AP-1.3
AutoPASS
EFC Security Architecture

Version: 2.01
Date: 13 April 2021

DOCUMENT STATUS

Document no	AP-1.3 AutoPASS EFC Security Architecture

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
0.9	22.05.20	NPRA	Totally rewritten from old document “4.5 Security Strategy”. Draft to a final ver. 2.0. NB: Exact definition of TTP role not yet finalized.
2.0	24.11.20	NPRA	Some changes after RBPS consultation
2.01	13.04.21	NRPA	Version for publication

Table of Contents

1. DEFINITIONS, ABBREVIATIONS AND REFERENCES

1.1. REFERENCED DOCUMENTS

The following table lists referenced documents:

Ref.	Document name	Description
1.	AP-1.0 AutoPASS_Definisjoner, Standarder og Direktiver	Describes the definitions, standards and directives relevant for AutoPASS.
2.	AP-1.6 Requirements for On-board Equipment (OBE) for use in AutoPASS Samvirke	Minimum requirements for OBE used in AutoPASS

1.2. NORMATIVE REFERENCES

The standards and directives referenced within this document are described with full titles in ref.[1].

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

1.3. TERMS AND DEFINITIONS

The Terms, definitions and standards used in this document are defined in ref.[1].

2. INTRODUCTION

2.1. SCOPE OF DOCUMENT

This document specifies a security architecture surrounding EFC keys (master keys used for authentication and access control in OBE). The goal of this document is to achieve uniform procedures for handling of EFC-keys.

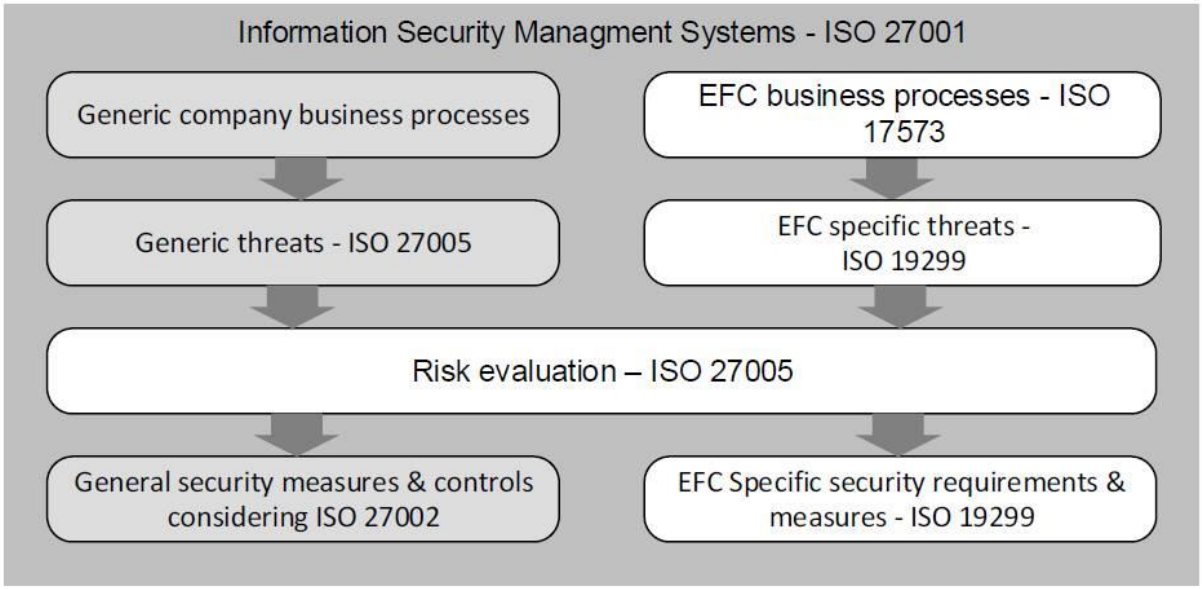
Handling of EFC keys is in ISO/IEC 11770-1 Information technology – Security techniques – Key management defined as *"The administration and use of the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction og keying material in accordance with a security policy."*

This document is aimed at TCs and TSPs, but also the functions where Trusted Third Party (TTP) and Interoperability Management (IM) are responsible. The TCs and TSPs may use subcontractors, typically CPE suppliers and OBE suppliers respectively, but the TC and TSP are responsible on behalf of their subcontractors for fulfillment of the requirements. Each actor in AutoPASS Samvirke has to implement the defined security measures and supervise the effectiveness. Security measures which do not work properly need to be improved.

This specification is based on general security principles for DSRC using OBE following the EN 15509 standard. It also follows and refers to relevant parts of international standards for information security described in the next subchapter.

2.2. INTERNATIONAL STANDARDS FOR INFORMATION AND EFC SECURITY

AutoPASS will use international and European security standards. Information security is based on the ISO "Information Security Management System" family of standards (ISO 27001 to 27007) and EFC specific standards ISO 17573 and ISO/TS 19299. The interrelations between these standards are shown in Figure 1.



Figur 1: International security standards

These standards deal with all relevant aspects of information security for a tolling environment.

- ISO/IEC 27001 Information technology -- Security techniques -- Information security management systems – Requirements covering all types of organisations (e.g. commercial enterprises, government agencies, non-profit organisations) and specifies the requirements for establishing,

implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system within the context of the organisation's overall business risks. It specifies requirements for the implementation of security controls customised to the needs of individual organisations or parts thereof;

- "ISO/IEC 27002 Information technology – Security techniques – Code of practice for information security management", establishing guidelines and general principles for initiating, implementing, maintaining and improving information security management in an organisation;

- ISO/TS 19299 EFC Security Framework, describing a set of requirements and security measures for stakeholders to implement and operate their part of an EFC system as required for a trustworthy environment according to its basic information security;

Information security is the protection of information (with focus on electronic data) stored and/or handled by the personnel and assets involved in the provision of the AutoPASS service and the service recipients.

Information and the supporting processes, systems and networks are very important business assets in EFC systems. The whole business model is based on collecting information, handling it and then collecting the payment from Service Users (SU) based on the collected toll data. Information security is essential for the accuracy, trustworthiness, reliability and availability of the EFC system as well as for the privacy of the SUs.

ISO/TS 19299 EFC Security Framework is vital regarding the approach and requirements in this specification.

2.3. THREAT ANALYSIS

A threat analysis with risk assessment is useful to define the security requirements. Such a threat analysis is described in Annex D in ISO 19299. The threats on the EFC system model and its assets are analysed both by considering several threat scenarios from the perspective of various attackers and by looking in depth on threats against the various identified assets (tangible and intangible).

Examples of such threats are computer-assisted fraud and service denial (e.g. 'I was not there') enabled by unauthorised access, computer hacking and malicious code.

2.4. TRUST MODEL

Three kinds of bidirectional peer-to-peer trust relations are present in the underlying EFC role model:

- between toll charger and toll service provider;
- between toll service provider and service user;
- between toll charger or toll service provider and interoperability management.

The trust model has two different levels, the contractual framework between the stakeholders (TC, TSP and SU) and the technical trust model between the IT infrastructure of the TC and TSP.

The definition of a trust model implies a choice between:

- hierarchical approach
- peer-to-peer approach
- or a combination of both

AutoPASS Samvirke has chosen a hierarchical trust model using a Trusted Third Party (TTP) described in chapter 3.1. Generally, the TTP may either be performed as a part of the interoperability management (IM), or as an external independent TTP.

3. AUTOPASS SECURITY ARCHITECTURE (INFORMATIVE)

3.1. ROLES AND RESPONSIBILITIES

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 (TSP) (In Norwegian: Utsteder)
- The User
- The Toll Charger (TC) (in Norwegian: Operatør)
- The Interoperability Manager (IM)

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

- The Trusted Third Party (TTP)

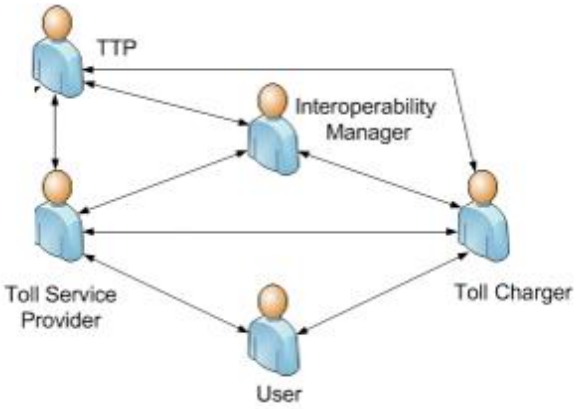


Figure 2: The AutoPASS Role model

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

TSP

The responsibilities of the TSP role related to OBE provision includes:

- Provide OBE compliant to the AutoPASS specifications
- Administrate end user contracts
- Ensure secure generation and handling of EFC security keys compliant to the AutoPASS specifications

The Interoperability Management

Norwegian Public Roads Administration (NPRA) and AutoPASS Forum (board with representatives from all relevant actors) have this role. The responsibilities of this role include:

- Manage the interoperability issues in AutoPASS Samvirke, which is the network for electronic payment of tolls on the public road network and ferry services in Norway
- Approval and supervision of actors and actors' technical equipment in AutoPASS Samvirke. This also includes security implementations.
- Define and maintain general requirements which all actors in AutoPASS must adhere to in order to be technically and functionally compliant with regards to interoperability

The Trusted Third Party (TTP)

As a trust model, it is established an agreement between the actors in AutoPASS Samvirke to have an

independent role called TTP, responsible for secure and proper handling of EFC keys in the entire AutoPASS domain. The TTP role was established by NPRA in 2007 using an external independent organization, but the scope of TTP has changed throughout the years due to organisational reforms. It is now a part of the Interoperability Management (IM), and NPRA as an authority body may take the role of independent, possibly with external consultancy. However, in this specification TTP is treated as a separate role.

The responsibilities of this role include:

- Secure central storage of security keys received from all TSPs
- Secure transfer of security keys to TC/CPE
- Verification that all actors have a sufficient level of security in their systems and processes before transfer of keys to or from TTP

TTP is responsible for operating a central Key Management System (KMS) in order to handle EFC keys securely. This system is air gaped from other networks to protect from all kinds of malicious attacks over the network. TTP collects EFC keys from TSPs in AutoPASS Samvirke (or alternatively generates keys for them if TSP prefers so), stores the keys securely in KMS and distributes the keys to TCs, possibly directly to their subcontractors/suppliers of CPE. These activities are executed when new suppliers/systems make this necessary or when there is a change of EFC-keys.

Figure 3 shows the concept of the TTP role distributing EFC keys to/from TSP and TC. In addition it shows what kind of information that are exchanged between the actors. TSPs use keys in their OBE in order to protect the use of them, and TCs use keys in their CPE in order to read and authenticate the OBE from TSPs.

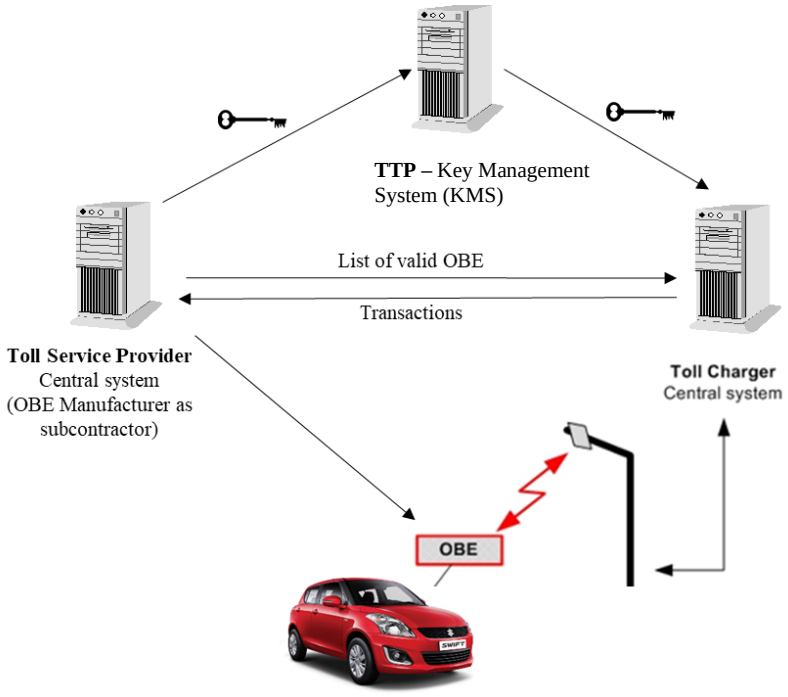


Figure 3: The physical architecture

3.2. EFC KEYS IN EN15509 OBE

EN 15509 defines two different levels of security – level 0 and level 1. In security level 0 the OBE shall be able to calculate authenticators based on authentication keys stored in the OBE to validate data integrity and origin of the transaction data. In security level 1 the OBE shall support (additionally to the functions of security level 0) the calculation of access credentials for the protection of user related data on the OBE.

Security level 1 is mandatory in AutoPASS Samvirke.

Access credentials master key

The access credentials master key is needed at the CPE to successfully communicate to the OBE at security level 1.

The access credentials master key has to be distributed by the TSP to all TCs in the regime.

Authenticator keys

There are 8 data elements defined for authentication keys on the OBE, 4 operator authentication keys and 4 issuer authentication keys.

The operator authenticator key is needed at the TCs systems to check during transaction or later whether the OBE is a genuine equipment of the corresponding TSP.

At least one operator authenticator key (usually with KeyRef 115 …118) has to be distributed by the TSP to all relevant TCs.

The issuer authenticator key is needed at the TSP's own systems to check if the transactions delivered by a TC were generated involving his own equipment.

The issuer authenticator keys are never distributed from TSP.

3.3. USAGE OF KEYS IN A TRANSACTION FLOW

Figure 3 shows how EFC keys may be used to protect an OBE transaction throughout the transmission of a transaction from generation in CPE to verification at the TSPs CS.

A tolling transaction is created in the roadside equipment. It might be sent through several systems largely in control of the TC before it reaches central systems that are controlled by the NPRA. From there the transactions are communicated to the TSP and end up as a line in a customer's bill. All actors handling these transactions can duplicate, create, remove or falsify these transactions. To make such actions as unlikely as possible, the authentication keys may be used to check transactions any place in the chain. In order to execute such checks, special values (Message Authenication Codes – MACs – for both TC and TSP) from the CPE authentication calculations have to follow the transaction from CPE to the different back-office systems. AutoPASS does not use all these checks in the current implementation (refer to step 6 and 7 in the figure below).

A special device HSM (Hardware Security Module) in the figure needs to be described. HSM is an on-line system connected to CPE and possibly also to central systems. This system contains EFC keys received from the actor´s key handling system and uses these EFC keys for computing access credentials and MAC verification. The secure/tamper-resistant hardware of these HSMs makes it impossible to copy EFC keys from HSM to other systems.

This process shows a simplified view of the key usage related to the transaction flow.

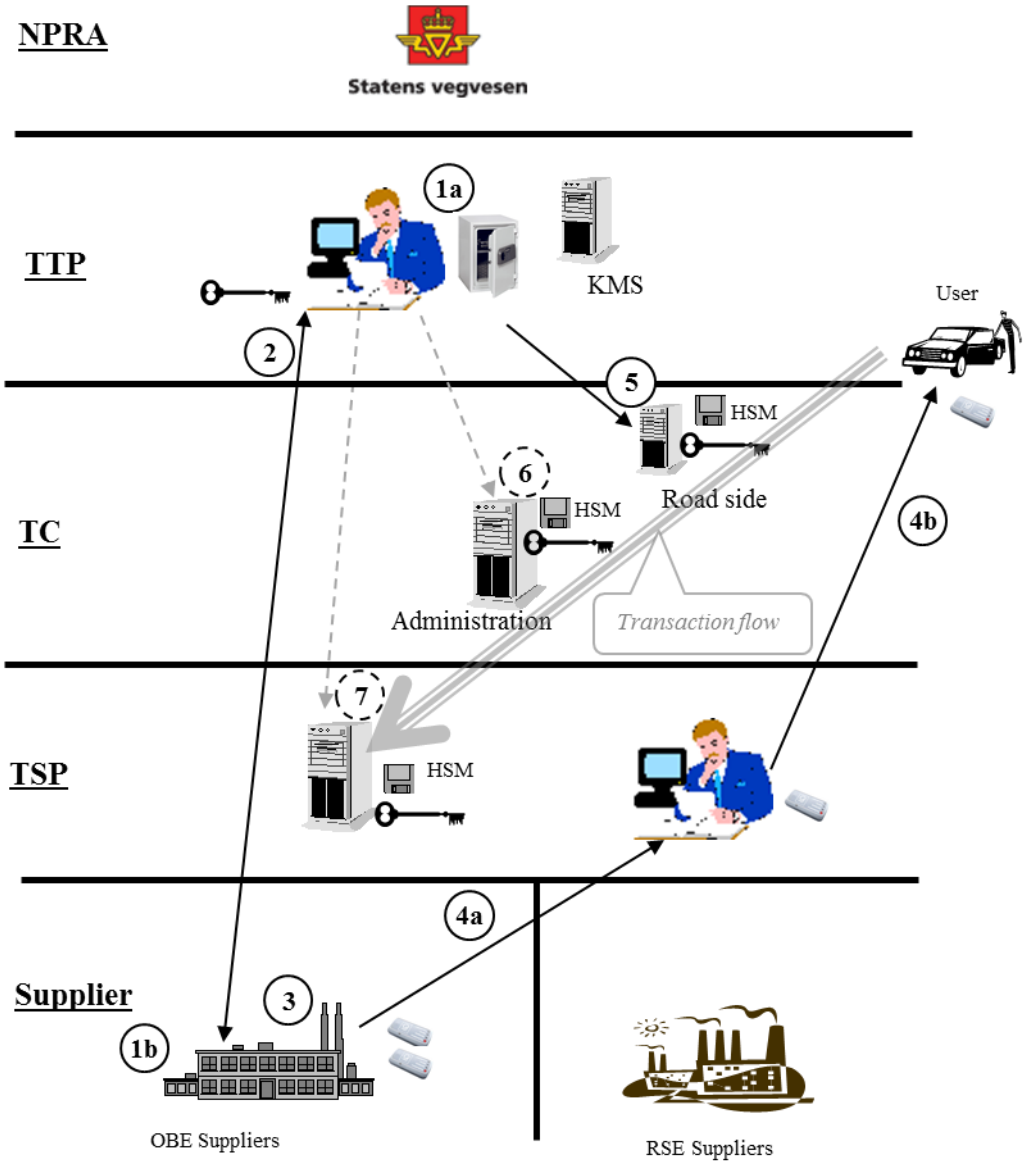


Figure 4 Usage og keys in a transaction flow

Descripion of the steps in the figure:

1 Either the TTP or OBE Supplier generates cryptographic master keys for a generation/batch of OBE for a TSP. The keys are of two types: Access keys and Authentication (TC & TSP) keys.

2 Keys are securely transferred between OBE Supplier (subcontractor of TSP) and TTP. The keys are securely stored by the TTP in the Key Management System (KMS).

3 OBE Supplier populates the manufactured OBE with keys. The keys are diversified, making each OBE key unique.

4 The OBE are delivered to the TSP for further distribution to customers.

5 The TTP distributes (TC) keys to the Road Side Equipment (CPE), normally through the CPE Supplier. The keys are stored in a hardware security module (HSM) in the CPE. The Access keys are used by the TC to be able to read the OBE. The Authentication keys are used by the TC to verify the authenticity of the OBE read by the CPE.

6 *(Additional verification step currently not in use)*

TC Authentication keys are stored in a HSM installed as an interfacing unit to the TC's central system. The keys are used by the TC to verify that the transferred transactions from the CPE are from genuine OBE transactions.

7 *(Additional verification step currently not in use by AutoPASS TSPs, but new TSPs may do so)* TSP Authentication keys are stored in a HSM installed as an interfacing unit to the TSP's central system. The keys are used by the TSP to verify that the claims from the TC are genuine.

3.4. PROCESS FOR GENERATING A NEW KEY SET FOR A NEW TSP OR OBE TYPE

There are 2 events that trigger this process:

- A new TSP is established
- An existing TSP issues a new generation/type of OBE

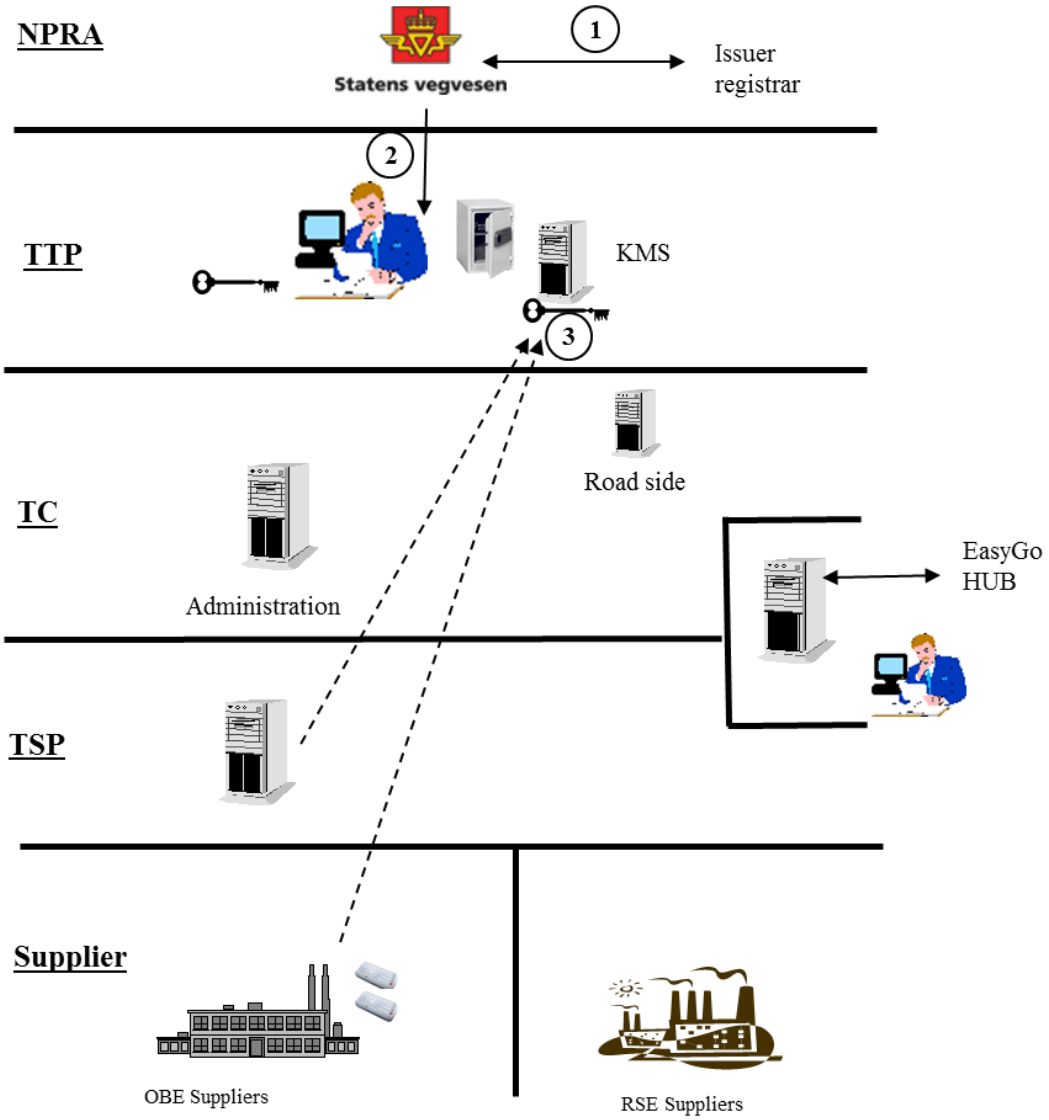


Figure 5 Generating a new key set for a new TSP or OBE type

1 *(Only if new nationally assigned TSP in Norway)* NPRA registers the new TSP in the official national TSP list maintained by Standard Norge according to ISO 14816. A TSP-ID is designated.

2 NPRA orders the TTP to establish in KMS:

a) (Only if new TSP) A registered new TSP with TSP-ID
b) Security keys for the OBE type(s) of the TSP

3 TTP either generates or receive from TSP (normally directly from the OBE Supplier as a subcontractor of the TSP) a set of cryptographic master keys and associates them with the new TSP. If received from the OBE Supplier, see process in chapter 3.5 step 1-2. Keys are stored securely in the KMS.

3.5. PROCESS FOR DISTRIBUTION OF KEYS AND KEY RELATED INFORMATION

When a new TSP or TC is added to AutoPASS Samvirke or a TSP decides to add or change DSRC keys, there is the need for the TSP to distribute new trust objects to all relevant TCs, and the TCs have to update his CPE's key data base.

Every distinct EFC context mark (defined by ContractProvider, TypeOfContract, ContextVersion), is connected to a defined DSRC keyset. Each key is uniquely defined based on the following information: EFC context mark, Type of key in the key set,The key – 16 bytes of information, Key Verification code.

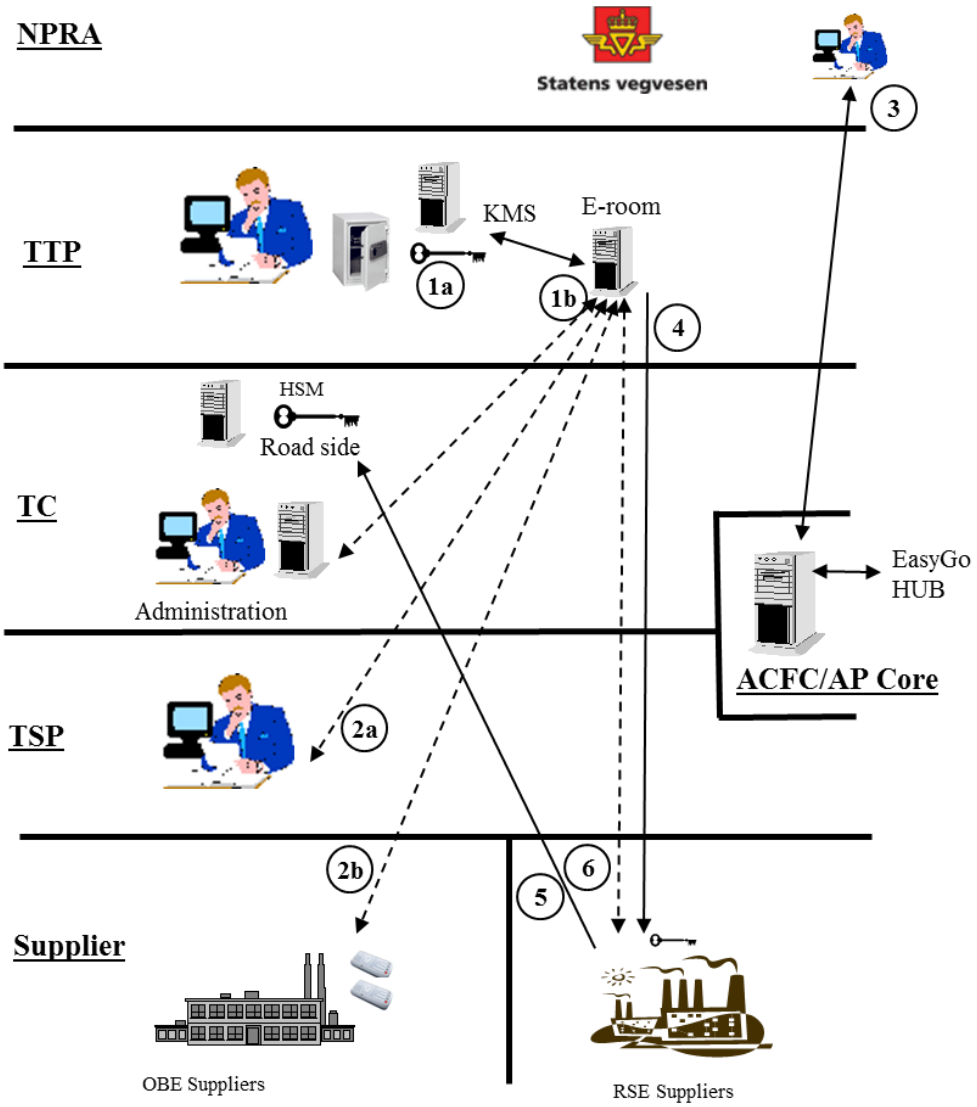


Figure 6 Distribution of keys and key related information

(Step 1-3 apply when new keys for AutoPASS, see process in chapter 3.4)

1. TTP will generate and provide the suppliers with X.509 certificates containing a public RSA key (transport key). The NPRA decides how this information is shared between the parties..
2. As both TTP and TSP (TSP normally through OBE Supplier as a subcontractor of TSP) can be the source of the EFC master keys, the keys must be exchanged between the two parties. The sender must encrypt each EFC master key individually with the transport key available before it is sent in xml-files on specified format via e-room. The receiver decrypts the transmitted EFC master keys and stores them securely.
3. In ACFC or EasyGo HUB (depending on nationally assigned or EasyGo TSP), key related information of the new/updated OBE is defined in a user interface, and the AIT file is updated with this information. Consistency between the AIT file and key file must be confirmed. The AIT file in ACFC/AutoPASS Core is exchanged/merged with EasyGo HUB.

Step 4-6 apply for distribution to AutoPASS CPE.

4. The TTP distributes EFC master keys (TC keys) to the Road Side Equipment (CPE) of the TC, normally through the CPE Supplier as a subcontractor of the TC (see step 5 in Process A). Distribution is done in the same encrypted manner with xml-files as described above.
5. The CPE Suppliers (or TCs) decrypt the keys with their native transport key, process the keys in theirs own Key Forwarding System (KFS) and upload the keys to their production equipment.
6. The CPE suppliers (or TCs) are informed that an updated AIT file is available and ready to be uploaded to their production equipment. Uploading to the production equipment may be done manually or automatically via ACFC/HUB.

4. SECURITY REQUIREMENTS FOR AUTOPASS

4.1. GENERAL REQUIREMENTS COMMON FOR ALL ACTORS HANDLING EFC KEYS

[R 1] Relevant actor (TSP, TTP) fulfils all requirements that can be derived from the process description in chapter 3.4: Process for generating a new key set for a new TSP or OBE type.

[R 2] Relevant actor (TSP, TC, TTP) fulfils all requirements that can be derived from the process description in chapter 3.5: Process for distribution of keys and key related information.

[R 3] EFC keys will always be sent encrypted between systems handling EFC keys and will always be stored securely. The transmission, storage and usage of cryptographic keys in a TC or TSP system shall fulfil the requirements of ISO TS 19299 chapter 9 (key management). In particular, for the handling of DSRC master keys, the requirements of chapter 9.3.4. apply.

[R 4] Actors shall have systems and procedures in place that prevents that EFC keys can be compromised. This includes an on-line or off-line system based on secure technology that receives and/or sends files with encrypted EFC keys from/to TTP. This system must be used for re-packaging and re-encryption of these keys including initializing HSMs with keys. The system must be installed in a secure location under sole control of the involved actor. Access to the keys stored in such systems requires at least two factor authentication mechanisms.

[R 5] The actor shall make all relevant documentation of compliance to EFC security requirements available to the NPRA and/or TTP on behalf of NPRA for the purposes of approving the systems/procedures. The requirements will be implemented by the actor and documentation will be approved by NPRA possibly by a verifification by TTP. The scope of this requirement includes all systems, procedures and personnel involved in handling EFC master keys. It also includes maintaining a list of all security equipment in their toll stations (HSMs and other systems) installed with EFC-keys, including the location of this equipment.

4.2. REQUIREMENTS FOR TC

[R 6] The TC must adhere to the security requirements in ISO/TS 19299 Clause 6 that are relevant for TC and DSRC communication. That applies for all such requirements except those which address equipment (and/or processes) not in use in AutoPASS Samvirke, e.g. ICC cards. The implementation shall fulfil all security measures (described in ISO/TS 19299 clause 7) that are associated to the relevant security requirements in Clause 6.

[R 7] The TC must always use HSM to store and handle keys in CPE. HSM must be able to handle Authentication keys and Access credentials for EN15509 OBE and be equipped with hardware able to perform AES encryption/decryption. Initialization of HSMs must only be performed by approved personnel, in secure environments and based on written procedures.

4.3. REQUIREMENTS FOR TSP

[R 8] The TSP must adhere to the security requirements in ISO/TS 19299 Clause 6 that are relevant for TSP and DSRC communication. That applies for all such requirements except those which address equipment (and/or processes) not in use in AutoPASS Samvirke, e.g. ICC cards. The implementation shall fulfil all security measures (described in ISO/TS 19299 clause 7) that are associated to the relevant security requirements in Clause 6.

[R 9] The security keys for all elements in the OBE will be supplied and managed under control and responsibility 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.

[R 10] Security keys for the EFC element in the OBE are for the sole use by toll stations in AutoPASS and

other European toll domains. This is further detailed in the requirements for the OBE given in ref.[2].

[R 11] TSPs may generate EFC keys for their OBE themselves, e.g. if they already have OBE with a set of keys that fulfills the EN 15509 specifications. To ensure the correct quality of the entire AutoPASS system, the TSP must document for approval at least:

- The origin of the master keys used to create these keys
- The methods of communication to move the master keys from the KMS they were created in to the supplier
- The methods of derivation used to create the derivated keys
- The way of transportation of keys between organizations,
- The ways of transportation of keys inside organizations
- The storage of keys and access to them

4.4. REQUIREMENTS FOR TTP

[R 12] The TTP is responsible for overseeing the secure transfer of security keys to TCs/CPE.

[R 13] The TTP is responsible for all tasks described for the TTP role in chapter 3.1.

[R 14] The TTP must adhere to the security requirements in ISO/TS 19299 Clause 6 that are relevant for their role and DSRC communication. That applies for all such requirements except those which address equipment (and/or processes) not in use in AutoPASS Samvirke, e.g. ICC cards. The implementation shall fulfil all security measures (described in ISO/TS 19299 clause 7) that are associated to the relevant security requirements in Clause 6.

[R 15] TTP must maintain a procedure to determine whether an AutoPASS actor can be allowed to receive EFC keys from the TTP. The security systems and procedures of the actor must be verified by TTP and approved by NPRA before EFC keys are transferred to this actor. In the cases where TTP detects unsufficiant security e.g. breach of the requirements that apply for TC/TSP in ISO/TS 19299, this shall be reported to the relevant actor and NPRA, and appropriate actions shall be agreed.