4.7 - EN 15509 AutoPASS On-board Equipment (OBE)

Functional and Technical requirements

Document status

Document number:	4.7

Status	Version	Description
Final	1.5	Version 1.3 updated

Authorisation	Name	Date	Signature
Author	Tord I. Reistad	15.06.2016	
Norwegian Public Roads Administration	Per Einar Pedersli	15.06.2016	

Document revision history

The objective of the Document Revision history is to reflect the evolution of the document.

Ver.	Date	Author	Main changes
1.0	30.04.2013	Trond Foss	Final version for Tender
1.1	01.11.2013	Trond Foss	Tender version updated based on supplier comments and quality assurance in the design phase Changes mainly in information architecture and data requirements
1.2	07.11.2013	Trond Foss	Security related comments from Tord Reistad included.
1.3	01.09.2014	Trond Foss	Change in CS5 (VIN) coding. Final Quality Assurance and implementation of minor changes defined during the design and implementation period before delivery of first batch of AutoPASS OBEs.
1.4	27.10.2014	Trond Foss	Note on the use of AID=6 Parking in 5.2.4.
1.5	15.06.2016	Tord Ingolf Reistad	Changed and clarified requirements for OBE initialisation key Maximum width of the OBE shall be 20 mm.

Contents

1. Definitions, Abbreviations and references

The Terms and definitions used in this document shall comply with:

AutoPASS Requirement specification
2.1 – AutoPASS definitions

2. Introduction

This document specifies the technical and physical requirements to the OBE to be used as part of the AutoPASS system. The document replaces the previous version of the AutoPASS OBU specification 2.7.1. On-board Unit (OBU) – Technical and physical requirements.

This OBE specification is based on the EN 15509 standard Road Transport and Traffic Telematics – Electronic Fee Collection – Interoperability application profile for DSRC.

The interface between OBE and Charging Point is briefly described.

3. Normative references

Whenever a standard is referenced it is referring to the latest version of the standard.

Reference	Full reference
ISO TS 19299	ISO/TS 19299 Electronic Fee Collection – Security Framework
Directive 2002/95/EC	Directive 2002/95/EC of the European Parliament and of the Council of 27 January 2003 on the restriction of the use of certain hazardous substances in electrical and electronic equipment
Directive 2002/95/EC	Directive 2002/95/EC of the European Parliament and of the council of 27 January 2003 on the restriction of the use of certain hazardous substances in electrical and electronic equipment.
Directive 2002/96/EC	Directive 2002/96/EC of the European Parliament and of the Council of 27 January 2003 on waste electrical and electronic equipment
Directive 2004/108/EC	Directive 2004/108/EC of the European Parliament and of the Council of 15 December 2004 on the approximation of the laws of the Member States relating to electromagnetic compatibility and repealing Directive 89/336/EEC
Directive 2006/95/EC	Directive 2006/95/EC of the European Parliament and of the council of 12 December 2006 on the harmonisation of the laws of Member States relating to electrical equipment designed for use within certain voltage limits
Directive 99/5/EC	Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity
EN 15509	EN 15509 Electronic Fee Collection – Interoperability application profile for DSRC
EN 16312	EN 16312 ITS – AVI/AEI – Interoperable application profile for AVI/AEI and Electronic Register Identification using dedicated short range communication
EN ISO 14906	EN ISO 14906 Road Transport and Traffic Telematics – Electronic Fee Collection – Application interface definition for dedicated short range communication
ETSI EN 300 674-2-2	ETSI EN 300 674-2-2 Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s / 250 kbit/s) operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band; Part 2: Harmonized EN under article 3.2 of the R&TTE Directive; Sub-part 2: Requirements for the On-Board Unit (OBU)
IEC 529	CEI IEC 529 Degrees of protection provided by enclosures (IP Code)

Reference	Full reference
IEC 60721-3-5	IEC 60721-3-5Classification of environmental conditions – Part 3: Classification of groups of environmental parameters and their severities – Section 5: Ground vehicle installations
ISO 1176	ISO 1176 Road vehicles -- Masses -- Vocabulary and codes
ISO 14814	ISO 14814:2006 Road transport and traffic telematics -- Automatic vehicle and equipment identification -- Reference architecture and terminology
ISO 14815	ISO 14815 Road transport and traffic telematics -- Automatic vehicle and equipment identification -- System specifications
ISO 17573	ISO 17573 Electronic Fee Collection – System architecture for vehicle related tolling
ISO 3166-1	ISO 3166-1 Codes for the representation of names of countries and their subdivisions – Part 1: Country codes
ISO 612	ISO 612 Road vehicles -- Dimensions of motor vehicles and towed vehicles -- Terms and definitions

4. System architecture

4.1. Roles and responsibilities with focus on the OBE lifetime

The AutoPASS EFC concept is based on the role and responsibilities model defined in ISO 17573. In line with the ISO standard the following roles and responsibilities are present in the AutoPASS EFC concept:

- The Toll Service Provider (In Norwegian: Utsteder)
- The User
- The Toll Charger (in Norwegian: Operatør)
- The interoperability Manager

In addition to the roles defined in ISO 17573 this specification also includes the following role:

- The OBE supplier
- The Trusted Third Party (TTP)

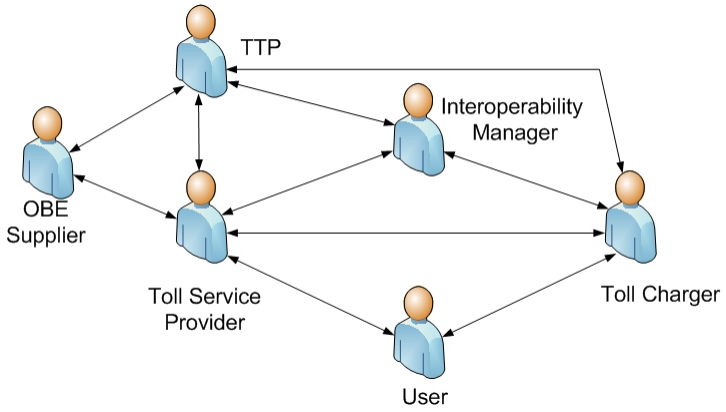

Figure 1 : The AutoPASS Role model for the OBE specification

The additional roles and their responsibilities regarding the OBE are described below. The ISO 17573 includes a complete description of the other roles and their responsibilities.

The OBE supplier

The responsibilities of this role include:

- Produce and deliver AutoPASS OBEs compliant with the AutoPASS specifications including replacing OBEs that do meet the lifetime requirements
- Initialise the OBE whenever requested by the Norwegian Public Roads Administration or Toll Service Provider

The Trusted Third Party (TTP)

The responsibilities of this role include:

- Providing security services to the Toll Service Provider (in this case the Norwegian Public Roads Administration) including:
    - Security key management

- Independent verification that the other actors have a sufficient level of security for interoperability.

4.2. Functional architecture

The functional architecture of the OBE is described by three use cases:

- Accept and store EFC and AVI/ERI attributes (Initialisation)
- Execute an EFC or AVI/ERI transaction (OBE – RSE communication)
- Maintain and update EFC or AVI/ERI attributes stored on the OBE

Accept and store EFC and AVI/ERI attributes

A prerequisite for the use case is that the OBE has got a memory that is already implemented and organised as defined in this specification. The OBE shall be initialised before the OBE is sent or given to the User. The OBE can be initialised by the OBE supplier or by the Transport Service Provider (TSP). In the first case the TSP provides the OBE supplier with the information that shall be written to the OBE. In the second case the TSP has its own initialisation equipment and writes the relevant information to the OBE. The relevant information may be collected from the AutoPASS Central system, The TSP Central system, national vehicle register or other sources.

The TSP may also make use of other actors for writing information to the OBE, e.g. TTP or certified service providers having specialised in OBE initialisation, as an alternative for OBE initialisation.

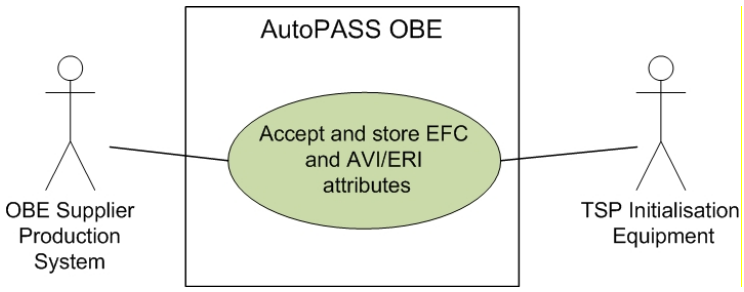

Figure 2 : The Initialisation use case

Execute an EFC or AVI/ERI transaction

The OBE communicates with the Toll Charger Roadside Equipment (RSE) as defined in EN ISO 14906, EN 15509 and EN 16312. Depending on the application and information element in the OBE the communication will be with or without access control to the EFC or AVI attributes stored in the OBE.

The OBE may communicate the result of the EFC transaction to the User (driver), e.g. OK, Not OK (NOK) or Contact the TSP.

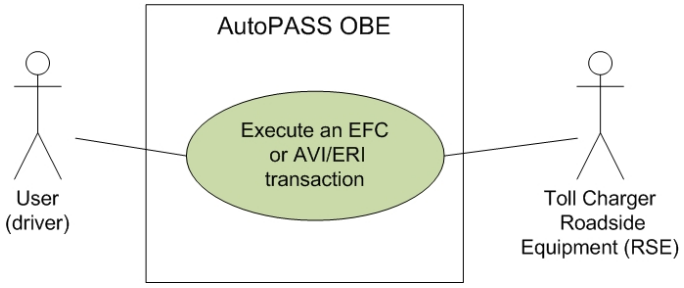

Figure 3 : The EFC/AVI/ERI transaction execution use case

Maintain and update EFC or AVI/ERI attributes stored on the OBE

The EFC and AVI/ERI attributes stored on the OBE may be subject to maintenance and/or updating, e.g. if the OBE carries vehicle related information and the OBE is moved from one vehicle to another or if there is a need for storing specific vehicle related information in specific tolling domains, e.g. charging in Low Emission Zones.

The use case will be different from the initialisation use case as the information on the OBE will be provided and written to the OBE by the TSP or a certified organisation.

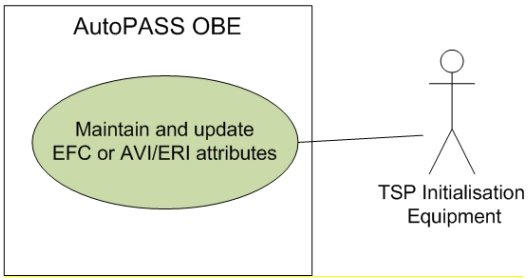

Figure 4 : The OBE information updating use case

4.3. Physical architecture

The physical architecture of the AutoPASS EFC system is shown in the figure below. This specification covers the OBE and the interface to the RSE and the OBE initialisation equipment marked with red in the figure.

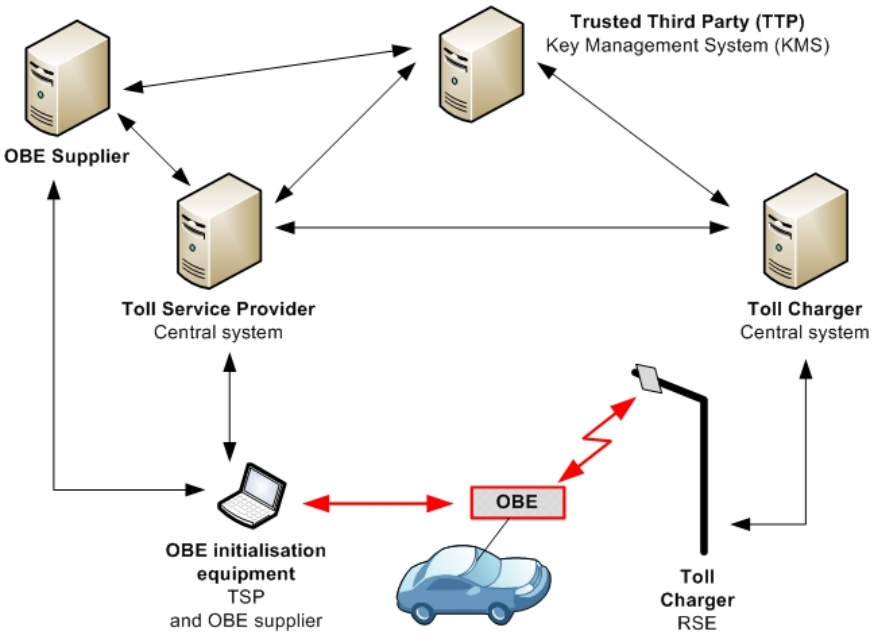

Figure 5 : The physical architecture

4.4. Information architecture

The information architecture is based on the EN ISO 14906, EN 15509 and EN 16312. The OBE shall support both the EFC, Parking, Automatic Vehicle Identification and Electronic Register Identification (AVI/ERI) and one private ITS application. The EFC application will have 2 elements for storing EFC attributes (EID=01 and EID=02). The private ITS application (owned by the Norwegian Public Roads Administration) will have one element (EID=03) and the Parking application will have one element (EID=04). The AVI/ERI application will have 1 element for the AVI/ERI attributes, see Figure 6. The Norwegian Public Roads Administration will be the owner of and responsible for the information stored on the OBE.

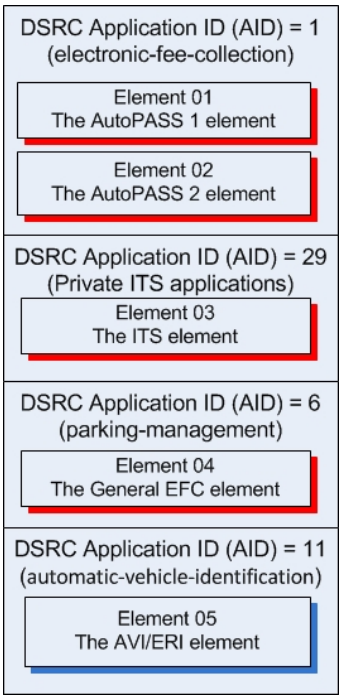

Figure 6 : OBE elements

Element 01 (the AutoPASS 1 element)

The element 01 will only be used by RSE installed in road user charging system, low emission zones charging and congestion charging system. There will be access control to the EFC attributes in the element in line with Security Level 1 in EN 15509 as recommended for EETS systems in ISO/TS 19299 EFC Security Framework.

Element 02 (the AutoPASS 2 element)

The element 02 is reserved for future use, e.g. other types of Road User Charging systems or EFC for ferries. There will be access control to the EFC attributes in the element in line with Security Level 1 in EN 15509.

Element 03 (the ITS element)

Element 03 will only store one ID without any relation to any EFC system. For privacy reasons there will be no relationship between the EFC attributes in the Element 01 and 02 and the Element 03. The ID will be used by the Norwegian Public Roads Administration (NPRA) for collection of traffic data, e.g. average speeds for traffic information systems or origin-destination matrixes for transport planning purposes. The ID will also be available for other ITS applications and ITS services for actors or service providers that have an agreement with NPRA enabling them to build applications or services based on the unique ID that can be read by RSEs without access credentials.

Element 04 (the Parking or general EFC element)

The elements 04 will be allocated for future payment services related to different types of transport services, e.g. parking, petrol or traffic information services. The element is also called the Parking element as the Application ID = 6.

Element 05 (Automatic Vehicle Identification (AVI) and Electronic Register Identification (ERI))

Element 05 is used by the AVI/ERI application in line with EN 16312. The AVI/ERI attributes in the element will be controlled by the use of access credentials. The AVI attributes will be used by the NPRA for vehicle controls enabling the vehicle control personnel to use the information read directly or to use the information as links to national or international vehicle registers.

4.5. Security

The EN 15509 AutoPASS OBE will adhere to the security requirements in EN 15509 and ISO/TS 19299.

Security Level 1 will be implemented for the AutoPASS 1 and 2 elements storing the crucial EFC attributes used for tolling, road pricing, etc. This implies that the AutoPASS OBE will require valid access credentials from the RSE enabling access to the EFC attributes in the OBE. Security level 1 will also be implemented for the parking element 04 and AVI/ERI element 05.

In addition, all element shall contain a security key for initialisation. The security key for initialisation key enables access to a method to change any value of any attribute in that element.

The security keys for all elements in the OBE will unless otherwise stated be supplied, owned and managed by the Norwegian Public Roads Administration on behalf of Norwegian Toll Service Providers and Norwegian Toll Chargers .

5. Data requirements

5.1. General

[R 1] The Customer will supply the master security keys and initialisation data for all elements in the OBE.

[R 2] The value AC_CR_keyref shall be the same for all elements. AC_CR_Keyref for all elements shall be equal to RndItsId (RndItsId is AttrID=87 in Element 3) see [R 7] and [R 8].

NOTE 1. This requirement is set so that no OBU can be uniquely identified based on publicly readable information and fulfil the requirements of the Norwegian Data Inspectorate concerning privacy.

NOTE 2. AC_CR_Keyref defines which access keys are used to authenticate the RSE see e.g. EN 15509.

[R 3] All elements shall include an initialisation key that enables write access to all attributes in that element.

NOTE 3. The write access to all attributes includes write access to the initialisation key attribute.

NOTE 4. The Initialisation key is not included in the tables in section 5.3 Element encoding

5.2. Element specification

5.2.1. The AutoPASS 1 element (AID = 1, EID = 1)

[R 4] The AutoPASS 1 element shall be organised and include the data attributes as shown in Figure 7.

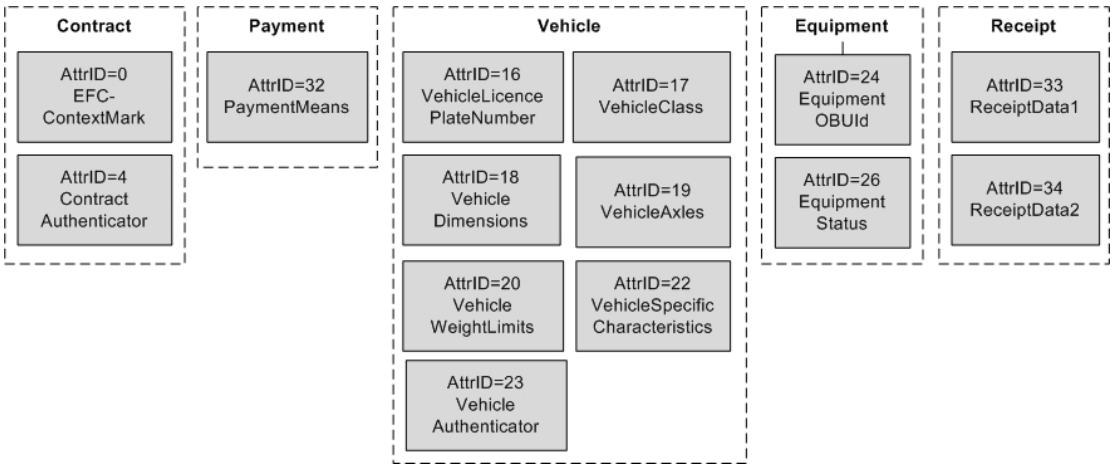

Figure 7 : AutoPASS 1 element

5.2.2. The AutoPASS 2 element (AID = 1, EID = 2)

[R 5] The AutoPASS 2 element shall be organised and include the data attributes as shown in Figure 8.

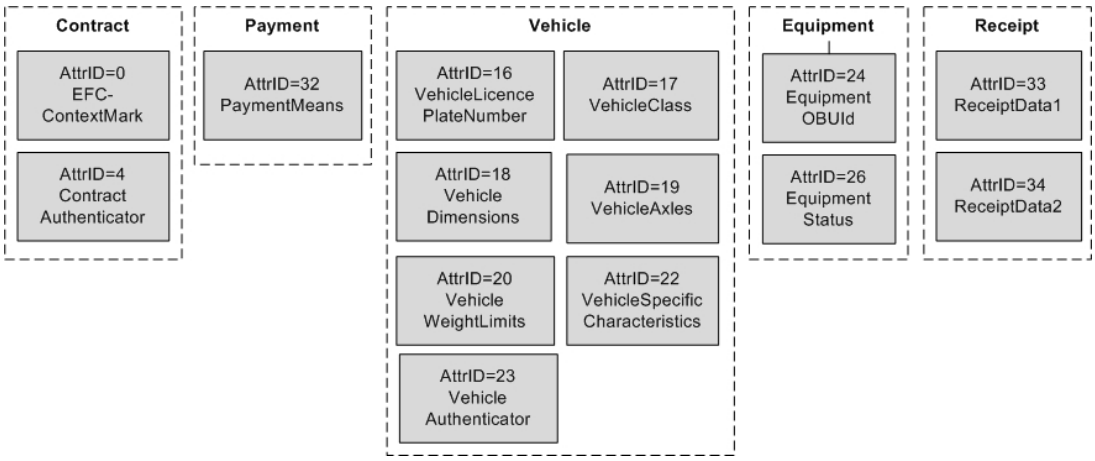

Figure 8 : AutoPASS 2 element

5.2.3. The ITS element (AID = 29, EID = 3)

[R 6] The ITS element shall be organised and include the data attributes as shown in Figure 9.

[R 7] The value of AttrID=87 shall be a random number between 0 and 32767 (0x0000 and 0x7FFF in hexadecimal).

[R 8] For each value for RndItsId there shall be 5 OBUs produced which have the same value for RndItsId. (Within the same production batch).

NOTE 5. The upper range for RndItsId (currently set to 49 151) and privacy sets (currently set to 5) might be subject to change.

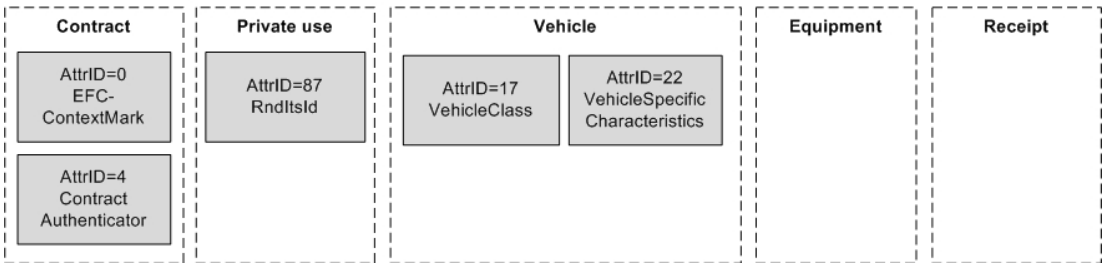

Figure 9 ITS element EID = 3

5.2.4. The Parking (General EFC) element (AID = 6, EID = 4)

[R 9] The General EFC element shall be organised and include the data attributes as shown in Figure 10.

NOTE 6. The AID=6 for the DSRC application Parking has been used as the main purpose and use of the element will be Parking. However, in lack of a DSRC application standard for parking, like the EN ISO 14906 for EFC, the attributes defined in EN ISO 14906 have also been used for the Parking element.

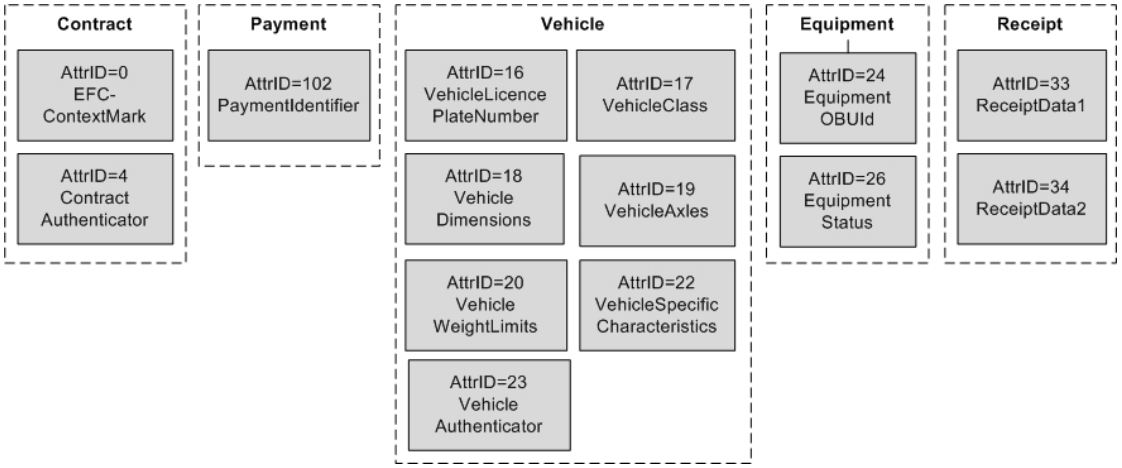

Figure 10 EFC element EID = 4

5.2.5. The AVI/ERI element (AID = 11, EID = 5)

[R 10] The AVI/ERI element shall be organised and include the data attributes as shown in Figure 11.

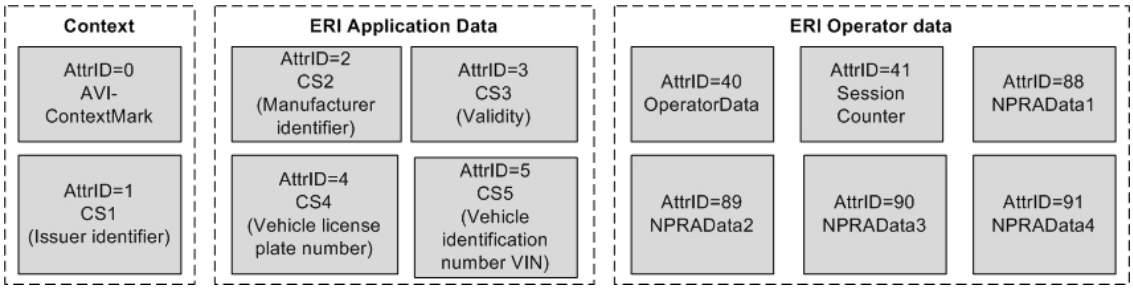

Figure 11 : AVI/ERI element EID = 5

5.3. Element coding

AID=1 (electronic-fee-collection), EID=1 (AutoPASS 1)			
AttrID	***Attribute***	***Bits in octet***	***Description and comments***
0	EFC-ContextMark 6 octets, read only	0011 0000	ContractProvider CountryCode, NO (Norway) as coded in EN ISO 14816, ITA-2 alphabet, IssuerIdentifier as assigned by Standards Norway
		11	
		xx xxxx	
		xxxx xxxx	
		0000 0000	TypeOfContract = 1 (AutoPASS 1)
		0000 0001	
		0000 0010	ContextVersion = 2 (first generation of 15509 OBEs)
4	ContractAuthenticator 5 octets (1+4), read only	0000 0100	Octet string size 4
		0000 0000	The contract authenticator is at the disposal for the Toll Service Providers (issuers) but will not be used in the Context version = 2
		0000 0000	
		0000 0000	
		0000 0000	
16	VehicleLicensePlateNumber 17 octets, read only	0011 0000	CountryCode, NO (Norway) as coded in EN ISO 14816, ITA-2 alphabet
		11	
		00 0000	Alphabet indicator = 0 LatinAlphabetNo1
		0000 1110	Length indicator = 14
		0000 0000	An LPN shorter than 14 characters is padded with NUL characters so as to achieve a total of 14 octets
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
17	VehicleClass 1 octet, read only	0000 0000	Not to be used in context version = 2 Future option for coding: 0001 0000 'B "Light vehicle" – UNECE class M1 small passenger vehicles ***and*** Norwegian local class Light vehicle 0111 0001' B "Heavy vehicles (European MoU) Other vehicles including vehicles above 3,5 t not included in previous groups ***and*** Norwegian local class Heavy Vehicle
18	VehicleDimensions 3 octets, read only	0000 0000	vehicleLengthOverall
		0000 0000	vehicleHeightOverall
		0000 0000	vehicleWidthOverall
19	VehicleAxles 2 octets, read only	0000 0000	VehicleFirstAxleHeight
		00	tyreType (VehicleAxleNumber)
		00 0	Number of axles of the trailer (VehicleAxleNumber)
		000	Number of axles of the tractor (VehicleAxleNumber)
20	VehicleWeightLimits 6 octets, read only	0000 0000	VehicleMaxLadenWeight
		0000 0000	
		0000 0000	VehicleTrainMaximumWeight
		0000 0000	
		0000 0000	VehicleWeightUnladen
		0000 0000	

AID=1 (electronic-fee-collection), EID=1 (AutoPASS 1)			
AttrID	***Attribute***	***Bits in octet***	***Description and comments***
22	VehicleSpecificCharacteristics 4 octets, read only	0000	Euro classes as defined in EC Directive 88/77/EEC and others
		0000	COP values as defined in EC Directive 2003/127/EC
		0000 0000	EngineCharacteristics
		0000 0000	DescriptiveCharacteristics
		0000 0000	FutureCharacteristics
23	VehicleAuthenticator 5 octets (1+4), read only	0000 0100	Length indicator = 4
		0000 0000	The vehicle authenticator is at the disposal for the Toll Service Providers (issuers) but will not be used in the Context version = 2
		0000 0000	
		0000 0000	
		0000 0000	
24	EquipmentOBUId 5 octets (1+4), read only	0000 0100	Length indicator = 4
		xxxx xxxx	OBE Identifier according to Manufacturer unique numbering scheme
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
26	EquipmentStatus 2 octets, read write	0000	Local use, coding and use at the discretion of the Toll Charger
		0000	Transaction Counter
		0000 0000	
32	PaymentMeans 14 octets, read only	xxxx xxxx	Personal Account Number (PAN) PAN = 9.578.XXXX.AAAAAAA.L where MII = 9_{10}, 578_{10} is country code for Norway and $XXXX_{10}$ is the Toll Service Provider (Issuer) identifier as assigned by Standards Norway. Please observe that XXXX is 4 digits in line with 7812-1, A.5 National schemes using Issuer Identification Number (IIN) greater than 6 digits. $AAAAAAA_{10}$ is the Individual Account Identification and L_{10} is the Check Digit. PAN is padded to achieve 10 octets.
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
		0000 0000	PaymentMeansExpiryDate (DateCompact)
		0000 0000	
		0000 0000	PaymentUsageControl
		0000 0000	
33	ReceiptData1 28 octets, read write	0000 0000	Session time according to EN ISO 14906
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	Session Service Provider
		0000 0000	
		0000 0000	
		0000 0000	Station location
		0000 0000	
		0000 0000	Session location
		0000 0000	Session type
		0000 0000	Session result
		0000 0000	Session tariff class
		0000 0000	Session claimed class
		0000 0000	Session fee
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	Session Contract Provider
		0000 0000	
		0000 0000	
		0000 0000	Session type of contract
		0000 0000	
		0000 0000	Session Context version
		0000 0000	Receipt authenticator
		0000 0000	
		0000 0000	

AID=1 (electronic-fee-collection), EID=1 (AutoPASS 1)			
AttrID	***Attribute***	***Bits in octet***	***Description and comments***
		0000 0000	
34	ReceiptData2 28 octets, read write	0000 0000	Session time according to EN ISO 14906
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	Session Service Provider
		0000 0000	
		0000 0000	
		0000 0000	Station location
		0000 0000	
		0000 0000	Session location
		0000 0000	Session type
		0000 0000	Session result
		0000 0000	Session tariff class
		0000 0000	Session claimed class
		0000 0000	Session fee
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	Session Contract Provider
		0000 0000	
		0000 0000	
		0000 0000	Session type of contract
		0000 0000	Session Context version
		0000 0000	Receipt authenticator
		0000 0000	
		0000 0000	
		0000 0000	
111	AuthenticationKey1-EID1 No access	XXXX XXXX	Key derivation according to EN 15509 Annex B.4.2
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
112	AuthenticationKey2-EID1 No access	XXXX XXXX	Key derivation according to EN 15509 Annex B.4.2
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
113	AuthenticationKey3-EID1 No access	XXXX XXXX	Key derivation according to EN 15509 Annex B.4.2
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
114	AuthenticationKey4-EID1 No access	XXXX XXXX	Key derivation according to EN 15509 Annex B.4.2
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	

AID=1 (electronic-fee-collection), EID=1 (AutoPASS 1)			
AttrID	***Attribute***	***Bits in octet***	***Description and comments***
115	AuthenticationKey5-EID1 No access	xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx	Key derivation according to EN 15509 Annex B.4.2
116	AuthenticationKey6-EID1 No access	xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx	Key derivation according to EN 15509 Annex B.4.2
117	AuthenticationKey7-EID1 No access	xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx	Key derivation according to EN 15509 Annex B.4.2
118	AuthenticationKey8-EID1 No access	xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx	Key derivation according to EN 15509 Annex B.4.2
120	AccessKey-EID1 No access	xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx	Key derivation according to EN 15509 Annex B.4.3

AID=1 (electronic-fee-collection), EID=2 (AutoPASS 2)			
AttrID	***Attribute***	***Bits in octet***	***Description and comments***
0	EFC-ContextMark 6 octets, read only	0011 0000	ContractProvider
		11	CountryCode, NO (Norway) as coded in EN ISO 14816, ITA-2 alphabet,
		xx xxxx	
		xxxx xxxx	IssuerIdentifier as assigned by Standards Norway
		0000 0000	TypeOfContract = 2 (AutoPASS 2)
		0000 0010	
		0000 0010	ContextVersion = 2 (first generation of 15509 OBEs)
4	ContractAuthenticator 5 octets (1+4), read only	0000 0100	Octet string size 4
		0000 0000	The contract authenticator is at the disposal for the Toll Service Providers (issuers) but will not be used in the Context version = 2
		0000 0000	
		0000 0000	
		0000 0000	
16	VehicleLicensePlateNumber 17 octets, read only	0011 0000	CountryCode, NO (Norway) as coded in EN ISO 14816, ITA-2 alphabet
		11	
		00 0000	Alphabet indicator = 0 LatinAlphabetNo1
		0000 1110	Length indicator = 14
		0000 0000	An LPN shorter than 14 characters is padded with NUL characters so as to achieve a total of 14 octets
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
17	VehicleClass 1 octet, read only	0000 0000	Not to be used in context version = 2 Future option for coding: 0001 0000 'B "Light vehicle" – UNECE class M1 small passenger vehicles ***and*** Norwegian local class Light vehicle 0111 0001' B "Heavy vehicles (European MoU) Other vehicles including vehicles above 3,5 t not included in previous groups ***and*** Norwegian local class Heavy Vehicle
18	VehicleDimensions 3 octets, read only	0000 0000	vehicleLengthOverall
		0000 0000	vehicleHeightOverall
		0000 0000	vehicleWidthOverall
19	VehicleAxles 2 octets, read only	0000 0000	VehicleFirstAxleHeight
		00	tyreType (VehicleAxleNumber)
		00 0	Number of axles of the trailer (VehicleAxleNumber)
		000	Number of axles of the tractor (VehicleAxleNumber)
20	VehicleWeightLimits 6 octets, read only	0000 0000	VehicleMaxLadenWeight
		0000 0000	
		0000 0000	VehicleTrainMaximumWeight
		0000 0000	
		0000 0000	VehicleWeightUnladen
		0000 0000	
22	VehicleSpecificCharacteristics 4 octets, read only	0000	Euro classes as defined in EC Directive 88/77/EEC and others
		0000	COP values as defined in EC Directive 2003/127/EC
		0000 0000	EngineCharacteristics
		0000 0000	DescriptiveCharacteristics
		0000 0000	FutureCharacteristics
23	VehicleAuthenticator	0000 0100	Length indicator = 4
		0000 0000	
		0000 0000	

AID=1 (electronic-fee-collection), EID=2 (AutoPASS 2)			
AttrID	***Attribute***	***Bits in octet***	***Description and comments***
	5 octets (1+4), read only	0000 0000	The vehicle authenticator is at the disposal for the Toll Service Providers (issuers) but will not be used in the Context version = 2
		0000 0000	
24	EquipmentOBUId	0000 0100	Length indicator = 4
		xxxx xxxx	OBE Identifier according to Manufacturer unique numbering scheme
		xxxx xxxx	
	5 octets (1+4), read only	xxxx xxxx	
		xxxx xxxx	
26	EquipmentStatus	0000	Local use, coding and use at the discretion of the Toll Charger
	2 octets, read write	0000	Transaction Counter
		0000 0000	
32	PaymentMeans	xxxx xxxx	Personal Account Number (PAN) PAN = 9.578.XXXX.AAAAAAA.L where MII = 9_{10}, 578_{10} is country code for Norway and $XXXX_{10}$ is the Toll Service Provider (Issuer) identifier as assigned by Standards Norway. Please observe that XXXX is 4 digits in line with 7812-1, A.5 National schemes using Issuer Identification Number (IIN) greater than 6 digits. $AAAAAAA_{10}$ is the Individual Account Identification and L_{10} is the Check Digit. PAN is padded with 2 octets containing fillbits to achieve 10 octets.
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
	14 octets, read only	xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
		0000 0000	PaymentMeansExpiryDate (DateCompact)
		0000 0000	
		0000 0000	PaymentUsageControl
		0000 0000	
33	ReceiptData1	0000 0000	Session time according to EN ISO 14906
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	Session Service Provider
		0000 0000	
		0000 0000	
	28 octets, read write	0000 0000	Station location
		0000 0000	
		0000 0000	Session location
		0000 0000	Session type
		0000 0000	Session result
		0000 0000	Session tariff class
		0000 0000	Session claimed class
		0000 0000	Session fee
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	Session Contract Provider
		0000 0000	
		0000 0000	
		0000 0000	Session type of contract
		0000 0000	
		0000 0000	Session Context version
		0000 0000	Receipt authenticator
		0000 0000	
		0000 0000	
		0000 0000	

AID=1 (electronic-fee-collection), EID=2 (AutoPASS 2)			
AttrID	***Attribute***	***Bits in octet***	***Description and comments***
34	ReceiptData2 28 octets, read write	0000 0000	Session time according to EN ISO 14906
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	Session Service Provider
		0000 0000	
		0000 0000	
		0000 0000	Station location
		0000 0000	
		0000 0000	Session location
		0000 0000	Session type
		0000 0000	Session result
		0000 0000	Session tariff class
		0000 0000	Session claimed class
		0000 0000	Session fee
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	Session Contract Provider
		0000 0000	
		0000 0000	
		0000 0000	Session type of contract
		0000 0000	
		0000 0000	Session Context version
		0000 0000	Receipt authenticator
		0000 0000	
		0000 0000	
		0000 0000	
111	AuthenticationKey1-EID2 No access	XXXX XXXX	Key derivation according to EN 15509 Annex B.4.2
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
112	AuthenticationKey2-EID2 No access	XXXX XXXX	Key derivation according to EN 15509 Annex B.4.2
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
113	AuthenticationKey3-EID2 No access	XXXX XXXX	Key derivation according to EN 15509 Annex B.4.2
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
114	AuthenticationKey4-EID2 No access	XXXX XXXX	Key derivation according to EN 15509 Annex B.4.2
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	

AID=1 (electronic-fee-collection), EID=2 (AutoPASS 2)			
AttrID	***Attribute***	***Bits in octet***	***Description and comments***
115	AuthenticationKey5-EID2 No access	xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx	Key derivation according to EN 15509 Annex B.4.2
116	AuthenticationKey6-EID2 No access	xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx	Key derivation according to EN 15509 Annex B.4.2
117	AuthenticationKey7-EID2 No access	xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx	Key derivation according to EN 15509 Annex B.4.2
118	AuthenticationKey8-EID2 No access	xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx	Key derivation according to EN 15509 Annex B.4.2
120	AccessKey-EID2 No access	xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx	Key derivation according to EN 15509 Annex B.4.3

AID=29 (Private Application Identifier = ITS) , EID=3 (ITS)			
AttrID	***Attribute***	***Bits in octet***	***Description and comments***
0	ITS-ContextMark 6 octets, read only	0011 0000	ContractProvider CountryCode, NO (Norway) as coded in EN ISO 14816, ITA-2 alphabet, IssuerIdentifier = 99 (Norwegian Public Roads Administration) as assigned by Standards Norway
		11	
		00 0000	
		0110 0011	
		0000 0000	TypeOfContract = 3 (ITS)
		0000 0011	
		0000 0010	ContextVersion = 2 (first generation of 15509 OBEs)
4	ContractAuthenticator 5 octets (1+4), read only	0000 0100	Octet string size (4)
		0000 0000	The contract authenticator is at the disposal for the Norwegian Public Roads Administration (Issuer) but will not be used in the Context version = 2
		0000 0000	
		0000 0000	
		0000 0000	
17	VehicleClass 1 octet, read only	0000 0000	Not to be used in context version = 2 Future option for coding: 0001 0000 'B "Light vehicle" – UNECE class M1 small passenger vehicles ***and*** Norwegian local class Light vehicle 0111 0001' B "Heavy vehicles (European MoU) Other vehicles including vehicles above 3,5 t not included in previous groups ***and*** Norwegian local class Heavy Vehicle
22	VehicleSpecificCharacteristics 4 octets, read only	0000	Euro classes as defined in EC Directive 88/77/EEC and others
		0000	COP values as defined in EC Directive 2003/127/EC
		0000 0000	EngineCharacteristics
		0000 0000	DescriptiveCharacteristics
		0000 0000	FutureCharacteristics
87	RndITS Private attribute 4 octets (1+3), read only	0000 0011	Length indicator, octet string size (3), read only
		xxxx xxxx	Random number to be used by ITS applications. The number is generated when the OBE is initialised and the value shall not be registered in any database for OBEs or Users. Generation of RndITS as specified in the AutoPASS OBE specification. See [R 8] and [R 9].
		xxxx xxxx	
		xxxx xxxx	

AID=6 (parking-management), EID=4 (General EFC)			
AttrID	***Attribute***	***Bits in octet***	***Description and comments***
0	EFC-ContextMark 6 octets, read only	0011 0000	ContractProvider CountryCode, NO (Norway) as coded in EN ISO 14816, ITA-2 alphabet, IssuerIdentifier = 99 (Norwegian Public Roads Administration) as assigned by Standards Norway
		11	
		00 0000	
		0110 0011	
		0000 0100	TypeOfContract = 4 (General EFC) Used for EFC payment for different types of transport services, e.g. parking
		0000 0001	
		0000 0010	ContextVersion = 2 (first generation of 15509 OBEs)
4	ContractAuthenticator 5 octets (1+4), read only	0000 0100	Octet string size 4
		0000 0000	The contract authenticator is at the disposal for the EFC system operators (issuers) but will not be used in the Context version = 2
		0000 0000	
		0000 0000	
		0000 0000	
16	VehicleLicensePlateNumber 17 octets, read only	0011 0000	CountryCode, NO (Norway) as coded in EN ISO 14816, ITA-2 alphabet
		11	
		00 0000	Alphabet indicator = 0 LatinAlphabetNo1
		0000 1110	Length indicator = 14
		0000 0000	An LPN shorter than 14 characters is padded with NUL characters so as to achieve a total of 14 octets
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
17	VehicleClass 1 octet, read only	0000 0000	Not to be used in context version = 2 Future option for coding: 0001 0000 'B "Light vehicle" – UNECE class M1 small passenger vehicles ***and*** Norwegian local class Light vehicle 0111 0001' B "Heavy vehicles (European MoU) Other vehicles including vehicles above 3,5 t not included in previous groups ***and*** Norwegian local class Heavy Vehicle
18	VehicleDimensions 3 octets, read only	0000 0000	vehicleLengthOverall
		0000 0000	vehicleHeightOverall
		0000 0000	vehicleWidthOverall
19	VehicleAxles 2 octets, read only	0000 0000	VehicleFirstAxleHeight
		00	tyreType (VehicleAxleNumber)
		00 0	Number of axles of the trailer (VehicleAxleNumber)
		000	Number of axles of the tractor (VehicleAxleNumber)
20	VehicleWeightLimits 6 octets, read only	0000 0000	VehicleMaxLadenWeight
		0000 0000	
		0000 0000	VehicleTrainMaximumWeight
		0000 0000	
		0000 0000	VehicleWeightUnladen
		0000 0000	
22	VehicleSpecificCharacteristics 4 octets, read only	0000	Euro classes as defined in EC Directive 88/77/EEC and others
		0000	COP values as defined in EC Directive 2003/127/EC
		0000 0000	EngineCharacteristics
		0000 0000	DescriptiveCharacteristics
		0000 0000	FutureCharacteristics
23	VehicleAuthenticator	0000 0100	Length indicator = 4
		0000 0000	

AID=6 (parking-management), EID=4 (General EFC)			
AttrID	***Attribute***	***Bits in octet***	***Description and comments***
	5 octets (1+4), read only	0000 0000	The vehicle authenticator is at the disposal for the Toll Service Providers (issuers) but will not be used in the Context version = 2
		0000 0000	
		0000 0000	
24	EquipmentOBUId 5 octets (1+4), read only	0000 0100	Length indicator = 4
		xxxx xxxx	OBE Identifier according to Manufacturer unique numbering scheme
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
26	EquipmentStatus 2 octets, read write	0000	Local use, coding and use at the discretion of the Toll Charger
		0000	Transaction Counter
		0000 0000	
33	ReceiptData1 28 octets, read only	0000 0000	Session time according to EN ISO 14906
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	Session Service Provider
		0000 0000	
		0000 0000	
		0000 0000	Station location
		0000 0000	
		0000 0000	Session location
		0000 0000	Session type
		0000 0000	Session result
		0000 0000	Session tariff class
		0000 0000	Session claimed class
		0000 0000	Session fee
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	Session Contract Provider
		0000 0000	
		0000 0000	
		0000 0000	Session type of contract
		0000 0000	
		0000 0000	Session Context version
		0000 0000	Receipt authenticator
		0000 0000	
		0000 0000	
		0000 0000	
34	ReceiptData2 28 octets, read only	0000 0000	Session time according to EN ISO 14906
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	Session Service Provider
		0000 0000	
		0000 0000	
		0000 0000	Station location
		0000 0000	
		0000 0000	Session location
		0000 0000	Session type
		0000 0000	Session result
		0000 0000	Session tariff class
		0000 0000	Session claimed class
		0000 0000	Session fee
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	

AID=6 (parking-management), EID=4 (General EFC)			
AttrID	***Attribute***	***Bits in octet***	***Description and comments***
		0000 0000	Session Contract Provider
		0000 0000	Session type of contract
		0000 0000	
		0000 0000	Session Context version
		0000 0000	Receipt authenticator
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0110	Length indicator, Octet string (6), Read only
102	PaymentIdentifier *(replaces AttrID 32 PaymentMeans)* *Private attribute* 1+6 octets, read only	xxxx xxxx	Payment Identifier Concatenation of ManufacturerId (2 octets) and EquipmentOBUId (4 octets, see AttrId 24) To be padded with 00 00'H to achieve 8 octets when used for AuthenticationKey calculation: MM MM NN NN NN NN 00 00'H
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
111	AuthenticationKey1-EID4 No access	xxxx xxxx	Key derivation based on EN 15509 Annex B.4.2 using element 102 (Payment Identifier) instead of element 32 (PAN)
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
112	AuthenticationKey2-EID4 No access	xxxx xxxx	Key derivation based on EN 15509 Annex B.4.2 using element 102 (Payment Identifier) instead of element 32 (PAN)
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
113	AuthenticationKey3-EID4 No access	xxxx xxxx	Key derivation based on EN 15509 Annex B.4.2 using element 102 (Payment Identifier) instead of element 32 (PAN)
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
114	AuthenticationKey4-EID4 No access	xxxx xxxx	Key derivation based on EN 15509 Annex B.4.2 using element 102 (Payment Identifier) instead of element 32 (PAN)
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	
		xxxx xxxx	

AID=6 (parking-management), EID=4 (General EFC)			
AttrID	***Attribute***	***Bits in octet***	***Description and comments***
115	AuthenticationKey5-EID4 No access	XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX	Key derivation based on EN 15509 Annex B.4.2 using element 102 (Payment Identifier) instead of element 32 (PAN)
116	AuthenticationKey6-EID4 No access	XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX	Key derivation based on EN 15509 Annex B.4.2 using element 102 (Payment Identifier) instead of element 32 (PAN)
117	AuthenticationKey7-EID4 No access	XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX	Key derivation based on EN 15509 Annex B.4.2 using element 102 (Payment Identifier) instead of element 32 (PAN)
118	AuthenticationKey8-EID4 No access	XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX	Key derivation based on EN 15509 Annex B.4.2 using element 102 (Payment Identifier) instead of element 32 (PAN)
120	AccessKey-EID4 No access	XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX	Key derivation according to EN 15509 Annex B.4.3

AID=11 (automatic-vehicle-identification), EID=5 (AVI/ERI)			
AttrID	***Attribute***	***Bits in octet***	***Description and comments***
0	AVI-ContextMark 3 octets, read only	0000 0000	aVIProfile = 12 , ref. EN 16312, 5.1.7
		0000 1100	
		0000 0001	profileVersion = 1 first version
1	CS1- AVI/AEI Numbering scheme 7 octets, read only	0011 0000	CountryCode, NO (Norway) as coded in EN ISO 14816, ITA-2 alphabet, *Used for security mechanisms.*
		11	
		00 0000	IssuerIdentifier = 99 (Norwegian Public Roads Administration) as assigned by Standards Norway. *Used for security mechanisms.*
		0110 0011	
		XXXX XXXX	ServiceNumber as defined by the Norwegian Public Roads Administration
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
2	CS2 – Manufacturers numbering 6 octets, read only	XXXX XXXX	Manufacturer Identifier as assigned by NEN
		XXXX XXXX	
		XXXX XXXX	ServiceNumber (0….4.294.967.295) as defined by the Manufacturer and described in EN 16312. *Used for security mechanisms.*
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
3	CS3 – Validity limitations 22 octets, read only	XXXX XXXX	Start time = UTCtime Format YYMMDDhhmm Time for OBE production Example: April 2, 2014 12:34 1404021234
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	Stop time = UTCtime Format YYMMDDhhmm Time for OBE production + 15 years
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		0000 0000	GeoGraphicalLimit = 0, no geographical limitation
		0000 0000	ServiceApplicationLimit, all 0's = no restrictions
4	CS4 – Vehicle License Number 17 octets, read only	0011 0000	CountryCode, NO (Norway) as coded in EN ISO 14816, ITA-2 alphabet
		11	
		00 0000	Alphabet indicator = 0 LatinAlphabetNo1
		0000 1110	Length indicator = 14
		0000 0000	License Plate Number (LPN) An LPN shorter than 14 characters is padded with 0's to achieve a total of 14 octets
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	

AID=11 (automatic-vehicle-identification), EID=5 (AVI/ERI)			
AttrID	***Attribute***	***Bits in octet***	***Description and comments***
5	CS5 – Vehicle Identification Number (VIN) AVI Container type 23 17 octets, type VISIBLE STRING read only	0001 0001	Length indicator = 17 in a VisibleString with PER coding
		0000 0000	17 x 7 bits defining the 17 characters in VIN = 119 bits which equals 14 octets and 7 bits
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	Padding with zeroes to have 17 octets
		0000 0000	
		0000 0000	
40	OperatorData 20 octets, read write	0001 0100	Length indicator = 20
		0000 0000	General ERI Data structure to be read and written
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
41	SessionCounter 2 octets, read write	0000 0010	Length indicator = 2
		0000 0000	Part of security requirements as defined in EN 16312
		0000 0000	
		xxxx xxxx	
88	NPRAData1 *Private attribute* 9 octets (1+8)	0000 1000	Length indicator, Octet string (8), read only
		0000 0000	Any Norwegian Public Roads Administration (NPRA) specific data
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
89	NPRAData2 *Private attribute* 9 octets (1+8)	0000 1000	Length indicator, Octet string (8), read only
		0000 0000	Any NPRA specific data
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	

AID=11 (automatic-vehicle-identification), EID=5 (AVI/ERI)			
AttrID	***Attribute***	***Bits in octet***	***Description and comments***
90	NPRAData3 *Private attribute* 9 octets (1+8)	0000 1000	Length indicator, Octet string (8), read write
		0000 0000	Any NPRA specific data
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
91	NPRAData4 *Private attribute* 9 octets (1+8)	0000 1000	Length indicator, Octet string (8), read write
		0000 0000	Any NPRA specific data
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
		0000 0000	
111	AuthenticationKey1-EID5 No access	XXXX XXXX	Key derivation according to EN 16312, Annex D
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
112	AuthenticationKey2-EID5 No access	XXXX XXXX	Key derivation according to EN 16312, Annex D
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
120	AccessKey-EID5 No access	XXXX XXXX	Key derivation according to EN 16312, Annex D
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	
		XXXX XXXX	

6. Functional requirements

6.1. DSRC requirements

[R 11] The OBE shall comply with the DSRC requirements in EN 15509

[R 12] The OBE shall comply with the DSRC requirements in EN 16312.

[R 13] The OBE shall comply with the DSRC L7 and EFC functions in EN 15509.

[R 14] The OBE shall comply with the DSRC L7 and ERI functions in EN 16312.

6.2. Initialisation requirements

[R 15] The OBE shall be initialised with the elements and attributes as organised and defined in section 5 Data requirements enabling values to be written to the different attributes in the different elements.

[R 16] The OBE shall be initialised with the security keys and Security related data as defined in Security requirements in EN 15509 and EN 16312.

[R 17] The OBE shall control access to the different elements by requesting an Element Access Key (EAK) as defined in EN 15509 and EN 16312 for all elements using security level 1.

[R 18] The OBE shall enable initialisation to take place via a secure DSRC interface based on the DSRC communication. The initialisation mechanism shall use SET_SECURE as defined in ISO EN 14906 and AES-128 for security calculations (see [R 19]).

NOTE 7. The security mechanism for initialisation shall be harmonised with the work on personalisation interface in CEN/TC278/WG1 and ISO/TC204/WG5.

[R 19] The OBE shall enable an authorised entity in possession of Element Initialisation Key (EIK) to change (read, delete, write) any value in any attribute in that element.

NOTE 8. Security keys must not be readable.

[R 20] The OBE attributes shall have the values defined in section 5.3 when delivered from the OBE supplier.

[R 21] The obeStatus being part of the ObeConfiguration sent in VST shall be initialised with 0000 0000 0000 0000 'B.

[R 22] All 16 bits in obeStatus for the AutoPASS OBE application shall not be changed from the value 0 during the OBE lifetime except bit 5 in the first octet, ref. ISO 14906, that is used for setting the flag 'Low battery' as defined in [R 65] .

6.3. EFC transaction requirements

6.3.1. EFC transactions

[R 23] The OBE shall respond to any combination of requests from the Roadside Equipment (including any combination of EFC elements and attributes) as defined in EN 15509.

[R 24] The OBE shall have implemented the required OBE security related data required for Security Level 0 and Security Level 1 compliant to EN 15509.

[R 25] The attributes in EID=01, EID = 02, EID = 04 and EID = 05 shall be protected by Security Level 1.

[R 26] The OBE shall execute the security algorithms and responses to the RSE enabling light vehicles with speeds up to 180 km/h and heavy vehicles with speeds up to 120 km/h to pay electronically via the OBE.

NOTE 9. The security algorithms and responses to the RSE cover the complete EFC transaction from BST to RELEASE including generation of two authenticators.

NOTE 10. By light vehicle is meant vehicles with a total weight ≤ 3.5 tons and the OBE mounted not more than 1.6 meters above the road surface. By heavy vehicle is meant vehicles with a total weight ≥ 3.5 tons and the OBE mounted not more than 2.7 meters above the road surface.

NOTE 11. The RSE is assumed to be compliant with the requirements in the AutoPASS RSE specification.

[R 27] The probability of OBE failure during transaction shall as a minimum be less than $5 \cdot 10^{-5}$ tested in a lab environment where the AutoPASS OBE is mounted on a rotor or similar equipment and where the OBE communicates with an RSE compliant with the requirements in the AutoPASS RSE specification.

[R 28] The test described in [R 27] shall simulate the operational environment as far as possible by fixing the OBE to a windscreen or similar material, by changing the windscreen angel between 90 and 140 degrees and by simulating the different time slots in the DSRC communication zone for OBEs installed in light and heavy vehicles as shown in Figure 12.

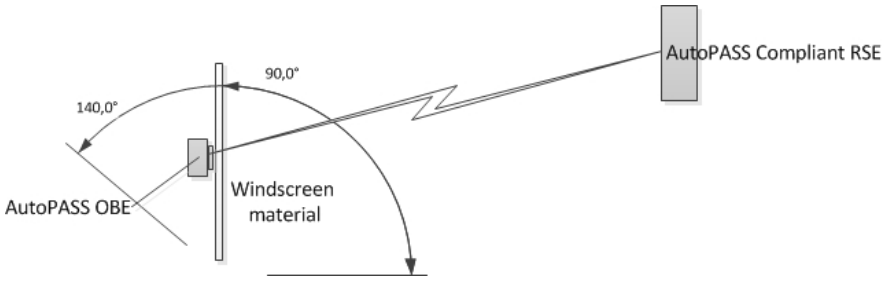

Figure 12 Wind screen angles in lab test environment

Figure 13 shows an example of a possible AutoPASS EFC transaction. After the BST and VST the RSE requests the OBE to return the value of the PaymentMeans attribute together with an authenticator calculated using the secret keys of the TSP and the TC. Further the RSE requests the OBE to return

the value of the attributes VehicleClass and EquipmentStatus. The attributes in EID=1 (the AutoPASS 1 element) is protected by an access control mechanisms and the requests includes the access credential (AC_CR) required to access the attributes in EID = 01.

The OBE responses to the requests returning the PaymentMeans value with the two different authenticators (two messages) and the values of the VehicleClass and EquipmentStatus attributes.

The RSE requests the OBE to write a new value to the EquipmentStatus attribute in EID = 01 as well as giving the driver a signal via the OBE buzzer. Both requests are executed and the OBE responses to the SET requests.

In a multilane environment there might be a need to follow the OBE through the charging point and the ECHO command maybe used for this. Finally the EFC transaction is closed by the RSE (RELEASE).

Figure 13 : EXAMPLE: Possible AutoPASS EFC transaction

6.3.2. ITS transactions

Figure 14 shows an example of a possible EFC/ITS transaction, e.g. for collection of traffic information to be used in traveller information systems.

The RSE requests the OBE to return the unique ID (RndItsId) which is a random number generated and initialised by the OBE supplier without any link to any register or other OBE information.

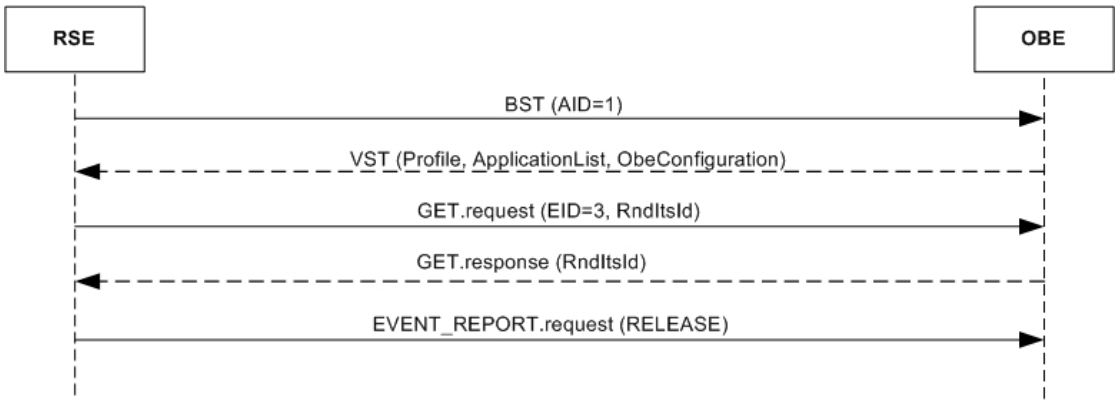

Figure 14 : EXAMPLE: Possible ITS transaction

6.3.3. AVI/ERI transactions

[R 29] The OBE shall respond to any combination of requests from the Roadside Equipment (including any combination of attributes) as defined in EN 16312.

[R 30] The OBE shall have implemented the required OBE security related data and security mechanisms compliant to EN 16312.

[R 31] The attributes in EID=5 (AVI/ERI element) shall be protected by Security Level 1.

[R 32] The OBE shall be able to perform an ERI session compliant to the requirements in EN 16312 and ISO 17264.

Figure 15 shows a possible example on an AVI/ERI transaction. The RSE requests the OBE to return the value of Vehicle Identification Number (VIN) with an authenticator calculated using the CS5 attribute and the RndRSE with the Authentication key 1.

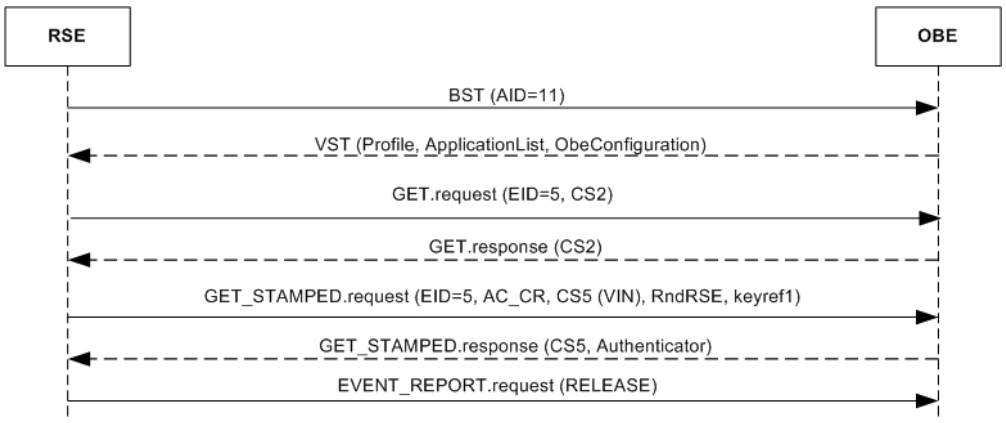

Figure 15 : EXAMPLE: Possible AVI/ERI transaction

6.4. Updating of OBE data attributes

[R 33] The OBE shall enable replacing of all data and Security keys belonging to one TSP, with data and Security keys from another TSP. This requires the authorised entity to be in possession of the Element Initialisation Key (EIK) for the relevant elements.

NOTE 12. This replacement requires write access to Security keys.

NOTE 13. This requirement enables an OBE from one issuer to be changed to an OBE from another issuer.

NOTE 14. Note the change of data within the elements must also affects data transmitted as part of the VST.

7. Technical requirements

7.1. Mechanical requirements

[R 34] The OBE shall not be possible to open without leaving clearly visible damages.

7.2. MMI requirement

[R 35] The OBE shall have a buzzer enabling the RSE to give the user an auditory signal in compliance with the EN ISO 14906 EFC function SET_MMI.

[R 36] The OBE buzzer shall have a sound with a frequency between 3,5 – 4,0 kHz.

[R 37] The OBE buzzer shall have a sound level between 75 and 85 dB A measured in front of the OBE, distance 10 cm, measured inside an anechoic chamber.

[R 38] The OBE shall enable the following audio signals (ActionParameters in parenthesis):

ok (0) with beep sequence BB000000

nok (1) with beep sequence B0B0B0B0

contactOperator (2) with bee sequence BBB00BBB

reservedForPrivateUse (128) with beep sequence BBBBBB00

noSignalling (255) ---- to be used in single lane with light signals

where B means sound in 0,1 second and 0 means silence in 0,1 second.

7.3. Environmental requirements

7.3.1. Climatic conditions

[R 39] The OBE including the battery shall comply with the Class 5K2 in IEC 60721-3-5.

7.3.2. Biological conditions

[R 40] The OBE shall comply with the Class 5B1 in IEC 60721-3-5.

7.3.3. Chemically active substances

[R 41] The OBE shall comply with the Class 5C1 in IEC 60721-3-5.

7.3.4. Mechanically active substances

[R 42] The OBE shall comply with the Class 5S1 in IEC 60721-3-5.

7.3.5. Contaminating fluids

[R 43] The OBE shall comply with the Class 5F1 in IEC 60721-3-5.

7.3.6. Mechanical conditions

[R 44] The OBE shall comply with the Class 5M3 in IEC 60721-3-5.

7.3.7. Other environmental requirements

[R 45] The OBE encapsulation shall be compliant with IP 40 as specified in IEC 529.

[R 46] The OBE shall be compliant with Directive 99/5/EC

[R 47] The OBE shall be compliant with Directive 2004/108/EC

[R 48] The OBE shall be compliant with EN 300 674-2-2

[R 49] The OBE shall be compliant with Directive 2002/96/EC

[R 50] The OBE shall be compliant with Directive 2002/95/EC

[R 51] The OBE shall be compliant with the Directive 2006/95/EC

7.4. Installation requirements

[R 52] The OBE shall be able to install in the windscreen by the user without any aid from expert and based on the installation guide provided by the OBE supplier.

NOTE 15. The requirement is based on the prerequisite that the user has cleaned the windscreen with a cleaning pad delivered together with the OBE and that the installation of the OBE is done according to the installation guide provided by the OBE supplier. Further, that the installation guide complies with the maximum tolerances for the position of the OBE in the windscreen as specified by the OBE manufacturer. The OBE should preferably be installed behind the back mirror in small/light vehicles unless physical characteristics, e.g. metallised windscreens, make it infeasible.

[R 53] The OBE shall be fixed to the windscreen by a dual lock tape system like 3M Dual Lock type SJ3560 Type 250 or equivalent.

NOTE 16. It is essential to have a standardized installation system, fixing the OBE to the car windscreen, independent of the OBE manufacturer.

[R 54] The density of interlocking stems shall be approximately 250 stems/Inch^2.

[R 55] The interlock function shall have a performance equal to “3M Dual Lock type SJ3560 Type 250” interlocking to itself.

[R 56] The fastening system, including the adhesive, shall be transparent.

[R 57] The adhesive bond used shall have the performance of 3MTM VHB™ acrylic adhesive or equivalent.

NOTE 17. It is assumed that the User has cleaned the windscreen with the cleaning pad delivered by the OBE supplier. Please refer to the tender documents.

[R 58] The OBE installation is to be effected according to an approved, documented procedure provided by the manufacturer.

[R 59] The OBE installation must comply with the maximum tolerances for the position of the OBE in the windscreen as defined by the OBE manufacturer's specification.

[R 60] The OBE shall be immune to damage caused by the normal handling, connection and disconnection that are necessary for installation and maintenance activities.

NOTE 18. This shall not preclude OBEs that are specifically designed to cease functioning upon removal or tampering.

7.5. Lifetime

[R 61] The OBE shall have a battery with a minimum lifetime of 7 years.

[R 62] The OBE battery shall be designed and constructed to prevent any leakage or explosion.

[R 63] The MTTF of the OBE shall be minimum 14 years (battery excluded).

[R 64] The OBE shall be compliant with Class A2 in ISO 14815, i.e. 10.000 identifications per year.

[R 65] The OBE shall have a low voltage detection mechanism setting a status bit in the obeStatus attribute sent in the VST.

[R 66] The OBE shall have a mechanism/algorithm that prevents the low voltage status bit in [R 65] to be set in other situations than when the battery lifetime is really close to an end.

7.6. Marking and identification

[R 67] The OBE shall have a unique ID (both in figures and barcode) printed (or burned) on the OBE enabling a visible reading of the OBE ID (both figures and barcode) throughout the lifetime of the OBE (i.e. UV resistant).

[R 68] The OBE ID (both figures and barcode) shall not be readable from the outside of the windscreen.

[R 69] The OBE ID printed (or burned) on the OBE outside shall be equal to the Personal Account number (PAN) as defined in 5.3 Element coding and the 16 digits in the PAN shall be printed in groups of four and four digits with a space between the number groups, e.g. 9578 XXXX AAAA AAAL (refer to 5.3 for further explanation).

NOTE 19. The values to be printed or burned will be provided by NPRA.

[R 70] The OBE unique ID barcode shall be of type "Interleaved 2 of 5" excluding the optional MOD 10 check character but including the one digit Luhn checksum.

[R 71] The OBE shall have a permanent AutoPASS logo on the windscreen side of the OBE.

[R 72] The AutoPASS logo shall have the background colour RAL = 5001, CMYK 100-100-40 or similar.

NOTE 20. The AutoPASS logo colour could be changed to differentiate between light and heavy vehicles. Please refer to Tender documents if such option is requested.

[R 73] The OBE shall be marked CE according to relevant EC directives.

7.7. Colour and size

[R 74] The OBE shall have a light grey colour.

NOTE 21. The light colour is to minimize solar heating of the OBE

[R 75] The size of the OBE (exclusive any object used for fixing the OBE to the windscreen) shall not exceed 82 x 48 x 20 mm (length x width x depth).

NOTE 22. The OBE should be as small as possible preventing a possible reduction in the driver view though the windscreen.

NOTE 23. OBE must have a depth less than 20 mm including the necessary protection and mail package/envelope. The reason for this is that the OBE shall be priced in the postal category letter with thickness less than 2 cm.

[R 76] The weight of the OBE (inclusive any object used for fixing the OBE to the windscreen) shall not exceed 50 grams.

7.8. Security and safety

[R 77] The OBE shall have a protection against any type of electrical or environmental impact on the data and software stored in the OBE, e.g. low, variable or empty power source, electrostatic discharge (ESD) and electromagnetic interference (EMI).

[R 78] The OBE shall ensure the continued correct operation of its security functions and the integrity of stored critical data (such as cryptographic keys), in both normal and extreme environmental conditions.

[R 79] The OBE shall prevent unauthorised alteration by physical or logical tampering of critical data (such as cryptographic keys) or software stored in the OBE.

[R 80] The OBE shall not interfere with the vehicle electronic system, e.g. vehicle electronic control units or airbags.