Request for Proposal

CPE Procurement

SSA-T / SSA-V, Appendix 1 Annex 5

4.5 Security Architecture for AutoPASS

Version log

Version	Initials	Date	Comments/amendments
1.0			RFP sent to Bidders
1.1			

TABLE OF CONTENTS

1. CUSTOMER REQUIREMENT SPECIFICATION

The

Req.	Description	Comp	Reference
[R 1]	The supplier shall, during the project design phase, document compliance to information security requirements. The requirements shall be implemented by the supplier and will be audited by the customer according to ISO/IEC 27001 Appendix A. The scope of this requirement shall include all systems, procedures and personnel involved in handling EFC master keys		
[R 2]	Equipment handling EFC key placed in non-secure locations , shall meet certification requirements in Common Criteria (ISO/IEC 15408). The level of security and the protection profile is to be defined in the project design phase, based on a risk analysis. Note: An more concrete version of this requirement is stated as follows: Equipment handling EFC key shall store and handle the keys in secure/tamper-resistant hardware. Administrative systems handling EFC keys shall implement two-factor authentication or equivalent security methods.		
[R 3]	The supplier shall be required to periodically document and demonstrate to the customer that compliance to the information security requirements in R1 and R2 is implemented. If the supplier has a valid ISO/IEC 27001 or ISO/IEC 15408 certification by an accredited organisation, the customer will accept this as sufficient proof of compliance to R1, R2 and R4, given that the scope of the independent certification is equivalent to the scope given in R1, R2 and R4.		
[R 4]	EFC keys shall always be sent encrypted between systems handling EFC keys.		
[R 5]	If the customers audit team is required to sign a non-disclosure agreement, the agreement shall be limited to information provided by the supplier during the audit process only. Any legal issued shall be resolved according to the main contract between the customer and the supplier. The customer may engage subcontractors to perform the audit(s).		

2. DEFINITIONS, ABBREVIATIONS AND REFERENCES

The Terms and definitions specific to this document:
FIPS-140 – Standard for secure hardware/software components. Document available http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
EFC-keys – Cryptographic keys used in AutoPASS or by EasyGo partner. Term used both for access and authentication keys.
KVC - Key Verification Code According to ISO 11568 part 2 calculated encrypting one block size of zeros with the plain key, then truncated to leftmost three bytes.

3. PURPOSE OF THIS DOCUMENT

This document specifies a security architecture surrounding EFC-keys (master keys used for authentication and access control in OBUs). The goal of this document is to achieve uniform procedures and secure hardware and for handling EFC-keys.
The document also includes a file formats for EFC context marks, transaction models for RSE to OBU communication and an outline of procedures. These related topics are not essential to describe the security architecture, but the inclusion of these elements give a uniform method of handling security and communicating with OBUs.
The main focus of this document is the secure handling of EFC-keys for road side equipment suppliers. The same security architecture, certification and review process can also be used for other actors such as OBU suppliers and other non-AutoPASS actors who have a need for EFC-keys.

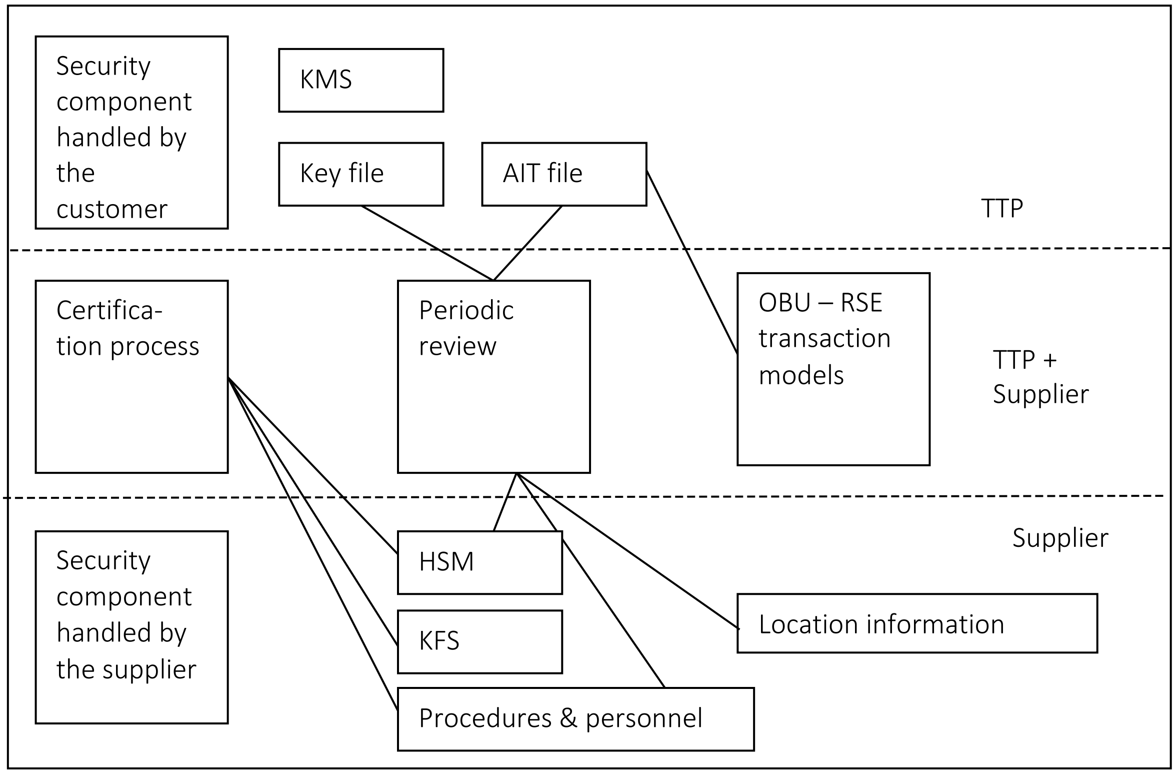


Figure 1 Overview of the components and processes described in this document

This document includes the following parts:

- Chapter 3 – An overview of security architecture in the AutoPASS system
- Chapter 4 – Functional requirements for supplier systems
- Chapter 5, 7 – Certification and review process
- Chapter 6, 8, 9, 10, 11 – File distribution methods and formats
- Chapter 12 – Expenses
- Appendix A – Transaction models

4. SECURITY ARCHITECTURE FOR AUTOPASS

4.1 Introduction

The overall security architecture in AutoPASS system can be shown with the following illustration: Note: This architecture is subject to change during the contract due to organisational changes in the AutoPASS system. Due to the Norwegian tolling reform.

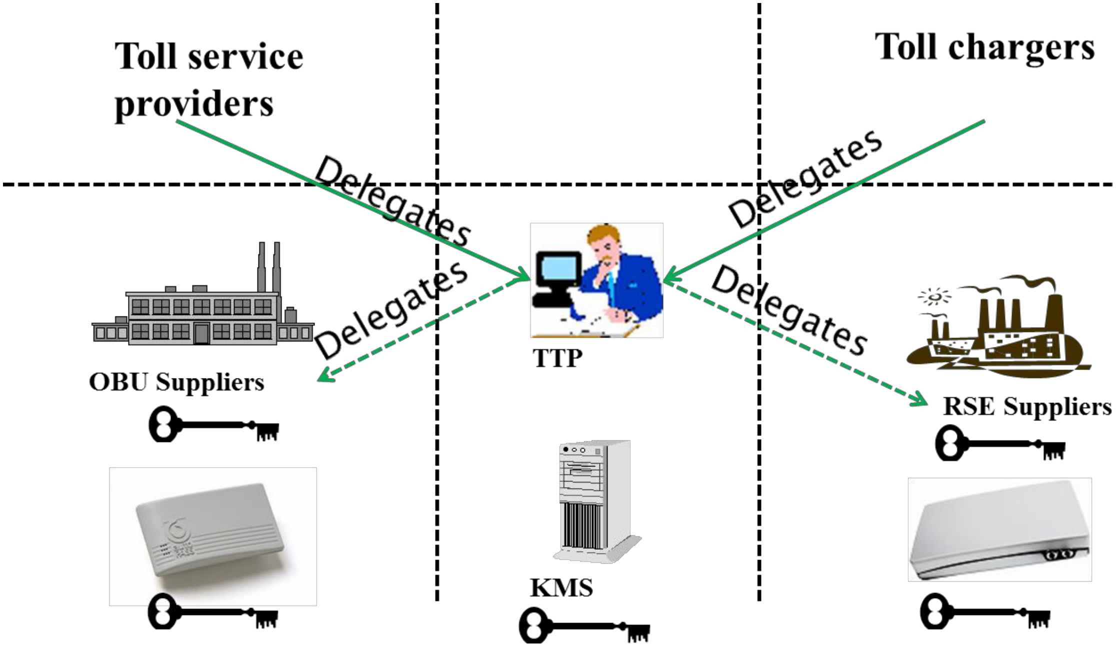


Figure 2 Delegation of responsibilities (organizational view)

The toll service providers and toll chargers do not handle EFC-keys themselves. This role is delegated to the TTP role. The TTP stands for Trusted Third Party and this role should be an independent organization tasked with overseeing the secure and proper handling of EFC-keys for all systems using AutoPASS OBUs.

The TTP role was established as an independent role in 2007. From 2007 to 2014 the TTP role took an active role in distributing EFC-keys directly to OBU supplier's production equipment and HSMs used in road-side equipment. The secure handling of EFC-keys rested then uniquely on the security

established within the TTP role. In 2014/2015 the TTP is in the process of changing to a more passive role, meaning that the EFC-keys are distributed only once from the TTP to the OBU and RSE suppliers at the start of a contract (or when there is a change of EFC-keys) and are subsequently only revoked at the end of a contract.
A centralized security approach with an active TTP is preferable when there are few actors and the underlying systems are stable. This is not the case for EFC-tolling where there is still rapid development and changes to supplier's side systems. This calls for a decentralized security approach (with a passive TTP) which is more flexible as each supplier can change their systems in the way they find best, but such a decentralized system is also more challenging to secure. Since the TTP cannot interface directly with supplier systems the TTP role will have to rely on performing periodic reviews and certification of suppliers to ensure that the supplier's system and procedures are secure.

4.2 security principles for suppliers handling EFC keys

Suppliers shall have systems and procedures in place that prevents that EFC keys will be compromised. Suppliers shall comply to the following set of information security requirements:

R1: The supplier shall, during the project design phase, document compliance to information security requirements. The requirements shall be implemented by the supplier and will be audited by the customer according to ISO/IEC 27001 Appendix A. The scope of this requirement shall include all systems, procedures and personnel involved in handling EFC master keys.

R2: Equipment handling EFC key placed in non-secure locations[1], shall meet certification requirements in Common Criteria (ISO/IEC 15408). The level of security and the protection profile is to be defined in the project design phase, based on a risk analysis.

Note: An more concrete version of this requirement is stated as follows: Equipment handling EFC key shall store and handle the keys in secure/tamper-resistant hardware. Administrative systems handling EFC keys shall implement two-factor authentication or equivalent security methods.

R3: The supplier shall be required to periodically document and demonstrate to the customer that compliance to the information security requirements in R1 and R2 is implemented.

If the supplier has a valid ISO/IEC 27001 or ISO/IEC 15408 certification by an accredited organisation, the customer will accept this as sufficient proof of compliance to R1, R2 and R4, given that the scope of the independent certification is equivalent to the scope given in R1, R2 and R4.

R4: EFC keys shall always be sent encrypted between systems handling EFC keys.

R5: If the customers audit team is required to sign a non-disclosure agreement, the agreement shall be limited to information provided by the supplier during the audit process only. Any legal issued shall be resolved according to the main contract between the customer and the supplier. The customer may engage subcontractors to perform the audit(s).

4.3 Systems

The security system for AutoPASS can be abstracted to the following set of components:

[1] E.g. HSM in road side equipment, OBE (tags) and other equipment placed in locations without adequate physical access control.

- KMS – Key Management System – A system operated by the TTP for distributing EFC-keys to other entities. This system is air gaped from other networks to protect from all kinds of malicious attacks over the network.
- TORD – Trusted Operator for key Re-Distribution – Note: This system is being discontinued and will instead be handled by manual procedures.
- KFS[2] – Key Forwarding System – An on-line or off-line system operated by the supplier. This system receives files with encrypted EFC-keys from the KMS (via the TORD system). The EFC-keys are decrypted by the KFS system for re-packaging and re-encryption to be later sent to HSMs under the control of the supplier.
- HSM – Hardware Security Module – An on-line system based on secure hardware operated by the supplier. This system receives EFC-keys from the KFS and uses the EFC-keys for computing access credentials, MAC verification or OBU-keys in the case of OBU suppliers. These HSMs are distinguished from the KFS by the fact that they cannot distribute EFC-keys to other systems.

The following figure shows the systems involved in distributing EFC-keys for AutoPASS. It also has a link to systems associated with EasyGo, as AutoPASS is part of larger system.

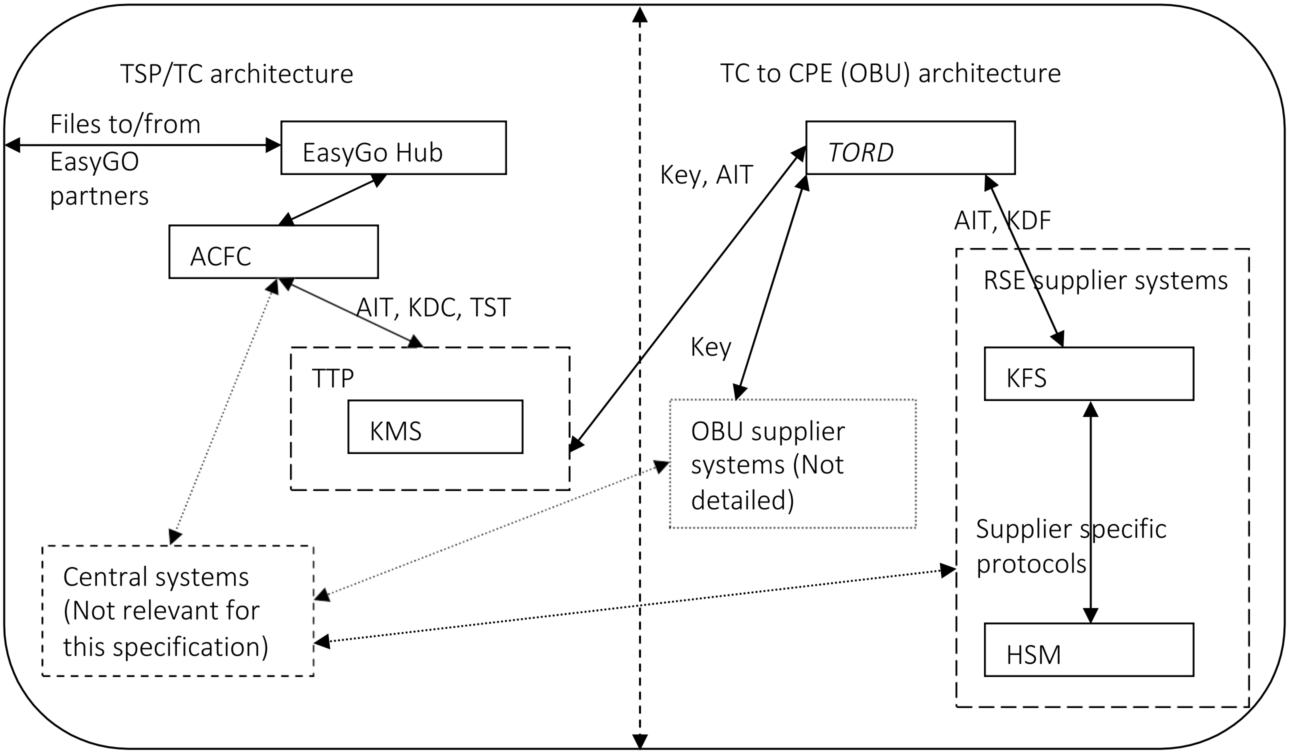

TSP/TC architecture
TC to CPE (OBU) architecture
Files to/from EasyGO partners
EasyGo Hub
ACFC
AIT, KDC, TST
TTP
KMS
Central systems (Not relevant for this specification)
Key, AIT
TORD
Key
OBU supplier systems (Not detailed)
AIT, KDF
RSE supplier systems
KFS
Supplier specific protocols
HSM

Figure 3 Overview of system architecture in AutoPASS (relevant for security)

Note: ACFC is AutoPASS Collection and Forwarding Central for Norway and EasyGo Hub is a collection and forwarding central for the rest of EasyGo. Only the most relevant file formats are included in this overview.

[2] The KFS might be better known under acronyms such as KMS, TTP-system, KDC, KIF and so on, this document uses the abbreviation KFS to distinguish it from the KMS.

4.4 Overview of procedures

The section gives an overview of the procedures associated with a contract. Only procedures relevant for the interaction between customer and the TTP[3] are detailed in this overview.
Note that this overview does not account for the fact that some suppliers might have several contracts which requires the use of EFC-keys. In theory each contract should be handled by a set of independent procedures, but most likely the procedures from several contracts can be combined.

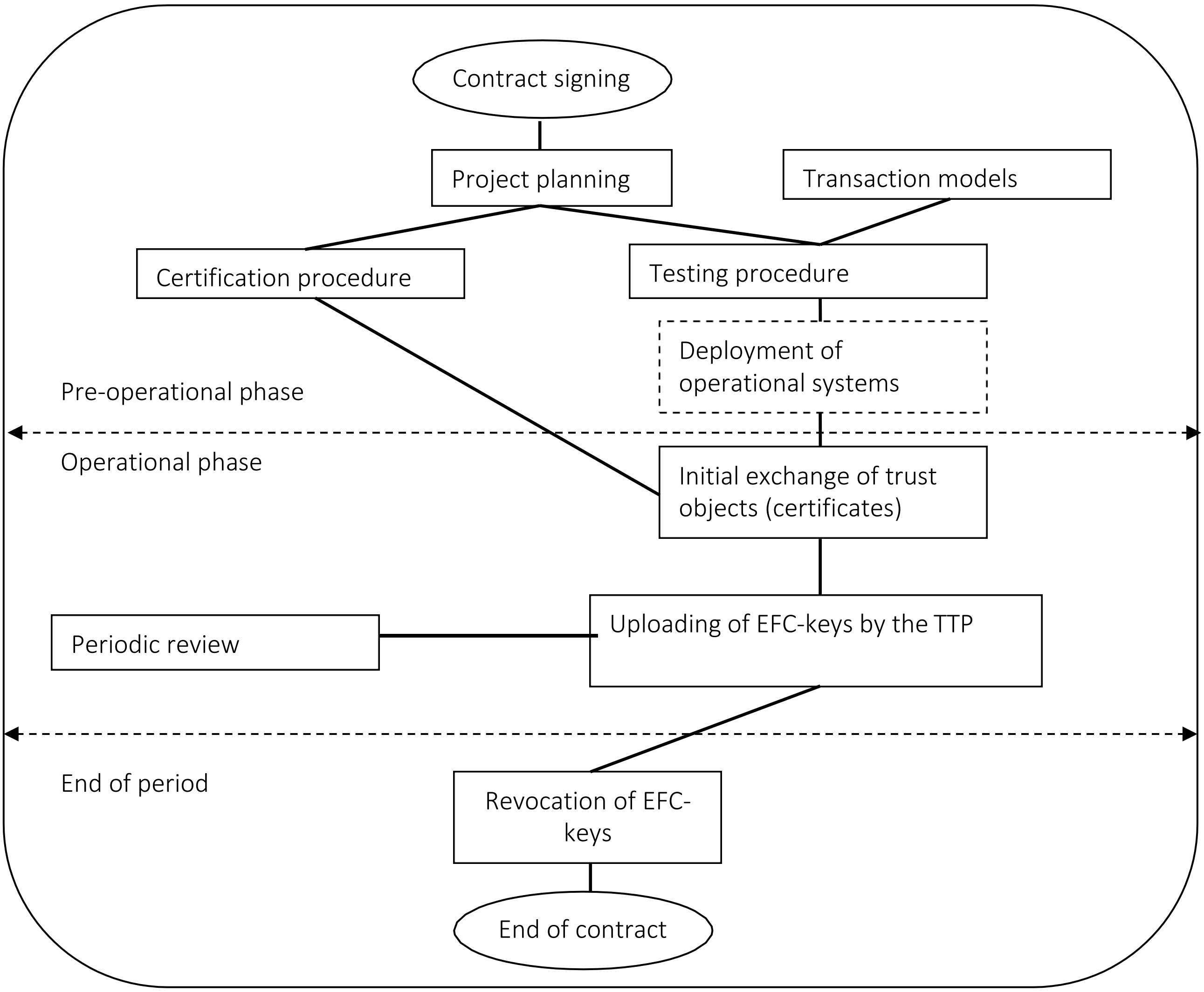


Figure 4 Overview of procedures

There is no interaction between the supplier and TTP in the procedure "deployment of operational systems" but it is included to improve clarity. In this process the supplier have finished testing and can deploy operational systems.
The procedures are given a brief description below and further elaborated in later chapters.

- Project planning – All projects start with a project planning phase, in this phase it is important to get a common understanding of the work to be done. E.g. the level and scope of testing and certification procedures. It is also important to assign roles and

[3] Note that a the two parties in a contract are usually referred to supplier and customer, but as shown in Figure 2 all security related functions are delegated to the TTP.

responsibilities, define scope, strategy for handling quality and risks, project plans, project controls, and so on.

- Transaction model – The protocols which are used in the AutoPASS system are defined in the AIT file. These protocols should in turn be mapped to a set of transaction models, which is the set of commands communicated between the OBU reader in RSE and the OBUs. An overview of the transaction models is given in Appendix A. These transaction models must be detailed as part of project planning.
- Certification procedure – The goal of this procedure is to ensure that the supplier has system and procedures in place, to ensure that the risk associated with the loss of confidentiality for the EFC-keys is minimised. The requirements for certification is detailed in chapter 4 and this procedure is subsequently detailed in chapter 5.
- Testing procedure – The goal of this procedure is to test the exchange of EFC-keys between the TTP and the supplier, to ensure that they will work for day-to-day operations. The testing procedures should be based on testing systems and procedures defined in this document and should be detailed as part of project planning.
- Initial exchange of trust objects (certificates) – This is a simple procedure where certificates are exchanged. This procedure will be detailed together with the procedure for uploading of EFC-keys by the TTP.
- Uploading of EFC-keys by the TTP – The goal of this procedure is to exchange with the supplier a set of files that uniquely defines which EFC-keys with associated EFC context marks that should be read and verified by the road side equipment. This procedure is detailed in chapter 6.
- Periodic review – The goal of this procedure is to have a complete list of all HSMs installed and an understanding of their location, to minimise the possible misuse of HSMs with installed EFC-keys. This procedure is detailed in chapter 7.
- Revocation of EFC-keys – The goal of this procedure is to ensure that no EFC-keys are left in any system operated by the supplier after the contract with the supplier is terminated. This procedure must be done even in the case of a premature termination of thecontract.

5. FUNCTIONAL REQUIREMENTS FOR KFS, HSM

This chapter describes the functional and security requirements on HSM and KFS equipment. The HSM is a secure module installed at the road-side and shall be able to calculate access credentials and authenticate OBUs. The KFS is a secure program or secure module installed in a secure location under sole control of the supplier. The KFS acts as a gateway between the TTP role and the HSMs.

5.1 Functional requirements for HSM

The purpose of having a HSM (Hardware Security Modules) in road-side equipment is to ensure that all cryptographic keys used for electronic fee collection are properly secured at the road side. There have been very few cases where road-side equipment has been stolen, but it is almost impossible to secure road side systems from a determined attacker[4]. Therefore the security of the EFC-keys at the road side must be based on secure hardware, which will not be able to export EFC-keys.

The HSMs must be able to support three different types of EFC-keys:

1. Authentication keys for original AutoPASS OBUs (supporting OBUs using the proprietary AutoPASS protocol)
2. Authentication keys for EN15509 OBUs (supporting OBUs using EN15509 protocol)
3. Access credentials for EN15509 OBUs (supporting OBUs using EN15509 security level 1 protocol)

The HSM should also be equipped with hardware able to perform AES encryption/decryption to handle the next generation of security protocols, which might be deployed within the next 3-5-10 years.

Functional Requirement	Comments
Generate public key	This function generates a public/private key-pair (equivalent to RSA 2048-bit length or stronger). Note: It might also be possible to use symmetric keys instead of public keys, but any supplier using symmetric encryption for transferring EFC-keys must show that this does not affect security adversely. This function can only be run at initialization.
Get public key	This function returns the public part of the HSMs key.
Get HSM identity	This function returns the unique identity of the HSM
Import EFC-key	This function imports an EFC-key into the HSM. The EFC key shall be encrypted with the HSM's private key, to be decrypted within the HSM only. The HSM shall be able to handle at least 300 EFC-keys.
Delete EFC-key	This function deletes an EFC-key from the HSM.
List EFC-keys	Returns a list of all EFC-keys stored in the HSM (along with their associated KVC and key identification (ContextMark and key reference)).
Calculate AutoPASS MAC	Calculates if the supplied MAC value is correct using the AutoPASS-protocol.
Calculate EN 15509 MAC	Calculates if the supplied MAC value is correct using the EN15509-protocol. (EN 15509 appendix B)

[4] The road side equipment is usually located in an unguarded location on or beside busy toll roads, this means that an attacker can easy gain access to such equipment and can make a quick getaway once such equipment has been hacked or stolen.

Calculate EN 15509 Access Credentials	Calculates the Access credential based on the EN15509-protocol for access credential. (EN 15509 appendix B).
Wipe HSM	Removes all Key information from the HSM (this functionality can be achieved using delete EFC-keys functionality)
Secure software update	HSM supplier specific functionality. Software in the HSM cannot be modified without knowledge of software update credentials. This functionality might be omitted. Omitting this functionality should not affect costs adversely (see expenses).

Security requirements	Comments
Secure initialization	Initialization of HSMs must only be performed: • By approved personnel • In secure environments • Based on written procedures.
Certified secure hardware	The software and hardware of a HSM shall be able to meet the requirement stated in an appropriate protection profile in Common Criteria , and /or in FIPS 140-2 level 2.
Integrated chip	The processor and memory (which handles unencrypted and private keys) must be integrated into a single chip.

5.2 Functional requirements for KFS

The functionality in a KFS (Key Forwarding System) can be relatively simple, but security is very important. The minimum requirements for a KFS is a system or program that acts as a gateway (man-in-the-middle) between the KMS and the suppliers HSM's. It should be able to generate an RSA key pair, read KDF files sent from the KMS and export files/data streams containing EFC-keys that can be read by the suppliers HSMs.

Functional Requirement	Comments
Generate public key	This function generates a public/private key-pair; this must be RSA 2048-bit length key. The private key shall be stored in a secure location and be protected against unauthorized access.
Get public key	This function returns the public part of the HSMs key. This function must be able to export the public key as a valid X.509 certificate. (Windows .DER file).
Import KDF file	This function imports a KDF file
Export HSM file	This function exports a file or data stream containing EFC-keys for a specific HSM.
Wipe KFS	Removes all Key information from the KFS

Security requirements	Comments
Initialized, stored and operated in a secure environment	Initialization, storage and operation of KFS must only be performed: • By approved personnel • In secure environments • Based on written procedures.

Documented security concept, treat analysis and methodology for handling threats.	The supplier shall provide documentation that the KFS is secure. The security documentation shall be based on a framework for information security. The supplier is recommended to use ISO/IEC 27001 - Information security management.
Two factor authentication	Access to the keys stored in the KFS requires at least two factor authentication mechanisms.

6. CERTIFICATION PROCEDURE

The HSM and KFS need to be certified on a system and procedure level before the systems can receive EFC-keys used in AutoPASS and EasyGo.
The functional and security requirements described above are the minimum requirements, a supplier is free to add or modify functionality, e.g. support additional protocols or merge two functionalites into one command, as long as any changes does not weaken the security surrounding EFC-keys, or are in conflict to the architecture described in this document.
Certification of a KFS and HSM for use in AutoPASS is tied to a specific combination of:

- Hardware components
- Software version
- Initialization and operating procedures

Certification for use in AutoPASS shall be approved by Norwegian Public Roads Administration based on a recommendation from the TTP. A certification is usually only valid for 1 to 3 years.

The supplier shall make all relevant documentation available to the TTP for the purposes of certifying the HSMs. This means that the TTP can ask for and have access to all business sensitive material and source code that the supplier has access to. The supplier can therefore ask for a non-disclosure or confidentiality agreement to be signed by the people involved in the certification process.

Changes to hardware, software or initialization procedures (or systems) require re-certification of HSMs before they can be used to receive EFC-keys. A certification for some equipment and procedures is not tied to a specific supplier.

The certification procedure is described below

6.1 Initial EFC key certification procedure

6.1.1 *Purpose*

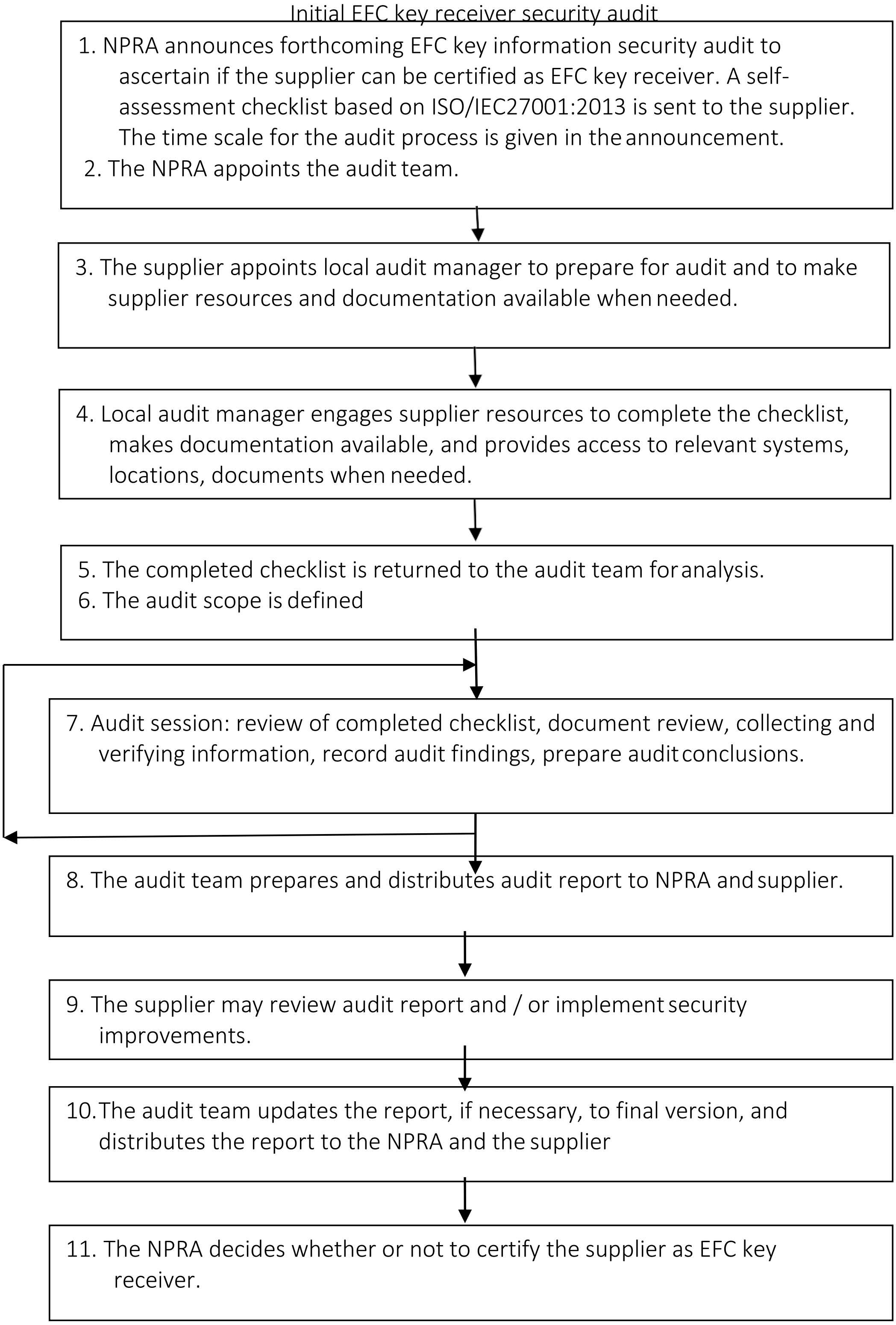
The purpose of this procedure is to determine whether an AutoPASS supplier can be allowed to receive EFC keys from the NPRA. The supplier must be certified as a EFC key receiver. Certification can be achieved through an information security audit, as defined in this document, of all information systems that will handle EFC keys.

6.1.2 *Audit objective*

The objective of the audit is to determine whether supplier has proper information security measures in place, on all systems and procedures that handle EFC keys, as well as security measures concerning personnel that have access to these systems. The objective is to ensure that the EFC keys will not be compromised or lost at the supplier.

6.1.3 *Audit procedure*

The audit procedure is shown below.



Initial EFC key receiver security audit

1. NPRA announces forthcoming EFC key information security audit to ascertain if the supplier can be certified as EFC key receiver. A self-assessment checklist based on ISO/IEC27001:2013 is sent to the supplier. The time scale for the audit process is given in the announcement.
2. The NPRA appoints the audit team.

3. The supplier appoints local audit manager to prepare for audit and to make supplier resources and documentation available when needed.

4. Local audit manager engages supplier resources to complete the checklist, makes documentation available, and provides access to relevant systems, locations, documents when needed.

5. The completed checklist is returned to the audit team for analysis.
6. The audit scope is defined

7. Audit session: review of completed checklist, document review, collecting and verifying information, record audit findings, prepare audit conclusions.

8. The audit team prepares and distributes audit report to NPRA and supplier.

9. The supplier may review audit report and / or implement security improvements.

10. The audit team updates the report, if necessary, to final version, and distributes the report to the NPRA and the supplier

11. The NPRA decides whether or not to certify the supplier as EFC key receiver.

Figure 5.1 - The audit procedure

6.1.4 *Announcement*

The NPRA announces to the AutoPASS supplier that, in order for the supplier to receive EFC keys, an information security audit of all relevant systems must be conducted. The audit process is based on recommendations in ISO 19011:2011 Guidelines for auditing management systems. A self - assessment checklist based on information security requirements in ISO/IES27001:2013 is sent to the supplier.

6.1.5 *The audit team*

The NPRA appoints an audit team of competent, independent resources that have no bindings to other AutoPASS suppliers, or to any of the supplier's competitors..

6.1.6 *The local audit manager*

In response to the audit announcement, the supplier is expected to appoint a local audit manager who will facilitate the audit. The local audit manager will be the primary contact point between the NPRA appointed audit team and the resources at the supplier.

6.1.7 *Completing the checklist*

The local audit manager engages supplier resources to complete the checklist and will ensure that necessary resources, documentation and information is made available to the audit team when required.

6.1.8 *Audit scope*

The information security audit will be based a checklist containing relevant recommendations from "ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems - Requirements". The following areas will be of prime interest:

Organization of information security
Human resource security
Asset management
Access control
Cryptography
Physical and environmental security
Operational security
Communications security

The completed checklist is to be returned to the audit team at least one week before the audit session.

6.1.9 *Audit session*

During the audit session the audit team will review the completed checklist and information security issues on all relevant systems that handle EFC keys, based on the completed checklist.
The audit team can inspect and verify the information security measures that are in place, or are missing, on systems, procedures and personnel that handle EFC keys.
The local audit manager will make available information, documentation, and personnel resources that are necessary for an efficient and timely implementation of the audit procedure.
The audit team will record audit findings and prepare for audit conclusions.
The audit team will decide whether additional audit sessions are necessary.

6.1.10 *Audit report*

Audit team prepares and distributes the audit report to the NPRA and the supplier.
The audit report presents the audit findings, these will be graded according to severity, from "serious defect" , "defect" to "recommendation".
The audit report shall be confidential, and shall be distributed in a secure manner.

6.1.11 *Review of audit report*

The supplier may review and comment the audit report, and point out any misunderstandings at the part of the audit team. The supplier may also offer to implement additions security improvements or correct any defects pointed out in the report.

6.1.12 *Final audit report*

The audit team updates the audit report, if necessary, to the final version, and distributes the report to the NPRA and the supplier.

The final report shall contain all audit findings, except for findings based on misunderstanding by the audit team. Issues that are corrected or improved by the supplier shall remain in the report, but shall be marked "corrected" or "improved".

The final report shall contain a recommendation to the NPRA whether or not the audit team recommends certification of the supplier as an EFC key receiver.

6.1.13 *NPRA decides based on the audition*

The NPRA decides whether or not to certify the supplier as EFC key receiver, or whether additions information security audit steps are necessary.

The NPRA informs the supplier of its decision.

7. FILE DISTRIBUTION METHOD AND PROCEDURE

This section gives an overview of the procedures for:

- Initial exchange of trust objects (certificates)
- Uploading of EFC-keys by the TTP

These initial exchange of trust objects is between the TTP role and the supplier, this procedure involves exchanging certificates. (TTP role signing certificate and supplier certificate for encrypting KDF files). This procedure ensures that the communication between the TTP and the supplier is secure and authenticated.

Note: The TORD system will be replaced by manual procedures. The procedues for handling of AIT files is also under review and will be superseded by other requirements.

The uploading of EFC-keys by the TTP is a process whereby the set of OBUs that are read and accepted by the road side equipment is updated. The outlined procedure should be expanded to include information on how to handle the most likely failure situations. The procedure is initiated by the TTP which informs the supplier that there will be new files uploaded to the TORD system. This initial warning should be given some time in advance so that the supplier can be prepared. The new AIT and KDF files are uploaded to the TORD system and are subsequently downloaded by the KFS. The supplier then has a maximum of 24 hours from the time the AIT file was uploaded to return an updated KDC file to the TORD system. This KDC should indicate that all road side equipment HSMs are updated. The specifications for the AIT, KDF and KDC file formats are given in chapters 9 to 11.

The protocol diagram given below gives an overview of the communication involved in these procedures:

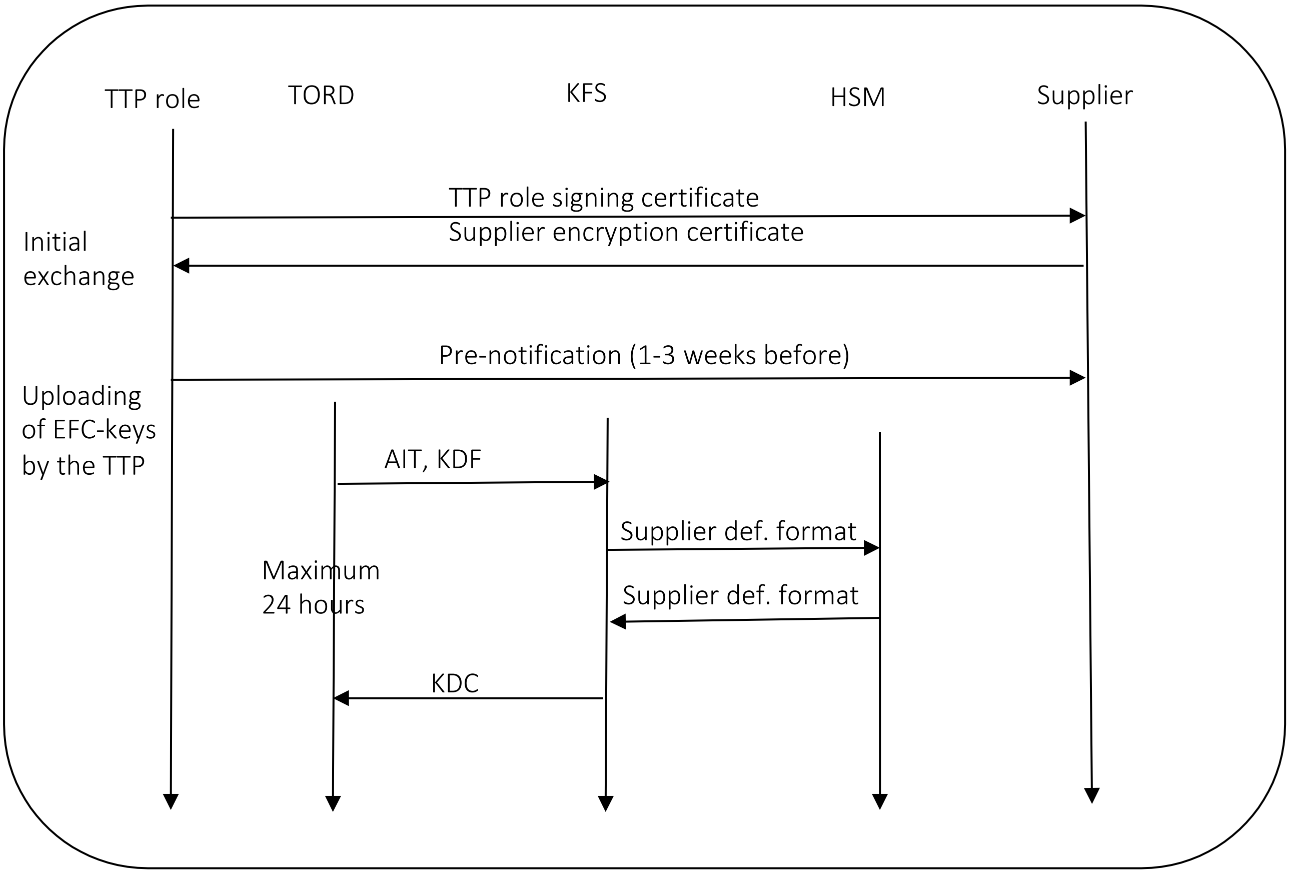

TTP role
TORD
KFS
HSM
Supplier
Initial exchange
TTP role signing certificate
Supplier encryption certificate
Uploading of EFC-keys by the TTP
Pre-notification (1-3 weeks before)
AIT, KDF
Supplier def. format
Maximum 24 hours
Supplier def. format
KDC

Figure 7-1 Overview of information exchange between TTP role and supplier

8. PERIODIC REVIEW PROCEDURE

This section gives an overview of the procedures for periodic review. The procedure for periodic review is different from the certification procedure in that the certification procedure is focused on the written hardware/software specifications and written operating procedures while the periodic review focuses on the actually installed HSMs and KFS and the personnel involved in the procedures.

Each periodic review consists of one meeting between the TTP role and the supplier, the following information must be prepared by the supplier before the meeting.

- The list of security equipment (HSMs and the KFS) installed with EFC-keys.
- The location of all security equipment.
- Personnel used for handling security related procedures and their roles.
- A comparison between the 3 lists above and the 3 lists from the previous periodic review meeting and an explanation of how the changes where handled.

The goal of this procedure is to ensure that no HSMs will be missing or mishandled by the supplier and the personnel involved understand their role in the secure handling of EFC-keys.

The TTP might performed spot tests before, during or after the meeting to verify that the lists are correct.

Severe discrepancies or severe breach of stated security measures and procedures regarding the handling of security equipment that are found as part of a periodic review will result in a revocation of the security certification for the equipment and/or personnel involved.

The revocation of security certification may in turn result in a breach of contract if the supplier cannot take appropriate measures to restore confidence. As a supplier without a security certification (see certification procedure) is no longer certified to handle EFC-keys and thus cannot read most OBUs.

9. KEY FILE

The Key File started as an EasyGo Key Distribution File described in EasyGo document 203 which is now obsolete. This is replaced by a XML with encrypted keys.Proposal for XML format:

<u>New xml file proposal</u>

```
<?xml version = '1.0' encoding = 'UTF-8'?>
<keyFile version = "1.1">
  <key keytype="1" name="Access" reference="120" algorithm=”2TDES”>
    <keyValue>6327….1525</keyValue>
    <ContextMark>30C00B00010B</ContextMark>
    <KVC>F2033E</KVC>
  </key>
  <key keytype="0" name="Authentication111" reference="111" algorithm=”2TDES”>
    <keyValue>3DD2….5284</keyValue>
    <ContextMark>30C00B00010B</ContextMark>
    <KVC>72B5B7</KVC>
   </key>
</keyFile>
```

“KeyType” shall be in line with table 25 in ISO/TS 19299:2015 (formerly CEN/TS 16439). The proposal is also to add a “version” to keyFile to distinguish between different versions of the XML, and an algorithm to distinguish the algorithm used for the key and for the KVC calculations. Key name should also reflect “KeyName” in table 25.

The EFC master keys are encrypted using RSA (Asymmetric public key encryption method). Each key is encrypted individually. Encryption is done according to scheme RSAES-OAEP using SHA-256 both in encryption and padding.

For example Java code for decryption:

```
OAEPParameterSpec oaeppara = new OAEPParameterSpec ("SHA-256",
OAEPParameterSpec.DEFAULT.getMGFAlgorithm(),
MGF1ParameterSpec.SHA256, OAEPParameterSpec.DEFAULT.getPSource());
Cipher cipher = Cipher.getInstance("RSA/ECB/OAEPWithSHA-256AndMGF1Padding");
cipher.init(Cipher.DECRYPT_MODE, privKey, oaeppara);
```

Table 25 – Overview of DSRC keys in 9.3.3.2 ISO 19299:2015

DSRC AID	Idenified by	Applicable standard	Key Name	KeyType	Resulting authentication code
1	EFC_ContextMark + KeyRef	EN 15509:2014	Authentication key1… AuthenticationKey4	0	MAC_TC
1	EFC_ContextMark + KeyRef	EN 15509:2014	Authentication key5… AuthenticationKey8	0	MAC_TSP
1	EFC_ContextMark	EN 15509:2014	Access Key	1	AC_CR
20	CCC_ContextMark + KeyRef	ISO DIS 12813:2014	Authentication key1… AuthenticationKey4	2	MAC_TC
20	CCC_ContextMark + KeyRef	ISO DIS 12813:2014	Authentication key5… AuthenticationKey8	2	MAC_TSP
20	CCC_ContextMark	ISO DIS 12813:2014	Access Key	3	AC_CR
21	LAC_ContextMark	ISO DIS 13141:2014	Access Key	4	AC_CR
21	LAC_ContextMark + KeyRefMAC_TC_LAC	ISO 19299:2015	LAC_ AuthenticationKey _TC	N.a.	MAC_TC

Table for legacy tags (under revision):

DSRC AID	Idenified by	Applicable standard	Key Name	KeyType	Resulting authentication code
	ContextMark + KeyRef	Upcomming EasyGo 202-F	AutoPASSNative1… AutoPASSNative5	100	Native MAC
	ContextMark + KeyRef	Upcomming EasyGo 202-F	AutoPASSForeign1… AutoPASSForeign5	101	Foreign MAC

XML schema for the SVV proposal using http://www.xmlforasp.net/codebank/system_xml_schema/buildschema/buildxmlschema.aspx for generating the XML schema

```
<?xml version="1.0" encoding="utf-16"?>
<xsd:schema attributeFormDefault="unqualified" elementFormDefault="qualified" version="1.0"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <xsd:element name="keyFile" type="keyFileType" />
  <xsd:complexType name="keyFileType">
    <xsd:sequence>
      <xsd:element maxOccurs="unbounded" name="key" type="keyType" />
    </xsd:sequence>
    <xsd:attribute name="version" type="xsd:decimal" />
  </xsd:complexType>
  <xsd:complexType name="keyType">
    <xsd:sequence>
      <xsd:element name="keyValue" type="xsd:string" />
      <xsd:element name="ContextMark" type="xsd:string" />
      <xsd:element name="KVC" type="xsd:string" />
    </xsd:sequence>
    <xsd:attribute name="keytype" type="xsd:int" />
    <xsd:attribute name="name" type="xsd:string" />
    <xsd:attribute name="reference" type="xsd:int" />
  </xsd:complexType>
</xsd:schema>
```

10. EXPENSES

The supplier is responsible for, and shall cover all expenses incurred by the supplier in:

- The production and installation of the HSMs and / or KFS
- Initialisation of HSMs.
- Obtaining security certification for all relevant security systems (HSM, KFS)
- Initialisation of each HSM-unit.
- Participating in the initial security audit and in periodic security reviews.

Also when considering expenses:
For security purposes the software in the HSMs might be write-once, this ensures that the no malicious software can be imported into the HSMs, but this will affect adversely the costs of changing HSM software. The HSMs are therefore specified with "secure software update" functionality. Should this functionality be omitted then the supplier must cover all costs of physically changing HSMs in road side equipment.

11. APPENDIX A TRANSACTION MODEL

A transaction model is a model for the communication between the road side antenna and the OBU. The set of transaction models shall correspond to the set of protocols defined in the AIT file.
All transaction models begin with an initialisation phase containing the BST and VST commands.
The next step is a presentation phase where identifying information is read from the OBU. The presentation phase might be followed by a receipt phase and the transaction model ends with a tracking or closing phase.
For all EFC Context Marks not defined in the AIT file, the road side antenna shall go directly from the initialisation phase to the tracking or closing phase.
The transaction models shall be detailed in the project planning phase for the following set of OBUs:
OBUs conformant to the proprietary AutoPASS protocol
OBUs conformant to the proprietary PISTA protocol
OBUs conformant to ISO 15509 level 0
OBUs conformant to ISO 15509 level 1
Example of a transaction model for AutoPASS OBUs:

Phase	RSE		OBU	Comments
Initialisation	Initialisation.request (BST)	→		
		←	PrWRq	
	PrWA	→		
		←	VST § EFC-ContextMark	
Presentation	GET_SECURE.request [RndRSE, KeyRef] § NtsData1	→		Attribute id = 99
		←	GET_SECURE.response § Authenticator	Master key required in RSE
Receipt	SET.request § NtsData2	→		Attribute id = 100
		←	SET.response	
Tracking or closing	ECHO.request	→		Optional
		←	ECHO.response	
	EVENT_REPORT.request [Release]	→		Optional