RDW

# DA12EN - Vehicle Registration Card Reading Manual

*Interface specification v3.0.0*


| | |
|---|---|
| Author | RDW ICT |
| Version | 3.0.0 |
| Date | 14 May 2024 |
| Status | Final |
| Classification | Public |

**Document properties.**

| | |
|---|---|
| Contracting authority | RDW ICT |
| Project manager | Sipke Folkertsma |
| Project code | SAP code R/01133 |
| Document title | DA12EN - Vehicle Registration Card Reading Manual, Interface specification v3.0.0 |
| File name | DA12EN - Vehicle Registration Card Reading Manual v 3 0 0.docx |
| Archive name | |
| Key words | |
| Status | Final |
| Distribution | |

RDW ICT
Rozenburglaan 5
9727 DL  Groningen

## Version history

| Version | Date | Status | Author |
|---|---|---|---|
| 2.1.1 | 19-03-2014 | Final | RDW ICT |
| 2.1.2 | 07-12-2016 | Final | RDW ICT |
| 3.0.0 | 14-05-2023 | Final | RDW ICT |
| | | | |

## Change history

| Version | Date | Reason for change |
|---|---|---|
| 2.1.2 | 07-12-2016 | Updated example Maximum speed in table 6. |
| 3.0.0 | 14-05-2023 | Added support for the 3rd generation of Vehicle Registration Cards. |
| | | |

# TABLE OF CONTENT

# MANAGEMENT SUMMARY

The Dutch Vehicle Registration Card (NL-eVRC) is provided with a chip. This document describes how the chip of the Dutch Vehicle Registration Card can be read and verified. Reading of the chip does not require access rights and is therefore available to all parties. To read the chip only a PC/SC card reader and reading software are required. For verification a PKI certificate and the corresponding Certificate Revocation List (CRL) are required. These data can be downloaded from the RDW website.

The Dutch vehicle registration card complies to European regulation 2003/123/EC [1]. The chip contains the data as specified in the regulation and is secured as specified. Furthermore, the chip of the Dutch vehicle registration card contains additional registration data and may contain Certificate of Origin (CVO) data. Besides, the chip of the Dutch vehicle registration card is additionally secured via two extra security mechanisms. All data on the vehicle registration card chip is secured via Passive Authentication (PA) [2]. This means that over all data on the chip an electronic signature has been placed by the issuing organisation, RDW, which ensures that can be verified that the data in the data groups is unaltered and belongs together. The authenticity of the chip can be verified by means of Active Authentication (AA) [2]. This means the chip can prove it is genuine via a challenge-response protocol.

This document describes how the Dutch vehicle registration card chip should be read and verified. The document also describes reading and verification of foreign vehicle registration card chips complying with [1]. Since Dutch vehicle registration cards comply with this regulation, they could be read and verified in the same way. However, then no use is made of the additional security mechanisms in the Dutch vehicle registration card chip. This is not advised.

# 1 INTRODUCTION

## 1.1 Scope

The Dutch Vehicle Registration Card (NL-eVRC) is provided with a chip. This document describes how the chip of the Dutch Vehicle Registration Card can be read and verified. Reading of the chip does not require access rights and is therefore available to all parties. To read the chip only a PC/SC card reader and reading software are required. For verification a PKI certificate, obtained via a trusted channel, and the corresponding Certificate Revocation List (CRL) are required. These data can be downloaded from the RDW website. However, this does not fully guarantee the authenticity of the certificate. To guarantee the certificate's authenticity, the initial certificate needs to be exchanged in a secure way. RDW will set up a process with recognized parties which should be able to verify the Dutch vehicle registration card chip, the so-called recognized relying parties.

The Dutch vehicle registration card complies to European regulation 2003/123/EC [1]. The chip contains the data as specified in the regulation and is secured as specified. Furthermore, the chip of the Dutch vehicle registration card contains additional registration data and may contain Certificate of Origin (CVO) data. Besides, the chip of the Dutch vehicle registration card is additionally secured via two extra security mechanisms. All data on the vehicle registration card chip is secured via Passive Authentication (PA) [2]. This means that over all data on the chip an electronic signature has been placed by the issuing organisation, RDW, which ensures that can be verified that the data in the data groups is unaltered and belongs together. The authenticity of the chip can be verified by means of Active Authentication (AA) [2]. This means the chip can prove it is genuine via a challenge-response protocol.

This document describes how the Dutch vehicle registration card chip should be read and verified.

## 1.2 Target Audience

This document is meant for all parties which want to read and verify the chip of the vehicle registration card. The document contains the required information to implement reading and verification software. Reading and verification software may be developed by a party itself, but will for recognized relying parties also be provided by RDW. The document also contains information about how the reading and verification software can be provided with the required PKI certificates and CRLs.

It is assumed that the reader is familiar with asymmetric cryptography and public key infrastructures.

## 1.3 Document Structure

Chapter 1 contains the scope, target audience and document structure. Chapter 2 contains the glossary and references. In Chapter 3 background information about the vehicle registration card chip, the public key infrastructure and the security mechanisms is provided. In Chapter 4 the reading and verification process is discussed in detail: section 4.1 contains a high-level flow chart, section 4.2 a step by step description of how a Dutch vehicle registration card chip should be read. Chapter 5 provides information about the communication between the vehicle registration card chip and the reading and verification software. Chapter 6 discusses the information exchange between the reading and verification software and other sources, like RDW.

The appendices contain the following information:

- App 1 contains the chip's Logical Data Structure,
- App 2 contains the APDUs for the Dutch vehicle registration card chip in the operational phase,
- App 3 provides an example of the communication trace between reading and verification software and the chip of a Dutch specimen vehicle registration card.,
- App 4 contains the CSCA certificate that has been used for the specimen vehicle registration card used in App 3.

# 2 GLOSSARY AND REFERENCES

## 2.1 Glossary

| Term | Explanation |
|---|---|
| **AA** | Active Authentication, cryptographic mechanism to prove the authenticity of the chip via an AA public-private key pair and a challenge-response mechanism. |
| **Challenge** | (Partly) random number generated by an entity to verify the authenticity of another entity. The challenge needs to be signed by the latter entity with its private key. |
| **CSCA** | Country Signing Certificate Authority, the highest certificate issuing entity in the PKI chain for signing data of the eVRC issuing organisation RDW. |
| **CSCA private key** | The secret key of the CSCA key pair which is only available in the CSCA and used to sign certificates. |
| **CSCA public key** | The non-secret key of the CSCA key pair which can be used to verify certificates and CRLs signed with the CSCS private key. |
| **CSCA root certificate** | A certificate issued by the CSCA with its own CSCA public key. The certificate links the public key to the CSCA and has a limited validity period. The CSCA root certificate is signed with the CSCA private key which belongs to the CSCA public key in the certificate. The certificate (the signature) can be verified with the public key from the certificate itself. The CSCA root certificate is available on the RDW website, but recognized relying parties with an official responsibility to verify vehicle registration cards (like Dutch and foreign police) should also obtain the certificate in a trusted way via separate process since the website does not provide enough assurance for these parties about the authenticity of the initial CSCA certificate. |
| **CSCA link certificate** | A certificate issued by the CSCA containing a new CSCA public key. The certificate is signed with the current CSCA private key and can be verified with the current CSCS public key. This enables a CSCA link certificate to be exchanged via an unsecured channel like the RDW website. The certificate links the new trust point to the current trust point. |
| **CRL** | Certificate Revocation List, a list with revoked certificates issued by the CSCA. The CSCA signs the CRL to enable the authenticity of the CRL to be verified. The CRL is available at the RDW website and is refreshed periodically. A new version is also published if a certificate is added to the CRL. For each CSCA key pair a separate CRL is issued. |
| **DS** | Document Signer, an entity within RDW which signs the data to be placed on the vehicle registration card chip. The DS has a key pair and a DS certificate issued by the CSCA. |
| **DS private key** | The secret key of the DS key pair which is only available in the DS and used to sign vehicle registration card chip data. |
| **DS public key** | The non-secret key of the DS key pair which can be used to verify data signed by the DS private key. This DS public key is available in the DS certificate issued by the CSCA. |
| **DS certificate** | A certificate issued by the CSCA containing the DS public key. The DS certificate is signed by the CSCA private key and can be verified with the corresponding CSCA public key which should be available in the verification software. The DS certificate is available on the chip. The DS certificate has a limited validity period. |
| **NL-eVRC** | Dutch electronic Vehicle Registration Card, secure document with a contact chip containing information about the vehicle registration. |
| **Hash** | A unique number calculated over data via a hash or digest algorithm, normally to be signed afterwards by a private key. When the data changes, the hash also |

| | |
|---|---|
| | changes. The original data cannot be derived from the hash. RDW uses the SHA-256 hash algorithm. |
| **Key Pair** | Mutually linked public and private keys used in asymmetric cryptographic algorithms as used for signing hashes and challenges. |
| **PA** | Passive Authentication, cryptographic mechanism to proof the authenticity of the chip data via a signature over the data with the DS private key. |

## 2.2 References

| Ref. | Title | Author | Version | Date |
|---|---|---|---|---|
| [1] | 2003/127/EU | European Commission | n.a. | 23-12-2003 |
| [2] | ISO/IEC 18013-3 | ISO/IEC WG 10 | n.a. | 2009 |
| [3] | ICAO Doc 9303 | ICAO | 6 | 2006 |
| [4] | RFC 5280 | D. Cooper *et. al.* | n.v.t. | May 2008 |
| [5] | CP/CPS NL-eVRD-PKI, see: http://www.rdw.nl/ | RDW | 2.0 | 30-12-2013 |
| [6] | RFC 5652 | R. Housley | n.a. | September 2009 |
| [7] | ISO/IEC 7816-4 | ISO/IEC JTC 1 | 2 | 15-01-2005 |
| [8] | ISO/IEC 7816-8 | ISO/IEC JTC 1 | 2 | 01-06-2004 |
| [9] | RFC 4055 | J. Schaad *et. al.* | n.a. | June 2005 |
| [10] | ISO 9796-2 | ISO | 2 | 01-10-2002 |
| [11] | DA12 – Kentekencard uitleesdocumentatie, interface specificatie | RDW ICT | 2.1.1 | 30-12-2013 |
| [12] | TR-03111 Elliptic Curve Cryptography | BSI | 2.10 | 2018-06-01 |

# 3 BACKGROUND INFORMATION

The European regulation 2003/127/EU [1] allows issuance of vehicle registration documents on credit card format provided with a contact chip. Both the vehicle registration card and the chip shall comply with the requirements stated in Annex 1 and 2 of [1]. The regulation prescribes amongst others the data structure of the chip and the presence of files which guarantee the authenticity of the data and make it verifiable. The Dutch vehicle registration cards comply with this regulation. Besides, the chips of Dutch vehicle registration cards contain two additional security mechanisms with corresponding data groups on the chip to guarantee the authenticity of the chip and all data on the chip. The data groups present on the Dutch vehicle registration card are described in App 1.

The authenticity of the Dutch vehicle registration card chip can be verified by a relying party via the Active Authentication (AA) security mechanism. This mechanism depends on the other security mechanism that has been added to the Dutch vehicle registration card chip and that also guarantees the authenticity of all data on the chip and that the different data groups belong together, namely Passive Authentication (PA).

Both AA and PA have been implemented conform the international ISO/IEC driving licence standard [2]. These security mechanisms are also used to secure passports as described in ICAO Doc 9303 [3] and to secure European residence permits and Dutch and some foreign national identity cards.

The security mechanisms are explained in this chapter, to support parties which develop verification software on basis of this document to implement the verification of the security mechanisms in the correct way. A detailed description of the steps to be performed by the verification software can be found in Chapter 4, section 4.2. In this chapter, in section 3.2, the used PKI structure is discussed.

## 3.1 Signatures on the Dutch Vehicle Registration Card Chip

On a Dutch vehicle registration card chip three electronic signatures are present to guarantee the authenticity of the data on the chip and to make it verifiable. Two of these signatures are required according to the European regulation [1]. The third signature has been added by the Netherlands to enable PA and AA. The signatures present are:

- the signature in EF.Signature_A over the data in EF.Registration_A;
- the signature in EF.Signature_B over the data in EF.Registration_B;
- the signature in EF.Sod over all data groups on the chip.

Dutch vehicle registration cards are issued by RDW. RDW has chosen to generate all signatures present on one vehicle registration card with the same DS private key and thus make them verifiable with the same public key certificate. This public key certificate, the DS certificate, is available on the chip. To comply to the European regulation [1] and the ISO/IEC 18013 [2] standard it is present on the chip 3 times, namely in EF.C.IA_A.DS, EF.C.IA_B.DS and in the EF.Sod.

## 3.2 Public Key Infrastructure

For generation of the signatures and required certificates RDW has established a PKI with a Country Signing Certificate Authority (CSCA) as highest trust point (root). The CSCA issues certificates to Document Signers (DS) which generate signatures over data groups to be placed on the card. This is represented in Figure 1.

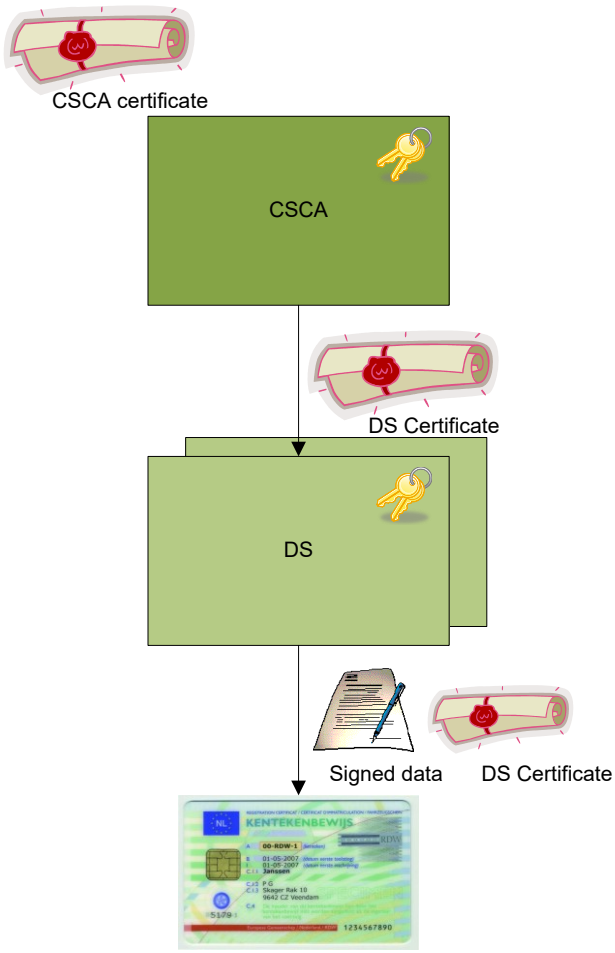


*Figure 1: Public Key Infrastructure for vehicle registration cards*

The CSCA has a key pair and corresponding (self-signed) CSCA root certificate. A CSCA root certificate has a validity period of 20 years. It is used for a period of 10 years to issue DS certificates. Shortly before the usage period ends a new key pair and corresponding CSCA root certificate are generated. Also, a CSCA link certificate is generated then. This certificate contains the new public key and is signed by the current private key. This enables the authenticity of the certificate to be verified via the current public key. This is represented in Figure 2.

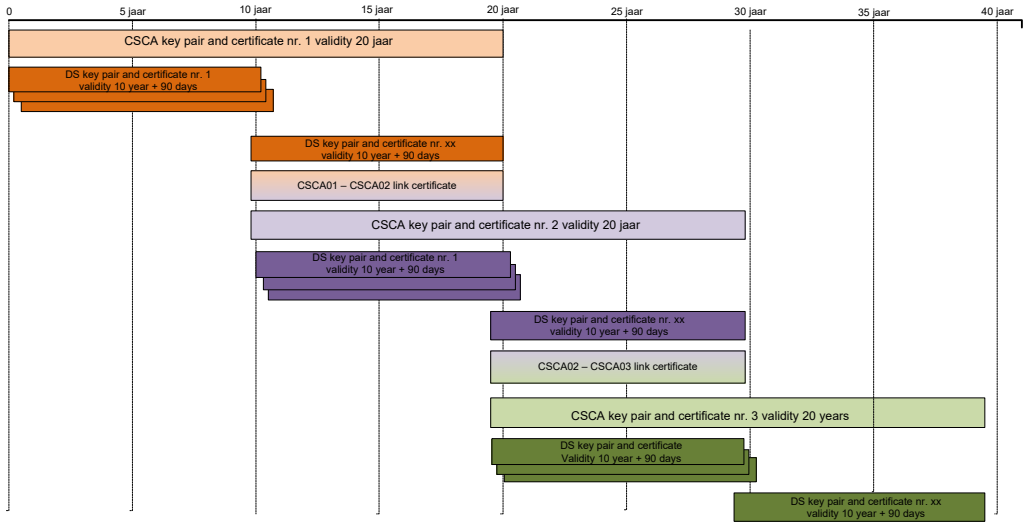


*Figure 2: Relation between CSCA root certificates, CSCA link certificates and DS certificates*

Relying parties require the CSCA certificate to verify the DS certificates. Therefore, RDW makes the CSCA certificates available on its website. Recognized relying parties with an official responsibility to verify vehicle registration cards (as the Dutch and foreign police) additionally need to obtain the certificate in a trusted way via a separate process, since the website does not provide sufficient assurance for these parties about the authenticity of the initial CSCA certificate. New CSCA certificates can successively be downloaded from the website since the authenticity of the link certificate for the new public key can be verified.

A DS has a key pair. The DS generates signatures over data groups with its private key of the key pair. The corresponding public key is available in the DS certificate issued by the CSCA. A DS certificate has a validity period of 10 years and 3 months. It is used at most 3 months to generate signatures. The validity period of a DS certificate always expires before the validity period of the CSCA certificate.

If the DS certificate has expired, in principle it cannot be used anymore for verification of signatures on the vehicle registration card chip. However, this does not mean that the vehicle registration card loses its validity. Also a vehicle registration card with expired certificates or with a non-functioning chip is valid.

If the DS private key is compromised or a suspicion of compromise exists, it is no longer used to generate signatures. The DS certificate is revoked and placed on the Certificate Revocation List (CRL). Signatures generated on basis of the revoked certificate are no longer valid.

The CRL is issued and signed by the CSCA. For each valid CSCA certificate a CRL will be published. The authenticity of the CRL shall be verified by relying parties on basis of the CSCA public key certificate. RDW publishes CRLs on its website. The location is indicated in the CDP extension of the DS and CSCA certificates. Periodically (every 180 days) a new CRL is generated and published. The CRL has a validity period of 200 days. RDW also generates a new CRL if a DS certificate is revoked. Recognized relying parties will be informed by RDW about this extra CRL.

The policy and procedures of the PKI are described in the combined Certificate Policy/Certification Practice Statement (CP/CPS) [5]. The object identifier (OID) of the CP/CPS is indicated in the Certificate Policy Extension of the DS and CSCA certificates.

## 3.3 Verification of Data Groups A and B conform 2003/127/EC

Conform the European regulation 2003/127/EC [1] electronic signatures are placed by the issuing organization over the data groups A and B on the chip (EF.Registration_A and EF.Registration_B). These signatures can be found in the files EF.Signature_A and EF.Signature_B. In these files also the used asymmetric algorithm and the hash algorithm can be found (for the format see App 1). The public key certificates with which the signatures and therewith the authenticity of the data in the data groups A and B can be verified, are stored in EF.C.IA_A.DS and EF.C.IA_B.DS. The format is X.509V3 (see [4]) conform the requirements in [1].

When reading the data groups A and B and verifying their authenticity according to the European regulation, first the authenticity of the certificates needs to be verified, then the signatures need to be verified ('deciphered') and then the hashes over which the signatures were placed need to be compared with the hashes over the data groups. Only if follows from this process that the data in the data groups A and B is authentic, it should be shown to the user. Step-by-step this process is described in section 4.2.

The DS certificates need to be verified for their validity period. The Dutch DS certificates have been issued by the Dutch CSCA and need to be verified with the CSCA public key certificate. Dutch DS certificates also need to be verified versus the certificate profile as described in the CP/CPS [5] and versus the CRL of which the URL is indicated in the certificate extension.

For most foreign certificates the DS certificate will be signed by the national CSCA. For verification the verification software needs to have these foreign CSCA certificates. Possibly RDW will provide in time foreign CSCA certificates via a reliable method to recognized relying parties or via its website. It is however possible that the foreign CSCA certificate is not available in the verification software. In that case the DS certificate cannot be verified and the software needs to issue a warning.

It could be that for some countries the DS certificates are not issued by a CSCA, but are self-signed certificates. Regulation 2003/127/EC does not require a CSCA, although this is obvious from the viewpoint of conformity with passports, driving licences and European residence permits. If the DS certificate has not been issued by a CSCA the verification software needs the DS certificate from a reliable source. Possibly RDW will in time provide the foreign DS certificates for these cases via a reliable method to recognized relying parties or via its website. It is possible however that a self-signed DS certificate is not available from a reliable source. In that case the DS certificate needs in any case to be verified with the public key from the certificate itself and the software needs to issue a warning.

If certificate verification is unsuccessful or incomplete, this needs to be reported to the user of the reading and verification software.

Since all data groups in the Dutch vehicle registration card chip are secured via Passive Authentication the verification described above does not need to be performed for the Dutch vehicle registration cards if verification is performed via Passive Authentication (see sections 3.4 and 4.2). Passive Authentication is preferred over the process described in this section since it also guarantees and verifies the authenticity of EF.Registration_C if present, it guarantees and verifies that the data groups belong together and it enables Active Authentication.

## 3.4 Passive Authentication

Before the data is written to the chip of a Dutch vehicle registration card, a signature is placed over this data by the issuing organisation RDW. This signature is also placed on the chip. The signature enables

verification of the data authenticity when the data is read from the chip. That means that by using the signature it can be verified that the data comes from RDW and has not been changed.

The electronic signature is placed by an entity which is called the Document Signer (DS). The DS has a public-private key pair. The DS certificate is issued by the CSCA, the highest trust point (the root) in the PKI (see section 3.2).

To generate a signature during the personalisation process first hashes are calculated over each data group which will be written to the chip. These hashes are included in the RDWIdsSecurityObject. The RDWIDsSecurityObject is part of the data object over which a signature is generated by the DS private key. The RDWIDsSecurityObject, the signature and the corresponding DS certificate are placed on the card as part of the EF.Sod (see App 1 for the exact format of the EF.Sod).

When reading and verifying the data on the Dutch vehicle registration card chip, first the authenticity of the certificate from the EF.Sod needs to be established, then the correctness of the signature from the EF.Sod needs to be verified and subsequently the authenticity of the data groups on basis of a comparison of the hash values (see section 4.2 for the full process). This is done conform RFC 5652 [6]. Only if it is clear that the data in the data groups is authentic, it should be shown to the user.

Verification on basis of Passive Authentication needs to be done instead of the process described in section 3.3 since Passive Authentication guarantees and verifies also the authenticity of EF.Registration_C if present, guarantees and verifies the data groups belong together and enables Active Authentication.

In the Passive Authentication process described here only verification of the correctness of the data on the chip is taken into account. Active Authentication to verify the authenticity of the chip itself is described in section 3.5. Active Authentication however is only possible since the authenticity of the AA public key (present in EF.AA) follows from the Passive Authentication verification. EF.AA is one of the data groups which is verified via PA. The full process for reading and verification of the Dutch vehicle registration card chip including AA is described in section 4.2.

## 3.5 Active Authentication

The chip of Dutch vehicle registration cards is provided with an Active Authentication (AA) key pair during personalisation. With this key pair the authenticity of the chip can be verified by the verification software. The AA key pair is unique for each chip. The AA private key is stored in secure memory of the chip and cannot be read. The AA private key can only be used by the chip. The AA public key is placed on the chip in EF.AA (see App 1 for the exact format) and can be freely read. EF.AA is part of the signature over all data groups. The hash over EF.AA is stored in the RDWIDsSecurityObject in the EF.Sod. This enables verification of the authenticity of the AA public key via Passive Authentication.

To verify the authenticity of the chip, the verification software can send a challenge (random) to the chip with the request to sign it with the AA private key. The response sent by the chip to the verification software can be verified with the AA public key from the chip. If from the response after verification (‘decryption’) the original challenge is recovered, then the authenticity of the chip has been proven.

# 4 VERIFICATION PROCESS

## 4.1 Flow Chart

The flow chart below describes at a high level the process for verifying of a Dutch vehicle registration card (see Figure 3). In section 4.2 the reading and verification of the chip are elaborated step by step.

Note:
All vehicles registered in The Netherlands are registered in the vehicle register that is maintained by RDW. The content of this register is leading. To facilitate verification and to enable verification offline, RDW issues vehicle registration cards. In case of doubt about the authenticity of a vehicle registration card, the register needs to be consulted.

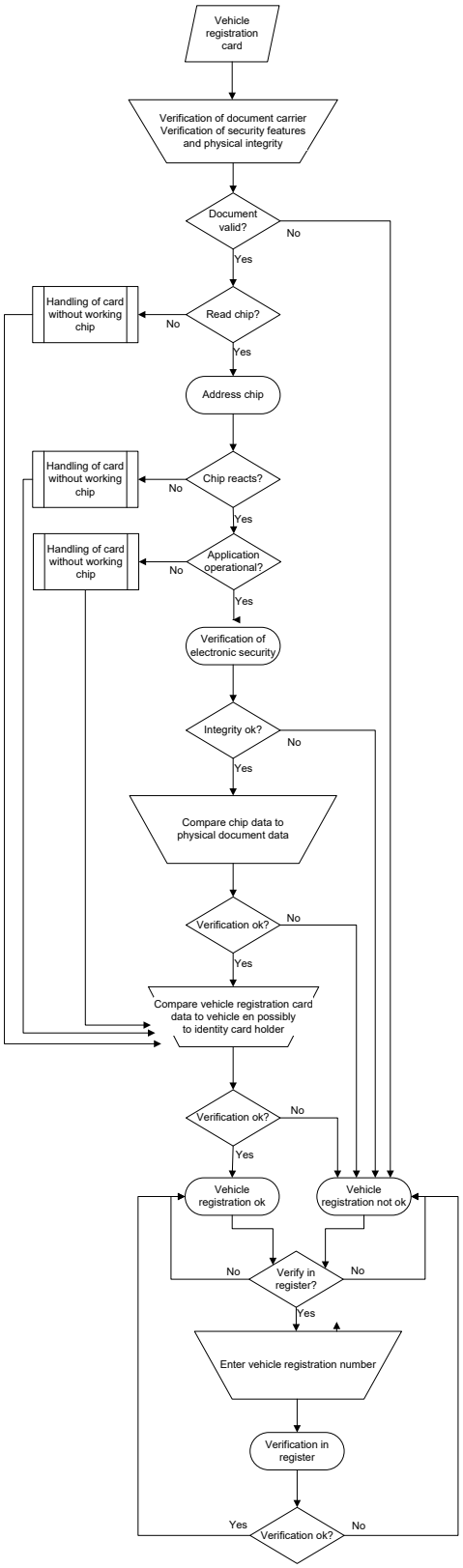


*Figure 3: Flow chart for verification of a Dutch vehicle registration card (and vehicle)*

## 4.2 Reading and Verification of the Dutch Vehicle Registration Card Chip

The process described below indicates what the reading and verification software needs to do to read and verify the chip of a Dutch vehicle registration card. The reading and verification software starts by selecting the eVRC application. The AID is identical for all eVRCs complying with [1]. Subsequently the reading software tries to select the EF.Sod. If this succeeds, the process as described in this section is followed. If selection of the EF.Sod is unsuccessful, the reading software follows the process described in section **Error! Reference source not found.** from step 2 onwards.

For reading the commands from App 2 need to be used. The process described below describes the happy-flow. In case the response to one of the commands is not the expected response, the process is terminated and an error message is shown to the user. Potentially in second line verification more advanced reading and verification software can establish the chip problem.

1. **Select eVRC application (AID = 'A0 00 00 04 56 45 56 52 2D 30 31')**

```
T→C: '00 A4 04 00 0B A0 00 00 04 56 45 56 52 2D 30 31 00'
C→T: 'XX … XX 90 00'
```

2. **Passive Authentication (1st part)**
   a. **Select and read EF.Sod (File ID = '00 1D')**

      Use the Select File command as defined in App 2.2 followed by one or more Read Binary commands as defined in App 2.3 to read the file. In case no EF.Sod is present (Response: `Status Words '6A 82' File not found` on the Select File command), it is a foreign card and the reading procedure as described in section **Error! Reference source not found.** from step 2 onwards needs to be followed.

      The Sod (EF.Sod data) complies with RFC 5652 [6].

   b. **Verify DS certificate from EF.Sod**
      i. **Extract DS certificate from EF.Sod data**
      DS certificate is located in the EF.Sod data under:

```
T: '30'(ContentInfo)
     T: 'A0'(Content)
          T: '30'(SignedData)
               T: 'A0'(Certificates)
                    V: '30 XX XX …XX'
```

      (DS certificate starts with tag `'30'`)

      ii. **DS certificate profile complies to CP/CPS**
      CP/CPS OID can be found in the DS certificate extension CertificatePolicies
      RDW publishes the CP/CPS in the following location:
      http://www-diensten.rdw.nl/
      Most of the time the reading software will already know the certificate profile. The reading software verifies that the critical extensions are present and that the indicated KeyUsage is solely DigitalSignature.

iii. **DS certificate not present on CRL**
CRL location can be found in the DS certificate extension CRLDistributionPoints. RDW publishes CRLs in the following location:
http://www-diensten.rdw.nl/crl/
The reading software shall use the most recent CRL for verification. Most of the time the reading software will already have the current CRL (see further chapter 6).

iv. **DS certificate is issued by CSCA (verification against CSCA certificate)**
The CSCA by which the DS certificate has been issued can be found in the DS certificate field Issuer and in the extension AuthorityKeyIdentifier.
The reading software requires the corresponding CSCA public key certificate for verification of the signature of the DS certificate (see chapter 6). The CSCA certificate is an X.509V3 certificate according to RFC 5280 [4].
The reading software uses the public key from the trusted CSCA certificate for verification of the signature (field signatureValue) from the DS certificate.
The signature has been placed by the CSCA over the TBSCertificate.
It has used the algorithm indicated in the field signatureAlgorithm and in the field Signature from the TBSCertificate.

v. **Store DS public key from DS certificate in memory**

c. **Verify signature from Ef.SOd with public key from DS certificate**

i. **Extract signature and algorithm from Ef.SOd**
The signature is located in Ef.SOd data under:

```
T: '30'(ContentInfo)
     T: 'A0'(Content)
          T: '30'(SignedData)
               T: '31'(SingerInfos)
                    T: '30'(SignerInfo)
                         T: '04'(Signature)
```

The algorithm used can be found in the Ef.SOd data under:

```
T: '30'(ContentInfo)
     T: 'A0'(Content)
          T: '30'(SignedData)
               T: '31'(SignerInfos)
                    T: '30'(SignerInfo)
                         T: '30'(SignatureAlgorithm)
                              T: '06'(algorithm)
```

This can be sha256WithRSAEncryption (OID ::= 1.2.840.113549.1.1.11) or id-RSASSA-PSS (OID ::= 1.2.840.113549.1.1.10). In the latter case the RSA PSS parameters can be found under Tag '30'.

ii. **'Verify'/ 'Decrypt' with DS public key**
By 'verification'/ 'decryption' of the signature with the DS public key from the DS certificate follows the signedAttrs TLV field with the proviso that this field starts with tag '31' instead of tag 'A0'.

iii. **Store signedAttrs from signature in memory**
Store signedAttrs in memory after having replaced the starting tag by 'A0'.

**iv. Extract signedAttrs from Ef.SOd**

The signedAttrs field is located in the Ef.SOd data under:

```
T: '30'(ContentInfo)
      T: 'A0'(Content)
            T: '30'(SignedData)
                  T: '31'(SignerInfos)
                        T: '30'(SignerInfo)
                              T': 'A0'(signedAttrs)
```

**v. Compare signedAttrs from Ef.SOd to signedAttrs from signature (memory)**

**vi. Extract AttributeValue from signedAttrs**

Within signedAttrs the AttributeValue is located under:

```
T: '30'(Attribute)
     T: '31' (AttrValues)
           T: '04' (AttributeValue)
```

This is the hash over eContent (= RDWIdsSecurityObject)
Store this has in memory.

The hash algorithm is located in Ef.SOd under:

```
T: '30'(ContentInfo)
     T: 'A0'(Content)
           T: '30'(SignedData)
                 T: '31'(SignerInfos)
                       T: '30'(SignerInfo)
                             T: '30'(digestAlgorithm)
                                   T: '06'(algorithm)
```

The NL-eVRC uses sha256 (OID ::= 2.16.840.1.101.3.4.2.1)

**vii. Extract eContent (=RDWIdsSecurityObject) from Ef.SOd**

eContent is located in the Ef.SOd under:

```
T: ''0 ' (ContentInfo)
     T: 'A0' (Content)
           T: '30' (SignedData)
                 T: '30' (encapContentInfo)
                       T:'A0' (explicit eContent)
                             T: '04' (eContent)
```

**viii. Calculate hash over eContent**

Use the hash algorithm from vi. (sha256)

**ix. Compare hashes**

Compare hash over eContents to hash from vi. (AttributeValue from signedAttrs).
If these 2 match the first part of PA is successful.

**d. Store eContent = RDWsecurityobject in memory**

3. **Active Authentication**

**a. Select and read EF.AA (File ID'= '00'0D')**

Use the Select File command as defined in App 2.2 followed by one or more Read Binary commands as defined in App 2.3 to read the file.

**b. Verify authenticity EF.AA (Passive Authentication (2nd part))**

Use the procedure from App 1.4.1 to verify the authenticity of the data group.

**c. Store AA public key from EF.AA in memory**

The AA public key is located in EF.AA under:

```
T: '6F'(ActiveAuthenticationPublicKeyInfo)
     L: '30' (SubjectPublicKeyInfo)
     T:'03' (subjectPublicKey)
```

The algorithm can be found in EF.AA under:

```
T: '6F'(ActiveAuthenticationPublicKeyInfo)
     T: '30' (SubjectPublicKeyInfo)
          T: '30'AlgorithmIdentifier)
               T:'06' (algorithm)
               (rsaEncryption = 1.2.840.113549.1.1.1 or
               id-ecPublicKey = 1.2.840.10045.2.1)
```

RDW uses RSA or ECC.

If the algorithm indicated in EF.AA is id-ecPublicKey, select and read EF.SecurityInfos (File ID'= '00'0E'). Use the Select File command as defined in App 2.2 followed by one or more Read Binary commands as defined in App 2.3 to read the file. Verify the authenticity of EF.SecurityInfos by using the procedure from App 1.4.1.

**d. Generate 8-byte challenge (RND.IFD)**

The reading and verification software generates an 8 bytes random.

**e. Chip authentication**

Send 8-byte challenge (RND.IFD) to the card via Internal Authenticate command.

| |
|---|
| T→': '00 88 00 00 08 XX XX XX XX XX XX XX XX'00' |
| C→': 'XX ... XX 90'00' |

**f. Verify response with AA public key**

Use the AA public key from EF.AA (stored in memory) to 'verify'the data from the response to the Internal Authenticate command (without the status wor's '90'00') with the algorithm from step d.

**In case of RSA:**

This produces a string which according to ISO 9796-2 [10] Digital Signature Scheme 1[1] should consist of:

`'6A ++ M1 ++ hash (M1 ++ RND.IFD) ++ 34 CC'`

where `M1` is a nonce generated by the chip.

[1] Digital Signature Scheme 1 with the modification that the 'alternative' signature production function is used. M will consist of M1 en M2, where M1 is a nonce of c-4 bits generated by the VR application and M2 is RND.IFD ('M', 'M1', 'M2' and 'c' as defined in ISO 9796-2 [10]). The SHA-256 hashing algorithm and trailer option 2 will be used.

Extract `M1` from the response.
Calculate with sha256 the hash over `M1 ++ RND.IFD`.

Compare this hash with the hash value from the response.
If the 2 match Active Authentication of the chip is successful.

**In case of ECC:**
The card returns ECC Signature in plain format as defined in [12], i.e. the concatenation R ++ S. Use the algorithm as specified in [12] clause 4.2.1.2 with the public key from EF.AA, the algorithm indicated in EF.SecurityInfos, the 8 byte nonce send in the Internal Authenticate command and the returned R ++ S concatenation.

4. **Read and verify data**
   a. **Select and read EF.Registration_A ('D0 01')**
      Use the Select File command as defined in App 2.2 followed by one or more Read Binary commands as defined in App 2.3 to read the file.

   b. **Verify authenticity EF.Registration_A (Passive Authentication (2nd part))**
      Use the procedure from App 1.4.1 to verify the authenticity of the data group.

   c. **Show EF.Registration_A data to user**

   d. **Select and read EF.Registration_B ('D0 11')**
      Use the Select File command as defined in App 2.2 followed by one or more Read Binary commands as defined in App 2.3 to read the file.

   e. **Verify authenticity EF.Registration_B (Passive Authentication (2nd part))**
      Use the procedure from App 1.4.1 to verify the authenticity of the data group.

   f. **Show EF.Registration_B data to user**

   g. **Select and read EF.Registration_C ('D0 21')**
      Use the Select File command as defined in App 2.2 followed by one or more Read Binary commands as defined in App 2.3 to read the file.

   h. **Verify authenticity EF.Registration_C (Passive Authentication (2nd part))**
      Use the procedure from App 1.4.1 to verify the authenticity of the data group.

   i. **Show EF.Registration_C data to user**

# 5 COMMUNICATION CARD – READ & VERIFICATION SOFTWARE

The vehicle registration cards complying with the European regulation are smart cards (ID-1 format) with a contact chip complying to ISO/IEC 7816-4 and -8 [7], [8]. The chips support in any case the T=1 protocol. Support of the T=0 protocol is optional. The chips can be read with a reader working according to ISO/IEC 7816.

Regarding the commands supported by the Dutch vehicle registration card chips the choices as indicated in App 2 have been made.

The vehicle registration card application on the chip has as Application Identifier
AID = 'A0 00 00 04 56 45 56 52 2D 30 31'.

# 6 INFORMATION EXCHANGE WITH VERIFICATION SOFTWARE

For verification of the Dutch vehicle registration card chip the verification software needs to have the CSCA certificate on basis of which the DS certificates of the chip can be verified. This CSCA certificate can be downloaded from the RDW website, but to be sure of its authenticity the certificate needs to be exchanged via a trusted channel. RDW will set up a process with recognized relying parties. If parties use the RDW reading and verification software the CSCA certificate will be present in (delivered with) the software.

After 10 years RDW will generate and use a new CSCA certificate. Possibly due to circumstances this may already be done earlier. Also the new certificate will be available on the website. Additionally, RDW will generate and make available on the website a CSCA link certificate in which the new CSCA public key is present and which is issued by the current key pair. Relying parties need to download from the website periodically, but in any case before the current CSCA certificate expires, the new CSCA (link) certificate, to verify its authenticity with the current certificate and to load and activate the new CSCA certificate in the reading and verification software. If RDW will generate and use a new CSCA certificate earlier than planned, known recognized relying parties will be informed.

For verification of the Dutch vehicle registration card chip the verification software needs to have the most recent CRL on basis of which the revocation status of a DS certificate of the chip can be verified. The CRLs can be downloaded from the RDW website. The authenticity of the CRL needs to be verified with the CSCA public key certificate that has been used to sign the CRL. A CRL is valid for 200 days and is re-issued every 180 days. Relying parties need to download from the RDW website periodically, but in any case every 200 days, a new CRL to be used in the reading and verification software. RDW may issue a new CRL earlier than planned if there are circumstances giving motive. Recognized relying parties will be informed about this. These relying parties need to use immediately after notification the new CRL in the reading and verification software.

In time RDW may possibly also make available CSCA certificates and CRLs (and possibly DS certificates) for verification of foreign vehicle registration cards.

# App 1 LOGICAL DATA STRUCTURE

## App 1.1 Overview of Elementary Files

| File ID | File Name | Description |
|---|---|---|
| 00 0D | EF.AA | Active Authentication Public Key Info |
| 00 0E | EF.SecurityInfos | SecurityInfos |
| 00 1D | EF.SOd | Document Security Object |
| C0 01 | EF.C.IA_A.DS | X.509v3 certificate of the issuing organisation that is used to verify the signature in EF.Signature_A (see [1]). |
| C0 11 | EF.C.IA_B.DS | X.509v3 certificate of the issuing organisation that is used to verify the signature in EF.Signature_B (see [1]). |
| D0 01 | EF.Registration_A | Registration data according to chapters II.4 en II.5 from [1]. |
| D0 11 | EF.Registration_B | Registration data according to chapter II.6 from [1]. |
| D0 21 | EF.Registration_C | Additional registration data and possibly CVO data. |
| E0 01 | EF.Signature_A | Electronic signature over all data of EF.Registration_A (see [1]). |
| E0 11 | EF.Signature_B | Electronic signature over all data of EF.Registration_B (see [1]). |

*Table 1: File identifiers in the NL-eVRC application*

## App 1.2 EF.AA

The structure of EF.AA is identical to that of the electronic driving licence (ISO/IEC 18013-3:2009, section 8.4.2 [2])
Tag = Tag, Len = Length, Val = Value.
The length is not specified but calculated during construction of the TLV object. This clause specifies two structures, i.e. RSA and ECC. The RSA structure is used for eVR generation 1 and 2, from 2024 onwards, the ECC structure shall be used.

### App 1.2.1 RSA

| Tag | Len | Val | | | |
|---|---|---|---|---|---|
| 6F | | ActiveAuthenticationPublicKeyInfo | | | |
| | **Tag** | **Len** | **Val** | | |
| | 30 | | subjectPublicKeyInfo | | |
| | | **Tag** | **Len** | **Val** | |
| | | 30 | | AlgorithmIdentifier | |
| | | | **Tag** | **Len** | **Val** |
| | | | 06 | | rsaEncryption = 1.2.840.113549.1.1.1 (algorithm (OID)) |
| | | | 05 | | NULL (Parameters (ANY DEFINED BY algorithm– OPTIONAL)) |
| | | **Tag** | **Len** | **Val** | |
| | | 03 | | subjectPublicKey (BITSTRING) | |

*Table 2: Format of EF.AA for RSA*

### App 1.2.2 ECC

| Tag | Length | Value |
|---|---|---|
| '6F' | X | ActiveAuthenticationPublicKeyInfo |
| '30' | X | subjectPublicKeyInfo |
| '30' | '82 01 1D' | AlgorithmIdentifier |
| '06' | '07' | '2A 86 48 CE 3D 02 01' |
| '30' | '82 01 10' | |
| '02' | '01' | '01' |
| '30' | | |
| '06' | '07' | '2A 86 48 CE 3D 01 01' |
| '02' | '29' | '00 D3 5E 47 20 36 BC 4F B7 E1 3C 78 5E D2 01 E0 65 F9 8F CF A6 F6 F4 0D EF 4F 92 B9 EC 78 93 EC 28 FC D4 12 B1 F1 B3 2E 27' |
| '30' | '54' | |
| '04' | '28' | '3E E3 0B 56 8F BA B0 F8 83 CC EB D4 6D 3F 3B B8 A2 A7 35 13 F5 EB 79 DA 66 19 0E B0 85 FF A9 F4 92 F3 75 A9 7D 86 0E B4' |
| '04' | '28' | '52 08 83 94 9D FD BC 42 D3 AD 19 86 40 68 8A 6F E1 3F 41 34 95 54 B4 9A CC 31 DC CD 88 45 39 81 6F 5E B4 AC 8F B1 F1 A6' |
| '04' | '51' | '04 43 BD 7E 9A FB 53 D8 B8 52 89 BC C4 8E E5 BF E6 F2 01 37 D1 0A 08 7E B6 E7 87 1E 2A 10 A5 99 C7 10 AF 8D 0D 39 E2 06 11 14 FD D0 55 45 EC 1C C8 AB 40 93 24 7F 77 27 5E 07 43 FF ED 11 71 82 EA A9 C7 78 77 AA AC 6A C7 D3 52 45 D1 69 2E 8E E1' |
| '02' | '29' | '00 D3 5E 47 20 36 BC 4F B7 E1 3C 78 5E D2 01 E0 65 F9 8F CF A5 B6 8F 12 A3 2D 48 2E C7 EE 86 58 E9 86 91 55 5B 44 C5 93 11' |
| '02' | '01' | '01' |
| '03' | X | '00' |
| | | 04 XX .. XX YY .. YY |

## App 1.3 EF.SecurityInfos

This datagroup shall be present when ECC is used for Active Authentication, this datagroup shall be absent in case Active Authentication is based on RSA.

| Tag | Length | Value | Comment |
|---|---|---|---|
| '6E' | '2F' | | DG14 tag |
| '31' | '2D' | | SET OF |
| '30' | '17' | | SEQUENCE ActiveAuthenticationInfo |
| '06' | '06' | '67 81 08 01 01 05' | OBJECT IDENTIFIER 2.23.136.1.1.5 id-AA |
| '02' | '01' | '01' | INTEGER Version 01 |
| '06' | '0A' | '04 00 7F 00 07 01 01 04 01 03' | OBJECT IDENTIFIER 0.4.0.127.0.7.1.1.4.1.3 ecdsa-plain-SHA256 |

## App 1.4 EF.SOd

The two tables below define the Document Security Object (SOd).

The SOd is a CMS Signed Data object (RFC 5652 [6]). The two tables below can be considered the chosen profile for the CMS Signed Data object and indicate which specific choices have been made, plus some additional information: the first number in each row is the (hexadecimal) tag for the TLV-field (tag value '??' indicates that the tag can be derived from the content); where applicable the value of a field is indicated.

The meaning of the 'Use' column is: m = mandatory, x = must not be used, c = conditional.
Notice that the structure of a CMS Signed Data object is rather complex, comprising several choices, sets and series. In case of doubt RFC 5652 [6] needs to be consulted. Also notice that the final signature is calculated *after* replacing the tag number.

Except for the fields Certificate(Choices), Issuer and rSASSA-PSS-SHA256-Params, the full TLV tree structure for the SOd is indicated below.

The full SOd shall be DER encoded (RFC 5652 [6] allows infinite length BER encoding to be compatible to outdated tape drive equipment).

The choice for sid is issuerAndSerialNumber (according to the electronic driving licence [2] and passport standards [3]), but notice that according to RFC 5652 [6] the alternative option subjectKeyIdentifier for sid should also be supported by implementations.

The current preference for the RSA signature algorithm is PKCS#1v1.5, but the option to use instead RSA-PSS is left open. The same signature algorithm needs to be used for the signatures over the CSCA certificate, DS certificate, Signature_A, Signature_B and the SOd.

| Field name | | | | | | | Use | Reference section (in RFC 5652 [6]) | Field value | Comment |
|---|---|---|---|---|---|---|---|---|---|---|
| 30 | ContentInfo | | | | | | m | 3 | | |
| | 06 | contentType | | | | | m | 3 | id-signedData ::= 1.2.840.113549.1.7.2 | OID |
| | A0 | Content | | | | | m | 3 | | |
| | | 30 | SignedData | | | | m | 5.1 | | |
| | | | 02 | Version | | | m | 5.1, 10.2.5 | 3 | INTEGER |
| | | | 31 | digestAlgorithms | | | m | 5.1 | | |
| | | | | 30 | DigestAlgorithmIdentifier | | m | 10.1.1 | | |
| | | | | | 06 | Algorithm | m | 2.1 in RFC 4055 [9] | id-sha256 ::= 2.16.840.1.101.3.4.2.1 | OID |
| | | | | | -- | Parameters | x | | | |
| | | | | -- | ... | | x | | | Only one digest algorithm is required |
| | | | 30 | encapContentInfo | | | m | 5.2 | | |
| | | | | 06 | eContentType | | m | | id-RDW-ldsSecurityObject ::= 2.16.528.1.1010.3.1.1 | OID |
| | | | | A0 | explicit eContent | | m | | | |
| | | | | | 04 | eContent | m | | RDWIdsSecurityObject | OCTEST STRING, see next table (Table 4: Format of RDWIdsSecurityObject) for values |
| | | | A0 | Certificates | | | m | 5.1, 10.2.3 | | |
| | | | | ?? | CertificateChoices | | m | 10.2.2 | Certificate | This is the DS X.509 certificate (starting with tag '30'), see RFC 5280 [4] |
| | | | | -- | ... | | x | | | Only one certificate required |
| | | | -- | Crls | | | x | | | CRLs are not used |
| | | | 31 | signerInfos | | | m | 5.1 | | |
| | | | | 30 | SignerInfo | | m | 5.3 | | |

| Field name | | | | | | | | | Use | Reference section (in RFC 5652 [6]) | Field value | Comment |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | 02 | Version | | | m | 5.3, 10.2.5 | 1 (sid=issuerAndSerialNumber ), or<br>3 (sid=subjectKeyIdentifier ) | INTEGER value depends on the choice for sid |
| | | | | | … | Sid | | | - | | | Formally a choice needs to be made between EITHER issuerAndSerialNumber OR subjectKeyIdentifier. In practice issuerAndSerialNumber is used. |
| | | | | | 30 | … | issuerAndSerialNumber | | c | | | |
| | | | | | | | ?? | issuer | m | 4.1.2.4 in RFC 5280 [4] | | Issuer DN Name of DS X.509 certificate (starting with tag '30') |
| | | | | | | | 02 | serialnumber | m | 4.1.2.2 in RFC 5280 [4] | CertificateSerialNumber | INTEGER Serial Number of DS X.509 certificate |
| | | | | | A0 | … | subjectKeyIdentifier | | c | | | subjectKeyIdentifier is only incorporated to be compliant to RFC 5652 [6], but is not used in practice. |
| | | | | | | | 04 | SubjectKeyIdentifier | m | 4.2.1.2 in RFC 5280 [4] | | subjectKeyIdentifier is only incorporated here to be compliant to RFC 5652 [6], but is not used in practice.<br>OCTET STRING subject key identifier from DS X.509 certificate SKI extension |
| | | | | | 30 | digestAlgorithm | | | m | 5.3 | | |
| | | | | | | 06 | algorithm | | m | 2.1 in RFC 4055 [9] | id-sha256 ::= 2.16.840.1.101.3.4.2.1 | OID |
| | | | | | | -- | parameters | | x | | | |
| | | | | | A0 | signedAttrs | | | m | | | |
| | | | | | | 30 | Attribute | | m | 11.1 | | |
| | | | | | | | 06 | attrType | m | 11.1 | id-contentType ::= 1.2.840.113549.1.9.3 | OID |

| Field name | Use | Reference section (in RFC 5652 [6]) | Field value | Comment |
|---|---|---|---|---|
| 31 attrValues | m | 11.1 | | |
| 06 AttributeValue | m | 11.1 | id-RDW-ldsSecurityObject ::= 2.16.528.1.1010.3.1.1 | OID |
| -- … | x | 11.1 | | Only one AttributeValue is allowed here |
| 30 Attribute | m | 11.2 | | |
| 06 attrType | m | 11.2 | id-messageDigest ::= 1.2.840.113549.1.9.4 | OID |
| 31 attrValues | m | 11.2 | | |
| 04 AttributeValue | m | 11.2, 5.4 | | This OCTET STRING contains the hash value over the *value* of the eContent OCTET STRING (e.g. over the RDWldsSecurityObject). |
| -- … | x | 11.2 | | Only one AttributeValue is allowed here |
| -- … | x | | | More Attributes are not required |
| 30 signatureAlgorithm | | | | |
| 06 Algorithm | c | 2.1 in RFC 4055 [9] | sha256WithRSAEncryption ::= 1.2.840.113549.1.1.11 | Conditional: use this field if the signature algorithm is PKCS#1v1.5. |
| 05 Parameters | c | 5 in RFC 4055 [9] | null | Conditional: use this field if the signature algorithm is PKCS#1v1.5.<br>Here the parameters must be set to NULL. |
| 06 Algorithm | c | RFC 4055 [9] | id-RSASSA-PSS ::= 1.2.840.113549.1.1.10 | Conditional: use this field if the signature algorithm is RSA-PSS. |
| 30 Parameters | c | RFC 4055 [9] | rSASSA-PSS-SHA256-Params structure | Conditional: use this field if the signature algorithm is RSA-PSS.<br>RSA PSS parameters must be used (mgf1, SHA256, saltlength 32). |
| 04 Signature | m | 11.2, 5.5 | | This OCTET STRING contains the signature over the signedAttrs TLV vels *as if encoded* |

| Field name | | | | | | | Use | Reference section (in RFC 5652 [6]) | Field value | Comment |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | *as EXPLICIT TAG OF (i.e. replace the leading tag 'A0' by '31').* |
| | | | | | -- | unsignedAttrs | x | | | No unsigned attributes are required |
| | | | | -- | ... | | x | | | Only one signerInfo is required. |

*Table 3: Format of EF.SOd*

| Field name | | | | | | | Use | Field value | Comment |
|---|---|---|---|---|---|---|---|---|---|
| 30 | RDWIdsSecurityObject | | | | | | m | | |
| | 02 | Version | | | | | m | 0 | INTEGER |
| | 30 | hashAlgorithm | | | | | m | | |
| | | 06 | algorithm | | | | m | id-sha256 ::= 2.16.840.1.101.3.4.2.1 | OID |
| | | -- | parameters | | | | x | | |
| | 30 | dataGroupHashValues | | | | | m | | |
| | | 30 | DataGroupHash | | | | m | | |
| | | | 04 | dataGroupFileIdentifier | | | m | | This is the two-byte OCTET STRING file-identifier |
| | | | 04 | dataGroupHashValue | | | m | | This is the 32-byte OCTET STRING SHA-256 hash of a data group |
| | | 30 | ... | | | | m | | Repeat for each data group, order on basis of file ID |

*Table 4: Format of RDWIdsSecurityObject*

### App 1.4.1 Verify the hash of a data group

The RDWIdsSecurityObject specified in Table 5 contains hashes over each data group ordered on basis of the File ID. During the inspection of a Kentekencard, the hash of each individual datagroup shall be verified by:

**Calculate hash over the data group**

Use the hash algorithm indicated in the RDWIdsSecurityObject. The hash algorithm is located in eContent under:

```
T:'30' (RDWIdsSecurityObject)
     T: '30' (hashAlgorithm)
          T: '06' (algorithm)
```

RDW uses sha 256 (OID ::= 2.16.840.1.101.3.4.2.1).
The hash is calculated over the data of the data group.

**Extract hash value from RDWIdsSecurityObject**

The hash value of data group is located in eContent under:

```
T:'30'(RDWIdsSecurityObject)
      T:'30'(dataGroupHashValues)
            T:'04'(dataGroupFileIdentifier)
            T:'04'(dataGroupHashValue)
```

The applicable hash can be found by looking up the applicable file identifier.

**Compare the hash values**

If the hash value from RDWIdsSecurityObject matches the calculated hash over data group. the data from the in data group is authentic and can be processed.

## App 1.5 EF.C.IA_A.DS

Conform 2003/127/EC the content of this data group is an X.509v3 formatted DS certificate used to generate the EF.Signature_A signature over the data in EF.Registration_A. The certificate profile for the DS certificate is defined in the CP/CPS [5].

## App 1.6 EF.C.IA_B.DS

Conform 2003/127/EC the content of this data group is an X.509v3 formatted DS certificate used to generate the EF.Signature_B signature over the data in EF.Registration_B. The certificate profile for the DS certificate is defined in the CP/CPS [5].

# App 1.7 EF.Registration_A

Conform 2003/127/EC the content of this data group is formatted in BER-TLV structure according the profile in 2003/127/EC Annex I, III.11, Table 2 [1].

| Tag | | | | Code | Field description | EU m/o | NL m/x | Corresponding DD10 XML element | Typical field value on the chip |
|---|---|---|---|---|---|---|---|---|---|
| 78 | | | | | Compatible tag allocation authority | m | m | | n/a |
| | 4F | | | | application identifier | m | m | | ‘A0 00 00 04 56 45 56 52 2D 30 31’ |
| 71 | | | | | inter-industry template corresponding to mandatory data | m | m | | n/a |
| | 80 | | | | version of tag definition | m | m | | ‘00’ |
| | 9F 33 | | | | name of the member state | m | m | LidstaatVanUitgifte | "Nederland" |
| | 9F 34 | | | | another designation of document | o | x | | |
| | 9F 35 | | | | name of competent authority | m | m | Autoriteit | "RDW" |
| | 9F 36 | | | | name of authority issuing registration certificate | o | x | | |
| | 9F 37 | | | | Character set used | m | m | | ‘00’ |
| | 9F 38 | | | | Unambiguous consecutive number of the document | m | m | Documentnummer | "1234567890" |
| | 81 | | | A | Registration number | m | m | Kenteken | "44-JBT-4" |
| | 82 | | | B | Date of first registration | m | m | DatumEersteToelatingEU | "20121231" |
| | A1 | | | C | Personal data | m | m | | n/a |
| | | A2 | | C.1 | Holder of the registration certificate | m | m | | n/a |
| | | | 83 | C.1.1 | Surname or business name | m | m | NaamHouder | "Achternaam-Houder" |
| | | | 84 | C.1.2 | Other names or initials | o | m | Voorletters | "V.L." |
| | | | 85 | C.1.3 | Address in the Member State | m | m | Adreshouder | "Talingweg 76, 8218 NX, Lelystad" |
| | | 86 | | C.4 | vehicle owner yes/no/unknown | m | m | Eigendomssituatie | ‘02’ |
| | A3 | | | D | Vehicle | m | m | | n/a |
| | | 87 | | D.1 | Make | m | m | Merk | "TOYOTA" |
| | | 88 | | D.2 | Type | m | m | Type | "LM ZVW30(H) ZVW30L-AHXEBW(1A)" |

| Tag | | | | Code | Field description | EU m/o | NL m/x | Corresponding DD10 XML element | Typical field value on the chip |
|---|---|---|---|---|---|---|---|---|---|
| | | 89 | | D.3 | commercial descriptions | m | m | Handelsbenaming | "TOYOTA PRIUS" |
| | 8A | | | E | Vehicle identification number | m | m | Voertuigidentificatienummer | "JTDKN36U801019282" |
| | A4 | | | F | Mass | m | m | | n/a |
| | | 8B | | F.1 | maximum technically permissible laden mass | m | m | TechMaxMassa | "12345 kg" |
| | 8C | | | G | Mass of the vehicle in service with bodywork | m | m | MassaRijklaar | "12345 kg" |
| | 8D | | | H | Period of validity | m | m | GeldigheidsDuur | "" |
| | 8E | | | I | Date of registration | m | m | DatumAanvangAansprEU | "210121231" |
| | 8F | | | K | Type approval number | m | m | Typegoedkeuringsnummer | "e11*2001/116*0264*00" |
| | A5 | | | P | Engine | m | m | | n/a |
| | | 90 | | P.1 | Engine capacity | m | m | Cilinderinhoud | "1798" |
| | | 91 | | P.2 | Engine maximum net power | m | m | Vermogen | "1234,23 kW" |
| | | 92 | | P.3 | Engine type of fuel | m | m | BrandstofEU | "B/E" |
| | 93 | | | Q | Power weight ratio | m | m | VermogenGedeeldDoorMasRijklaar | "9,99 kW/kg" |
| | A6 | | | S | Seating capacity | m | m | | n/a |
| | | 94 | | S.1 | Number of seats | m | m | Zitplaatsen | "5" |
| | | 95 | | S.2 | Number of standing places | m | m | Staanplaatsen | "0" |

*Table 6: Format of EF.Registration_A*

# App 1.8 EF.Registration_B

Conform 2003/127/EC the content of this data group is formatted in BER-TLV structure according to the profile in 2003/127/EC Annex I, III.11, Table 3 [1].

| Tag | | | | Code | Field description | EU m/o | NL m/x | Corresponding DD10 XML element | Typical field value on the chip |
|---|---|---|---|---|---|---|---|---|---|
| 78 | | | | | Compatible tag allocation authority | m | m | | n/a |
| | 4F | | | | application identifier | m | m | | 'A0 00 00 04 56 45 56 52 2D 30 31' |
| 72 | | | | | inter-industry template corresponding to optional data | m | m | | n/a |
| | 80 | | | | version of tag definition | m | m | | '00' |
| | A1 | | | C | Personal data | o | x | | |
| | | A7 | | C.2 | Vehicle owner | o | x | | |
| | | | 83 | C.2.1 | Surname or business name | o | x | | |
| | | | 84 | C.2.2 | Other names or initials | o | x | | |
| | | | 85 | C.2.3 | Address in the Member State | o | x | | |
| | | A8 | | C.2 | Second vehicle owner | o | x | | |
| | | | 83 | C.2.1 | Surname or business name | o | x | | |
| | | | 84 | C.2.2 | Other names or initials | o | x | | |
| | | | 85 | C.2.3 | Address in the Member State | o | x | | |
| | | A9 | | C.3 | Person who may use the vehicle | o | x | | |
| | | | 83 | C.3.1 | Surname or business name | o | x | | |
| | | | 84 | C.3.2 | Other names or initials | o | x | | |
| | | | 85 | C.3.3 | Address in the Member State | o | x | | |
| | A4 | | | F | Mass | o | m | | n/a |
| | | 96 | | F.2 | Maximum permissible laden mass of the vehicle in service | o | m | ToegestMaxMassa | "12345 kg" |
| | | 97 | | F.3 | Maximum permissible laden mass of the whole vehicle in service | o | m | ToegestMaxMassaComb | "12345 kg" |
| | 98 | | | J | Vehicle category | o | m | Voertuigcategorie | "M2G" |
| | 99 | | | L | Number of axles | o | x | | |
| | 9A | | | M | Wheelbase | o | x | | |

| Tag | | | | Code | Field description | EU m/o | NL m/x | Corresponding DD10 XML element | Typical field value on the chip |
|---|---|---|---|---|---|---|---|---|---|
| | AD | | | N | Distribution among axles | o | x | | |
| | | 9F 1F | | N.1 | Axle 1 | o | x | | |
| | | 9F 20 | | N.2 | Axle 2 | o | x | | |
| | | 9F 21 | | N.3 | Axle 3 | o | x | | |
| | | 9F 22 | | N.4 | Axle 4 | o | x | | |
| | | 9F 23 | | N.5 | Axle 5 | o | x | | |
| | AE | | | O | maximum towable mass of the trailer | o | m | | n/a |
| | | 9B | | O.1 | Braked | o | m | TechMaxMassaGeremd | "12345 kg" |
| | | 9C | | O.2 | Unbraked | o | m | TechMaxMassaOngeremd | "12345 kg" |
| | A5 | | | P | Engine | o | x | | |
| | | 9D | | P.4 | Rated speed | o | x | | |
| | | 9E | | P.5 | Engine identification number | o | x | | |
| | 9F 24 | | | R | Colour | o | m | Kleur | "Oranje/Oranje" |
| | 9F 25 | | | T | Maximum speed | o | m | MaxSnelheid | "999 km/h" or "999/999 km/h" |
| | AF | | | U | Sound level, | o | x | | |
| | | 9F 26 | | U.1 | Stationary | o | x | | |
| | | 9F 27 | | U.2 | Engine speed | o | x | | |
| | | 9F 28 | | U.3 | Drive by | o | x | | |
| | B0 | | | V | Exhaust emissions | o | m | | n/a |
| | | 9F 29 | | V.1 | CO | o | x | | |
| | | 9F 2A | | V.2 | HC | o | x | | |
| | | 9F 2B | | V.3 | NOx | o | x | | |
| | | 9F 2C | | V.4 | HC+NOx | o | x | | |
| | | 9F 2D | | V.5 | Particulates of diesel | o | x | | |
| | | 9F 2E | | V.6 | diesel absorption coefficient | o | x | | |
| | | 9F 2F | | V.7 | CO2 | o | x | | |
| | | 9F 30 | | V.8 | Combined fuel consumption | o | x | | |
| | | 9F 31 | | V.9 | environmental category | o | m | Milieuklasse | "70/222*1970/222" |
| | 9F 32 | | | W | Fuel tanks capacity | o | x | | |

*Table 7: Format of EF.Registration_B*

# App 1.9 EF.Registration_C

| Tag | Length | Value | | | |
|---|---|---|---|---|---|
| BF8700 | X | Registration_C Template | | | M |
| | **Tag** | **L** | **Value** | | |
| | 9F8701 | X | Version (current = 1) | Binary | M |
| | BF8710 | X | RegistrationDates | | M |
| | conditional | C | IndividualVehicleInformation (1) | C | C |
| | conditional | C | IndividualVehicleInformation (2) | C | C |
| | conditional | C | IndividualVehicleInformation (3) | C | C |
| | conditional | C | IndividualVehicleInformation (4) | C | C |
| | conditional | C | IndividualVehicleInformation (5) | C | C |
| | … | … | … | … | … |

*Table 8: Format of EF.Registration_C*

## App 1.9.1 Registration data

EF.Registration_C always contains registration data as indicated in Table 9. This data contains in addition to the data in EF.Registration_A, the date of first registration in the Netherlands.

| Tag | L | Value | Format | M/O | Corresponding DD10 XML element | Typical value |
|---|---|---|---|---|---|---|
| 9F8711 | | Date of first registration of the vehicle | YYYYMMDD | M | DatumEersteToelatingEU | 19970702 |
| 9F8712 | | Date of first registration of the vehicle in the Netherlands | YYYYMMDD | M | DatumEersteInschrijvingEU | 20110701 |
| 9F8713 | | Date of registration to which this certificate refers (Laatste Tenaamstelling) | YYYYMMDD | M | DatumAanvangAansprEU | 20130628 |
| 9F8714 | | Registration number (Kenteken) | | M | Kenteken | 44-JBT-4 |

*Table 9: Format of registration data in EF.Registration_C*

## App 1.9.2 Individual Vehicle Information

EF.Registration_C contains an arbitrary number (0, 1, 2, 3, ....) of IndividualVehicleInformation data elements. For each applicable COC/CVO there will be an IndividualVehicleInformation data element. For each individual IndiviualVehicleInformation data element three choices are allowed for formats and

only one representation (XML, Compressed XML of TLV) will be present (for each individual IndividualVehicaleInformation data element).

| IndividualVehicleInformation | Tag | L | Value | | |
|---|---|---|---|---|---|
| (choice 1) | 9F8702 | X | IndividualVehicleInformation (XML) | A-N | C |
| (choice 2) | BF8703 | X | IndividualVehicleInformation (Compressed XML) | | C |
| (choice 3) | BF8100 | X | IndividualVehicleInformation (TLV) | | C |

*Table 10: Format of Individual Vehicle Information*

### App 1.9.2.1 IndividualVehicleInformation (XML)

XML encoded Vehicle Information will be specified later.

### App 1.9.2.2 IndividualVehicleInformation (Compressed XML)

| Tag | L | Value | | |
|---|---|---|---|---|
| 9F8704 | X | Compression Algorithm Identifier (zie Table 12:) | Binary | M |
| 9F8705 | X | XML geëncodeerde Vehicle Information zoals gespecificeerd zal worden, gecomprimeerd volgens het algoritme aangegeven in het veld met tag 9F8704 | Binary | M |

*Table 11: Format of IndividualVehicleInformation (Compressed XML)*

| Identifier | Algorithm |
|---|---|
| 0 | GZIP |
| * | RFU |

*Table 12: Compression Algorithm Identifiers*

### App 1.9.2.3 IndividualVehicleInformation (TLV)

L(max) indicates the maximum allowed length (in bytes) of the corresponding value field.

| **Tag** | **L(max)** | **Value** | | |
|---|---|---|---|---|
| BF8101 | X | Header | | |
| | **Tag** | **L(max)** | **Value** | |
| | 9F8102 | 36 | MessageId | |
| **Tag** | **L(max)** | **Value** | | |
| BF8103 | X | Body | | |
| | **Tag** | **L(max)** | **Value** | |
| | BF8104 | X | CocDataGroup (TLV) | |
| | | **Tag** | **L(max)** | **Value** |
| | | 9F8105 | 17 | VehicleIdentificationNumber |
| | | 9F8106 | 17 | BaseVin |
| | | 9F8107 | 1 | StageOfCompletionCode |
| | | 9F8108 | 1 | ProvisionalApprovalIndicator |
| | | 9F8109 | 3 | TypeApprovalTypeCode |
| | | 9F810A | 1 | IndividualApprovalTypeCode |
| | | 9F810B | 4 | ProductionYear |
| | | 9F810C | 4 | ProductionSequentialNumber |
| | | 9F810D | 4 | NumberOfTheMemberState |
| | | 9F810E | 50 | Type |
| | | 9F810F | 25 | Variant |
| | | 9F8110 | 35 | Version |
| | | 9F8111 | | RevisionDate |
| | | 9F8112 | 150 | MeansOfIdentificationOfType |
| | | 9F8113 | 150 | ManufacturerPlateLocation |
| | | 9F8114 | 150 | ManufacturerPlateMethodOfAffix |
| | | 9F8115 | 10 | VehicleCategoryCode |
| | | 9F8116 | 1 | AdditionalVehCat23WheelCode |
| | | 9F8117 | 2 | LocOfTheStatutoryPlatesCode |

| Tag | L(max) | Value | | |
|---|---|---|---|---|
| | | 9F8118 | 2 | MethodOfAttachmStatPlatesCode |
| | | 9F8119 | 2 | LocationOfTheVinCode |
| | | 9F811A | 50 | LocationOfTheVinCode23Wheel |
| | | 9F811B | 80 | NumericAlphanumIdentifCode |
| | | 9F811C | 1 | CompletedAlteredCode |
| | | 9F811D | 500 | DescriptionOfCompletion |
| | | 9F811E | 35 | TypeApprovalNumber |
| | | 9F811F | | TypeApprovalDateOfIssue |
| | | 9F8120 | 1 | RightLeftHandTrafficCode |
| | | 9F8121 | 1 | MetricImperialSpeedometerCode |
| | | 9F8122 | | DateOfApplicationIndividualApp |
| | | 9F8123 | 35 | IndividualApprovalNumber |
| | | 9F8124 | 2 | IndividualApprovalVersionNr |
| | | 9F8125 | 2 | NumberOfAxles |
| | | 9F8126 | 2 | NumberOfWheels |
| | | 9F8127 | 2 | NumberOfAxlesWithTwinWheels |
| | | 9F8128 | 2 | NumberOfSteeredAxles |
| | | 9F8129 | 2 | NumberOfPoweredAxles |
| | | 9F812A | 2 | NumberOfBrakedAxles |
| | | 9F812B | 1 | ReversibleDrivingPositionInd |
| | | 9F812C | 5 | Wheelbase |
| | | 9F812D | 5 | WheelbaseMinimum |
| | | 9F812E | 5 | WheelbaseMaximum |
| | | 9F812F | 5 | Length |
| | | 9F8130 | 5 | LengthMinimum |
| | | 9F8131 | 5 | LengthMaximum |
| | | 9F8132 | 5 | MaximumPermissibleLength |
| | | 9F8133 | 4 | Width |
| | | 9F8134 | 4 | WidthMinimum |
| | | 9F8135 | 4 | WidthMaximum |
| | | 9F8136 | 4 | MaximumPermissibleWidth |

| Tag | L(max) | Value | | |
|---|---|---|---|---|
| | | 9F8137 | 4 | Height |
| | | 9F8138 | 4 | HeightMinimum |
| | | 9F8139 | 4 | HeightMaximum |
| | | 9F813A | 4 | MaximumPermissibleHeight |
| | | 9F813B | 150 | MaxPermPosCOGCompletedVeh |
| | | 9F813C | 5 | LengthOfTheLoadingArea |
| | | 9F813D | 5 | LengthOfTheLoadingAreaMinimum |
| | | 9F813E | 5 | LengthOfTheLoadingAreaMaximum |
| | | 9F813F | 4 | RearOverhang |
| | | 9F8140 | 4 | RearOverhangMinimum |
| | | 9F8141 | 4 | RearOverhangMaximum |
| | | 9F8142 | 4 | MaximumPermissibleRearOverhang |
| | | 9F8143 | 6 | MassOfTheVehicleInRunningOrder |
| | | 9F8144 | 6 | ActualMassOfTheVehicle |
| | | 9F8145 | 6 | UnladenMassVehRunningOrderMin |
| | | 9F8146 | 6 | UnladenMassVehRunningOrderMax |
| | | 9F8147 | 6 | UnladenMassOfTheVehicle |
| | | 9F8148 | 6 | MassIncompleteVehRunningOrder |
| | | 9F8149 | 6 | MinMassVehCompleted |
| | | 9F814A | 6 | TechnPermMaxLadenMass |
| | | 9F814B | 6 | TechnPermMaxMassCombination |
| | | 9F814C | 6 | BallastMassTotal |
| | | 9F814D | 50 | BallastMassMaterial |
| | | 9F814E | 2 | BallastMassNumberOfComponents |
| | | 9F814F | 15 | BallastMassNumberOfComponents |
| | | 9F8150 | 1 | BodyIndicator |
| | | 9F8151 | 2 | PrimaryColourCode |
| | | 9F8152 | 2 | SecondaryColourCode |
| | | 9F8153 | 5 | TankCapacityTankerVehicle |
| | | 9F8154 | 1 | NumberOfDoors |
| | | 9F8155 | 40 | ConfigurationOfDoors |

| Tag | L(max) | Value | | |
|---|---|---|---|---|
| | | 9F8156 | 50 | FrameOrCabMake |
| | | 9F8157 | 40 | EcTypeApprovalNrFrameCab |
| | | 9F8158 | 1 | PositionRollOverHoopCode |
| | | 9F8159 | 2 | TypeOfRollOverHoopCode |
| | | 9F815A | 40 | MakeRollOverHoop |
| | | 9F815B | 40 | EcTypeApprovalNrRollOverHoop |
| | | 9F815C | 3 | NrOfSeatingPositionExclDriver |
| | | 9F815D | 3 | NrOfSeatingPositions |
| | | 9F815E | 40 | PositionOfSeats |
| | | 9F815F | 3 | SeatForUseOnlyWhenTheVehStat |
| | | 9F8160 | 3 | NrOfPassSeatingPosLowerDeck |
| | | 9F8161 | 3 | NrOfPassSeatingPosUpperDeck |
| | | 9F8162 | 3 | NrOfWheelchairUserAccessPos |
| | | 9F8163 | 3 | NumberOfStandingPlaces |
| | | 9F8164 | 5 | LoadPlatformDimensionsLength |
| | | 9F8165 | 5 | LoadPlatformDimensionsWidth |
| | | 9F8166 | 5 | LoadPlatformDimensionsHeight |
| | | 9F8167 | 6 | LoadPlatformTechPermLoad |
| | | 9F8168 | 150 | OptionalLightSignallingDevices |
| | | 9F8169 | 1 | HydrLiftThreePointCouplingInd |
| | | 9F816A | 1 | TypeApprTranspDangerGoodsInd |
| | | 9F816B | 1000 | Remarks |
| | | 9F816C | 1 | ExceedingDimensionsIndicator |
| | | 9F816D | 200 | Exemptions |
| | | 9F816E | 400 | AdditionalInformation |
| | | 9F816F | 7 | OdometerReading |
| | | 9F8170 | 1 | OdometerUnitCode |
| | | 9F8171 | 3 | IntendedCountryOfRegistrCode |
| | | 9F8172 | 2 | VersionCoc |
| | | 9F8173 | | VersionDateIVI |
| | | 9F8174 | 1 | VehicleFittedWithEcoInnovInd |

| Tag | L(max) | Value | | | | |
|---|---|---|---|---|---|---|
| | | 9F8175 | 5 | TotalCO2EmisSavingDueEcoInnov | | |
| | | 9F8176 | 1 | FuelTypeCode | | |
| | | BF8177 | | BrakingTable | | |
| | | | **Tag** | **L(max)** | **Value** | |
| | | | BF8178 | | BrakingGroup | |
| | | | | **Tag** | **L(max)** | **Value** |
| | | | | 9F8179 | 200 | BrakingDesc |
| | | **Tag** | **L(max)** | **Value** | | |
| | | BF817A | | FiscalPowerOrNatCodeNrsTable | | |
| | | | **Tag** | **L(max)** | **Value** | |
| | | | BF817B | | FiscalPowerOrNatCodeNrsGroup | |
| | | | | **Tag** | **L(max)** | **Value** |
| | | | | 9F817C | 3 | FiscPowOrNatCodeNrsCountryCode |
| | | | | 9F817D | 40 | FiscalPowerOrNatCodeNrs |
| | | **Tag** | **L(max)** | **Value** | | |
| | | BF817E | | SigningAuthorityTable | | |
| | | | **Tag** | **L(max)** | **Value** | |
| | | | BF817F | | SigningAuthorityGroup | |
| | | | | **Tag** | **L(max)** | **Value** |
| | | | | 9F8200 | 80 | NameOfSigner |
| | | | | 9F8201 | 80 | PositionOfSigner |
| | | | | 9F8202 | 80 | PlaceOfSignature |
| | | | | 9F8203 | | DateOfSignature |
| | | **Tag** | **L(max)** | **Value** | | |
| | | BF8204 | | GearGroup | | |
| | | | **Tag** | **L(max)** | **Value** | |
| | | | 9F8205 | 1 | GearboxTypeCode | |
| | | | 9F8206 | 2 | NumberOfRatiosFront | |
| | | | 9F8207 | 2 | NumberOfRatiosRear | |
| | | | BF8208 | | GearRatioTable | |
| | | | | **Tag** | **L(max)** | **Value** |

| Tag | L(max) | Value | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | BF8209 | | GearRatioGroup | |
| | | | | | **Tag** | **L(max)** | **Value** |
| | | | | | 9F820A | 1 | DrivingDirectionCode |
| | | | | | 9F820B | 2 | GearNumber |
| | | | | | 9F820C | 7 | GearRatio |
| | | **Tag** | **L(max)** | **Value** | | | |
| | | BF820D | | RegulationsTable | | | |
| | | | **Tag** | **L(max)** | **Value** | | |
| | | | BF820E | | RegulationsGroup | | |
| | | | | **Tag** | **L(max)** | **Value** | |
| | | | | 9F820F | 5 | RegulActInclLastAmendSubjNr | |
| | | | | 9F8210 | 25 | RegulationAct | |
| | | | | 9F8211 | 25 | RegulActInclLastAmend | |
| | | | | 9F8212 | 200 | RegulActInclLastAmendRemark | |
| | | | | 9F8213 | 1 | RegulActApprovalCode | |
| | | **Tag** | **L(max)** | **Value** | | | |
| | | BF8214 | | MakeTable | | | |
| | | | **Tag** | **L(max)** | **Value** | | |
| | | | BF8215 | | MakeGroup | | |
| | | | | **Tag** | **L(max)** | **Value** | |
| | | | | 9F8216 | 52 | Make | |
| | | **Tag** | **L(max)** | **Value** | | | |
| | | BF8217 | | CommercialNameTable | | | |
| | | | **Tag** | **L(max)** | **Value** | | |
| | | | BF8218 | | CommercialNameGroup | | |
| | | | | **Tag** | **L(max)** | **Value** | |
| | | | | 9F8219 | 50 | CommercialName | |
| | | **Tag** | **L(max)** | **Value** | | | |
| | | BF821A | | StageNrOfManufacturingTable | | | |
| | | | **Tag** | **L(max)** | **Value** | | |
| | | | BF821B | | StageNrOfManufacturingGroup | | |

| Tag | L(max) | Value | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | **Tag** | **L(max)** | **Value** | | |
| | | | | 9F821C | 2 | StageManufacturerNumber | | |
| | | | | 9F821D | 80 | StageManufacturerName | | |
| | | | | 9F821E | 40 | StageEcTypeApprovalNumber | | |
| | | | | 9F821F | | StageDate | | |
| | | | | BF8220 | | AddressTable | | |
| | | | | | **Tag** | **L(max)** | **Value** | |
| | | | | | BF8221 | | AddressGroup | |
| | | | | | | **Tag** | **L(max)** | **Value** |
| | | | | | | 9F8222 | 3 | AddressTypeCode |
| | | | | | | 9F8223 | 80 | Name |
| | | | | | | 9F8224 | 150 | AddressLine1 |
| | | | | | | 9F8225 | 150 | AddressLine2 |
| | | | | | | 9F8226 | 150 | AddressLine3 |
| | | | | | | 9F8227 | 80 | PlaceOfResidence |
| | | | | | | 9F8228 | 80 | CountryOfResidence |
| | | | | | | 9F8229 | 20 | PhoneNumber |
| | | | | | | 9F822A | 130 | EMailAddress |
| | | **Tag** | **L(max)** | **Value** | | | | |
| | | BF822B | | TypeApprTranspDangerGoodsTable | | | | |
| | | | **Tag** | **L(max)** | **Value** | | | |
| | | | BF822C | | TypeApprTranspDangerGoodsGroup | | | |
| | | | | **Tag** | **L(max)** | **Value** | | |
| | | | | 9F822D | 30 | TypeApprTranspDangerGoodsClass | | |
| | | **Tag** | **L(max)** | **Value** | | | | |
| | | BF822E | | BodyworkTable | | | | |
| | | | **Tag** | **L(max)** | **Value** | | | |
| | | | BF822F | | BodyworkGroup | | | |
| | | | | **Tag** | **L(max)** | **Value** | | |
| | | | | 9F8230 | 2 | CodeForBodywork | | |
| | | | | 9F8231 | 3 | NumberForBodywork | | |

| Tag | L(max) | Value | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | 9F8232 | 2 | CodeForBodyworkSpecPurpVeh | | |
| | | | | BF8233 | | VehicleClassTable | | |
| | | | | | **Tag** | **L(max)** | **Value** | |
| | | | | | BF8234 | | VehicleClassGroup | |
| | | | | | | **Tag** | **L(max)** | **Value** |
| | | | | | | 9F8235 | 5 | ClassOfVehicleCode |
| | | **Tag** | **L(max)** | **Value** | | | | |
| | | BF8236 | | TyreTable | | | | |
| | | | **Tag** | **L(max)** | **Value** | | | |
| | | | BF8237 | | TyreGroup | | | |
| | | | | **Tag** | **L(max)** | **Value** | | |
| | | | | 9F8238 | 100 | TyreSpecification | | |
| | | | | 9F8239 | 6 | TechnPermMaxLadenMassTyreSpec | | |
| | | **Tag** | **L(max)** | **Value** | | | | |
| | | BF823A | | AxleTable | | | | |
| | | | **Tag** | **L(max)** | **Value** | | | |
| | | | BF823B | | AxleGroup | | | |
| | | | | **Tag** | **L(max)** | **Value** | | |
| | | | | 9F823C | 2 | AxleNumber | | |
| | | | | 9F823D | 1 | TwinWheelsAxleInd | | |
| | | | | 9F823E | 1 | SteeredAxleInd | | |
| | | | | 9F823F | 4 | TrackOfEachSteeredAxle | | |
| | | | | 9F8240 | 1 | PoweredAxleInd | | |
| | | | | 9F8241 | 1 | BrakedAxleInd | | |
| | | | | 9F8242 | 4 | AxleTrack | | |
| | | | | 9F8243 | 4 | AxleTrackMinimum | | |
| | | | | 9F8244 | 4 | AxleTrackMaximum | | |
| | | | | 9F8245 | 4 | TrackOfAllOtherAxles | | |
| | | | | 9F8246 | 1 | LiftAxleInd | | |
| | | | | 9F8247 | 1 | LoadableAxleInd | | |
| | | | | 9F8248 | 1 | RetractableOrLoadableAxleInd | | |

| Tag | L(max) | Value | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | 9F8249 | 1 | DriveAxleWithAirSuspOrEquivInd | | |
| | | | | 9F824A | 1 | AxleWithAirSuspOrEquivInd | | |
| | | | | 9F824B | 5 | AxleSpacing | | |
| | | | | 9F824C | 5 | AxleSpacingMinimum | | |
| | | | | 9F824D | 5 | AxleSpacingMaximum | | |
| | | | | 9F824E | 5 | DistrOfMassRunningOrderAxle | | |
| | | | | 9F824F | 5 | DistribUnladenMassAxle | | |
| | | | | 9F8250 | 5 | DistribMassIncompleteVehAxle | | |
| | | | | 9F8251 | 5 | DistribMassCompletedVehAxleMin | | |
| | | | | 9F8252 | 5 | TechnicallyPermMassAxle | | |
| | | | | BF8253 | | MaxPermLadenMassAxleNatTable | | |
| | | | | | **Tag** | **L(max)** | **Value** | |
| | | | | | BF8254 | | MaxPermLadenMassAxleNatGroup | |
| | | | | | | **Tag** | **L(max)** | **Value** |
| | | | | | | 9F8255 | 2 | MaxPermLadenMassAxleCountrCode |
| | | | | | | 9F8256 | 5 | MaxPermLadenMassAxleNational |
| | | | | **Tag** | **L(max)** | **Value** | | |
| | | | | BF8257 | | MaxPermLadenMassAxleIntTable | | |
| | | | | | **Tag** | **L(max)** | **Value** | |
| | | | | | BF8258 | | MaxPermLadenMassAxleIntGroup | |
| | | | | | | **Tag** | **L(max)** | **Value** |
| | | | | | | 9F8259 | 40 | MaxPermLadenMassTrafficRegul |
| | | | | | | 9F825A | 5 | MaxPermLadenMassAxleInt |
| | | | | **Tag** | **L(max)** | **Value** | | |
| | | | | BF825B | | InterconnWithPoweredAxleTable | | |
| | | | | | **Tag** | **L(max)** | **Value** | |
| | | | | | BF825C | | InterconnWithPoweredAxleGroup | |
| | | | | | | **Tag** | **L(max)** | **Value** |
| | | | | | | 9F825D | 1 | InterconnWithPoweredAxleNumber |
| | | | | | | 9F825E | 40 | InterconnOfPoweredAxles |
| | | | | **Tag** | **L(max)** | **Value** | | |

| Tag | L(max) | Value | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | BF825F | | InterconnWithBrakedAxleTable | | |
| | | | | | **Tag** | **L(max)** | **Value** | |
| | | | | | BF8260 | | InterconnWithBrakedAxleGroup | |
| | | | | | | **Tag** | **L(max)** | **Value** |
| | | | | | | 9F8261 | 1 | InterconnWithBrakedAxleNumber |
| | | | | | | 9F8262 | 80 | InterconnOfBrakedAxle |
| | | | | **Tag** | **L(max)** | **Value** | | |
| | | | | BF8263 | | TyreAxleTable | | |
| | | | | | **Tag** | **L(max)** | **Value** | |
| | | | | | BF8264 | | TyreAxleGroup | |
| | | | | | | **Tag** | **L(max)** | **Value** |
| | | | | | | 9F8265 | 6 | DistrMaxLadenMassTyreAxleSpec |
| | | | | | | 9F8266 | 6 | TechnPermisMaxMassAxle |
| | | | | | | 9F8267 | 5 | DistrTechnPermisMassAxle |
| | | | | | | 9F8268 | 6 | TechPermMaxStatVertLoadCouplPt |
| | | | | | | 9F8269 | 20 | TyreSize |
| | | | | | | 9F826A | 3 | LoadCapacityIndexSingleWheel |
| | | | | | | 9F826B | 3 | LoadCapacityIndexTwinWheel |
| | | | | | | 9F826C | 2 | SpeedCategorySymbol |
| | | | | | | 9F826D | 20 | RimSizeIncludingOffSet |
| | | **Tag** | **L(max)** | **Value** | | | | |
| | | BF826E | | AxleGroupTable | | | | |
| | | | **Tag** | **L(max)** | **Value** | | | |
| | | | BF826F | | AxleGroupGroup | | | |
| | | | | **Tag** | **L(max)** | **Value** | | |
| | | | | 9F8270 | 2 | AxleGroupNumber | | |
| | | | | 9F8271 | 6 | TechPermMassAxleGroup | | |
| | | | | BF8272 | | MaxPermLadenMassAxleGrNatTable | | |
| | | | | | **Tag** | **L(max)** | **Value** | |
| | | | | | BF8273 | | MaxPermLadenMassAxleGrNatGroup | |
| | | | | | | **Tag** | **L(max)** | **Value** |

| Tag | L(max) | Value | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | 9F8274 | 2 | MaxPermLadenMassAxleGrCCode |
| | | | | | | 9F8275 | 5 | MaxPermLadenMassAxleGrNat |
| | | | | **Tag** | **L(max)** | **Value** | | |
| | | | | BF8276 | | MaxPermLadenMassAxleGrIntTable | | |
| | | | | | **Tag** | **L(max)** | **Value** | |
| | | | | | BF8277 | | MaxPermLadenMassAxleGrIntGroup | |
| | | | | | | **Tag** | **L(max)** | **Value** |
| | | | | | | 9F8278 | 40 | MaxPermLadenMassGrTrafficRegul |
| | | | | | | 9F8279 | 5 | MaxPermLadenMassAxleGrInt |
| | | **Tag** | **L(max)** | **Value** | | | | |
| | | BF827A | | EngineTable | | | | |
| | | | **Tag** | **L(max)** | **Value** | | | |
| | | | BF827B | | EngineGroup | | | |
| | | | | **Tag** | **L(max)** | **Value** | | |
| | | | | 9F827C | 52 | ManufacturerOfTheEngine | | |
| | | | | 9F827D | 40 | EngineCodeAsMarkedOnTheEngine | | |
| | | | | 9F827E | 40 | EngineEcTypeApprovalNumber | | |
| | | | | 9F827F | 25 | EngineNumber | | |
| | | | | 9F8300 | 80 | IdentEngineTypeLocation | | |
| | | | | 9F8301 | 80 | IdentEngineTypeMethodAffixing | | |
| | | | | 9F8302 | 2 | WorkingPrincipleCode | | |
| | | | | 9F8303 | 1 | DirectInjectionIndicator | | |
| | | | | 9F8304 | 1 | PureElectricIndicator | | |
| | | | | 9F8305 | 1 | HybridIndicator | | |
| | | | | 9F8306 | 2 | NumberOfCylinders | | |
| | | | | 9F8307 | 3 | ArrangementOfCylindersCode | | |
| | | | | 9F8308 | 7 | EngineCapacity | | |
| | | | | 9F8309 | 1 | ElectricEngineIndicator | | |
| | | | | 9F830A | 1 | OffVehicleChargingIndicator | | |
| | | | | 9F830B | 1 | LpgFuellingSystemIndicator | | |
| | | | | 9F830C | 1 | CngFuellingSystemIndicator | | |

| Tag | L(max) | Value | | | | |
|---|---|---|---|---|---|---|
| | | | | 9F830D | 5 | MaxPercentBiofuelAcceptInFuel |
| | | **Tag** | **L(max)** | **Value** | | |
| | | BF830E | | TrailerBrakeTable | | |
| | | | **Tag** | **L(max)** | **Value** | |
| | | | BF830F | | TrailerBrakeGroup | |
| | | | | **Tag** | **L(max)** | **Value** |
| | | | | 9F8310 | 3 | TrailerBrakeConnectionsCode |
| | | | | 9F8311 | 7 | PressFeedLineTwoLineBraking |
| | | | | 9F8312 | 7 | PressFeedLineSingleLineBraking |
| | | **Tag** | **L(max)** | **Value** | | |
| | | BF8313 | | MechanicalCouplingTable | | |
| | | | **Tag** | **L(max)** | **Value** | |
| | | | BF8314 | | MechanicalCouplingGroup | |
| | | | | **Tag** | **L(max)** | **Value** |
| | | | | 9F8315 | 40 | MechnicalCouplingType |
| | | | | 9F8316 | 52 | MechnicalCouplingMake |
| | | | | 9F8317 | 4 | HeightCouplingAboveGroundMax |
| | | | | 9F8318 | 4 | HeightCouplingAboveGroundMin |
| | | | | 9F8319 | 4 | FifthWheelLead |
| | | | | 9F831A | 4 | FifthWheelLeadMinimum |
| | | | | 9F831B | 4 | FifthWheelLeadMaximum |
| | | | | 9F831C | 5 | DistFrontVehCentreCouplDev |
| | | | | 9F831D | 5 | DistFrontVehCentreCouplDevMin |
| | | | | 9F831E | 5 | DistFrontVehCentreCouplDevMax |
| | | | | 9F831F | 5 | DistCentreCouplDevRearVeh |
| | | | | 9F8320 | 5 | DistCentreCouplDevRearVehMin |
| | | | | 9F8321 | 5 | DistCentreCouplDevRearVehMax |
| | | | | 9F8322 | 4 | DistAxisFifthWheelForemost |
| | | | | 9F8323 | 4 | DistAxisFifthWheelForemostMin |
| | | | | 9F8324 | 4 | DistAxisFifthWheelForemostMax |
| | | | | 9F8325 | 6 | TechPermMaxTowMassBrakedTrail |

| Tag | L(max) | Value | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | 9F8326 | 6 | TechPermMaxTowMassDrawbarTrail | | |
| | | | | 9F8327 | 6 | TechPermMaxTowMassSemiTrailer | | |
| | | | | 9F8328 | 6 | TechPermMaxTowMassCentAxTrail | | |
| | | | | 9F8329 | 6 | TechPermMaxTowMassUnbrTrailer | | |
| | | | | 9F832A | 6 | TechPermMaxTowableMassTrailer | | |
| | | | | 9F832B | 6 | TechPermMaxStatVertMassCouplPt | | |
| | | | | 9F832C | 6 | TechPermMaxStatMassCouplPoint | | |
| | | | | 9F832D | 6 | DistanceCouplPointFirstAxle | | |
| | | | | 9F832E | 6 | DistanceCouplPointFirstAxleMin | | |
| | | | | 9F832F | 6 | DistanceCouplPointFirstAxleMax | | |
| | | | | 9F8330 | 6 | IndependBrakedTowableMass | | |
| | | | | 9F8331 | 6 | InertiaBrakedTowableMass | | |
| | | | | 9F8332 | 6 | ContinuousBrakedTowableMass | | |
| | | | | 9F8333 | 35 | ApprovalNrCouplingDevice | | |
| | | | | 9F8334 | 6 | CouplCharTechnPermTrailerMass | | |
| | | | | BF8335 | | CouplingDevicesFittedTable | | |
| | | | | | **Tag** | **L(max)** | **Value** | |
| | | | | | BF8336 | | CouplingDevicesFittedGroup | |
| | | | | | | **Tag** | **L(max)** | **Value** |
| | | | | | | 9F8337 | 80 | TypeOfCouplingDeviceFitted |
| | | | | **Tag** | **L(max)** | **Value** | | |
| | | | | 9F8338 | 6 | CouplingCharacteristicValueD | | |
| | | | | 9F8339 | 6 | CouplingCharacteristicValueDC | | |
| | | | | 9F833A | 6 | CouplingCharacteristicValueV | | |
| | | | | 9F833B | 6 | CouplingCharacteristicValueS | | |
| | | | | 9F833C | 6 | CouplingCharacteristicValueU | | |
| | | **Tag** | **L(max)** | **Value** | | | | |
| | | BF833D | | EcoInnovationsTable | | | | |
| | | | **Tag** | **L(max)** | **Value** | | | |
| | | | BF833E | | EcoInnovationsGroup | | | |
| | | | | **Tag** | **L(max)** | **Value** | | |

| Tag | L(max) | Value | | | | |
|---|---|---|---|---|---|---|
| | | | | 9F833F | 120 | GeneralCodeOfTheEcoInnovations |
| | | **Tag** | **L(max)** | **Value** | | |
| | | BF8340 | | FuelTable | | |
| | | | **Tag** | **L(max)** | **Value** | |
| | | | BF8341 | | FuelGroup | |
| | | | | **Tag** | **L(max)** | **Value** |
| | | | | 9F8342 | 2 | FuelCode |
| | | | | 9F8343 | 6 | MaximumNetPower |
| | | | | 9F8344 | 5 | EngineSpeedMaximumNetPower |
| | | | | 9F8345 | 6 | MaximumContinuousRatedPower |
| | | | | 9F8346 | 3 | PowerMassRatio |
| | | | | 9F8347 | 4 | PowerPowerTakeOff |
| | | | | 9F8348 | 5 | EngineSpeedPowerPowerTakeOff |
| | | | | 9F8349 | 5 | CalculatedMaximumSpeed |
| | | | | 9F834A | 5 | MaximumSpeed |
| | | | | 9F834B | 35 | ExtSoundLevelNrBaseRegulAct |
| | | | | 9F834C | 5 | SoundLevelStationary |
| | | | | 9F834D | 5 | SoundLevelStatEngineSpeed |
| | | | | 9F834E | 5 | SoundLevelDriveBy |
| | | | | 9F834F | 35 | DriverPercSoundLevNrBaseRegAct |
| | | | | 9F8350 | 3 | DriverPerceivedSoundLevel |
| | | | | 9F8351 | 10 | ExhaustEmissionLevelEuro |
| | | | | 9F8352 | 40 | OtherEmissionLegislation |
| | | | | 9F8353 | 35 | NrBaseRegulActLastAmendMotVeh |
| | | | | 9F8354 | 35 | NrBaseRegulActLastAmendEngines |
| | | | | 9F8355 | 9 | SmokeCorrectedAbsorptionCoeff |
| | | | | 9F8356 | 3 | UrbanConditionsCO2 |
| | | | | 9F8357 | 4 | UrbanConditionsFuelConsumption |
| | | | | 9F8358 | 3 | ExtraUrbanConditionsCO2 |
| | | | | 9F8359 | 4 | ExtraUrbanConditionsFuelCons |
| | | | | 9F835A | 3 | CombinedCO2 |

| Tag | L(max) | Value | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | 9F835B | 4 | CombinedFuelConsumption | |
| | | | | 9F835C | 9 | WeightedCombinedCO2 | |
| | | | | 9F835D | 5 | WeightedCombinedFuelCons | |
| | | | | 9F835E | 9 | CombinedCO2ConditionA | |
| | | | | 9F835F | 9 | CombinedCO2ConditionB | |
| | | | | 9F8360 | 5 | CombinedFuelConsConditionA | |
| | | | | 9F8361 | 5 | CombinedFuelConsConditionB | |
| | | | | 9F8362 | 7 | ElectricEnergyConsConditionA | |
| | | | | 9F8363 | 7 | ElectricEnergyConsConditionB | |
| | | | | 9F8364 | 7 | ElectricEnergyConsPureElectric | |
| | | | | 9F8365 | 7 | ElectricEnergyConsWeightedComb | |
| | | | | 9F8366 | 5 | ElectricRange | |
| | | | | 9F8367 | 5 | ElectricRangeExternChargeable | |
| | | | | BF8368 | | TestprocedureType1Group | |
| | | | | | **Tag** | **L(max)** | **Value** |
| | | | | | 9F8369 | 9 | TestprocType1CO |
| | | | | | 9F836A | 9 | TestprocType1HC |
| | | | | | 9F836B | 9 | TestprocType1NOx |
| | | | | | 9F836C | 9 | TestprocType1NMHC |
| | | | | | 9F836D | 9 | TestprocType1HC_NOx |
| | | | | | 9F836E | 9 | TestprocType1Particulates |
| | | | | | 9F836F | 9 | TestprocType1NrOfParticles |
| | | | | | 9F8370 | 2 | TestProcType1ExponentParticles |
| | | | | **Tag** | **L(max)** | **Value** | |
| | | | | BF8371 | | TestprocedureType2Group | |
| | | | | | **Tag** | **L(max)** | **Value** |
| | | | | | 9F8372 | 9 | TestprocType2CO |
| | | | | | 9F8373 | 9 | TestprocType2HC |
| | | | | | 9F8374 | 6 | TestprocType2COAtNormIdleSp |
| | | | | | 9F8375 | 5 | TestprocType2EngSpNormalMin |
| | | | | | 9F8376 | 5 | TestprocType2EngSpNormalMax |

| Tag | L(max) | Value | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | 9F8377 | 6 | TestprocType2COAtHighIdleSp |
| | | | | | 9F8378 | 5 | TestprocType2EngSpHighIdleMin |
| | | | | | 9F8379 | 5 | TestprocType2EngSpHighIdleMax |
| | | | | **Tag** | **L(max)** | **Value** | |
| | | | | BF837A | | TestprocedureEscGroup | |
| | | | | | **Tag** | **L(max)** | **Value** |
| | | | | | 9F837B | 9 | TestprocEscCO |
| | | | | | 9F837C | 9 | TestprocEscTHC |
| | | | | | 9F837D | 9 | TestprocEscNOx |
| | | | | | 9F837E | 9 | TestprocEscParticulates |
| | | | | | 9F837F | 9 | TestProcEscNumberOfParticles |
| | | | | | 9F8400 | 2 | TestProcEscExponentParticles |
| | | | | **Tag** | **L(max)** | **Value** | |
| | | | | BF8401 | | TestprocedureNrscGroup | |
| | | | | | **Tag** | **L(max)** | **Value** |
| | | | | | 9F8402 | 9 | TestprocNrscCO |
| | | | | | 9F8403 | 9 | TestprocNrscHC |
| | | | | | 9F8404 | 9 | TestprocNrscNOx |
| | | | | | 9F8405 | 9 | TestprocNrscNMHC_NOx |
| | | | | | 9F8406 | 9 | TestprocNrscParticulates |
| | | | | | 9F8407 | 9 | TestprocNrscNumberOfParticles |
| | | | | | 9F8408 | 2 | TestProcNrscExponentParticles |
| | | | | **Tag** | **L(max)** | **Value** | |
| | | | | BF8409 | | TestprocedureWhscGroup | |
| | | | | | **Tag** | **L(max)** | **Value** |
| | | | | | 9F840A | 9 | TestprocWhscCO |
| | | | | | 9F840B | 9 | TestprocWhscTHC |
| | | | | | 9F840C | 9 | TestprocWhscNOx |
| | | | | | 9F840D | 9 | TestprocWhscNMHC |
| | | | | | 9F840E | 9 | TestprocWhscCH4 |
| | | | | | 9F840F | 9 | TestprocWhscNH3 |

| Tag | L(max) | Value | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | 9F8410 | 9 | TestprocWhscParticulates |
| | | | | | 9F8411 | 9 | TestprocWhscNumberOfParticles |
| | | | | | 9F8412 | 2 | TestProcWhscExponentParticles |
| | | | | **Tag** | **L(max)** | **Value** | |
| | | | | BF8413 | | TestProcedureElrGroup | |
| | | | | | **Tag** | **L(max)** | **Value** |
| | | | | | 9F8414 | 9 | TestProcElrSmokeValue |
| | | | | **Tag** | **L(max)** | **Value** | |
| | | | | BF8415 | | TestprocedureEtcGroup | |
| | | | | | **Tag** | **L(max)** | **Value** |
| | | | | | 9F8416 | 9 | TestprocEtcCO |
| | | | | | 9F8417 | 9 | TestprocEtcNOx |
| | | | | | 9F8418 | 9 | TestprocEtcNMHC |
| | | | | | 9F8419 | 9 | TestprocEtcTHC |
| | | | | | 9F841A | 9 | TestprocEtcCH4 |
| | | | | | 9F841B | 9 | TestprocEtcParticulates |
| | | | | | 9F841C | 9 | TestprocEtcNumberOfParticles |
| | | | | | 9F841D | 2 | TestProcEtcExponentParticles |
| | | | | **Tag** | **L(max)** | **Value** | |
| | | | | BF841E | | TestprocedureNrtcGroup | |
| | | | | | **Tag** | **L(max)** | **Value** |
| | | | | | 9F841F | 9 | TestprocNrtcCO |
| | | | | | 9F8420 | 9 | TestprocNrtcNOx |
| | | | | | 9F8421 | 9 | TestprocNrtcNMHC |
| | | | | | 9F8422 | 9 | TestprocNrtcNMHC_NOx |
| | | | | | 9F8423 | 9 | TestprocNrtcTHC |
| | | | | | 9F8424 | 9 | TestprocNrtcCH4 |
| | | | | | 9F8425 | 9 | TestprocNrtcParticulates |
| | | | | | 9F8426 | 9 | TestprocNrtcNumberOfParticles |
| | | | | | 9F8427 | 2 | TestProcEscExponentParticles |
| | | | | **Tag** | **L(max)** | **Value** | |

| Tag | L(max) | Value | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | BF8428 | | TestprocedureWhtcGroup | |
| | | | | | **Tag** | **L(max)** | **Value** |
| | | | | | 9F8429 | 9 | TestprocWhtcCO |
| | | | | | 9F842A | 9 | TestprocWhtcNOx |
| | | | | | 9F842B | 9 | TestprocWhtcNMHC |
| | | | | | 9F842C | 9 | TestprocWhtcTHC |
| | | | | | 9F842D | 9 | TestprocWhtcCH4 |
| | | | | | 9F842E | 9 | TestprocWhtcNH3 |
| | | | | | 9F842F | 9 | TestprocWhtcParticulates |
| | | | | | 9F8430 | 9 | TestprocWhtcNumberOfParticles |
| | | | | | 9F8431 | 2 | TestProcWhtcExponentParticles |
| | | **Tag** | **L(max)** | **Value** | | | |
| | | BF8432 | | InServiceMaxMassNatTable | | | |
| | | | **Tag** | **L(max)** | **Value** | | |
| | | | BF8433 | | InServiceMaxMassNatGroup | | |
| | | | | **Tag** | **L(max)** | **Value** | |
| | | | | 9F8434 | 2 | MaxPermMassNatTraffCountryCode | |
| | | | | 9F8435 | 6 | MaxPermLadenMassNational | |
| | | | | 9F8436 | 6 | MaxPermMassCombinationNational | |
| | | **Tag** | **L(max)** | **Value** | | | |
| | | BF8437 | | InServiceMaxMassIntTable | | | |
| | | | **Tag** | **L(max)** | **Value** | | |
| | | | BF8438 | | InServiceMaxMassIntGroup | | |
| | | | | **Tag** | **L(max)** | **Value** | |
| | | | | 9F8439 | 40 | MaxPermMassIntTrafficRegul | |
| | | | | 9F843A | 6 | MaxPermLadenMassInternational | |
| | | | | 9F843B | 6 | MaxPermMassCombinationInt | |
| | **Tag** | **L(max)** | **Value** | | | | |
| | BF843C | | TechnicalAdditionalDataGroup | | | | |
| | | **Tag** | **L(max)** | **Value** | | | |
| | | 9F843E | | DateOfProduction | | | |

| Tag | L(max) | Value | | |
|---|---|---|---|---|
| | | 9F843F | 1 | BrakeAssistSystemIndicator |
| | | 9F8440 | 1 | ProtectionPedestriansIndicator |
| | | 9F8441 | 1 | DaytimeRunningLightsIndicator |
| | | 9F8442 | 1 | ElectronicStabilityProgramInd |
| | | 9F8443 | 1 | TyrePressureMonitoringSystInd |
| | | 9F8444 | 1 | LaneDepartureWarningIndicator |
| | | 9F8445 | 1 | AdvancEmergencyBrakingSystInd |
| | | 9F8446 | 1 | BrakeRetarderIndicator |
| | | 9F8447 | 1 | PressureChargerInd |
| | | 9F8448 | 1 | InterCoolerIndicator |
| | | 9F8449 | 1 | CatalyticConvertorInd |
| | | 9F844A | 1 | OxygenSensorInd |
| | | 9F844B | 1 | AirInjectionInd |
| | | 9F844C | 1 | ExhaustGasRecirculationInd |
| | | 9F844D | 1 | EvaporativeEmisControlSysInd |
| | | 9F844E | 1 | ParticulateTrapInd |
| | | 9F844F | 1 | OnBoardDiagnosInd |
| | | 9F8450 | 1 | AntilockBrakeSysInd |
| | | 9F8451 | 1 | FrontAirbagInd |
| | | 9F8452 | 1 | SideAirbagInd |
| | | 9F8453 | 1 | BeltPreloadDeviceInd |
| | | 9F8454 | 1 | HeadAirbagInd |
| | | 9F8455 | 1 | LowerAirbagInd |
| | | 9F8456 | 1 | BeltForceLimiterInd |
| | | 9F8457 | 1 | RearRegistrationPlateCode |
| | | 9F8458 | 10 | CodeEmissionCategory |
| | | 9F8459 | 8 | NumberRegistrationCertifPart2 |
| | | 9F845A | 378 | RemarksExceptions |
| | | 9F845B | 4 | CodeOfManufacturer |
| | | 9F845C | 3 | CodeOfType |
| | | 9F845D | 5 | CodeOfVariantVersion |

| Tag | L(max) | Value | | | | |
|---|---|---|---|---|---|---|
| | | 9F845E | 1 | CheckDigitCodeOfVariantVersion | | |
| | | BF845F | | TechnAddDataGrAxleTable | | |
| | | | **Tag** | **L(max)** | **Value** | |
| | | | BF8460 | | TechnAddDataGrAxleGroup | |
| | | | | **Tag** | **L(max)** | **Value** |
| | | | | 9F8461 | 2 | TechnAddDataGrAxleNumber |
| | | | | 9F8462 | 1 | PendulumAxleIndicator |
| | | | | 9F8463 | 1 | SelfTrackingAxleIndicator |
| | **Tag** | **L(max)** | **Value** | | | |
| | BF843D | | NationalDataGroup (no children defined) | | | |

*Table 13: Format of IndividualVehicleRegistration*

## App 1.10 EF.Signature_A

| Tag | Len | Val | | |
|---|---|---|---|---|
| 30 | | SIGNATURE | | |
| | **Tag** | **Len** | **Val** | |
| | 30 | | AlgorithmIdentifier | |
| | | **Tag** | **Len** | **Val** |
| | | 06 | | algorithm (OID) |
| | | ?? | | Parameters (ANY DEFINED BY algorithm– OPTIONAL) |
| | **Tag** | **Len** | **Val** | |
| | 03 | | signatureValue (BITSTRING) | |

*Table 14: Format of EF.Signature_A*

The current preference for the RSA signature algorithm is PKCS#1v1.5, but the possibility is kept to use instead RSA-PSS. Reading and verification software should also support the RSA-PSS signature algorithm.
The same signature algorithm is used for the signatures over the CSCA certificate, DS certificate, Signature_A, Signature_B and the EF.SOd.
Notice that for RSA PKCS#1v1.5 the optional parameters must have the NULL value (RFC 4055 [9]).

## App 1.11 EF.Signature_B

| Tag | Len | Val | | |
|---|---|---|---|---|
| 30 | | SIGNATURE | | |
| | **Tag** | **Len** | **Val** | |
| | 30 | | AlgorithmIdentifier | |
| | | **Tag** | **Len** | **Val** |
| | | 06 | | algorithm (OID) |
| | | ?? | | Parameters (ANY DEFINED BY algorithm– OPTIONAL) |
| | **Tag** | **Len** | **Val** | |
| | 03 | | signatureValue (BITSTRING) | |

*Table 15: Format of EF.Signature_B*

The current preference for the RSA signature algorithm is PKCS#1v1.5, but the possibility is kept to use instead RSA-PSS. Reading and verification software should also support the RSA-PSS signature algorithm.
The same signature algorithm is used for the signatures over the CSCA certificate, DS certificate, Signature_A, Signature_B and the EF.SOd.
Notice that for RSA PKCS#1v1.5 the optional parameters must have the NULL value (RFC 4055 [9]).

# App 2 NL-eVRC Commands and Responses

For an explanation of the Command and Response APDUs and the abbreviations used see ISO/IEC 7816-4 and 7816-8 [7], [8].

## App 2.1 SELECT APPLICATION

### App 2.1.1 Command APDU

| Field | Value | Description |
|---|---|---|
| CLA | 00 | |
| INS | A4 | |
| P1 | 04 | Select by DF Name |
| P2 | 00 | Return FCI Data |
| Lc | 0B | Length of the Data field |
| Data | A0 00 00 04<br>56 45 56 52<br>2D 30 31 | AID of the VR Application |
| Le | 00 | |

*Table 16: SELECT APPLICATION Command APDU*

### App 2.1.2 Response APDU

| Field | Value | Description |
|---|---|---|
| FCI Template | | |
| Tag | 6F | |
| Length | XX | |
| Value | XX … XX | |
| SW1 SW2 | 90 00 | Successful processing |

*Table 17: Response on successful processing*

# App 2.2 SELECT FILE

## App 2.2.1 Command APDU

| Field | Value | Description |
|---|---|---|
| CLA | 00 | |
| INS | A4 | |
| P1 | 02 | Select EF under current DF |
| P2 | 04 | Return FCP Data |
| Lc | 02 | |
| Data | XX XX | File Identifier |
| Le | 00 | |

*Table 18: SELECT FILE Command APDU*

## App 2.2.2 Response APDU

| Field | Value | Description |
|---|---|---|
| FCP Template | | |
| Tag | 62 | |
| Length | XX | |
| Value | XX … XX | |
| SW1 SW2 | 90 00 | |

*Table 19: Response on successful processing*

As part of the FCP template, the value of tag 80 encodes the File Size of the selected file.

# App 2.3 READ BINARY

## App 2.3.1 Command APDU

| Field | Value | Description |
|---|---|---|
| CLA | 00 | |
| INS | B0 | |
| P1 | XX | Offset, most significant byte, value between 00 and 7F |
| P2 | XX | Offset, least significant byte |
| Lc | - | Absent |
| Data | - | Absent |
| Le | XX | Maximum number of bytes expected in the response data, 0x00 codes for 256. |

*Table 20: READ BINARY Command APDU*

Note: Possibly this command needs to be repeated with the correct offset in order to read the complete file.

### App 2.3.2 Response APDU

| Field | Value | Description |
|---|---|---|
| Response Data | XX ... XX | Le data bytes, starting at offset P1P2 |
| SW1 SW2 | 90 00 | |

*Table 21: Response on successful processing*

## App 2.4 INTERNAL AUTHENTICATE

### App 2.4.1 Command APDU

| Field | Value | Description |
|---|---|---|
| CLA | 00 | |
| INS | 88 | |
| P1 | 00 | |
| P2 | 00 | |
| Lc | 08 | |
| Data | XX ... XX | RND.IFD<br>8-byte random value generated by the off-card entity |
| Le | 00 | |

*Table 22: INTERNAL AUTHENTICATE Command APDU*

### App 2.4.2 Response APDU

| Field | Value | Description |
|---|---|---|
| Response Data | XX … XX | Signature |
| SW1 SW2 | 90 00 | |

*Table 23: Response on successful processing*

| Field | Value | Description |
|---|---|---|
| SW1 SW2 | XX XX | See section App 2.4.3 |

*Table 24: Response in case of an error condition*

### App 2.4.3 Status Words

| Value | Description | |
|---|---|---|
| 90 00 | Successful processing | |
| 66 00 | Error: Security related issues | Signature generation has failed |
| 67 00 | Error: Wrong Length | Le is not equal to 00<br>Lc is not equal to 08 |
| 69 85 | Error: Conditions of use not satisfied | Active Authentication Session Flag is set<br>or<br>Maximum Active Authentication Counter exceeds the Active Authentication Counter Maximum. |
| 6A 81 | Error: Function not supported | The card has been blocked |

| | | |
|---|---|---|
| 6A 86 | Error: Incorrect parameters P1-P2 | The bytes P1 P2 do not have the value 00 00. |
| 6A 88 | Error: Referenced Data not found | The Active Authentication Private Key has not been personalized. |

*Table 25: INTERNAL AUTHENTICATE Status Words*

## App 2.5 Status Words Summary

| Value | Description |
|---|---|
| 90 00 | Succesful processing |

*Table 26: Status Words indicating successful processing*

| Value | Description |
|---|---|
| 62 82 | Warning: End of file reached before reading Ne bytes |
| 63 00 | Warning: No information given (authentication failure) |

*Table 27: Status Words indicating a warning*

| Value | Description |
|---|---|
| 66 00 | Error: Security related issues |
| 67 00 | Error: Wrong Length |
| 68 81 | Error: Logical Channel not supported |
| 69 82 | Error: Security Status not satisfied |
| 69 85 | Error: Conditions of use not satisfied |
| 69 86 | Error: Command not allowed |
| 6A 80 | Error: Incorrect parameters in the command data field |
| 6A 81 | Error: Function not supported |
| 6A 82 | Error: File not Found |
| 6A 84 | Error: Not enough memory space in the file |
| 6A 86 | Error: Incorrect parameters P1-P2 |
| 6A 87 | Error: Nc inconsistent with parameters P1-P2 |
| 6A 88 | Error: Referenced Data not found |
| 6B 00 | Error: Wrong parameters P1-P2 |
| 6D 00 | Error: Instruction code not supported or invalid |
| 6E 00 | Error: Class not supported |

*Table 28: Status Words indicating an error condition*

# App 3 TRACES OF COMMUNICATION BETWEEN READING AND VERIFICATION SOFTWARE AND THE CHIP (INFORMATIVE)

The APDU traces have been made on basis of a specimen Dutch vehicle registration card. The DS certificates in the APDU trace can be valided with the CSCA certificate from App 4.

## App 3.1 Reading of the Dutch Vehicle Registration Card Chip

APDU trace according to the inspection procedure specified in 4.2.

**1. Select eVRC application (AID = 'A0 00 00 04 56 45 56 52 2D 30 31')**

```
T→C: '00 A4 04 00 0B A0 00 00 04 56 45 56 52 2D 30 31 00'
C→T: '6F 0D 84 0B A0 00 00 04 56 45 56 52 2D 30 31 90 00'
```

**2. Passive Authentication**

**a. Select EF.SOd (File ID = '00 1D')**

```
T→C: '00 A4 02 04 02 00 1D 00'
C→T: '62 08 83 02 00 1D 80 02 08 9C 90 00'
```

**b. Read EF.SOd (length = 'LL LL')**

```
T→C: '00 B0 00 00 00'
C→T: '30 82 08 98 06 09 2A 86 48 86 F7 0D 01 07 02 A0 82 08 89 30 82
08 85 02 01 03 31 0D 30 0B 06 09 60 86 48 01 65 03 04 02 01 30 82 01
6B 06 09 60 84 10 01 87 72 03 01 01 A0 82 01 5C 04 82 01 58 30 82 01
54 02 01 00 30 0B 06 09 60 86 48 01 65 03 04 02 01 30 82 01 40 30 26
04 02 00 0D 04 20 E6 AC A0 C2 08 A2 53 C5 82 C8 DC BA D9 A2 06 BE 83
F1 A8 2A 76 0F 16 4F 1A 78 4E 0F 47 EB 32 32 30 26 04 02 C0 01 04 20
63 3A E7 9A 1D E8 B8 80 1D 1D 2E 99 09 AF 7E 59 B7 D1 9E 59 2F 1A C1
70 61 36 DD 16 45 36 1F 55 30 26 04 02 C0 11 04 20 63 3A E7 9A 1D E8
B8 80 1D 1D 2E 99 09 AF 7E 59 B7 D1 9E 59 2F 1A C1 70 61 36 DD 16 45
36 1F 55 30 26 04 02 D0 01 04 20 77 89 04 A9 1F D3 BB A2 A2 56 15 75
D9 AA 21 0E 22 33 F0 64 17 90 7F D5 9E EC 06 A2 F6 04 70 57 30 26 04
02 D0 11 04 20 90 00'

T→C: '00 B0 01 00 00'
C→T: 'C1 55 02 FC A1 28 16 60 04 1B BA DD 03 93 E1 A6 23 D4 B8 BC 80
EB B4 61 01 9B 8E 56 DD D0 34 A2 30 26 04 02 D0 21 04 20 18 F0 83 CB
FD 72 92 B6 34 B3 2E 96 79 15 B3 78 D4 81 B7 B2 9E 2F C6 09 0A 4E 65
9E 3D 13 91 91 30 26 04 02 E0 01 04 20 8E E7 D9 80 DF 89 0D A1 08 09
09 77 4F 9D 53 B0 7D 5A AF A7 B7 F5 9C D3 D9 0D 2F 64 CE 94 DB E1 30
26 04 02 E0 11 04 20 10 4A 20 74 C1 0B 96 67 87 34 A5 F2 C4 D0 79 C6
D8 67 9E E1 8B AC F1 35 3F 8E 3F B8 3F 41 E6 E5 A0 82 05 0B 30 82 05
07 30 82 02 EF A0 03 02 01 02 02 11 00 FA 27 62 08 72 1F DE F1 64 23
4E CE 0F 92 AC F7 30 0D 06 09 2A 86 48 86 F7 0D 01 01 0B 05 00 30 66
31 19 30 17 06 03 55 04 03 13 10 43 53 43 41 20 47 41 54 20 4E 4C 20
```

RDW

```
65 56 52 44 31 0B 30 09 06 03 55 04 05 13 02 30 31 31 0C 30 0A 06 03
55 04 0B 13 03 90 00'

T→C: '00 B0 02 00 00'
C→T: '52 44 57 31 21 30 1F 06 03 55 04 0A 13 18 53 74 61 74 65 20 6F
66 20 74 68 65 20 4E 65 74 68 65 72 6C 61 6E 64 73 31 0B 30 09 06 03
55 04 06 13 02 4E 4C 30 1E 17 0D 31 33 31 31 32 36 30 31 33 33 32 36
5A 17 0D 32 34 30 32 32 34 30 31 33 33 32 37 5A 30 63 31 0B 30 09 06
03 55 04 06 13 02 4E 4C 31 21 30 1F 06 03 55 04 0A 0C 18 53 74 61 74
65 20 6F 66 20 74 68 65 20 4E 65 74 68 65 72 6C 61 6E 64 73 31 0C 30
0A 06 03 55 04 0B 0C 03 52 44 57 31 16 30 14 06 03 55 04 03 0C 0D 44
53 2D 30 32 20 4E 4C 20 65 56 52 44 31 0B 30 09 06 03 55 04 05 13 02
32 31 30 82 01 22 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03 82
01 0F 00 30 82 01 0A 02 82 01 01 00 C8 FE E0 20 75 27 77 40 BD 19 66
64 EE 5A 07 07 27 24 EA 82 3D D0 41 2C BE EC 5A AC 6C 8B 15 F1 B4 E9
E4 F6 47 33 76 90 00'

T→C: '00 B0 03 00 00'
C→T: '5A 16 96 41 74 32 C4 30 50 B6 65 1B 22 4F F1 6F 68 A1 4C D0 E5
ED 28 B0 8A 26 D3 27 C1 B5 C9 B7 55 70 1B DE C3 8E 2F BB B8 B0 79 73
BD DF 81 B9 AA 4C D4 2D D6 87 FF 51 CF 6C C1 6F E4 4E EF 51 27 37 C0
CA 64 24 E0 66 CE AE 66 B0 3A E2 11 EA 94 12 0F DA A3 06 6F 25 57 E9
7A 54 0A 8C 08 06 6E 32 C2 57 30 48 F6 4F 80 DE 29 62 B9 E0 99 45 DE
DF 6A 90 93 4B BB 32 78 B8 F5 BB 47 9F 7E 1E 82 7B 6E E2 50 9A 8B 77
A5 52 57 6B 9F BE E8 BF C5 68 94 1C AB CB 2F 7C 14 18 A9 A9 C0 98 60
0A 58 B2 3F 70 95 D0 66 97 86 66 3B BE 96 C9 6F D9 4E C6 2F 44 19 4F
21 43 E3 04 5F 0C 1C 8A 7B 94 8F 81 83 28 03 3A 29 D9 5F 8D E6 F7 B5
4B C9 4F 24 C6 07 B3 BA 99 AF 58 41 02 03 01 00 01 A3 81 B2 30 81 AF
30 1D 06 03 55 1D 0E 04 16 04 14 66 E4 AB D3 C8 03 26 55 B9 A0 3E D6
BB EF 85 68 41 90 00'

T→C: '00 B0 04 00 00'
C→T: 'C5 5B 74 30 1F 06 03 55 1D 23 04 18 30 16 80 14 92 51 87 BD 8D
E7 DF BF 32 3C 66 69 29 7F DA EB 8A B4 AB B4 30 17 06 03 55 1D 20 04
10 30 0E 30 0C 06 0A 60 84 10 01 87 72 02 01 03 01 30 44 06 03 55 1D
1F 04 3D 30 3B 30 39 A0 37 A0 35 86 33 68 74 74 70 3A 2F 2F 77 77 77
2D 64 69 65 6E 73 74 65 6E 2E 72 64 77 2E 6E 6C 2F 63 72 6C 2F 43 53
43 41 47 41 54 4E 4C 65 56 52 44 2D 30 31 2E 63 72 6C 30 0E 06 03 55
1D 0F 01 01 FF 04 04 03 02 07 80 30 0D 06 09 2A 86 48 86 F7 0D 01 01
0B 05 00 03 82 02 01 00 82 FC C7 80 1E 6D 47 35 1D 40 7B B5 B4 F7 77
09 C7 4F 6F DF C7 CF 32 CF 6F 48 5C 29 99 E7 E2 3C 71 87 70 26 9C 6F
E1 E7 6F 22 BB BB BE 53 5A 4B F3 C5 3A 2F 84 56 1D 7A 69 24 26 C8 50
C1 7E C7 06 8E 35 67 82 A5 28 22 C4 82 DC 7E 70 2F FF 1D C4 3D 52 FD
86 88 19 44 1A 90 00'

T→C: '00 B0 05 00 00'
C→T: 'AB CA 36 92 B4 70 2D B4 11 85 E8 AC 6A 55 57 BA 55 DA 42 56 73
A5 49 88 1E 6D CD 22 4A 88 99 A5 D6 C1 90 96 09 07 5F 89 5D 35 20 8D
70 13 C7 B9 7A 6F 9F 6B DB 17 CE EC 0D 56 FC 45 92 B2 E4 4F 9E 3F 16
14 7F CF D7 DE 38 A5 01 BE F4 0E BE D9 AC 79 76 19 C0 4E 33 AB 8C BB
F6 BA 7E 78 6B 8A 6C 93 5F AB BB 0A E5 31 DA 2C 7B 4C 3C 48 9C 1B A9
78 0D 56 55 20 48 72 80 A9 16 6F 92 5D F0 CD F9 2F 49 B6 CC 4C 47 42
```

RDW

```
F8 64 4A 73 1C 57 0B 95 04 AE 24 E9 24 6E 33 B3 DD 06 AA B3 EA 2C A3
0D 2E 0F 5B 0A 8D 51 BE 21 C5 62 F4 FA 7B FE A5 A8 65 CE EE E5 2D A9
49 E4 11 B0 93 4D B7 92 83 DA 69 75 70 E1 0B 7C 84 4E B8 1F 06 CE 7A
FE 92 ED DF 77 12 FA A4 49 FE A4 11 4E F4 41 CA 6C 57 11 38 21 96 D7
E6 73 3F 0B 66 6A 93 0B 4E 04 9F 4D 2D 4B 24 78 36 20 A5 01 C2 AD BD
06 AB D4 D7 EA 90 00'

T→C: '00 B0 06 00 00'
C→T: '4D E9 EB 40 9F C8 A7 3C D7 9C 8D 91 65 ED FA 7C C3 8B FA 2E B9
E7 C7 54 C1 9D 2E 6D B4 17 8B 0F 38 72 24 A9 39 CD 60 96 BE 4D 14 FA
61 22 88 0F B1 9E E4 46 DF 5A 26 93 3E 93 CB D7 5B C0 9E F4 3E 25 EA
38 DC 4A DD 1C 48 4A B5 F3 A4 B1 8C 36 4A 91 25 3C B0 0E 79 37 F2 04
E1 59 92 8A DD 0E 5B D2 FE 90 00 C4 BE 66 19 FE 9A 90 EC C7 30 CD 49
A7 0B A7 30 19 42 D3 42 2C ED 5A A4 38 D7 C8 2C BE 41 6A C7 00 E0 00
E7 2C EC 1B E0 D2 79 79 CC 15 D7 6A CF FC 30 40 43 FC C1 9C FD 4A 4C
9C 96 56 F0 44 33 18 74 31 82 01 F1 30 82 01 ED 02 01 01 30 7B 30 66
31 19 30 17 06 03 55 04 03 13 10 43 53 43 41 20 47 41 54 20 4E 4C 20
65 56 52 44 31 0B 30 09 06 03 55 04 05 13 02 30 31 31 0C 30 0A 06 03
55 04 0B 13 03 52 44 57 31 21 30 1F 06 03 55 04 0A 13 18 53 74 61 74
65 20 6F 66 20 90 00'

T→C: '00 B0 07 00 00'
C→T: '74 68 65 20 4E 65 74 68 65 72 6C 61 6E 64 73 31 0B 30 09 06 03
55 04 06 13 02 4E 4C 02 11 00 FA 27 62 08 72 1F DE F1 64 23 4E CE 0F
92 AC F7 30 0B 06 09 60 86 48 01 65 03 04 02 01 A0 4B 30 18 06 09 2A
86 48 86 F7 0D 01 09 03 31 0B 06 09 60 84 10 01 87 72 03 01 01 30 2F
06 09 2A 86 48 86 F7 0D 01 09 04 31 22 04 20 A9 56 9F B9 20 04 CD 19
0F A1 14 0E 97 D2 35 99 13 3A 84 28 2A 65 1D FD F4 AE 10 9B C3 C5 F8
73 30 0D 06 09 2A 86 48 86 F7 0D 01 01 0B 05 00 04 82 01 00 72 26 A5
37 A4 83 EB 5D 64 36 2E EE E6 01 8C 04 B9 06 75 B2 08 F5 18 88 A4 76
CB 17 3D 71 C7 FF 0A A5 0B 40 75 DD 36 E0 74 33 53 05 72 72 BE D3 60
93 15 A1 F7 5F D2 19 93 A2 36 E1 D1 CA 56 E4 B4 3E 57 94 D7 8E 71 AB
B5 81 EB EB AD 3A 18 85 1C 49 45 3C 12 F4 CF 93 DA 9A 97 AA D9 05 C2
7B 71 8C 67 C8 90 00'

T→C: '00 B0 08 00 00'
C→T: 'E4 AA AD 1C 22 B7 B9 DA D5 1A EA EE 09 23 B4 7F 9E 8F 8F 63 2D
4C 1B 0D 5B 8C 95 0F 0A A4 38 9A BB BE 0C 3B A5 B2 D1 0E 36 F0 DD C9
14 A3 F9 EC 18 74 FC F0 9E B8 0D 65 29 FC 6F BB 9B F8 9E 16 DF F5 74
72 27 86 A7 46 9A 06 D5 4B 31 23 C1 8E 4C B8 1E 14 9D EA B0 5C 4D 16
D7 DA 2E F6 AD 80 F2 BD 57 91 CB 73 27 5C E6 A4 B6 93 27 C1 8F 89 5E
51 CC EE 85 DA 33 58 88 87 8B 3E 1A A7 CC A8 5E 3A CD 20 83 44 B6 21
D4 42 8D 4E 1D 18 01 EF BB DE 07 77 26 C4 A5 56 CE 57 29 3A 90 00'
```

3. **Active Authentication**

   a. **Select EF.AA (File ID = '00 0D')**

```
T→C: '00 A4 02 04 02 00 0D 00'
C→T: '62 08 83 02 00 0D 80 02 01 2A 90 00'
```

   b. **Read EF.AA**

RDW

```
T→C: '00 B0 00 00 00'
C→T: '6F 82 01 26 30 82 01 22 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01
05 00 03 82 01 0F 00 30 82 01 0A 02 82 01 01 00 B7 59 31 B3 75 FE 3A
40 40 C6 B1 07 54 AB 07 42 B5 D8 88 FE 30 07 93 FE F5 EC C4 E0 54 DE
84 E9 10 32 DC 79 E5 46 3F 28 E4 DD 50 0D DD 55 A9 A5 71 32 53 63 63
48 9E 6E 20 DB FB 93 EA 77 B2 A4 64 AC 1F 15 DB 21 AA 9E 45 31 0F B3
F0 04 1C 66 F7 60 3E 14 F9 C8 2E AE 40 FF 16 F3 31 98 9D 5A B6 50 F5
00 09 BD DE CC 94 D2 09 F4 6F 91 83 C9 6F BB 14 7C A4 5D 9B FD 6C F8
7F 6D C1 AE AB 7F FA CD 3F 2E A4 43 83 8A 14 61 27 9B 68 7F 38 32 9E
6B D5 16 51 B6 02 76 AF 8D F3 CD 76 A8 B5 DA 12 DC 5B 66 8E C4 13 1F
FF AF 5A B2 23 19 A6 3A A3 B6 A7 3F 95 AE 0B A5 4F 50 83 59 E6 6D 48
C2 16 64 39 12 AF 82 1F DA 13 9A CC 25 A5 9E FC F2 6A B7 63 19 7E DF
E4 50 4B 4C 94 90 00'

T→C: '00 B0 01 00 00'
C→T: '3C 75 86 C5 48 AA 31 BB 5A 9B B4 C5 B5 FF C9 F5 2F 39 AA 91 D8
67 D3 2D 55 7E 8B E9 AC 72 E2 6F 35 DD 90 94 9B 02 03 01 00 01 90 00'
```

### c. Chip authentication

```
T→C: '00 88 00 00 08 AB C6 06 94 68 B5 44 3A 00'
C→T: 'B4 EB 4B 65 14 01 CC 0E 91 4E 2A 11 74 60 2C 16 5F 52 CB 98 A1
56 38 74 B4 41 C0 44 75 33 B7 FC 64 9E 8C BE 29 6D F8 07 31 7D C0 59
FF 93 81 6C 0A 6F CC 1B A0 A1 85 71 AA C3 AC 8A 22 D3 73 41 49 5A C6
3E AE 98 65 CB F0 B1 D2 0B 32 46 CF 57 13 E6 D3 72 AC 01 6B 34 ED 2C
A8 17 44 3B A9 E7 B6 3C 24 E9 2A 35 53 68 52 0D 6E 7B DB E2 BA C6 F3
2A 87 64 9D 0A AB 2A 54 6D 40 D6 BD 1A CB 28 CD 78 BF 14 BD CE B2 C6
CB 66 27 41 C6 BE 1B 49 EE DB 41 D8 51 8D 2A 2E FC DA 0F D3 81 AE 0F
5B E5 FC E4 F2 80 66 76 D2 C5 A7 1C 9D 56 02 BE 3D B3 B1 B5 96 2A 04
08 6F 47 2F 4C EE 93 6B 93 9E 1E 90 4E 0C AA 78 E4 7F 2D 06 AC D6 D8
CC 0C B3 87 96 E2 98 4B 3C 7B FE CF C6 47 1D 19 EB 92 24 1F 0C 8A 6A
F3 B9 CB 78 72 06 0E A0 7F 51 FC 34 B5 DD 90 86 51 0F 47 A8 8D 8D A2
3F 65 D0 30 03 90 00'
```

## 4. Read and verify data

### a. Select EF.Registration_A ('D0 01')

```
T→C: '00 A4 02 04 02 D0 01 00'
C→T: '62 08 83 02 D0 01 80 02 01 18 90 00'
```

### b. Read EF.Registration_A

```
T→C: '00 B0 00 00 00'
C→T: '78 0D 4F 0B A0 00 00 04 56 45 56 52 2D 30 31 71 82 01 05 80 01
00 9F 33 09 4E 65 64 65 72 6C 61 6E 64 9F 35 03 52 44 57 9F 37 01 00
9F 38 0A 30 30 39 33 39 32 33 38 38 34 81 08 31 2D 52 44 57 2D 30 31
82 08 32 30 31 34 30 31 30 31 A1 34 A2 2F 83 08 56 69 73 73 63 68 65
72 84 03 57 20 47 85 1E 53 6B 61 67 65 72 20 52 61 6B 20 31 30 20 39
36 34 32 20 43 5A 20 20 56 65 65 6E 64 61 6D 86 01 02 A3 1A 87 07 43
49 54 52 4F 45 4E 88 0A 4B 46 20 52 48 43 20 38 2F 50 89 03 44 53 35
8A 11 56 46 37 4B 46 52 48 43 38 43 53 31 32 33 34 35 36 A4 09 8B 07
32 32 36 35 20 6B 67 8C 07 31 37 33 35 20 6B 67 8D 01 30 8E 08 32 30
```

RDW

```
31 34 30 31 30 31 8F 12 65 32 2A 32 30 30 37 2F 34 36 2A 30 31 35 36
2A 30 31 A5 1A 90 08 31 39 39 37 20 63 6D 33 91 09 31 32 30 2C 30 30
20 6B 57 92 03 90 00'

T→C: '00 B0 01 00 00'
C→T: '45 2F 44 93 06 6E 2E 76 2E 74 2E A6 0B 94 01 35 95 06 6E 2E 76
2E 74 2E 90 00'
```

**c. Select EF.Registration_B ('D0 11')**

```
T→C: '00 A4 02 04 02 D0 11 00'
C→T: '62 08 83 02 D0 11 80 02 00 68 90 00'
```

**d. Read EF.Registration_B**

```
T→C: '00 B0 00 00 00'
C→T: '78 0D 4F 0B A0 00 00 04 56 45 56 52 2D 30 31 72 57 80 01 00 A4
11 96 07 32 32 36 35 20 6B 67 97 06 6E 2E 76 2E 74 2E 98 05 4D 31 20
41 46 AE 10 9B 06 38 30 30 20 6B 67 9C 06 35 30 30 20 6B 67 9F 24 05
42 4C 41 55 57 9F 25 06 6E 2E 76 2E 74 2E B0 15 9F 31 12 37 31 35 2F
32 30 30 37 2A 36 39 32 2F 32 30 30 38 41 90 00'
```

**e. Select EF.Registration_C ('D0 21')**

```
T→C: '00 A4 02 04 02 D0 21 00'
C→T: '62 08 83 02 D0 21 80 02 09 73 90 00'
```

**f. Read EF.Registration_C**

```
T→C: '00 B0 00 00 00'
C→T: 'BF 87 00 82 09 6D 9F 87 01 01 01 BF 87 10 30 9F 87 11 08 32 30
31 34 30 31 30 31 9F 87 12 08 32 30 31 34 30 31 30 31 9F 87 13 08 32
30 31 34 30 31 30 31 9F 87 14 08 31 2D 52 44 57 2D 30 31 BF 87 03 82
09 2E 9F 87 04 01 00 9F 87 05 82 09 23 1F 8B 08 00 00 00 00 00 04 00
EC BD 07 60 1C 49 96 25 26 2F 6D CA 7B 7F 4A F5 4A D7 E0 74 A1 08 80
60 13 24 D8 90 40 10 EC C1 88 CD E6 92 EC 1D 69 47 23 29 AB 2A 81 CA
65 56 65 5D 66 16 40 CC ED 9D BC F7 DE 7B EF BD F7 DE 7B EF BD F7 BA
3B 9D 4E 27 F7 DF FF 3F 5C 66 64 01 6C F6 CE 4A DA C9 9E 21 80 AA C8
1F 3F 7E 7C 1F 3F 22 1E FF 1E EF 16 65 7A 99 D7 4D 51 2D 3F FB 68 77
BC F3 51 9A 2F A7 D5 AC 58 5E 7C F6 D1 BA 3D DF 3E F8 E8 F7 38 FA 8D
93 C7 67 CB 59 71 59 CC D6 59 F9 93 F9 BC 98 96 F9 D9 F2 BC AA 17 59
4B EF D1 F7 69 90 00'

T→C: '00 B0 01 00 00'
C→T: 'FA F8 49 35 BB E6 DF E8 F7 93 6A FA 34 6B B3 CF EB 6A BD D2 CF
E8 53 F3 E6 2C 5F B6 C5 79 31 E5 97 5F AC 17 93 BC 3E FA C9 67 0F 7E
AF 67 AF BE 7D 72 70 F2 FA FE EE CE FD 87 F7 1F DF DD D4 DC C2 7C DD
66 17 F9 97 E7 27 D5 62 55 E6 68 70 52 CD F2 A3 93 C7 77 E3 5F D8 F7
DE 5C AF F2 E3 D5 AA AE 2E B3 12 BF F3 B7 A7 F4 5E F4 8B E0 B5 A3 DF
EB 99 34 F3 46 96 D5 45 B6 6C 8F 68 00 84 B7 FE E1 8D 9B C9 7B 74 70
F7 25 46 25 7F D8 6F 5F E5 97 05 3E 21 82 E5 47 7B 3B BB BB DB 3B F7
B7 F7 3E 7D 7C 37 F8 A2 4B C4 13 FA F0 A2 AA AF 19 BD 2F 76 2D B5 82
CF ED 4B CF AB E9 97 E7 6F E6 39 11 A5 5D B7 F4 F5 CB 92 DA 35 DC E8
```

RDW

```
78 E7 F1 DD 4D DF 5B 20 5F E4 ED BC 9A 7D 79 7E DC B6 D9 74 BE 40 5B
1F CC BD C7 77 37 B7 F0 B1 E1 B9 E4 2E 7F B2 58 FA 68 F4 BF 88 4E 99
B2 41 BE F7 AD 90 00'

T→C: '00 B0 02 00 00'
C→T: 'BD 9D 9D 07 77 F7 3F FD D6 CE EE 7D FC 13 4E 60 97 5B FC EF 40
D6 2F CF CF 9A 66 1D 92 7D A8 8D 9B B0 E2 62 DE 3E CF CF DB 6F 67 CB
D9 9B 3A 3B 27 DE 64 4C 9F D0 9C 0D 7D E7 53 B1 2E A6 67 8B 55 4E 5C
52 BE 5E E5 F9 AC 5A E4 6D 5E 1B 10 9B 1B 58 38 32 34 A2 F5 BB 32 6F
8E F6 1E DF 0D 3F E8 B5 FB EE 3C CF CB E6 68 DF 35 D4 4F 7A 2D 5F 56
57 79 9D CF 7A 80 83 CF ED 5B 0C 65 92 35 44 C4 07 7B 0F 1E DF 75 7F
BB F9 CE 97 17 ED FC 68 FF FE 3D CC B1 FC E1 DE 2F 66 F4 E7 EE C1 03
9A 3A F9 DD 7E F5 ED 1C D4 3C DA BD 7F EF E1 E3 BB FA 87 A3 63 D6 34
C2 27 46 1F BD 5A 2F 97 A4 B6 BE AC 67 34 E5 BB 07 F7 69 2E 6F 68 E4
F8 22 9F CE 97 2F F3 7A F1 45 F6 EE 79 46 0A 07 2F 1E ED ED 7D 4A 6A
28 FE 5D F4 55 7C 43 0A 67 52 2C 45 2F EE 3D E8 02 E8 B6 B0 60 5E D6
C5 22 83 D8 96 90 00'

T→C: '00 B0 03 00 00'
C→T: 'D5 5A 66 9A E8 D1 FF B0 37 59 4F AB AA 0E 66 55 3E B0 ED 4E AA
E5 79 71 B1 AE 55 AE E4 DB BD E7 A3 BD 57 8F EF 46 BF 73 3D 10 B0 D7
39 7D B7 BC 78 59 35 05 DA 34 47 34 9C E8 E7 F6 AD B3 65 9B 2F 67 F9
EC A4 5A 2F DB FA FA CB F3 57 F9 45 D1 B4 82 FD 8B E7 8F EF 6E 6C D0
55 99 64 47 8E C8 26 59 AD 89 BF 6D 9B 67 EB DC 69 E8 2F 1E DF 0D FE
76 06 A2 B8 C0 84 1F AF 49 35 D5 45 7B FD 26 9B 94 EE EB 48 83 D0 68
09 29 B2 05 A9 01 34 24 A6 F9 A2 98 CE F3 32 FD C9 E3 E7 A7 6F 88 1A
FE 57 C1 4B 86 38 F6 5B 1A 03 99 85 2B A2 F2 2C 2F 8B 9F 7E 9B A7 AF
AF 97 ED 3C 6F F2 F4 65 5D 5D D4 D9 62 91 37 F4 AB AA FD 94 30 AA 16
D5 A4 20 71 4B 4F 8A B6 AE F2 25 B1 44 17 6A D8 67 99 4D 15 1D 52 E4
75 7E F4 92 6C D1 4F 37 F4 5A F7 8B E0 35 51 73 EE 4B 5F 1D 76 BF F3
28 77 77 90 74 90 00'

T→C: '00 B0 04 00 00'
C→T: '3F F6 FE 64 FD FC F4 F4 C5 E9 8B F4 F9 E9 97 1F 48 D4 6F 13 D1
CA EA 82 18 34 7F 5A E4 CB A6 7D 6F A2 3D A9 D7 4D 93 97 5F 83 6A 7B
A0 DA CE 83 AF 49 B5 81 EF 43 8E 25 C5 F7 36 EF 31 31 3E 8C 50 18 1F
1F 59 DE E1 BF 7C 4C FA 6F C9 67 9D 1E 49 61 2D F2 7A 4A D6 08 13 D3
EB 3B FC 3A 82 45 D8 E0 E8 E9 EB FB D0 3D C1 67 3E 56 9B E0 75 BF ED
60 CA 4E 1F 14 D4 17 D9 72 7D 9E 4D 89 F6 44 C9 BE C8 47 9B F5 31 4F
1F 1F CF 66 75 DE 34 5D 08 FE 77 91 D7 FC 37 8D 42 7A F9 9A 54 54 F7
C3 DE 5B 4C 8C 40 F0 CF DE BC FA F2 F4 85 C8 C4 60 2F CF 8B 65 BE 7B
F4 E9 28 AD D7 79 FA AC 5E 4F DB 62 56 D5 B6 3F F9 7A D3 CB 7B 47 0F
EE EF EC 3E 08 DE D8 EB BF A1 02 F1 2A 6F 0A 32 84 53 D1 2F 4E BD B8
CF F1 E6 8F E9 4B 9E A6 37 5F 3F 23 A1 9D E6 98 CC DE 57 1D 22 1B 84
22 6C 65 A9 D9 90 00'

T→C: '00 B0 05 00 00'
C→T: '9D DE BB B7 99 DF A1 56 3E 34 8E 69 AE AA FA AD 7C 98 A6 F6 65
F3 45 94 DB 67 F9 B3 AA 36 2D 8E 8E 9F 61 9C E1 67 DE 0B 8F EF C6 61
B9 CF 3B 3C 0E FF AB 37 64 7C 18 C1 05 1F AB 0F 4C EE 84 F7 57 D0 CA
73 EC 28 CC 3B FA 7D A0 30 83 4F 7A 30 C9 B3 9D BE 25 C7 EC 60 4F A0
CA DF BD 66 AF 57 D9 94 48 AA 9E A1 FF 49 D0 94 1D 24 8A EF CA F2 5A
```

RDW

```
DC A4 A6 41 DB A3 5D F2 ED D5 7D 8A 7C EB 8D FE CD 75 9D 3B B2 58 C0
3E 95 4D 93 01 69 C5 D7 AF 8B 1F 90 12 BF 77 FF EE FE FD F4 D5 EE 01
22 01 FD B0 D7 FC 79 95 CD 4E 32 8C A5 BD 26 02 E5 EF 5E D3 A0 CA 9C
7D DF A3 87 F7 10 C9 6C 68 D0 03 C7 4E BE 89 DC 5E 5F 2F 26 55 79 F4
93 C4 A0 91 8F 7B EF BE 2A 16 C0 F1 6C 39 2D D7 88 DA BF 3C 27 EF AC
3D 3A 18 EF EC BC DB 3D 48 B7 F2 CF F6 1E DC 41 60 12 6D 16 0A D4 30
91 DE 8F 7E 3B 90 00'

T→C: '00 B0 06 00 00'
C→T: '44 BF 87 FF 5F A7 DF 7D A2 DF 43 A6 DF C3 DB D1 6F 23 01 DF 83
82 7B F7 EF DE 07 05 1F FC 7F 9B 82 0F 98 82 0F 84 03 D3 6A 9D E6 DF
04 21 DD 57 1B 84 FD 6E EC D5 5B E8 48 D5 66 DF A8 8E FC 74 E7 E1 A0
8E 1C 54 7C BB 0F 6F A5 F8 BA 9A EF 47 0A EF 47 0A EF EB D3 EF 47 0A
EF C3 28 F8 7E 0A CF 57 58 7D 4A A6 81 42 EB AB BD 90 8D 03 2A AB B6
09 9D C6 D3 E5 05 79 F4 3D B7 51 3E 8E 06 8E C6 25 46 4E 89 12 68 D2
F2 C8 86 23 43 0D 02 28 F2 19 9C DF E3 E6 8B AC 7E 9B CF BE 5C BA A6
AF BE BD 43 0A 77 73 9B 00 DC 77 C9 19 26 02 52 56 6C 39 2D 56 A5 E6
EC 29 F7 15 FD 22 54 DF 84 E7 69 99 4F 39 B5 4A 4B 19 94 67 AE EA 23
1A 47 FC 8B E0 DD 6F 5F 4F EA 62 E6 BE FC 0E 25 23 3B 1F 05 ED 4D 26
EE E4 BA 2C 88 0F C3 F4 9C FB 30 34 18 35 45 44 17 F9 82 96 3A BC 36
3C 8E E7 67 34 90 00'

T→C: '00 B0 07 00 00'
C→T: 'A3 C3 5F C7 08 AE 52 70 B4 FB F0 E1 03 4B 61 F3 A1 6F 24 38 65
D6 33 1D F8 74 40 68 F1 15 77 BB B7 23 09 B7 78 18 4B 99 CE 62 B1 5E
BC C8 5B B6 92 F0 E4 C7 F0 E5 BB 9F F7 5E 14 5C 59 0A BB 6D EF 1D DC
DF 31 83 89 36 18 C2 82 1B 1F ED ED EE DA FE E5 93 B0 75 5F 43 50 6C
3A 7B 9E 5F E6 25 D6 31 28 7B 44 99 58 8A 92 49 47 C4 BE B8 E1 75 0F
ED A3 BD 83 83 83 2E 14 FF FB 0D A0 9E D6 C5 65 FE 84 D0 D8 1F 1F EC
F8 30 CC 17 7D 82 BE 9B 67 EB A6 3D 5D 14 0D 92 8A DC F8 74 5D 57 47
F8 27 A5 D1 0C 36 E8 81 7A 51 3F A1 B4 3E A5 6B D7 E5 F1 B4 7D 9E 35
ED 31 31 E4 EC 8B AA A5 EC FA D1 83 DD FB 77 B1 16 F3 AD 4F 1F EE E1
97 83 63 A4 8A 37 BD C1 1D 98 24 C1 EB 45 F5 96 E4 B6 AE 49 14 C9 A9
9A 34 55 BD 92 55 BB FC FC FC 68 67 7C 9F 66 6F 73 9B 1E BE 5F D5 93
8C BE 23 21 E5 90 00'

T→C: '00 B0 08 00 00'
C→T: '1C F5 C9 97 7B E4 58 11 D5 22 9F DF F4 AE 70 FA B2 59 2F B8 C3
A3 FD F1 5E 1F 50 B7 51 64 2E DA 3A 8B 61 B5 C3 F3 10 FF F2 56 50 4C
D7 84 18 C4 6C 63 93 1E 40 59 8F 20 B3 C7 A8 3C E0 14 9B FD 60 B0 75
9F 24 A0 ED D0 B7 1D 30 E4 F9 36 2D 2D B1 4D F3 19 E9 5F A4 C3 76 E3
0A C7 6B CA AD 4E BE 24 5E D8 7D F8 00 EB 74 9D CF 6F 7A F5 C5 97 EF
F0 EE BD FB 92 54 E8 7C 73 D3 DB DF 3E F9 FD 15 C0 FD FD BD 2E 00 FD
F2 26 18 94 2C 6B 8B E9 9A 57 44 8F A0 10 77 0E EE 75 20 05 4D 7A B4
B7 6D 6F 20 9B A8 E6 D8 57 BA 4A 62 55 BE F9 34 E2 08 98 0F 83 C6 EF
ED 48 C4 6D F6 E9 B0 CD FE 31 40 53 83 2C 50 9D 99 A5 A8 6B E8 AB 1B
AD 9A FD 66 C0 B2 A9 69 20 A6 A5 95 AD 75 B5 6E 5E D1 1C CC C4 B2 84
D6 2B DA A4 6B 3F BE 91 29 88 CF 01 D6 90 A7 F3 8C 43 43 4A A0 AE C8
1B E8 A7 B8 FB 90 00'

T→C: '00 B0 09 00 00'
```

RDW

```
C→T: '4D 62 31 0E 35 D2 85 C9 37 D5 15 AF 4D 92 87 71 FC 8E 42 D5 A2
3C 3A 10 41 D9 D4 E4 06 68 5F 2D 27 35 37 24 02 A9 D8 6D 6A 32 04 0D
06 92 D6 79 5A 59 3C A5 D1 BC 6C D9 10 DF D0 C4 82 C3 9A FA 66 6A C4
5A 84 7C 4F 9A 6D 4A 8B 3A 99 7B 4F 12 B4 F4 2B D6 34 67 C5 65 31 5B
67 A5 5D 67 3E AF EA 85 2C F1 FE 3F 01 00 00 FF FF 4A 5E B2 FC 63 23
00 00 90 00'
```

# App 4 SPECIMEN CSCA CERTIFICATE

```
-----BEGIN CERTIFICATE-----
MIIGHjCCBAagAwIBAgIRAKx4L8nRF1m12piT8OIPZ+UwDQYJKoZIhvcNAQELBQAw
ZjEZMBcGA1UEAxMQQ1NDQSBHQVQgTkwgZVZSRDELMAkGA1UEBRMCMDExDDAKBgNV
BAsTA1JEVzEhMB8GA1UEChMYU3RhdGUgb2YgdGhlIE51dGhlcmxhbmRzMQswCQYD
VQQGEwJOTDAeFw0xMzAzMTQwODQ5NDlaFw0zMzAzMTQwODQ5NTBaMGYxGTAXBgNV
BAMTEENTQ0EgR0FUIE5MIGVWUkQxCzAJBgNVBAUTAjAxMQwwCgYDVQQLEwNSRFcx
ITAfBgNVBAoTGFN0YXRlIG9mIHRoZSBOZXRoZXJsYW5kczELMAkGA1UEBhMCTkww
ggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDEVBXMMSULG/KPwuoBHrGi
tqCyRn/DEmt+Wa40TuwCJ4IXB7IAP6hwUA74uKx8V80eIYlIrvCTcU93r4o0l7jB
3kFVGYxfF05BBpZM0+DpJOdEsVdkaHqMULcLu06JBzPEvqG1hUbQhUIXm0w9Dloz
kKQG1MONvYi9aUVHgWPZmyfWIIGhLqiPXa72EXt6FV1u4eMZKoW7yVW3/9tFk7KO
E5/aFW1kOkn0PvmZbpkQMjMAQCfNJ3v9kdsWJvIVlZrccKsxB4jilM5h3UV4oCPX
lBop6ik71XoB9XChQkZw9sHquzbrfRc4OI5wxOLcuDkaA8w7AKTuLYibgni0M95f
Q4nIaSwrmT/8suNddOOWQBGPyf8WrYq9p/VMtB87l8x9iE59IRPAzjk/SkjHKy6x
rt3vD41O4j23AM/1uxuVV+DnwBll6rkm0AUwsnqYAcop7M4+Fr8VDdKaXrypo4+X
DNypKgyfsac9wsd9HdvvT+3alTkftGsXil93S2wLThBgEU6VhChuhSeMwxhR64T4
YO3CZrgGg8bXTEJG6np+8r7R+MIgLbKcK0jtc7vZ3Aol25G+CxP82QfP+ocICMHy
7oq6tfOdS8kCfI3p9+VtLyfFRAWzD3f3yWj8odeWVgIQpKQincmh/kmHAPGEAsT8
V7Ptodm52qNcnXkzkFrcZQIDAQABo4HGMIHDMBcGA1UdIAQQMA4wDAYKYIQQAYdy
AgEDATBEBgNVHR8EPTA7MDmgN6A1hjNodHRwOi8vd3d3LWRpZW5zdGVuLnJkdy5u
bC9jcmwvQ1NDQUdBVE5MZVZSRC0wMS5jcmwwDgYDVR0PAQH/BAQDAgEGMBIGA1Ud
EwEB/wQIMAYBAf8CAQAwHQYDVR0OBBYEFJJRh72N59+/MjxmaSl/2uuKtKu0MB8G
A1UdIwQYMBaAFJJRh72N59+/MjxmaSl/2uuKtKu0MA0GCSqGSIb3DQEBCwUAA4IC
AQBSzTXBto0qCrP0WsKNyuVorNv4M102sEoVh5OlEN5/XgjI3yTcaitrxYr78YWH
rdkE0gw8dT126eOHeeAig2hrwLRXwmh9/nMGcB1LIyw60IfF1UBhD1dO0UVH3FfS
0AYHbuwPdKfpxvZZN8xlA0p00ZgNELLTY0v5UHX/L3D5hyJnibhECRn1fsaIt/fh
DRWDZNU8SIuD4SLliDqAPAGEPlyLp+/kx7WE/eMagZAXlGSXggwhM8fFAH+F/pYn
czYP/VkxQo8BZqCGP9Km7CQQNx4Tx6tLHFma9YsYWBwuvkk4yOsSswXcSHUhD4oG
6fzFPqr1LICX8N9yFMQjc/ERb3/Y0oiFrJDQ3embQdwygYzVvH7MuwBZcu4kh5PI
AP6wu3tnnym7bNqQoRKBceMEnYgupw4Vdyp0Jm8KONJbwUAJPcKIAZwLlcn0vQE1
5uNpkeRzX8EzzYFuBD5htdhGP4VIeSr6vFiTrRtW+/+EAVfcM1Z4BzvHvalF8Akf
W/YYbW9Pp6o2ziKlXQIgxPjG6g7l9FZF/BEvqqHO+EhG60wdmflFR8n0Uui172H7
6A3HUH/lU9dG5As0c38KkxPyNfQ59ixB26rO8hxhh0GV6wpWWO6WzzU6rfesvccr
SmoCIT5eP5V7MYr0AR9ve9XYb8A2UxBZkGQ8YNdmHaCaDw==
-----END CERTIFICATE-----
```