AP-1.6
Requirements for On-board Equipment (OBE) for use in AutoPASS Samvirke

Functional and Technical requirements

Version: 2.01
Date: 13 April 2021

Document status

Document no	AP-1.6 Requirements for OBE for use in AutoPASS Samvirke

Status	Version	Description
Final	2.01	

Document Version log

The purpose of the document version log is to describe the development of the document including the changes.

Version	Date	Author	Comments/amendments
1.0	NPRA	06.08.19	Based on doc. "4.7 EN 15509 AutoPASS OBE specification - Functional and Technical requirements ver 1.5". Adapted for reorganised AutoPASS Samvirke.
1.1	NPRA	21.04.20	Some adjustments. Removed mandatory attributes no 16-22, 33-34
1.2	NPRA	23.04.20	Minor modifications
1.9	NPRA	15.06.20	Rewritten chapter 4.1. Removed R 54 from ver 1.0-1.2. Moved to ref.[2]
1.99	NPRA	15.09.20	Corrected text in R 6
2.0	NPRA	24.11.20	Final version
2.01	NPRA	13.04.21	Version for publising

Table of contents

1. DEFINITIONS, ABBREVIATIONS AND REFERENCES

The Terms and definitions used in this document are defined in:

AutoPASS Requirement specification: AP-1.0 - Definisjoner, Standarder og Direktiver

2. INTRODUCTION

This document specifies the technical and physical requirements to the OBE to be used by TSPs which applies for being part of the AutoPASS system.

This OBE specification is based on the EN 15509 standard.

The interface between OBE and Charging Point is briefly described.

3. REFERENCES

The following AutoPASS documents are referenced in this document:

Ref.	Document name	Description
1.	AP-1.0 AutoPASS_Definisjoner, Standarder og Direktiver	The standards and directives referenced within this document are described with full titles in thus reference. Whenever a standard is referenced it is referring to the latest version of the standard.
2.	AP-1.3 AutoPASS EFC Security Architecture	Describes the principles of security keys handling and other EFC security aspects.

4. AUTOPASS ARCHITECTURE (INFORMATIVE)

4.1. ROLES AND RESPONSIBILITIES

The AutoPASS EFC concept is based on the role and responsibilities model defined in ISO 17573. AutoPASS Samvirke has chosen a hierarchical trust model using a Trusted Third Party (TTP).

In line with the ISO standard the following roles and responsibilities are present in the AutoPASS EFC concept:

- The Toll Service Provider (TSP) (In Norwegian: Utsteder)
- The User
- The Toll Charger (TC) (in Norwegian: Operatør)
- The Interoperability Manager
- The Trusted Third Party (TTP)

TSPs may use subcontractors for provision of OBE, but it is the TSP which is responsible on behalf of its subcontractors for fulfillment of the requirements.

The TTP role is important for the provision of OBE in AutoPASS Samvirke as this role is responsible for central storage and handling of EFC keys. This also includes the responsibility for overseeing the secure transfer of security keys to/from any actor using the keys, including verification of sufficient security in the key related systems and procedures of the actor. See also chapter 4.5.

For a detailed description of the roles, responsibilities and processes with regards to handling of EFC security keys it is referred to [ref. 2].

4.2. FUNCTIONAL ARCHITECTURE

The functional architecture of the OBE for AutoPASS Samvirke is described by this case:

- Execute an EFC transaction (OBE – RSE communication)

Execute an EFC transaction

The OBE communicates with the Toll Charger Roadside Equipment (RSE) as defined in EN ISO 14906 and EN 15509.

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

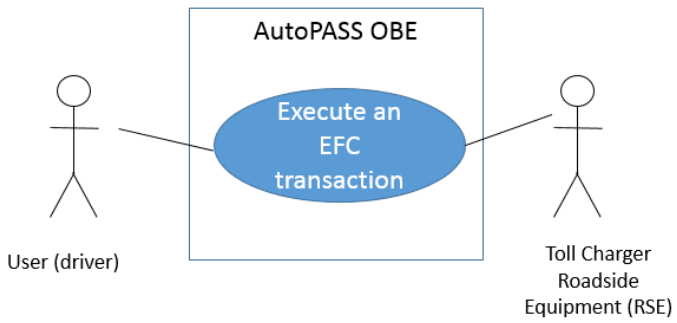

Figure 1 : The EFC transaction execution use case

4.3. PHYSICAL ARCHITECTURE

The high level 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.

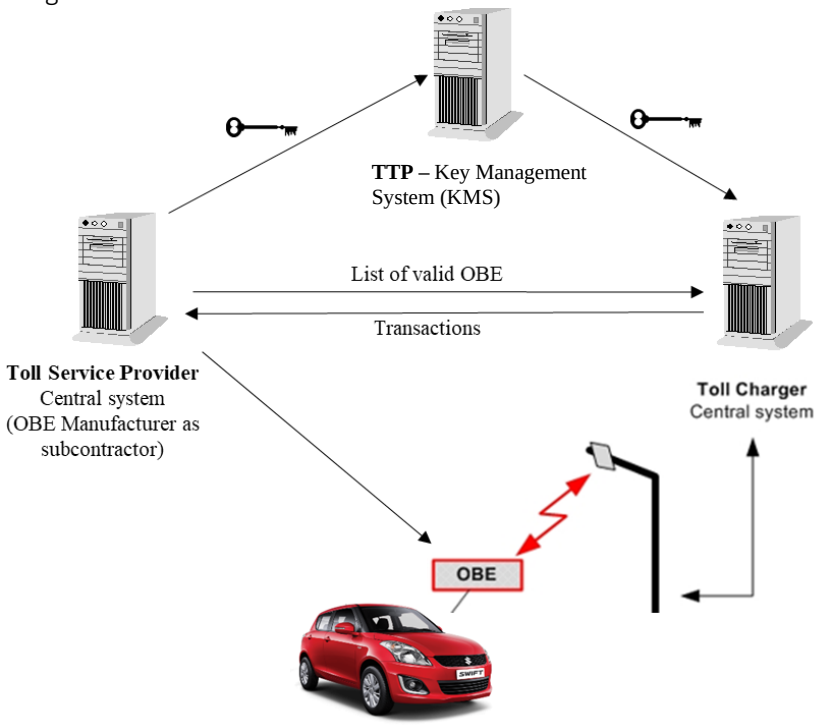

Figure 2 : The physical architecture

4.4. INFORMATION ARCHITECTURE

The information architecture is based on the EN ISO 14906 and EN 15509. It allows several elements in the OBE, each with individual security level, set of attributes and attribute values.

This specification only deals with the element used in AutoPASS and other toll domains interoperable with AutoPASS, hereafter called the EFC element. The TSP is free to define other elements used for other purposes. However, if the use of other elements have privacy and/or security implications on the EFC element, this specification defines some restrictions to the use of other elements in the OBE. An important reason is that other uses cannot be restricted to organisations guaranteed to maintain a high level of security. The requirements for general use of elements other than the EFC element are defined in section 7.6.

The description also includes an optional “ITS” element which is useful for some ITS applications.

The EFC element

This 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.

The ITS element (option)

The ITS element may, if implemented, store a non-unique ID without any relation to any EFC system. For privacy reasons there cannot be any relationship between the attributes in the EFC element and the ITS element.

The ITS element according to this specification is in use by the Norwegian Public Roads Administration (NPRA) for collection of anonymised traffic data in travel time information systems.

The ID may 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 non-unique ID that can be read by RSEs without access credentials (security level 0). See chapter 7.6.

4.5. SECURITY

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

Security Level 1 is required for the EFC element storing the crucial EFC attributes used for tolling. This implies that the OBE will require valid access credentials from the RSE enabling access to the EFC attributes in the OBE.

The security keys for all elements in the OBE will be supplied and managed by the TSP, - or the OBE manufacturer on behalf of the TSP. The keys for the EFC element shall be made available for AutoPASS and will be managed by the TTP on behalf of NPRA. The TTP is responsible for overseeing the secure transfer of security keys to TCs/RSE.

5. DATA REQUIREMENTS

5.1. GENERAL

[R 1] The TSP shall provide all necessary information regarding master security keys and initialisation data for all elements in the OBE based on requirements in this document.

5.2. ELEMENT SPECIFICATION

5.2.1. The EFC element (AID = 1 “electronic fee collection”)

[R 2] The EFC element shall be organised and include the data attributes as shown in Figure 3. OBE shall support these attributes and a guideline for initialisations with values according to Appendix A Example of element coding in EFC element.

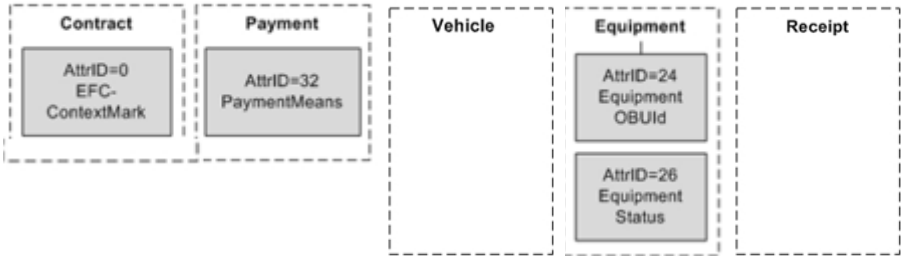

Figure 3 EFC element

5.2.2. (Option) The ITS element (AID = 29)

[R 3] The ITS element shall, if implemented, be organised and include the data attributes as shown in Figure 4.

[R 4] The ITS element shall, if implemented, not have access control (security level 0).

[R 5] The value of AttrID=87 shall be a random number between 0 and 32767 (0x0000 and 0x7FFF in hexadecimal).

[R 6] For each value for RndItsId there shall be 5 OBE produced which have the same value for RndItsId. (Within the same production batch).

NOTE 1. The upper range for RndItsId (currently set to 49 151) and privacy sets (currently set to 5) might be subject to change.

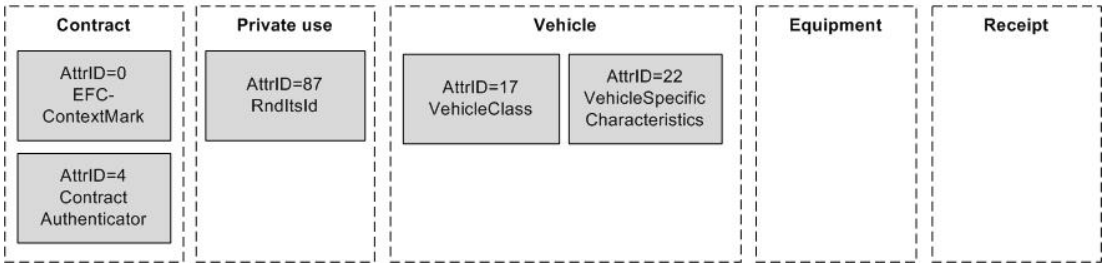

Figure 4 ITS element

If implemented, for historical reasons it is desirable that the OBE support these attributes and are initialized with values according to Appendix C Example of element coding in ITS element.

5.3. EFC ELEMENT CONTENT

The table below shows a more detailed overview of the application data for the EFC element. Each attribute contains one or several data fields.

[R 7] Personalization shall be made by the Contract Issuer (TSP) in a way that is compatible with the specification in Appendix A, which is based on EN ISO 14906.

"Read" and "Write" define access rights to a given attribute for GET, GET_STAMPED or SET used by RSE.

Attributes (EID>0)	AttrId	Type	Length in bytes	Read	Write	Remarks
CONTRACT						Information associated with the service rights of the Contract Provider
EFC Context Mark	0	32	6	Yes	No	Contains the Contract Provider Identification. Transmitted as part of the VST. See *)
PAYMENT						Data associated with the Payment transaction.
PaymentMeans (including PAN)	32	64	14	Yes	No	Includes: - The Personal Account Number, including the Payment Means Issuer (identified by the IIN), see **) - The PAN Expiry Date - The payment means Usage Control
EQUIPMENT						Information pertaining to the OBE.
EquipmentOBEId	24	56	5 (=4+1)	Yes	No	
EquipmentStatus	26	58	2	Yes	Yes	

Figure 5 EFC element content

Implementation of additional attributes for compatibility reasons to other existing systems (like AttrID. 4 and 23) is up to the TSP.

*) EFC Context Mark consists of:
ContractProvider: Identifies the organisation that issued the service rights given in the Contract, i.e. the Toll Service Provider. Numbers shall be assigned on a national basis. It is outside the scope of this document to identify the data that specify the service rights.

TypeOfContract: ContractProvider-specific designation of the rules that apply to the Contract. Allows, e.g., for the determination of the tariff or designating the type of purse associated with the contract.

ContextVersion: ContextVersion denotes the implementation version of the concerned contract within the context of the given ContractProvider, value assigned at the discretion of the ContractProvider. The ContextVersion may also be used as a security key reference.

**) PersonalAccount Number (PAN): Coded according to financial institutions, consists of the Major Industry Identifier (MII), the Issuer Identifier Number (IIN), the account number and a check digit (calculated with the Luhn algorithm) acc. to ISO7812.

6. FUNCTIONAL REQUIREMENTS

6.1. DSRC REQUIREMENTS

[R 8] The OBE shall comply with the DSRC requirements in EN 15509

[R 9] The OBE shall comply with the EFC functions in EN 15509 and must conform to the base standards as shown in figure 7.

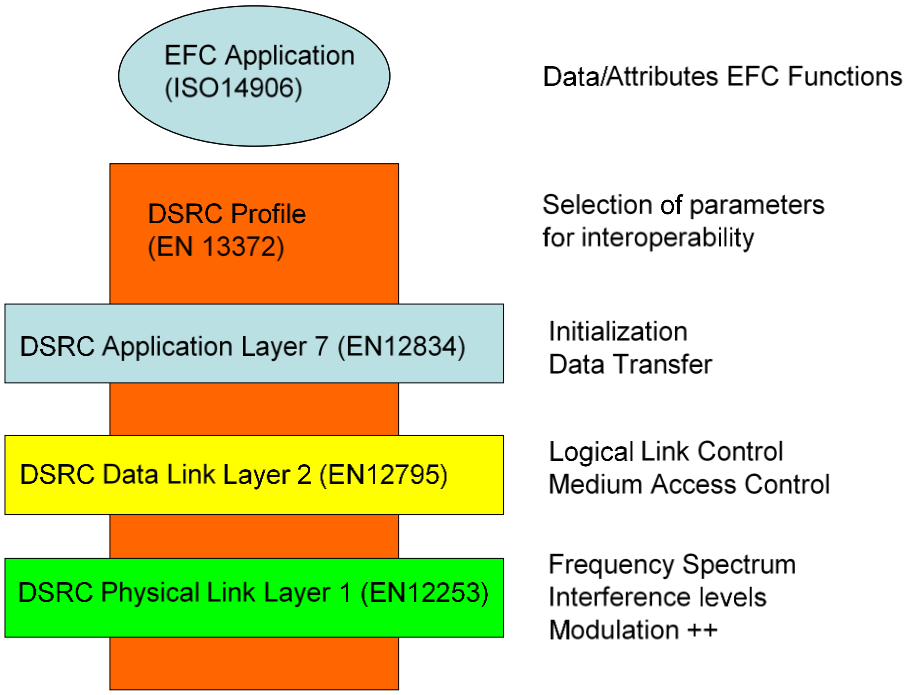

Figure 7 EFC base standards

6.2. INITIALISATION REQUIREMENTS

[R 10] The OBE shall be initialised with the EFC element and attributes as organised and defined in section 5 Data requirements enabling values to be written to the different attributes in the element.

[R 11] The TSP shall describe the use of obeStatus being part of the ObeConfiguration sent in the VST. Recommended use (from prior AutoPASS specification): “Shall be initialised with 0000 0000 0000 0000 'B. All 16 bits in obeStatus for the OBE application shall not be changed from the value 0 during the OBE lifetime except bit 6 in the first octet, ref. ISO 14906, that is used by a low voltage detection mechanism for setting the flag ”Low battery”. If instead bit 5 is used (for historical reasons), this must be specified by the TSP.

6.3. EFC TRANSACTION REQUIREMENTS

Appendix B shows an example of a transaction model for the EFC element.

6.3.1. EFC transactions

[R 12] The OBE shall respond to any combination of requests from the RSE (including any combination of attributes) as defined in EN 15509.

[R 13] The OBE shall have implemented the required OBE security related data required for Security Level 1 compliant to EN 15509. The attributes in the EFC element shall be protected by Security Level 1.

[R 14] The RndOBE value to calculate the OBE access credentials (AC_CR) shall be set randomly for each communication.

[R 15] In order to support free-flow systems at high speeds, the OBE shall execute the tolling transaction successfully in less than 40ms.

NOTE 2. The security algorithms and responses to the RSE cover the complete EFC transaction from BST to RELEASE including generation of two authenticators.

NOTE 3. 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 4. The RSE is assumed to be compliant with the requirements in the AutoPASS RSE specification.

[R 16] The applicant must document that the OBE has a high rate of readability when communicating with an RSE environment compliant with the requirements in the AutoPASS RSE specification.

6.3.2. Multilane free-flow ability

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).

Tests have shown that some existing OBE types have troubles under multilane free-flow conditions. The main requirements are:

[R 17] The OBE must be able to handle - without decrease of its performance - simultaneous radiation of different carrier frequencies in case of overlapping communication zones of neighbouring beacons.

[R 18] The OBE shall support all 4 downlink channels (D1 in EN 12253 [L1]).

6.3.3. Data storage

[R 19] Personalisation and transaction data shall be stored in a way that data integrity is ensured under all operating conditions, including battery low-voltage situations.

[R 20] In situations where data integrity cannot be guaranteed, the OBE shall not respond on the DSRC link (i.e. in case the OBE cannot ensure that stored data are correctly retrieved, or that received data are correctly stored).

[R 21] It must be assured, that transaction data written to OBE are corresponding to the transaction data of the RSE.

6.3.4. Multiple transactions

[R 22] The OBE shall not produce more than one transaction inside the RSE communication zone, even for a longer period.

7. TECHNICAL REQUIREMENTS

7.1. MMI REQUIREMENTS AND GUIDELINES

[R 23] 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 24] The OBE buzzer is recommended to have a sound with a frequency between 3,5 – 4,0 kHz.

[R 25] The OBE buzzer is recommended to 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 26] The OBE must respond to the following ActionParameters (in parenthesis) and is recommended to enable the following audio signals:

ok (0) with beep sequence BB000000
nok (1) with beep sequence B0B0B0B0
contactOperator (2) with bee sequence BBB00BBB
noSignalling (255) ---- no beeps (e.g. 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.

[R 27] To retain compatibility with existing OBE (and RSE), the OBE shall accept SET_MMI with any value of the EID, and with Container type = 69(dec). The AutoPASS RSE will use Container type = 69 (dec) unless otherwise agreed.

7.2. ENVIRONMENTAL REQUIREMENTS

7.2.1. Climatic conditions

[R 28] The OBE including the battery shall comply with the Class 5K2 in IEC 60721-3-5.

7.2.2. Biological conditions

[R 29] The OBE shall comply with the Class 5B1 in IEC 60721-3-5.

7.2.3. Chemically active substances

[R 30] The OBE shall comply with the Class 5C1 in IEC 60721-3-5.

7.2.4. Mechanically active substances

[R 31] The OBE shall comply with the Class 5S1 in IEC 60721-3-5.

7.2.5. Contaminating fluids

[R 32] The OBE shall comply with the Class 5F1 in IEC 60721-3-5.

7.2.6. Mechanical conditions

[R 33] The OBE shall comply with the Class 5M3 in IEC 60721-3-5.

7.2.7. Other environmental requirements

[R 34] The OBE encapsulation shall be compliant with IP 40 as specified in IEC 529.

[R 35] The OBE shall be compliant with Radio Equipment Directive (RED) 2014/53/EU

[R 36] The OBE shall be compliant with Directive 2004/108/EC

[R 37] The OBE shall be compliant with EN 300 674-2-2

[R 38] The OBE shall be compliant with Directive 2012/19/EU

[R 39] The OBE shall be compliant with Directive 2011/65/EU

[R 40] The OBE shall be compliant with the Directive 2006/95/EC

7.3. INSTALLATION REQUIREMENTS

[R 41] The TSP must facilitate correct installation of the OBE.

[R 42] The OBE installation procedure must ensure proper OBE to RSE communication by complying with the maximum tolerances for the position and orientation of the OBE in the windscreen, as defined by the OBE manufacturer's specification.

[R 43] The OBE installation procedure must ensure proper OBE to RSE communication for windscreens mounted at all normal angles found in light and heavy vehicles.

7.4. MARKING AND IDENTIFICATION

[R 44] It shall be possible to visually verify the OBE identity. This may be achieved by a printed or burned OBE unique ID on the unit case, alternatively by use of a display (MMI). Any print must be visible throughout the lifetime of the OBE, i.e. UV resistant etc.

The OBE unique ID print shall not be easily identifiable from the outside of the windscreen.

[R 45] The OBE unique ID displayed or printed/burned on the OBE shall be either:

a. Equal to the Personal Account number (PAN) as defined in section 5.3.

b. An alphanumeric ID which is unique for every OBE issued by the TSP. Information on the identity of the vehicle (LPN and nationality) associated with the OBE unique ID must be available to the User so that the customer can verify that the OBE is installed in the vehicle that is on the AutoPASS contract.

   Since the PAN of the EFC element to be used in AutoPASS cannot be read off the OBE, there must be a way for the User to find this PAN without having to contact the customer service of the TSP.

[R 46] If the OBE unique ID is not the PAN, service users of vehicles heavier than 3500 kg must be issued with a declaration from the TSP containing the following information:

- The OBE unique ID, printed alphanumerically and as a barcode.
- If applicable, the OBE ID as shown in the display if it differs from the printed OBE unique ID. An acceptable deviation will be the addition or removal of a check digit. If present, it shall be printed alphanumerically and as a barcode.
- The PAN of the EFC element to be used in AutoPASS, printed alphanumerically and as a barcode.
- The LPN and nationality of the vehicle.

The TSP must inform Users of vehicles heavier than 3500kg that this declaration must always be carried on board when driving in Norway. The driver must always be prepared to show the declaration together with the OBE for control purposes.

[R 47] Preferably there may also be a barcode representation of the OBE unique ID. The OBE unique ID barcode is recommended to be of barcode type code 128 including the Luhn digit of the PAN.

[R 48] The OBE shall be marked CE according to relevant EC directives.

7.5. SECURITY AND SAFETY

[R 49] 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 50] The OBE shall prevent unauthorised read out or alteration by physical or logical tampering of critical data (such as cryptographic keys) or software stored in the OBE. There shall be no read access to authentication keys as well as to access keys.

[R 51] The master access key and one master TC authentication key for the EFC element shall be made available for AutoPASS. These will be managed by the AutoPASS TTP on behalf of NPRA. The TTP is responsible for overseeing the secure transfer of security keys to TCs/RSE.

[R 52] The OBE shall not interfere with the vehicle electronic system, e.g. vehicle electronic control units or airbags.

[R 53] The OBE shall be protected 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).

7.6. USE OF OTHER ELEMENTS IN THE OBE

As mentioned in chapter 4.4, the TSP is free to add other elements to the OBE to be used for other purposes. However, there are some restrictions for the design and use of other elements in the OBE used in AutoPASS. An important reason is that other uses cannot be restricted to organisations guaranteed to maintain a high level of security. As such, security keys may be compromised, causing damage to the reputation of AutoPASS and added cost for AutoPASS TCs.

[R 54] Security keys for the EFC element are for the sole use by toll stations in AutoPASS and other European toll domains. Practically, this means:

c. Security keys for the EFC element cannot be distributed to actors other than those involved in tolling within AutoPASS/EETS.

d. Other elements that the TSP may add to the OBE are not allowed to use the same master keys as the ones used for the EFC element

[R 55] Other elements that the TSP may add to the OBE may use the same OBE identifier (eg. PAN) as the EFC element, but only if the element is protected with security level 1. It shall not be possible to derive the ID/PAN of the EFC element from the ID of an open element with security level 0 (e.g. adding a “0” or other ways of altering the ID).

8. APPENDIX A – EXAMPLE OF ELEMENT CODING IN EFC ELEMENT

The column "Bits in octet" describes guidelines for contents. When attribute is not in use, this is a recommendation of how to initialize with zero data.

The AttrID 24 is not in active use in AutoPASS. To retain compatibility with existing RSE, the OBE shall accept transaction models where this attribute is used.

AID=1 (electronic-fee-collection)			
AttrID	***Attribute***	***Bits in octet***	***Description and comments***
0	EFC-ContextMark 6 octets, read only	0011 0000	ContractProvider CountryCode, as coded in EN ISO 14816, ITA-2 alphabet, this shows an example NO (Norway) IssuerIdentifier as assigned by Standards Norway
		11	
		xx xxxx	
		xxxx xxxx	
		0000 0000	TypeOfContract = xx (to be decided by TSP)
		0000 00xx	
		0000 00xx	ContextVersion = xx (to be decided by TSP)
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) coded according to ISO7812. Recommended number of digits is 16. Example from current AutoPASS EN15509 OBE: 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	
		xxxx xxxx	
		0000	

		0000	PaymentMeansExpiryDate (DateCompact)
		0000 0000	
		0000 0000	PaymentUsageControl
		0000 0000	
		0000 0000	
		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	
		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	
		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	
		xxxx xxxx	
		xxxx xxxx	Key derivation according to EN 15509 Annex B.4.2
		xxxx	

114	AuthenticationKey4-EID1 No access	xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx	
115	AuthenticationKey5-EID1 No access	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	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	Key derivation according to EN 15509 Annex B.4.2
		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	
120	AccessKey-EID1 No access	xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx	Key derivation according to EN 15509 Annex B.4.3

9. APPENDIX B – EXAMPLE OF TRANSACTION MODEL FOR EFC ELEMENT

The figure below shows an example of an 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 (OBS: This is just an example as the attribute VehicleClass is not in use in AutoPASS). The attributes in EFC element is protected by an access control mechanisms and the requests includes the access credential (AC_CR) required to access the attributes in EFC element.

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 EFC element as well as giving the driver a signal via the OBE buzzer. Both requests are executed and the OBE responses to the SET requests.

Figure 8: Example of EFC transaction

10. APPENDIX C – EXAMPLE OF ELEMENT CODING IN ITS ELEMENT

AID=29 (Private Application Identifier = ITS)			
AttrID	***Attribute***	***Bits in octet***	***Description and comments***
0	ITS-ContextMark 6 octets, read only	0011 0000	ContractProvider
		11	
		00 0000	Example from current AutoPASS EN15509 OBE:
		0110 0011	CountryCode, NO (Norway) as coded in EN ISO 14816, ITA-2 alphabet, IssuerIdentifier = 99 (Norwegian Public Roads Administration) as assigned by Standards Norway
		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
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 section 5.2.2
		xxxx xxxx	
		xxxx xxxx	

11. APPENDIX D – EXAMPLE OF TRANSACTION MODEL FOR ITS ELEMENT

The figure below shows an example of a possible 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.

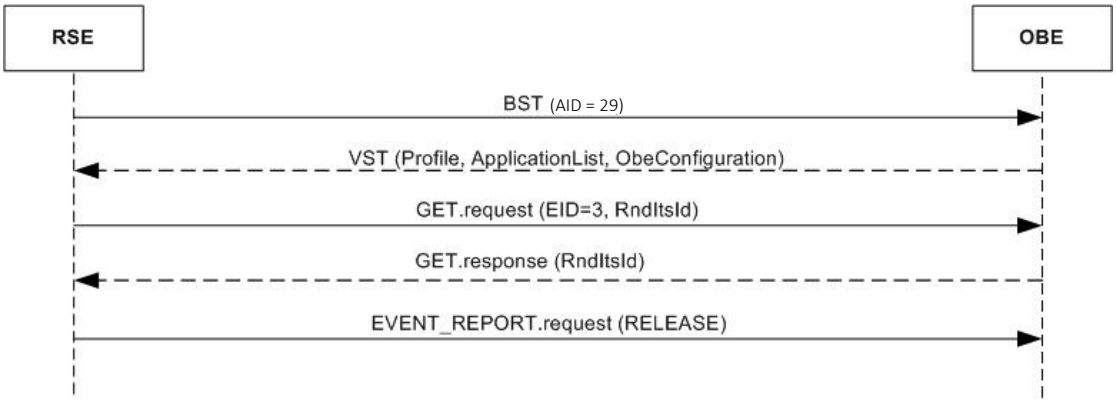

Figure 9: EXAMPLE: Possible ITS transaction