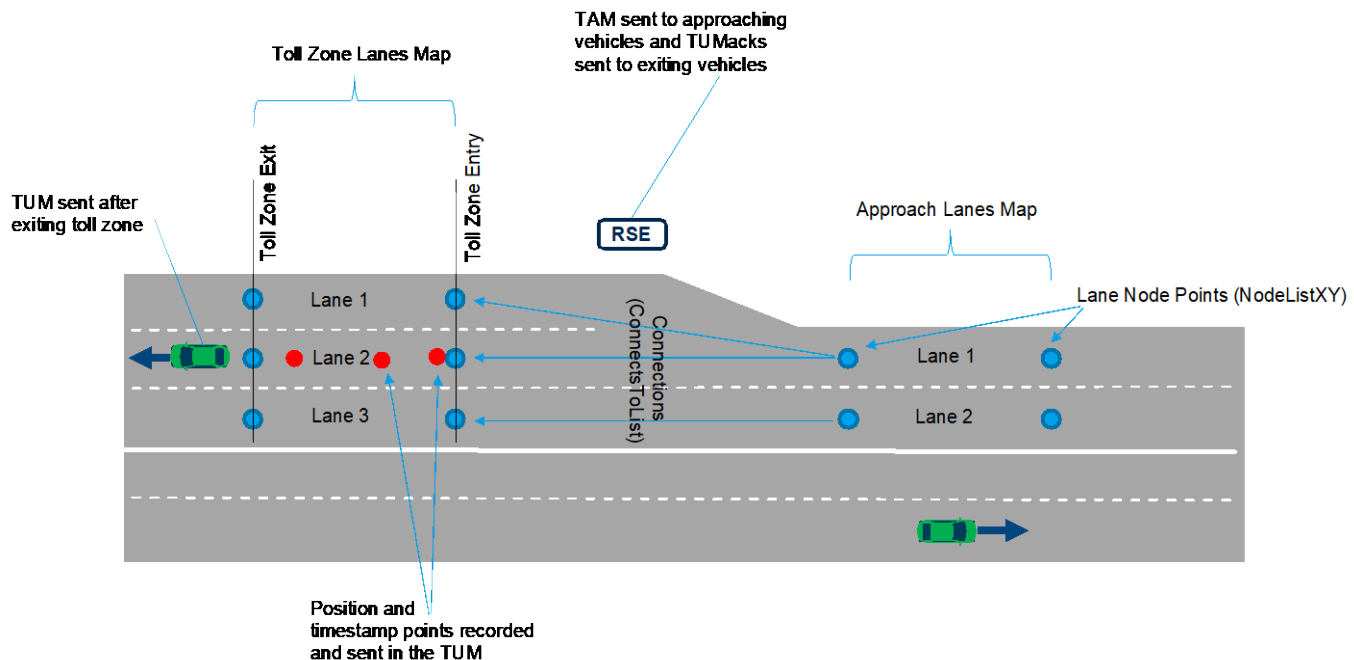
The SAE J2735 GenericLane object is used to describe the lanes in a map. Entering a toll zone is always defined by the crossing the line through the first point in the rightmost lane of the toll zone lanes map, perpendicular to the point of travel. Exiting the toll zone is always defined the by the line through the last point in the rightmost lane of the toll zone lanes map, perpendicular to the point of travel.

Use of GenericLane is described in detail in [Table 3](#). Certain fields in GenericLane are static, and certain fields are not permitted to be used for implementations conformant with this document.

Table 3 - Use of GenericLane

Data Object	Description
laneID	LaneID: Use as described in Table 1.
name	DescriptiveName: Do not include.
ingressApproach	ApproachID: Do not include.
egressApproach	ApproachID: Do not include.
laneAttributes	LaneAttributes: LaneDirection: set to ingressPath. LaneSharing: set to all 0s (zero). LaneTypeAttributes.LaneAttributes-Vehicle: Bits are set according to the corresponding lane attributes, e.g., in the case of a gate/barrier that opens/closes, bit 7 is set to 1 (permissionOnRequest). Lanes can also be restricted based on other bits (e.g., hovLaneUseOnly). Bit 5 may be used to restrict a lane to only emergency vehicles. RegionalExtension: Do not include.
maneuvers	AllowedManeuvers: Do not include.
nodeList	NodeListXY: include at least two nodes for the rightmost lane. ComputedLane may be used by referencing the rightmost lane with LaneID 1 (e.g., lanes 2, 3 and 4 may be computed lanes).
connectsTo	ConnectsToList: This field is used in the approachLanesMap to indicate connections to lanes in the tollZoneLanesMap. Approach lanes connect to one or more toll zone lanes.
overlays	OverlayLaneList: Do not include.
regional	Regional extensions are not permitted to be used in systems conformant with this document.

An illustration of how approach and toll zone lanes are mapped and used is shown in [Figure 7](#). A TAM is received as a vehicle approaches a toll point. Once the vehicle enters the toll zone, it records the number of position and timestamp pairs requested in the TAM, and when it exits the toll zone, the OBE transmits the recorded position and timestamp pairs to the RSE via a TUM. Other items such as lane IDs and connections are also illustrated in [Figure 7](#).

**Figure 7 - Toll point maps and map use**

6.2.2 Toll Usage

The toll usage message (TUM) shall be used by the OBE to provide toll payment information to the RSE and is transmitted immediately after the OBE exits the toll zone defined in the corresponding TAM (see [6.2.1.2.2](#)). Receipt of the TUM is acknowledged by the RSE using the TUMack message ([6.2.3](#)).

6.2.2.1 TUM Contents

The contents of the TUM are described in [Table 4](#). See [8.1.2](#) for the ASN.1 definitions of the messages.

Table 4 - Toll usage message (TUM) contents summary

Data Object (ASN.1 Entity)	Description	Type	Source
tollPointInfo	Top level toll usage container	Sequence	This document.
tempID	TemporaryID: use a random value that is re-randomized prior to the transaction at each toll point.	Octet String (4)	SAE J2735, SAE J3161/1.
tumSequenceNum	MsgCount: This value is incremented when retries occur. The first TUM sent at any toll point has a MsgCount set to zero.	Integer (0-127)	SAE J2735.
tamSequenceNum	MsgCount: This is the tamSequenceNum received in the TAM.	Integer (0-127)	SAE J2735.
tumHash	This is a SHA-256 hash of the plain text of TumData (before encryption).	Octet String (32)	This document.
encryptedTumData	TumData is encrypted and sent within this field. See Table 5 for the contents of TumData.	Octet String (1-7000)	This document. Note that implementations based on DSRC may be further limited; this document allows larger sizes to accommodate the capabilities of LTE-V2X. However, the TUM is unlikely to exceed 1400 octets.

6.2.2.1.1 Toll Usage Data

The user information associated with a TUM is included in the TumData object, which is encrypted and included in the encryptedTumData object. TumData includes the information necessary to pay the toll as summarized in [Table 5](#).

Table 5 - Toll usage data (TumData) contents summary

Data Object (ASN.1 Entity)	Description	Type	Source
tollUserData	Toll user information.	Sequence	This document
timeStamp	DDateTime: time of TUM generation.	Sequence	SAE J2735
tspld	Identifier of the toll service provider.	Object Identifier	This document
vehicleID	Used to identify the vehicle. See the formal TUM ASN.1 definition for details.	Sequence	This document
vehType	FHWA vehicle class.	Enumeration	This document
vehNumAxles	Number of axles.	Integer (1-10)	This document
vehWeight	Vehicle weight in pounds.	Integer (1-80000)	This document
numOccupants	Number of vehicle occupants. A value of five is used for five or more.	Integer (2-5)	This document
locAndTimeStamps	A sequence of up to tumInstructions (6.2.1.2) pairs of position and timestamp spaced 100 ms apart. This provides the vehicle trajectory through a toll zone.	Sequence	This document
lastTollPoint	If requested in the TAM, this includes up to the five most recently passed toll point and the time of the TUM that was acknowledged at that toll point.	Sequence	This document
charge	Payment Fee: the fee the OBE intends to pay. This should correspond with what was advertised in the TAM. For the closed network use case, when the vehicle enters the network, the fee on entry is zero, and this field is omitted. The fee paid on exit is based on the Fee advertised in the TAM(s) received upon entry, and in the case of a discrepancy between entry and exit, the OBE uses the lesser of the two fees.	Integer (1-200000)	This document and ISO 17573-3
tollServiceProviderData	This optional field can only be read by the toll service provider. How the service provider accesses this information is outside the scope of this document.	Octet String (1-1024)	This document



6.2.3 TUMack Message

The TUMack message shall be used by the RSE to indicate to OBEs that the RSE received a corresponding instance of the TUM. The TUMack does not inform the OBE of toll payment status. Toll payment status may be provided on a separate interface between the OBE/user and the service provider (out of scope of this document).

The TUM ack is a broadcast message that contains acknowledgements of corresponding TUMs sent by one or more OBEs. The TUM contains up to 32 acknowledgements, one for each OBE that sent a corresponding TUM.

6.2.3.1 TUMack Contents

The contents of the TUMack are described in [Table 6](#). See [8.1.3](#) for the ASN.1 definitions of the messages.

Table 6 - TUMack contents summary

Data Object (ASN.1 Entity)	Description	Type	Source
tumAck	A sequence of up to 32 instances of TUM acknowledgements (up to 32 OBEs can be provided acknowledgement via one TUMack message).	Sequence	This document.
signedTumHash	A SHA-256 hash of the entire SPDU of the TUM being acknowledged (after encrypting and signing of the TUM).	Octet String (32)	This document.
tempID	TemporaryID: Echo the value used in the TUM being acknowledged.	Octet String (4)	SAE J2735.
tumSequenceNum	MsgCount: Echo the value used in the TUM being acknowledged.	Integer (0-127)	SAE J2735.
ackMaxAge	The maximum age in milliseconds of any TUM being acknowledged.	Integer (100-10000)	This document.

6.3 Security Requirements

6.3.1 Interface Between RSE and OBE

The interface between RSE and OBE shall be secured using IEEE 1609.2 security.

6.3.1.1 TAM

The TAM transmitted by the RSE shall be signed using 1609.2 certificates. The TAM is transmitted within the application data field of a WAVE service advertisement (WSA), as defined in IEEE 1609.3, so the entire WSA is signed. The TAM information inside the WSA is not signed separately. Permission to send a TAM and corresponding Serviceinfo instance (refer to IEEE 1609.3) is provided by the SSP design in [Appendix D](#).

6.3.1.2 TUM

The TUM transmitted by the OBE to the RSE shall be encrypted then signed using 1609.2 certificates. TUM is encrypted using the public key received in the TAM. The TUM optionally includes a SHA-256 hash of the TUM plain text to support non-repudiation.

If a TUMack is not received by the OBE within the timeout indicated in the TAM, the OBE retries sending TUM (based on ackPolicy). For retries, signature and encryption must be regenerated, as TUM contents (tumSequenceNum) will have changed. See [6.2.1.2](#) and [6.2.2.1](#).

6.3.1.3 TUMack

The TUMack transmitted to the OBE by the RSE shall be signed using 1609.2 certificates. Permission to send a TUMack is provided by the SSP design in [Appendix D](#).

6.3.2 Hardware Tamper Prevention

The RSE and OBE shall store private keys in a FIPS 140-2 level 3 or higher conformant hardware security module (HSM).

6.3.3 OBE Private Key Generation

The OBE shall only allow the TUM generating application to have access to (1) the private signing key used to sign the TUM, and (2) the generation and use of the ephemeral encryption key used to encrypt the TUM.

NOTE: The charger may from time to time change the public encryption key transmitted by each RSE.

6.3.4 Certificate Change

To preserve privacy, the OBE shall not use the same certificate for consecutive toll transactions. Note that the same certificate is used at a single toll point, including TUM retries. A different certificate shall be used when signing the TUM sent at any two consecutive toll points, unless the same certificate is being used to sign BSMs, in which case the rules in SAE J2945/1 take precedence.

NOTE: The OBE typically rotates through a pool of many certificates, and the number of certificates in the pool is dependent on the capabilities of the OBE and the policy of the service provider. The more certificates in the pool, the greater the user privacy. Certificate pools may also be updated regularly; at least 20 certificates per week is recommended (certificate lifetime should be set so that it expires within one week of its first use).

NOTE: RSE certificate changes and lifetimes are outside the scope of this document, but RSE certificate lifetimes are expected to be substantially longer than OBE certificate lifetimes.

6.3.5 Certificate Revocation List (CRL)

The OBE and RSE shall be capable of receiving and storing a CRL. A CRL is issued by the SCMS and used to indicate a compromised RSE or OBE from a security perspective, while the deny/allow list is used by a service provider to indicate responsibility for a toll user/OBE to a charger.

6.3.6 1609.2 Message Validity

The OBE and RSE shall be capable of determining the validity of received IEEE 1609.2 signed data per the security profile provided in this document.

6.3.7 Trust Management Information

The OBE and RSE shall be capable of obtaining from a trust management service the trust management information needed to determine the validity of received IEEE 1609.2 signed data, including but not limited to certificate revocation lists (CRLs), certificate trust lists (CTLs), and CA certificates.

7. SYSTEM DESIGN

7.1 Dialogs (Message Exchanges)

This section includes the communications dialog used between the RSE and OBE. Note that the lower-layer physical interface between OBE and RSE may use DSRC or LTE-V2X (PC5 mode 4). See [Appendix C](#) for details on the lower-layer interface configuration.

7.1.1 Infrastructure-Based Tolling

The data exchange between RSE and OBE starts with a broadcast toll advertisement message (TAM) that is signed but not encrypted. The TAM is periodically broadcast at a rate typically once per second or once per 2 seconds (configurable by the charger). Some locations may use higher rates depending on traffic conditions; IEEE 1609.3 permits a much higher rate, but 1 to 2 Hz is recommended.

The OBE is required to respond to any TAM associated with a toll point through which it passes, including upon entry to a toll road that uses entry/exit based charging, even though there is no fee at the entry point. Fees are applied at the exit points in that case.

The OBE responds to the TAM with a toll usage message (TUM) that is generated immediately after exiting the toll zone. A vehicle exits the toll zone when the front of the vehicle crosses the toll zone exit. The TUM is encrypted then signed and contains the information necessary for the charger and service provider to bill for the toll. The TUM is encrypted with a public encryption key received in the TAM, and the TUM is transmitted after the vehicle exits the toll point (see tollIDRoadGeometry in 8.1.1.1).

TUM is acknowledged by the RSE (TUMack) to ensure delivery. The TUMack policy (timeout and max retries) is provided to the OBE within the TAM. If a TUMack is not received within the timeout, the OBE retries its TUM. If the OBE is no longer receiving the TAM, or it has received a corresponding TUMack, it ceases attempts to retry the TUM. Note that the timeout can be adjusted by the RSE based on traffic conditions (e.g., average vehicle speed).

The TUMack is sent by the RSE to provide acknowledgement of receipt of the TUM, and multiple TUMs from different vehicles may be acknowledged with a single TUMack. The TUMack does not indicate proof of payment, only receipt of the TUM. The OBE/user must access the toll billing records at a later time through its relationship with the service provider.

The TAM is transmitted within a WSA, and the TUM and TUMack messages are transmitted using the WAVE Short Message Protocol (WSMP) over V2X as defined in IEEE 1609.3. See [Appendix B](#) for the WSA, WSMP, and V2X communications interface profiles. The corresponding dialog is shown in [Figure 8](#).

Note that multiple RSEs can be deployed in the area around a toll point to support extended coverage (e.g., one RSE may be used for transmitting TAMs, and one may be used for receiving TUMs).

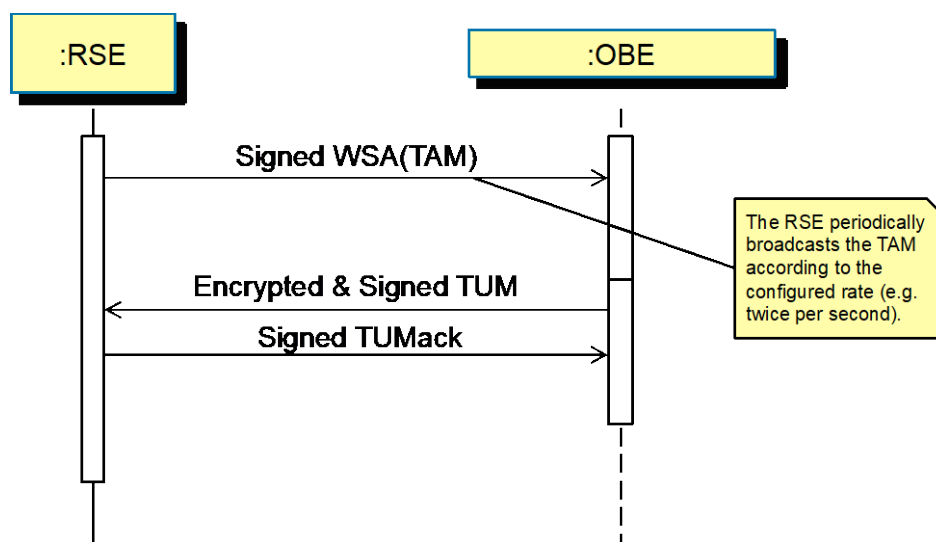


Figure 8 - Infrastructure-based tolling data exchange dialog

7.2 Security

7.2.1 TAM and TUMack Security Profile

Because the TAM and TUMack are broadcast messages and do not contain sensitive information, they are signed but not encrypted. The TAM is embedded inside of the WSA using the applications data field; therefore the entire WSA is signed using the TAM security profile. The security certificate used with the TAM is fixed for the lifetime of the certificate; there is no certificate rotation because the RSE does not need privacy. The same certificate used to sign the WSA containing the TAM is also used to sign the TUMack, but certain values in the security profile are different for TUMack as indicated in the Notes column.

7.2.1.1 IEEE 1609.2 Security Profile Identification

Field	Value	Notes
Name	SAE J3217 TAM and TUMack V1	
PSIDs	0x87, 0x8F	The PSIDs assigned to the WSA ² and SAE J3217.
Other considerations	This TAM security profile is designated for electronic fee collection implemented conformant to this document.	A description of the conditions under which this security profile is to be used.

7.2.1.2 Sending

Field	Value	Notes
Sign Data	True	Sign all TAMs for data origin authentication and non-repudiation.
Signed Data in Payload	True	
External Data	False	
External Data Source	N/A	
External Data Hash Algorithm	N/A	
Set Generation Time in Security Headers	True	
Set Generation Location in Security Headers	False	Signed messages do not need to indicate generation location. The signing certificate will indicate "authority to sign" for a given region.
Set Expiry Time in Security Headers	True	Lane closures or other roadway impediments may be somewhat dynamic, requiring message updates within the signer authorization certificate's validity period.
Signed SPDU Lifetime	Variable	This parameter is deployment specific.
Signer Type Self	TRUE	
Signer Identifier Policy Type	Simple	
Simple Signer Identifier Policy: Minimum Inter Cert Time	Always	All TAM and TUMack messages will contain the signing public key certificate.
Simple Signer Identifier Policy: Exceptions	False	
Simple Signer Identifier Policy: Signer Identifier Cert Chain Length	1	
Text Signer Identifier Policy	N/A	
Sign With Fast Verification	Yes-Compressed	
EC Point Format	Compressed	
p2pcd_flavor	N/A	
p2pcd_maxResponseBackoff	N/A	
p2pcd_responseActiveTimeout	N/A	
p2pcd_requestActiveTimeout	N/A	
p2pcd_observedRequestTimeout	N/A	
p2pcd_currentlyUsedTriggerCertificateTime	N/A	
p2pcd_responseCountThreshold	N/A	
Repeat Signed SPDUs	True	Following the initial, transmitted TAM, each following one may be a repeat transmission of the first so long as they are within the validity period of the message (as set by the signing application). For the TUMack, this is N/A because the TUMack will not be repeated.
Time Between Signing	Set to TAM lifetime	N/A for TUMack.
Encrypt Data	FALSE	
pduFunctionalTypes	N/A	

² The PSID 0x87 identifies the received message as a WSA; however, the PSID being advertised in the WSA identifies the SAE J3217 tolling application. The certificate attached to the signed WSA contains both the WSA and SAE J3217 PSID.

7.2.1.3 Receiving

Field	Value	Notes
Use Preprocessing	True	The full cert chain will not be sent with TAM messages.
Verify Data	True	Verify all TAM and TUM-ACK messages.
Maximum Certificate Chain Length	4	
Relevance: Replay	False	
Relevance: Generation Time in Past	False	Security services won't take control. The application must decide.
Validity Period	N/A	
Relevance: Generation Time in Future	True	This allows RSE to set future expectations for a given toll location (e.g., a planned lane closure) even if the message doesn't reflect the current tolling context.
Acceptable Future Data Period	Variable	Specific to TAM for given deployment. Recommended default value = 1 hour. For TUMack this value is zero (future generation times are not allowed).
Generation Time Source	Security Header	
Relevance: Expiry Time	True	
Expiry Time Source	Security Header	
Consistency: Generation Location	False	
Relevance: Generation Location Distance	False	
Validity Distance	N/A	
Generation Location Source	N/A	
Additional Geographic Consistency Conditions	N/A	
Overdue CRL Tolerance	30 days	
Relevance: Certificate Expiry	True	
Accept Encrypted Data	No	

7.2.1.4 Security Management

Field	Value	Notes
Signing Key Algorithm	ecdsaNistP256withSha256	
Encryption Algorithm	N/A	
Implicit or Explicit Certificates	Implicit	What is supported by SCMS.
EC Point Format	Compressed	Point compression more vital on rapidly transmitted messages.
Supported Geographic Regions	Rectangular, Polygon, or Circular	Deployment specific—the type of shape depends on the needs of the deployment; in most cases a circle or rectangle will be sufficient. This region informs the OBE where the certificate is valid and should be large enough to cover at least one toll zone.
Maximum Full Certificate Chain Length	8	
Use Individual Linkage ID	True	Enables revocation of multiple certificates from a single RSE.
Use Group Linkage ID	True	Enables revocation of certificates from multiple RSE.
Signature Algorithms in Chain or CRL	ecdsaNistP256withSha256	

7.2.1.5 Other

Field	Value	Notes
Fields that may be subject to policy update	N/A	

7.2.2 TUM Security Profile

The TUM may contain sensitive information and is therefore encrypted before signing.

NOTE: TUM pseudonym certificates are distinct from BSM certificates (they are separate certificates).