DSRC Key Management

Annex 2.5 to
Joint Venture Agreement
Toll Service Provider Agreement

Document: 205
Version: 3.0
Date: 30 March 2017

Table of contents

Document Revision History

Version	Date	Author	Main changes
2.0	2014.11.03		Last edition with KDF/KDC key exchange
3.0	2017.03.30	TR	RSA encryption added in ch 3.2, manual key exchange between TSP and TD, DKF/DKC removed Approved by ESC (written procedure)

1 Purpose and scope

The purpose of this document is to describe the minimum requirements for DSRC key management within EasyGo regarding DSRC master keys (Access credential key and authenticator keys).

2 DSRC related trust objects

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

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.

It has been agreed that security level 1 has to be used in EasyGo+.

2.1 Access credentials master key

The access credentials master key is needed at the RSE 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.

2.2 Authenticator keys

2.2.1 Operator authenticator key

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.

2.2.2 Issuer authenticator key

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.

3 DSRC key distribution

When a new TSP or TC is added to EasyGo+ (or EasyGo basic when relevant) 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 RSE's key data base.

Every distinct EFC context mark (defined by EFCContextmarkContractProvider, EFCContextmarkTypeOfContract, EFCContextmarkContextVersion), 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

3.1 Transmission of keys based on bilateral agreements

The distribution of keys is done based on bilateral agreements for key transfer. Chapter 3.2 below: "DSRC key input interface" gives guidelines for a minimum set of requirements for key transfer. These requirements are not binding for the agreements on how keys are transferred between each individual TSP and TC.

It is possible to outsource the central storage and distribution of keys to a service partner who handles the key distribution on behalf of the TSP/TC. In this case, all conditions on DSRC key input interface described below apply.

3.2 DSRC key input interface

In minimum following requirements apply:

The TCs systems shall provide means for a centralised input of key information by the TSP (or other authorised personnel), which is to be carried out within the scope of a formal key handover procedure at the TC's premises.

This interface shall offer as a minimum:

- Definition of a unique key ID
- Input of RSA encrypted keys **):

  Mandatory for all existing TC's from July 1st, 2019 and all new TC's. Existing TC's are TC's accepted as part of EasyGo (according to annex 4.2 and 4.4) before 1st of July 2017. New TC's are TC's accepted after 1st of July 2017.

- Input of split XOR key parts (2 or 3 parts) of a key in hexadecimal format with or without parity check:

  Mandatory as long no RSA key input is possible

- A key check value (KCV) shall be calculated and displayed
- After the key is saved encrypted together with the ID and KCV to the system, no further readout of the key value shall be possible
- It must be possible to retrieve the key KCV by using the key ID
- It must be possible to delete key information indicated by a key ID
- Key input activities are allowed only for authorised persons, therefore suitable means for user authorisation (like a user login procedure or key cards etc.) must be established
- Activities for key input or deletion shall be logged

**) RSA encryption method:

Each key is encrypted individually as a set of bytes (usually 16 bytes) before transmission/ input. The encryption algorithm is RSA as defined in PKCS#1v2.1. The key length of the RSA key is 2048 bit and the value of 65537 should be used as the exponent. Encryption is done according to scheme RSAES-OAEP.

3.3 DSRC key handling at the TC's system

All DSRC keys must be stored and distributed to RSE only in encrypted form and must be protected against access.

The TC is responsible to take adequate security measures (secure transmission and storage, physical access control, user access control, security policies, etc.) to avoid a key compromise.

There are several possible solutions for distribution of DSRC keys in the local environment of the TC. The implementation details are left to the TC, but shall comply with the requirements of this document. The TCs shall describe their local security solution. The solutions shall be audited by the EasyGo security group and approved by the EasyGo management.

Examples for solutions are e.g.:

a) Storage of keys at the CS:

   The encrypted DSRC keys are stored at the CS of the TC and fetched by the RSE at start up in a secure way and held only in volatile memory.

b) Storage of keys at the CS in a Hardware Security Module (HSM):

   The DSRC keys are stored in a HSM at the CS of the TC and fetched by the RSE at start up in a secure way and held only in volatile memory.

c) Storage at the RSE in a HSM:

   The encrypted DSRC keys are transferred via the CS but stored in a HSM at the RSE

d) A combination of b) and c)

   Storing the keys in a Key Distribution System where the keys are only accessible through HSM or two-factor solutions, the keys are then distributed to other Key Distribution Systems in encrypted form that are likewise protected.

Fetching the DSRC keys "in a secure way" in this context means transmission over VPN tunnels and/or in encrypted format.

The recommended solution for the DSRC key handling, especially in new systems, is the use of HSM at both CS and RSE.

When the keys are only distributed in encrypted format, the transfer of public keys must be authenticated by other channels than e-mail.

4 General security requirements

In general, the following documents apply:

- EasyGo document 103 (EasyGo security policy)
- ISO/ TS 19299

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.

5 References

References	Doc. Ref	Document title	Date / Version
PKCS#1v2.1	RFC 3447	PKCS #1 V2.1: RSA CRYPTOGRAPHY STANDARD (June 14, 2002)	14.06.2002 / 2.1
	EN 15509	Road transport and traffic telematics - Electronic fee collection - Interoperability application profile for DSRC	
	ISO/TS 19299	Electronic fee collection — Security framework	1.10.2015
	EasyGo doc. 103	EasyGo security policy	