AP-3.6
DSRC Keyfile

Version: 1.0
Date: 4 July 2024

DOCUMENT STATUS

Document No.	AP-3.6 DSRC Keyfile

Status	Version	Description
Approved	1.0	

REVISION HISTORY

Version	Date	Author	Main Changes
1.0	4 July 2024	NPRA	New document. Documents the format already in use.

TABLE OF CONTENTS

1 PREFACE

1.1 Description

The DSRC communication in AutoPASS relies on the use of encryption keys for access control and authentication. The master keys for every type of OBE to be read must be installed on the RSE. The TSPs, or the OBE manufacturers on their behalf, will make the necessary master keys available to the NPRA on DSRC Keyfiles. The NPRA will then distribute the master keys to the TCs, or the RSE suppliers on their behalf, also using the DSRC Keyfile format.

The Keyfile is on XML format.

1.2 Format Versions

The format is the same as is used in other toll domains. Format version 1.1 is used.

1.3 File Name Generation

The file name syntax is not restricted to a certain format. It is encouraged to use a short descriptive filename for easy identification.

1.4 Data Formats

1.4.1 Character Set

The Keyfile uses standard XML UTF-8 character encoding.

2 KEYFILE FORMAT

The following XML Schema defines the XML format used in the DSRC Keyfile:

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema" attributeFormDefault="unqualified"
elementFormDefault="qualified" version="1.0">
  <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" use="required"/>
  </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" use="required"/>
    <xsd:attribute name="name" type="xsd:string"/>
    <xsd:attribute name="reference" type="xsd:int" use="required"/>
    <xsd:attribute name="algorithm" type="xsd:string"/>
  </xsd:complexType>
</xsd:schema>
```

2.1 Example Keyfile

The following is an example of a Keyfile with a keyset of one access and one authentication master key.

```
<?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>
```

2.2 Parameters

2.2.1 Keytype

The keytype according to ISO 19299.

- Authentication keys: 0
- Access keys: 1

2.2.2 Name

Free text. The use of descriptive names is encouraged, as all master keys in AutoPASS will end up in the NPRA Key Management System and in the RSE. Easy identification is appreciated for improved ease of maintenance.

2.2.3 Reference

Attribute ID of the key reference.

- Authentication keys: 111-118
- Access key: 120

2.2.4 KeyValue

The encrypted master key. The encryption shall be according to ISO 19299. That implies that RSA-2048 is used for encrypting the key with RSAES-OAEP in PKCS#1 v2.2 and SHA256 KDF1.

2.2.5 ContextMark

The EFC Context Mark the master key is associated with.

2.2.6 KVC

The Key Verification Code of the KeyValue (aka KCV). Following ISO 11568-2, calculated encrypting one block size of zeros with the plain key, then truncated to the leftmost three bytes.