RDW

DA12 - Kentekencard Uitleesdocumentatie

Interface specificatie

Auteur	RDW
Versie	2.1.1
Datum	30-12-2013
Status	Definitief
Classificatie	-

Documentgegevens

Opdrachtgever	RDW
Document titel	DA12 - Kentekencard Uitleesdocumentatie, Interface specificatie
Bestandsnaam	DA12 - Kentekencard Uitleesdocumentatie v2 1 1.docx
Archief naam	
Trefwoorden	
Status	Definitief
Verspreiding	

RDW
Rozenburglaan 5
9727 DL Groningen

Versieoverzicht

Versie	Datum	Status	Auteur
2.1.1	30-12-2013	Definitief	RDW

Wijzigingshistorie

Versie	Datum	Reden wijziging

INHOUDSOPGAVE

MANAGEMENTSAMENVATTING 1

1 INLEIDING 2

1.1 SCOPE 2
1.2 LEZERSDOELGROEP 2
1.3 DOCUMENTOPBOUW 2

2 BEGRIPPENLIJST EN REFERENTIES 4

2.1 BEGRIPPENLIJST 4
2.2 REFERENTIES 5

3 ACHTERGRONDINFORMATIE 6

3.1 HANDTEKENINGEN OP DE NEDERLANDSE KENTEKENCARD CHIP 6
3.2 PUBLIC KEY INFRASTRUCTUUR 6
3.3 VERIFICATIE VAN DATAGROEPEN A EN B CONFORM 2003/127/EC 9
3.4 PASSIVE AUTHENTICATION 10
3.5 ACTIVE AUTHENTICATION 11

4 VERIFICATIEPROCES 12

4.1 PROCESSTROOM 12
4.2 LEZEN EN VERIFIËREN VAN DE NEDERLANDSE KENTEKENCARD CHIP 14
4.3 LEZEN EN VERIFIËREN VAN BUITENLANDSE KENTEKENCARD CHIPS 23

5 COMMUNICATIE TUSSEN KAART EN UITLEES- EN VERIFICATIESOFTWARE 33

6 INFORMATIEUITWISSELING MET VERIFICATIESOFTWARE 34

APP 1 LOGICAL DATA STRUCTURE 35

APP 1.1 OVERZICHT VAN ELEMENTARY FILES 35

APP 1.2 EF.AA 35

APP 1.3 EF.SOD 36

APP 1.4 EF.C.IA_A.DS 41

APP 1.5 EF.C.IA_B.DS 41

APP 1.6 EF.REGISTRATION_A 42
APP 1.7 EF.REGISTRATION_B 44
APP 1.8 EF.REGISTRATION_C 46
APP 1.8.1 REGISTRATIEDATA 46
APP 1.8.2 INDIVIDUAL VEHICLE INFORMATION 46
APP 1.8.2.1 INDIVIDUALVEHICLEINFORMATION (XML) 47
APP 1.8.2.2 INDIVIDUALVEHICLEINFORMATION (COMPRESSED XML) 47
APP 1.8.2.3 INDIVIDUALVEHICLEINFORMATION (TLV) 48
APP 1.9 EF.SIGNATURE_A 68
APP 1.10 EF.SIGNATURE_B 68
APP 2 NL-EVRD COMMANDO'S EN RESPONSES 69
APP 2.1 SELECT APPLICATION 69
APP 2.1.1 COMMAND APDU 69
APP 2.1.2 RESPONSE APDU 69
APP 2.1.3 STATUS WORDS 69
APP 2.2 SELECT FILE 70
APP 2.2.1 COMMAND APDU 70
APP 2.2.2 RESPONSE APDU 70
APP 2.2.3 STATUS WORDS 71
APP 2.3 READ BINARY 71
APP 2.3.1 COMMAND APDU 71
APP 2.3.2 RESPONSE APDU 71
APP 2.3.3 STATUS WORDS 72
APP 2.4 INTERNAL AUTHENTICATE 72

APP 2.4.1 COMMAND APDU 72

APP 2.4.2 RESPONSE APDU 72

APP 2.4.3 STATUS WORDS 73

APP 2.5 STATUS WORDS SUMMARY 73

APP 3 TRACES COMMUNICATIE UITLEES/VERIFICATIESW & CHIP (INFORMATIEF) 75

APP 3.1 LEZEN EN VERIFIEREN VAN DE NEDERLANDSE KENTEKENCARD CHIP 75

APP 3.2 LEZEN EN VERIFIEREN VAN BUITENLANDSE KENTEKENCARD CHIPS 82

APP 4 SPECIMEN CSCA CERTIFICAAT 90

MANAGEMENTSAMENVATTING

De Nederlandse kentekencard (NL-eVRD) is voorzien van een chip. Dit document beschrijft hoe de chip van de Nederlandse kentekencard kan worden uitgelezen en geverifiëerd. Het uitlezen van de chip kan onbeveiligd en daardoor door alle partijen gedaan worden. Hiervoor is slechts een PC/SC kaartlezer en uitleessoftware nodig. Voor verificatie is een betrouwbaar verkregen PKI certificaat en de bijbehorende Certificate Revocation List (CRL) nodig. Deze gegevens kunnen van de website van RDW gedownload worden.

De Nederlandse kentekencard voldoet aan de Europese richtlijn 2003/123/EC [1]. De chip bevat de data zoals gespecificeerd in de richtlijn en beveiligd zoals beschreven in de richtlijn. Ook bevat de chip in de Nederlandse kentekencard additionele registratiedata en kan deze Certificaat van Oorsprong (CVO) data bevatten. De chip van de Nederlandse kentekencard is daarnaast voorzien van twee additionele beveiligingsmechanismen. Alle data op de kentekencard chip is beveiligd door middel van Passive Authentication (PA) [2]. Dit houdt in dat over alle data op de chip een elektronische handtekening is gezet door de uitgevende instantie, RDW, die ervoor zorgt dat gecontroleerd kan worden dat de data in de verschillende datagroepen ongewijzigd is en bij elkaar hoort. Daarnaast kan de echtheid van de chip gecontroleerd worden door middel van Active Authentication (AA) [2]. Dit betekent dat de chip zijn echtheid kan aantonen door middel van een challenge-response protocol.

Dit document beschrijft hoe de Nederlandse kentekencard chip hoort te worden uitgelezen en geverifiëerd. Het document gaat ook in op het uitlezen en verifiëren van buitenlandse kentekencard chips die voldoen aan [1]. Aangezien Nederlandse kentekencards ook aan deze richtlijn voldoen, zouden die ook op deze manier uitgelezen en geverifiëerd kunnen worden. Er wordt dan echter geen gebruik gemaakt van de additionele beveiligingsmechanismen die in de Nederlandse kentekencard chip zijn geïmplementeerd, waardoor dit niet aan te raden is.

1 INLEIDING

1.1 Scope

De Nederlandse kentekencard (NL-eVRD) is voorzien van een chip. Dit document beschrijft hoe de chip van de Nederlandse kentekencard kan worden uitgelezen en geverifiëerd. Het uitlezen van de chip kan onbeveiligd en daardoor door alle partijen gedaan worden. Hiervoor is slechts een PC/SC kaartlezer en uitleessoftware nodig. Voor verificatie is een betrouwbaar verkregen PKI certificaat en de bijbehorende Certificate Revocation List (CRL) nodig. Deze gegevens kunnen van de website van RDW gedownload worden. Het is daarmee echter niet 100 % zeker dat dit het authentieke certificaat is. Daarvoor is vereist dat het initiële certificaat op een betrouwbare manier wordt uitgewisseld. RDW zal hiervoor een proces opzetten met erkende partijen die in staat moeten zijn de chip van de Nederlandse kentekencard te verifiëren, de zogenaamde erkende relying parties.

De Nederlandse kentekencard voldoet aan de Europese richtlijn 2003/123/EC [1]. De chip bevat de data zoals gespecificeerd in de richtlijn en beveiligd zoals beschreven in de richtlijn. Ook bevat de chip in de Nederlandse kentekencard additionele registratiedata en kan deze Certificaat van Oorsprong (CVO) data bevatten. De chip van de Nederlandse kentekencard is daarnaast voorzien van twee additionele beveiligingsmechanismen. Alle data op de kentekencard chip is beveiligd door middel van Passive Authentication (PA) [2]. Dit houdt in dat over alle data op de chip een elektronische handtekening is gezet door de uitgevende instantie, RDW, die ervoor zorgt dat gecontroleerd kan worden dat de data in de verschillende datagroepen ongewijzigd is en bij elkaar hoort. Daarnaast kan de echtheid van de chip gecontroleerd worden door middel van Active Authentication (AA) [2]. Dit betekent dat de chip zijn echtheid kan aantonen door middel van een challenge-response protocol.

Dit document beschrijft hoe de Nederlandse kentekencard chip hoort te worden uitgelezen en geverifiëerd. Het document gaat ook in op het uitlezen en verifiëren van buitenlandse kentekencard chips die voldoen aan [1]. Aangezien Nederlandse kentekencards ook aan deze richtlijn voldoen, zouden die ook op deze manier uitgelezen en geverifiëerd kunnen worden. Er wordt dan echter geen gebruik gemaakt van de additionele beveiligingsmechanismen die in de Nederlandse kentekencard chip zijn geïmplementeerd, waardoor dit niet aan te raden is.

1.2 Lezersdoelgroep

Dit document is bedoeld voor alle partijen die de chip van de kentekencard willen uitlezen en verifiëren. Het document bevat de benodigde informatie voor het implementeren van de uitlees- en verificatiesoftware. Uitlees- en verificatiesoftware kan door een partij zelf ontwikkeld worden, maar is voor erkende relying parties ook verkrijgbaar via RDW. Daarnaast bevat het document informatie over hoe de uitlees- en verificatiesoftware voorzien kan worden van de benodigde PKI certificaten en CRLs.

Er wordt van uitgegaan dat de lezers bekend zijn met asymmetrische cryptografie en public key infrastructuren.

1.3 Documentopbouw

Hoofdstuk 1 bevat de scope, lezersdoelgroep en documentopbouw. In Hoofdstuk 2 staat een uitleg van begrippen en referenties. Hoofdstuk 3 bevat achtergrondinformatie over de kentekencard chip, de

public key infrastructuur, en de beveiligingsmechanismen. In Hoofdstuk 4 staat in detail uitgewerkt hoe het uitlees- en verificatieproces dient plaats te vinden. Paragraaf 4.1 geeft de processtroom op hoog niveau, paragraaf 4.2 geeft stap voor stap aan hoe een Nederlandse kentekencard chip uitgelezen en geverifieerd dient te worden en in paragraaf 4.3 staat dit voor (buitenlandse) kentekencardchips die voldoen aan de Europese richtlijn 2003/127/EC [1]. In Hoofstuk 5 is informatie te vinden over de communicatie tussen de kentekencard chip en de uitlees- en verificatiesoftware. Hoofdstuk 6 gaat in op de informatieuitwisseling met de uitlees- en verificatiesoftware. Het gaat hierbij niet om de informatieuitwisseling met de chip, maar met andere bronnen, zoals de RDW.

In de appendices is de volgende informatie opgenomen:

- App 1 bevat de Logical Data Structure van de chip,
- App 2 bevat de APDUs voor de Nederlandse kentekencard chip in de operationele fase.
- App 3 geeft als voorbeeld een trace van de communicatie tussen uitlees- en verificatiesoftware en de chip van een Nederlandse kentekencard en een mogelijke buitenlandse kentekencard.
- App 4 bevat het CSCA certificaat dat is gebruikt voor de specimen kentkencard

2 BEGRIPPENLIJST EN REFERENTIES

2.1 Begrippenlijst

Begrip	Verklaring
AA	Active Authentication, cryptografisch mechanisme om de authenticiteit van de chip aan te tonen via een AA public-private key pair en een challenge-response mechanisme.
Challenge	(Deels) random getal dat gegenereerd wordt om door een andere entiteit ondertekend te worden met de private key van die entiteit en op die manier gebruikt wordt voor controle van de authenticiteit van die entiteit.
CSCA	Country Signing Certificate Authority, de hoogste certificaat uitgevende entiteit van de uitgevende instantie RDW in de PKI keten voor het ondertekenen van data.
CSCA private key	De geheime sleutel van het CSCA key pair die uitsluitend beschikbaar is in de CSCA en gebruikt wordt voor het ondertekenen van certificaten.
CSCA public key	De publieke sleutel van het CSCA key pair die gebruikt kan worden voor controle van met de CSCA private key ondertekende certificaten en CRLs.
CSCA root certificaat	Een door de CSCA uitgegeven certificaat met daarin de eigen CSCA public key. Het certificaat koppelt de publieke sleutel aan de CSCA en heeft een beperkte geldigheidstermijn. Het CSCA root certificaat is ondertekend door de CSCA private key behorend bij de CSCA public key in het certificaat. Het certificaat (de handtekening) kan gecontroleerd worden met de publieke sleutel uit het certificaat zelf. Het CSCA root certificaat is beschikbaar op de RDW website, maar erkende relying parties met een officiële verantwoordelijkheid voor het controleren van kentekencards (zoals de Nederlandse en buitenlandse politie) moeten het certificaat daarnaast verkrijgen op een betrouwbare manier via een separaat proces aangezien de website voor deze partijen niet voldoende zekerheid geeft over de authenticiteit van het initiële CSCA certificaat.
CSCA link certificaat	Een door de CSCA uitgegeven certificaat met daarin een nieuwe CSCA public key. Het certificaat is ondertekend met de huidige CSCA private key en kan gecontroleerd worden met de huidige CSCA public key. Hierdoor kan een CSCA link certificaat uitgewisseld worden via een onbetrouwbaar kanaal zoals publicatie op de RDW website. Het certificaat koppelt het nieuwe trust point aan het huidige trust point.
CRL	Certificate Revocation List, een lijst met ingetrokken certificaten uitgegeven door de CSCA. De CSCA ondertekent de CRL zodat de authenticiteit van de CRL gecontroleerd kan worden. De CRL is beschikbaar op de RDW website en wordt periodiek vernieuwd. Ook wordt een nieuwe versie gepubliceerd als een certificaat aan de CRL wordt toegevoegd. Voor ieder CSCA sleutelpaar wordt een aparte CRL uitgegeven.
DS	Document Signer, een entiteit binnen RDW die de data die op een kentekencard chip geplaatst wordt, voorziet van een elektronische handtekening. De DS beschikt hiervoor over een key pair en een door de CSCA uitgegeven DS certificaat.
DS private key	De geheime sleutel van het DS key pair die uitsluitend beschikbaar is in de DS en gebruikt wordt voor het ondertekenen van de kentekencard chip data.
DS public key	De publieke sleutel van het DS key pair die gebruikt kan worden voor controle van met de DS private key ondertekende data. Deze DS public key is beschikbaar in het door de CSCA uitgegeven DS certificaat.
DS certificaat	Een door de CSCA uitgegeven certificaat met daarin de DS public key. Het DS certificaat is ondertekend door de CSCA private key en kan gecontroleerd worden

	met de bijbhorende CSCA public key waarover de verificatiesoftware dient te beschikken. Het DS certificaat is beschikbaar op de chip.Het DS certificaat heeft een beperkte geldigheidsduur.
Hash	Uniek getal dat berekend wordt met behulp van een hash of digest algoritme over data, meestal om vervolgens getekend te worden met een private key. Als de data verandert, verandert ook de hash. Uit de hash is niet de oorspronkelijke data te herleiden. RDW maakt gebruik van het SHA256 hash algoritme.
Key Pair	Aan elkaar gekoppelde public en private keys gebruikt in asymmetrische cryptografische algoritmen zoals gebruikt voor het tekenen van hashes en challenges.
NL-eVRD	Nederlandse elektronische kentekencard (vehicle registration document).
PA	Passive Authentication, cryptografisch mechanisme om de authenticiteit van de chip data aan te tonen via een handtekening over die data met de DS private key.

2.2 Referenties

Ref.	Titel	Auteur	Versie	Datum
[1]	2003/127/EU	Europese Commissie	n.v.t.	23-12-2003
[2]	ISO/IEC 18013-3	ISO/IEC WG 10	n.v.t.	2009
[3]	ICAO Doc 9303	ICAO	6	2006
[4]	RFC 5280	D. Cooper *et. al.*	n.v.t.	mei 2008
[5]	CP/CPS NL-eVRD-PKI, zie: http://www.rdw.nl/	RDW	2.0	30-12-2013
[6]	RFC 5652	R. Housley	n.v.t.	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.v.t.	juni 2005
[10]	ISO 9796-2	ISO	2	01-10-2002

3 ACHTERGRONDINFORMATIE

De Europese Richtlijn 2003/127/EU [1] staat uitgifte van kentekenbewijzen op credit card formaat toe voorzien van een contact chip. Zowel de kentekencard als de chip dienen daarbij te voldoen aan de eisen vastgelegd in Annex 1 en 2 van [1]. De richtlijn schrijft onder andere de datastructuur van de chip voor en de aanwezigheid van files die de authenticiteit van de data garanderen en controleerbaar maken. De Nederlandse kentekencards voldoen hieraan. Daarnaast zijn de chips van de Nederlandse kentekencards voorzien van twee additionele beveiligingsmechanismen met bijbehorende datagroepen op de chip om de echtheid van de chip en alle data op de chip te garanderen. De op de Nederlandse kentekencard aanwezige datagroepen zijn beschreven in App 1.

De echtheid van de chip van een Nederlandse kentekencard kan door een relying party gecontroleerd worden door gebruik te maken van het Active Authentication (AA) beveiligingsmechansime. Dit mechanisme is afhankelijk van het andere beveiligingsmechansime dat is toegevoegd aan de chip van de Nederlandse kentekencard en dat tevens de echtheid van alle data op de chip en het bij elkaar horen van de datagroepen garandeert, namelijk Passive Auhthentication (PA). Zowel AA als PA zijn geïmplementeerd conform de internationale ISO/IEC rijbewijs standaard [2]. Daarnaast worden deze beveiligingsmechanismen ook gebruikt voor het beveiligen van paspoorten, zoals vastgelegd in ICAO Doc 9303 [3] en voor het beveiligen van Europese verblijfsvergunningen en Nederlandse en sommige buitenlandse identiteitskaarten.

De beveiligingsmechanismen worden in dit hoofdstuk nader uitgelegd, zodat partijen die op basis van dit document verificatiesoftware maken in staat zijn de controle van de beveiligingsmechanismen op de juiste manier te implementeren. Een gedetailleerde beschrijving van de door de verificatiesoftware uit te voeren stappen en controles is te vinden in Hoofdstuk 4, paragraaf 4.2. In dit hoofdstuk, in paragraaf 3.2, wordt daarnaast ingegaan op de PKI structuur die gebruikt wordt.

3.1 Handtekeningen op de Nederlandse kentekencard chip

Op een Nederlandse kentekencard chip zijn drie elektronische handtekeningen aanwezig om de authenticiteit van de data op de chip te garanderen en verifiëren. Twee van deze handtekeningen zijn verplicht conform de Europese richtlijn [1]. De derde handtekening is door Nederland toegevoegd om PA en AA mogelijk te maken. De aanwezige handtekeningen zijn:

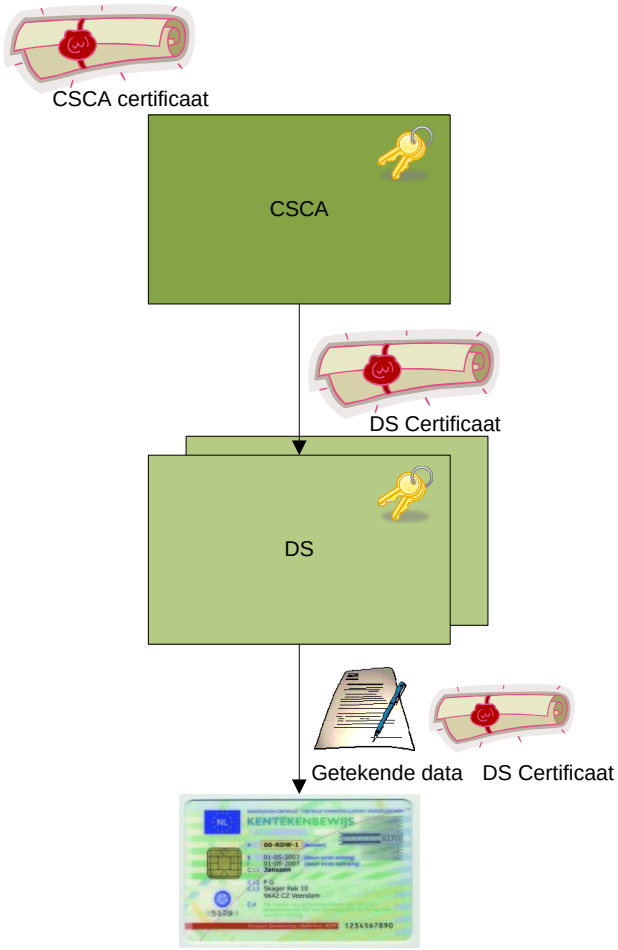
- de handtekening in EF.Signature_A over de data in EF.Registration_A;
- de handtekening in EF.Signature_B over de data in EF.Registration_B;
- de handtekening in EF.SOd over alle datagroepen op de chip.

Nederlandse kentekencards worden uitgegeven door RDW. RDW heeft ervoor gekozen alle handtekeningen voor één kentekencard te genereren met dezelfde DS private key en daardoor verifieerbaar te maken met hetzelfde public key certificaat. Dit public key certificaat, het DS certificaat, is beschikbaar op de chip en staat om te voldoen aan de Europese richtlijn [1]en de ISO/IEC 18013 [2] standaard 3 x op de chip, namelijk in EF.C.IA_A.DS, EF.C.IA_B.DS en in de EF.SOd.

3.2 Public Key Infrastructuur

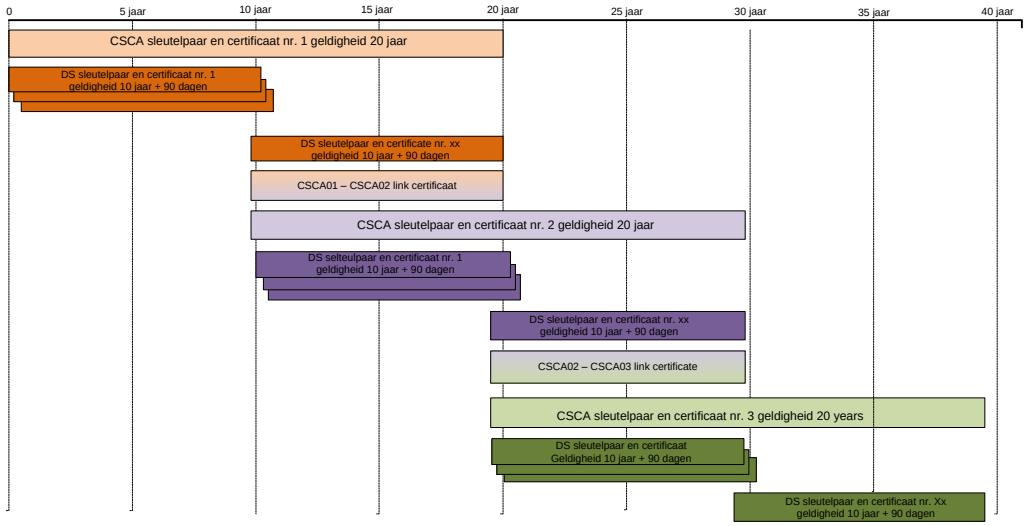
Voor generatie van de handtekeningen en benodigde certificaten heeft RDW een PKI opgezet met een Country Signing Certification Authority (CSCA) als hoogste trust point (root). De CSCA geeft certificaten

uit aan Document Signers (DS) die de handtekeningen over de datagroepen voor op de kaart genereren. Dit is weergegeve in Figuur 1.



Figuur 1: Public Key Infrastructuur voor kentekencards

De CSCA beschikt over een key pair en bijbehorend (self-signed) CSCA root certificaat. Een CSCA root certificaat heeft een geldigheidsduur van 20 jaar. Het wordt gedurende 10 jaar gebruikt voor het uitgeven van DS certificaten. Kort daarvoor wordt een nieuw key pair en bijbehorend CSCA root certificaat gegenereerd. Ook wordt dan een CSCA link certificaat gegenereerd. Dit certificaat bevat de nieuwe public key en is ondertekend met de huidige private key. Het kan daardoor met de huidige public key gecontroleerd worden op authenticiteit. Dit is weergegeven in Figuur 2.



Figuur 2: Relatie tussen CSCA root certificaten, CSCA link certificaten en DS certificaten

Relying parties hebben het CSCA certificaat nodig voor het controleren van de DS certificaten. Daarom stelt RDW de CSCA certificaten beschikbaar op haar website. Erkende relying parties met een officiële verantwoordelijkheid voor het controleren van kentekencards (zoals de Nederlandse en buitenlandse politie) moeten het certificaat daarnaast verkrijgen op een betrouwbare manier via een separaat proces aangezien de website voor deze partijen niet voldoende zekerheid geeft over de authenticiteit van het initiële CSCA certificaat. Nieuwe CSCA certificaten kunnen vervolgens van de website gedownload worden aangezien via het link certificaat de authenticiteit van de nieuwe public key gecontroleerd kan worden.

Een DS beschikt over een key pair. Met de private key van het key pair genereert de DS de handtekeningen over de datagroepen. De bijbehorende public key is beschikbaar in het DS certificaat dat door de CSCA is uitgegeven. Een DS certificaat heeft een geldigheidstermijn van 10 jaar en 3 maanden. Het wordt maximaal 3 maanden gebruikt voor het zetten van handtekeningen. De geldigheidstermijn van een DS certificaat loopt altijd eerder af dan de geldigheidstermijn van het bovenliggende CSCA certificaat.

Als het DS certificaat verlopen is, kan het in principe niet meer gebruikt worden voor het controleren van de handtekeningen op de kentekencard chip. Dit wil echter niet zeggen dat de kentekencard zijn geldigheid verliest. Ook een kentekencard met verlopen certificaten of met een niet werkende chip is geldig.

Indien de private key van een DS gecompromitteerd raakt of hiervan een vermoeden bestaat, wordt die niet meer gebruikt voor ondertekeningen. Het DS certificaat wordt ingetrokken en op de Certificate Revocation List (CRL) geplaatst. Op basis van het certificaat gezette handtekeningen zijn dan niet langer geldig.

De CRL wordt uitgegeven en ondertekend door de CSCA. Voor ieder geldig CSCA certificaat zal een CRL gepubliceerd worden. De authenticiteit van de CRL dient door relying parties gecontroleerd te worden op basis van het CSCA public key certificaat. RDW publiceert de CRLs op haar website. De locatie is aangegeven in de CDP extensie van de DS en CSCA certificaten. Periodiek (eens per 180 dagen) genereert en publiceert RDW een nieuwe CRL. De CRL is 200 dagen geldig. RDW genereert ook een

nieuwe CRL als een DS certificaat wordt ingetrokken. Erkende relying parties zullen van deze extra CRL op de hoogte gesteld worden door RDW.

Het beleid en de procedures voor de hierboven beschreven PKI staan beschreven in de gecombineerde Certificate Policy/Certification Practice Statement (CP/CPS) [5]. Dit document is te vinden op de website van RDW: http://www.rdw.nl. De object identifier (OID) van de CP/CPS is aangegeven in de Certificate Policy Extension van de DS en CSCA certificaten.

3.3 Verificatie van datagroepen A en B conform 2003/127/EC

Conform de Europese richtlijn 2003/127/EC [1] worden door de uitgevende instantie elektronische handtekeningen geplaatst over de datagroepen A en B op de chip (EF.Registration_A en EF.Registration_B). Deze handtekeningen zijn te vinden in de files EF.Signature_A en EF.Signature_B. In deze files is ook het gebruikte asymmetrische algoritme en het hash algoritme te vinden (voor het formaat zie App 1). De bij de handtekeningen horende public key certificaten waarmee de handtekeningen en daarmee de authenticiteit van de data in de datagroepen A en B te controleren is staan in EF.C.IA_A.DS en EF.C.IA_B.DS. Het format is X.509V3 (zie [4]) conform de eisen in [1].

Bij uitlezen van de datagroepen A en B en controle op authenticiteit volgens de Europese richtlijn dient eerst de authenticiteit van de certificaten gecontroleerd te worden, dienen vervolgens de handtekeningen te worden 'gecontroleerd'/'ontcijferd' en dienen daarna de hashes waarover de handtekeningen waren gezet vergeleken te worden met de hashes over de datagroepen. Pas als hieruit volgt dat de data in datagroepen A en B authentiek is dient deze aan de gebruiker getoond te worden. Stapsgewijs is het proces beschreven in paragraaf 4.3.

De DS certificaten dienen onder andere gecontroleerd te worden op geldigheidstermijn. Voor de Nederlandse DS certificaten geldt dat deze uitgegeven zijn door de Nederlandse CSCA en met behulp van het CSCA public key certificaat gecontroleerd dienen te worden. Ook dienen Nederlandse DS certificaten daarnaast gecontroleerd worden tegen het certificaat profiel zoals beschreven in de CP/CPS 5 en tegen de CRL waarvan de URL aangegeven is in de certificaat extensie.

Ook voor de meeste buitenlandse certificaten zal het DS certificaat getekend zijn door de nationale CSCA. Voor controle dient de verificatiesoftware te beschikken over deze buitenlandse CSCA certificaten. Mogelijk stelt RDW op termijn buitenlandse CSCA certificaten beschikbaar via een betrouwbare methode aan erkende relying parties of via haar website. Het kan echter gebeuren dat het buitenlandse CSCA certificaat niet beschikbaar is in de verificatiesoftware. In dat geval kan het DS certificaat niet gecontroleerd worden en dient de software een waarschuwing af te geven.

Het zou kunnen dat voor sommige landen de DS certificaten niet zijn uitgegeven door een CSCA, maar self-signed certificaten zijn. 2003/127/EC eist geen CSCA, al ligt dit wel voor de hand uit oogpunt van conformiteit met paspoorten, het rijbewijs en Europese verblijfsvergunningen. In dat geval dient de verificatiesoftware te beschikken over het DS certificaat uit een betrouwbare bron. Mogelijk stelt RDW op termijn voor deze gevallen de buitenlandse DS certificaten beschikbaar via een betrouwbare methode aan erkende relying parties of via haar website. Het kan echter gebeuren dat een self-signed DS certificaat niet beschikbaar is uit een betrouwbare bron. In dat geval dient het DS certificaat in ieder geval gecontroleerd te worden met de public key uit het certificaat zelf en dient de software een waarschuwing af te geven.

Indien de verificatie van het certificaat niet goed gaat dient dit duidelijk gemeld te worden aan de gebruiker van de uitlees- en verificatiesoftware.

Aangezien alle datagroepen op de Nederlandse kentekencard chip beveiligd zijn door middel van Passive Authentication hoeven deze verificaties niet uitgevoerd te worden op Nederlandse kentekencards mits verificatie door middel van Passive Authentication wordt uitgevoerd (zie paragrafen 3.4 en 4.2). Passive Authentication verdient de voorkeur boven het in deze paragraaf beschreven proces aangezien daarmee ook de authenticiteit van EF.Registration_C gegarandeerd en geverifieerd wordt indien aanwezig, duidelijk wordt dat de verschillende datagroepen bij elkaar horen en Active Authentication mogelijk is.

3.4 Passive Authentication

Voordat de data op de chip van een Nederlandse kentekencard geschreven wordt, wordt over deze data een handtekening geplaatst door de uitgevende instantie RDW. Deze handtekening wordt op de chip geplaatst. De handtekening maakt het mogelijk als de data van de chip gelezen wordt de authenticiteit ervan te controleren. Dat wil zeggen dat met behulp van de handtekening gecontroleerd kan worden dat de data afkomstig is van de RDW en niet gewijzigd is.

De elektronische handtekening wordt geplaatst door een entiteit die de Document Signer (DS) wordt genoemd. De DS beschikt hiervoor over een public-private key pair. Het certificaat van de DS is uitgegeven door de CSCA, het hoogste trust point (de root) binnen de PKI (zie paragraaf 3.2).

Om de handtekening te zetten worden tijdens het personalisatieproces eerst hashes berekend over iedere datagroep die op de chip geschreven zal worden. Deze hashes worden opgenomen in het RDWldsSecurityObject. Het RDWIDsSecurityObject maakt deel uit van het data object waarover met de DS private key een handtekening gegenereerd wordt. De RDWIDsSecurityObject, de handtekening en het bijbehorende DS certificaat worden als onderdeel van de EF.SOd op de kaart geplaatst (zie App 1 voor het exacte format van de EF.SOd).

Bij uitlezen en verifiëren van de data op de Nederlandse kentekencard chip dient eerst de authenticiteit van het certificaat uit de EF.SOd bepaald te worden, dan de correctheid van de handtekening uit de EF.SOd gecontroleerd te worden en vervolgens de authenticiteit van de datagroepen op basis van vergelijking van de hash-waarden (zie paragraaf 4.2 voor het volledige proces). Dit gebeurt conform RFC 5652 [6]. Pas als duidelijk is dat de data in de datagroepen authentiek is, dient deze aan de gebruiker getoond te worden.

Controle op basis van Passive Authentication dient gevolgd te worden in plaats van het proces geschreven in paragraaf 3.3 aangezien met Passive Authentication ook de authenticiteit van EF.Registration_C gegarandeerd en geverifieerd wordt indien aanwezig, duidelijk wordt dat de verschillende datagroepen bij elkaar horen en Active Authentication mogelijk is.

In het hier beschreven Passive Authentication proces wordt alleen ingegaan op het controleren van de correctheid van de data op de chip. Active Authentication om de authenticiteit van de chip zelf te verifiëren wordt beschreven in 3.5. Active Authentication is echter alleen mogelijk doordat de authenticiteit van de AA public key (opgenomen in EF.AA) volgt uit de Passive Authentication controle. EF.AA is één van de datagroepen die met behulp van PA gecontroleerd wordt. Het volledige proces voor het lezen en verifiëren van de Nederlandse kentekencard chip inclusief AA staat beschreven in paragraaf 4.2.

3.5 Active Authentication

De chip van Nederlandse kentekencards is bij personalisatie voorzien van een Active Authentication (AA) key pair. Hiermee kan de authenticiteit van de chip gecontroleerd worden door de verificatiesoftware. Het AA key pair is voor iedere chip uniek. De AA private key is opgeslagen in secure memory van de chip en is niet uit te lezen. De AA private key kan alleen door de chip gebruikt worden. De AA public key is op de chip geplaatst in EF.AA en vrij uit te lezen (zie App 1 voor het exacte format). EF.AA is meegenomen in de ondertekening van alle datagroepen. De hash over EF.AA bevindt zich in het RDWIDsSecurityObject in de EF.SOd. Daarmee kan de authenticiteit van de AA public key gecontroleerd worden door middel van Passive Authentication.

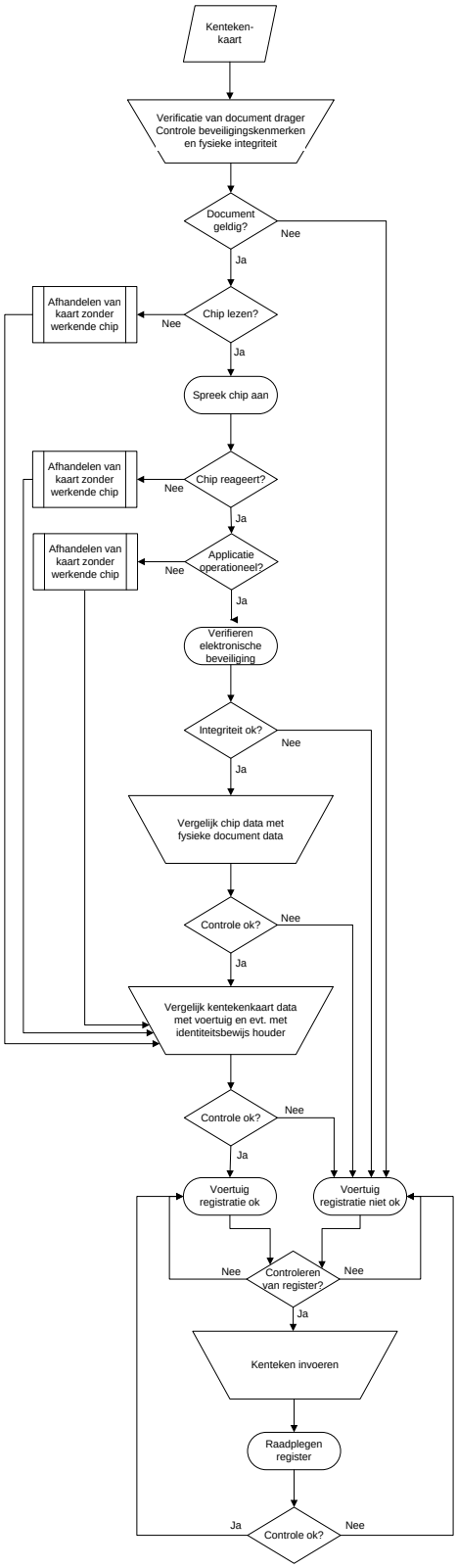
De verificatiesoftware kan om de authenticiteit van de chip te verifieren een challenge (random) naar de chip sturen met het verzoek deze te ondertekenen met de AA private key. Het door de chip aan de verificatiesoftware teruggestuurde antwoord kan gecontroleerd worden met behulp van de AA public key van de chip. Als uit het teruggestuurde antwoord na 'controle'/'ontcijfering' dezelfde challenge komt als die oorspronkelijk naar de chip gestuurd is, dan is daarmee de authenticiteit van de chip aangetoond.

4 VERIFICATIEPROCES

4.1 Processtroom

Het stroomschema hieronder geeft op hoog niveau de processtroom voor verificatie van een Nederlandse kentekencard aan (zie Figuur 3). In paragraaf 4.2 wordt nader ingegaan op het uitlezen en verifiëren van de chip. Paragraaf 4.3 beschrijft dit voor buitenlandse kentekencards die voldoen aan de Europese richtlijn [1].

Voor het onderstaande stroomschema is het belangrijk om te weten dat alle in Nederland geregistreerde voertuigen geregistreerd staan in het voertuigenregister dat door RDW onderhouden wordt. Het register is leidend. Uitsluitend om voertuig verificatie te vergemakkelijken en ook offline mogelijk te maken, geeft RDW kentekencards uit. Het register is echter leidend. In geval van twijfel over de echtheid van een kentekencard dient altijd het register geraadpleegd te worden.



Figuur 3: Stroomschema verificatie Nederlandse kentekencard (en registratie Nederlands voertuig)

4.2 Lezen en verifiëren van de Nederlandse kentekencard chip

Het onderstaande proces geeft aan wat de uitlees- en verificatiesoftware moet doen voor het uitlezen en controleren van de chip van de Nederlandse kentekencard. Ongeacht of het om een Nederlandse of buitenlandse kentekencard gaat, begint de uitlees- en verificatiesoftware met het selecteren van de eVRD applicatie. De AID is identiek voor alle eVRDs die voldoen aan [1]. Vervolgens probeert de uitleessoftware de EF.SOd te selecteren. Indien dat lukt, wordt verder het proces gevolgd dat in deze paragraaf beschreven is. Indien dit niet lukt, wordt door de uitleessoftware het proces gevolgd beschreven in paragraaf 4.3 vanaf stap 2.

Voor het uitlezen dient gebruik gemaakt te worden van de commando's uit App 2. Het hieronder aangegeven proces beschrijft de happy-flow. In geval op een van de commando's die naar de kaart gestuurd worden niet de verwachte response wordt teruggestuurd, wordt het proces gestopt en aan de gebruiker een foutmelding gegeven. Eventueel kan in de 2e lijn met meer geavanceerde uitlees- en verificatiesoftware worden vastgesteld wat het probleem is met de chip.

1. Selecteer eVRC applicatie (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'
```

```
T: 6F ( = FCI template)
L: 0D
      T: 84 ( = DF name)
      L: 0B
      V: A0 00 00 04 56 45 56 52 2D 30 31 (= AID)
SW: 90 00 (= successful processing)
```

2. Passive Authentication (1e deel)

a. Selecteer 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 LL LL 90 00'
```

```
T:'62'(= FCP template)
L:'08'
     T:'83' (= File ID)
     L:'02'
     V:'00 1D' (= EF.SOd)
     T:'80' ( = File size)
     L:'02'
     V:'LL LL'
SW:'90 00' (=successful processing)
```

Indien geen EF.SOd aanwezig is (Response: `Status Words '6A 82' File not found`), gaat het om een buitenlandse kaart en moet de uitleesprocedure gevolgd worden zoals beschreven in paragraaf 4.3 vanaf stap 2.

b. Lees EF.SOd (lengte = 'LL LL')

Lees commando vanaf offset '00 00'

```
T→C: '00 B0 00 00 00'
C→T: 'XX ...XX 90 00'
```

Response heeft lengte van '01 02' ofwel 258 bytes. Dit is '01 00' ofwel 256 bytes aan data plus de status words '90 00' (successful processing).

Lees commando vanaf offset '01 00'

```
T→C: '00 B0 01 00 00'
C→T: 'XX ...XX 90 00'
```

Response heeft lengte van '01 02' ofwel 258 bytes. Dit is '01 00' ofwel 256 bytes aan data plus de status words '90 00' (successful processing).

Herhaal lees commando's met juiste offset ('00 00', '01 00', '02 00', ...) totdat alle bytes van de file zijn uitgelezen. Lengte van de file volgt uit response op het hiervoor gegeven select commando: 'LL LL'.

Plaats alle data uit de responses op de lees commando's (dus zonder de status bytes '90 00') achter elkaar om de EF.SOd data te krijgen. Dit moet een totale lengte hebben van 'LL LL' bytes. De SOd (EF.SOd data) voldoet aan RFC 5652 [6].

c. Controleer DS certificaat uit EF.SOd

i. Haal DS certificaat uit EF.SOd data

DS certificaat bevindt zich in de EF.SOd data onder:

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

(DS certificaat begint met tag '30')

ii. DS certificaat profiel voldoet aan CP/CPS

CP/CPS OID is te vinden in de DS certificaat extensie CertificatePolicies
RDW publiceert de CP/CPS op de volgende locatie:
http://www-diensten.rdw.nl/
Meestal zal de uitleessoftware al bekend zijn met het certificaatprofiel.
De uitleessoftware controleert dat de kritieke extensies aanwezig zijn en dat de aangegeven KeyUsage uitsluitend DigitalSignature is.

iii. DS certificaat is niet verlopen

Certificaat valid to date ligt na huidige datum

iv. DS certificaat komt niet voor op CRL

CRL locatie is te vinden in de DS certificaat extensie CRLDistributionPoints
RDW publiceert CRLs op de volgende locatie:
http://www-diensten.rdw.nl/crl/

De uitleessoftware dient de meest recente CRL te gebruiken voor verificatie. Meestal zal de uitleessoftware al de actuele CRL bezitten (zie verder hoofdstuk 6).

v. **DS certificaat is uitgegeven door CSCA (controle tegen CSCA certificaat)**
De CSCA waardoor het DS certificaat is uitgegeven is te vinden in het DS certificaat veld Issuer en in de extensie AuthorityKeyIdentifier.
De uitleessoftware heeft het bijbehorende CSCA public key certificaat nodig voor het controleren van de signature van het DS certificaat (zie hoofdstuk 6). Het CSCA certificaat is een X.509V3 certificaat volgens RFC 5280 [4].
De uitleessoftware gebruikt de public key uit het vertrouwde CSCA certificaat voor controle van de handtekening (veld signatureValue) uit het DS certificaat.
De handtekening is door de CSCA gezet over het TBSCertificate.
Het gebruikt daartoe het algoritme zoals aangegeven in het veld signatureAlgorithm en in het veld Signature van het TBSCertificate.

vi. **Sla DS public key uit DS certificaat op in geheugen**

d. Controleer handtekening uit EF.SOd met public key uit DS certificaat

i. **Haal handtekening en algoritme uit EF.SOd**
De handtekening bevindt zich in de EF.SOd data onder:

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

Het gebruikte algoritme is te vinden in de EF.SOd data onder:

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

Dit kan sha256WithRSAEncryption (OID::= 1.2.840.113549.1.1.11) of id-RSASSA-PSS (OID ::= 1.2.840.113549.1.1.10) zijn. In het laatste geval is onder Tag '30' the RSA PSS parameters te vinden

ii. **'Controleer' / 'Ontcijfer' met DS public key**
Door 'controle' / 'ontcijfering' van de handtekening met de DS public key uit het DS certificaat volgt het signedAttrs TLV veld met dien verstande dat dit veld begint met tag '31' i.p.v. met tag 'A0'.

iii. **Sla signedAttrs uit handtekening op in geheugen**
Sla signedAttrs op in geheugen na de begintag vervangen te hebben door 'A0'.

iv. **Haal signedAttrs uit EF.SOd**
Het signedAttrs veld bevindt zich in de EF.SOd data onder:

```
T: '30'(ContentInfo)
```


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

v. Vergelijk signedAttrs uit EF.SOd met signedAttrs uit handtekening (geheugen)

vi. Haal AttributeValue uit signedAttrs

Binnen signedAttrs bevindt de AttributeValue zich onder:

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

Dit is de hash over eContent (= RDWIdsSecurityObject)
Sla deze hash op in het geheugen.

Het hash algoritme bevindt zich in EF.SOd onder:

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

De NL-eVRD maakt gebruik van sha256 (OID ::= 2.16.840.1.101.3.4.2.1)

vii. Haal eContent (=RDWIdsSecurityObject) uit EF.SOd

eContent bevindt zich in de EF.SOd onder:

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

viii. Bereken hash over eContent

Gebruik hiervoor het hash algoritme ui vi. (sha256)

ix. Vergelijk hashes

Vergelijk hash over eContents met hash uit vi. (AttributeValue uit signedAttrs).
Indien deze 2 overeenkomen is het eerste deel van PA geslaagd.

e. Sla eContent = RDWsecurityobject op in geheugen

3. **Active Authentication**

a. Selecteer 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 LL LL 90 00'
```

```
T: '62' ( = FCP template)
L: '08'
```


```
     T: '83' (= File ID)
     L: '02'
     V: '00 0D' (= EF.AA)
     T: '80' ( = File size)
     L: '02'
     V: 'LL LL'
SW: '90 00' (=successful processing)
```

b. Lees EF.AA

```
T→C: '00 B0 00 00 00'
C→T: 'XX ...XX 90 00'
```

Eventueel moet dit commando herhaald worden met de juiste offset.

c. Controleer authenticiteit EF.AA (Passive Authentication (2e deel))

i. Haal hash algoritme uit RDWIdsSecurityObject

Het RDWIdsSecurityObject (eContent) afkomstig uit de EF.SOd is onder stap 2.e opgeslagen in het geheugen van de uitlees- en verificatiesoftware.
Het hash algoritme bevindt zich in eContent onder:

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

RDW maakt gebruik van id-sha256 ::= 2.16.840.1.101.3.4.2.1.

ii. Bereken hash over EF.AA

De hash wordt berekend over de data (dus zonder status words) uit EF.AA met het hash algoritme uit i.

iii. Haal hash waarde van EF.AA uit RDWIdsSecurityObject

Het RDWIdsSecurityObject (eContent) afkomstig uit de EF.SOd is onder stap 2.e opgeslagen in het geheugen van de uitlees- en verificatiesoftware.
De hash waarde bevindt zich in eContent onder:

```
T: '30'(RDWIdsSecurityObject)
     T: '30' (dataGroupHashValues)
          T: '04' (dataGroupFileIdentifier)
               V: '00 0D'
          T: '04' (dataGroupHashValue)
```

De file identifier van EF.AA is '00 0D'.

iv. Vergelijk de hash-waarden

Vergelijk de hash waarde van EF.AA uit RDWIdsSecurityObject met de over EF.AA berekende hash waarde in ii.

d. Sla AA public key uit EF.AA op in geheugen

De AA public key bevindt zich in EF.AA onder:

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

Het algoritme is te vinden in EF.AA onder:

```
T: '6F'(ActiveAuthenticationPublicKeyInfo)
     T: '30' (SubjectPublicKeyInfo)
          T: '30' (AlgorithmIdentifier)
```

```
T:'06' (algorithm)
(rsaEncryption = 1.2.840.113549.1.1.1)
```

RDW maakt gebruik van RSA.

e. Genereer 8-byte challenge (RND.IFD)
De uitlees- en verificatiesoftware genereert een random van 8 bytes.

f. Chip authenticatie
Stuur 8-byte challenge (RND.IFD) naar kaart via Internal Authenticate commando.

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

g. Controleer reponse met behulp van AA public key
Gebruik de AA public key uit EF.AA (opgeslagen in geheugen) om de data uit de response op het Internal Authenticate commando (dus zonder de status words '90 00') te 'ontcijferen' / 'controleren' met behulp van het algoritme uit stap d. (RSA).

Dit levert een string op die volgens ISO 9796-2 [10] Digital Signature Scheme 1[1] moet bestaan uit:
`'6A ++ M1 ++ hash (M1 ++ RND.IFD) ++ 34 CC'`
waarbij `M1` een nonce is gegenereerd door de chip.

Haal `M1` uit de response.
Bereken met behulp van sha256 de hash over `M1 ++ RND.IFD.`

Vergelijk deze hash met de hash-waarde uit de response.
Indien de 2 overeenkomen is Active Authentication van de chip geslaagd.

4. Lees en controleer data

a. Selecteer 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 LL LL 90 00'

```
T: '62' ( = FCP template)
L: '08'
     T: '83' (= File ID)
     L: '02'
     V: 'D0 01' (= EF.Registration_A)
     T: '80' ( = File size)
     L: '02'
```

[1] Digital Signature Scheme 1 met de modificatie dat de 'alternative' signature production function wordt gebruikt. M zal bestaan uit M1 en M2, waarbij M1 een nonce is die gegenereerd is door de VR applicatie van c-4 bits en M2 is RND.IFD ('M', 'M1', 'M2' en 'c' zoals gedefinieerd in ISO 9796-2 [10]). Het SHA-256 hashing algoritme and trailer optie 2 zullen gebruikt worden.

```
     V: 'LL LL'
SW: '90 00' (=successful processing)
```

b. Lees EF.Registration_A

```
T→C: '00 B0 00 00 00'
C→T: 'XX ...XX 90 00'
```

Response heeft lengte van '01 02' ofwel 258 bytes. Dit is '01 00' ofwel 256 bytes aan data plus de status words '90 00' (successful processing).

Lees commando vanaf offset '01 00'.

```
T→C: '00 B0 01 00 00'
C→T: 'XX ...XX 90 00'
```

Response heeft lengte van '01 02' ofwel 258 bytes. Dit is '01 00' ofwel 256 bytes aan data plus de status words '90 00' (successful processing).

Herhaal lees commando's met juiste offset ('00 00', '01 00', '02 00', ...) totdat alle bytes van de file zijn uitgelezen. Lengte van de file volgt uit response op het hiervoor gegeven select commando: 'LL LL'.

Plaats alle data uit de responses op de lees commando's (dus zonder de status bytes '90 00') achter elkaar om de EF.Registration_A data te krijgen. Dit moet een totale lengte hebben van 'LL LL' bytes.

c. Controleer authenticiteit EF.Registration_A (Passive Authentication (2e deel))

i. Bereken hash over EF.Registration_A

Gebruik hiervoor het hash algoritme aangegeven in de het RDWIdsSecurityObject. Het hash algoritme bevindt zich in eContent onder:

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

RDW maakt gebruik van sha 256 (OID ::= 2.16.840.1.101.3.4.2.1).
De hash wordt berekend over de data (dus zonder status words) uit EF.Registration_A.

ii. Haal hash waarde uit RDWIdsSecurityObject

De hash waarde van EF.Registration_A bevindt zich in eContent onder:

```
T:'30'(RDWIdsSecurityObject)
     T:'30'(dataGroupHashValues)
          T:'04'(dataGroupFileIdentifier)
               V: 'D0 01'
          T: '04' (dataGroupHashValue)
```

De file identifier van EF.Registration_A is 'D0 01'.

iii. Vergelijk de hash-waarden

Indien de hash waarde uit RDWIdsSecurityObject overeenkomt met de

berekende hash over EF.Registration_A uit i. is de data in EF.Registration_A authentiek en kan aan de gebruiker getoond worden.

d. Toon EF.Registration_A data aan gebruiker

e. Selecteer EF.Registration_B ('D0 11')

```
T→C: '00 A4 02 04 02 D0 01 00'
C→T: '62 08 83 02 D0 11 80 02 LL LL 90 00'
```

```
T: '62' ( = FCP template)
L: '08'
     T: '83' (= File ID)
     L: '02'
     V: 'D0 11' (= EF.Registration_B)
     T: '80' ( = File size)
     L: '02'
     V: 'LL LL'
SW: '90 00' (=successful processing)
```

f. Lees EF.Registration_B

```
T→C: '00 B0 00 00 00'
C→T: 'XX ...XX 90 00'
```

Response heeft lengte van '01 02' ofwel 258 bytes. Dit is '01 00' ofwel 256 bytes aan data plus de status words '90 00' (successful processing).

Lees commando vanaf offset '01 00'

```
T→C: '00 B0 01 00 00'
C→T: 'XX ...XX 90 00'
```

Response heeft lengte van '01 02' ofwel 258 bytes. Dit is '01 00' ofwel 256 bytes aan data plus de status words '90 00' (successful processing).

Herhaal lees commando's met juiste offset ('00 00', '01 00', '02 00', ...) totdat alle bytes van de file zijn uitgelezen. Lengte van de file volgt uit response op het hiervoor gegeven select commando: 'LL LL'.

Plaats alle data uit de responses op de lees commando's (dus zonder de status bytes '90 00') achter elkaar om de EF.Registration_B data te krijgen. Dit moet een totale lengte hebben van 'LL LL' bytes

g. Controleer authenticiteit EF.Registration_B (Passive Authentication (2e deel))

i. Bereken hash over EF.Registration_B
Gebruik hiervoor het hash algoritme aangegeven in de het RDWIdsSecurityObject. Het hash algoritme bevindt zich in eContent onder:

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

RDW maakt gebruik van sha 256 (OID ::= 2.16.840.1.101.3.4.2.1).
De hash wordt berekend over de data (dus zonder status words) uit EF.Registration_B.

ii. Haal hash waarde uit RDWIdsSecurityObject

De hash waarde van EF.Registration_B bevindt zich in eContent onder:

```
T:'30'(RDWIdsSecurityObject)
     T:'30'(dataGroupHashValues)
            T:'04'(dataGroupFileIdentifier)
                 V: 'D0 11'
            T: '04' (dataGroupHashValue)
```

De file identifier van EF.Registration_B is 'D0 11'.

iii. Vergelijk de hash-waarden

Indien de hash waarde uit RDWIdsSecurityObject overeenkomt met de berekende hash over EF.Registration_B uit i. is de data in EF.Registration_B authentiek en kan aan de gebruiker getoond worden.

h. Toon EF.Registration_B data aan gebruiker

i. Selecteer 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 LL LL 90 00'
```

```
T: '62' ( = FCP template)
L: '08'
     T: '83' (= File ID)
     L: '02'
     V: 'D0 21' (= EF.Registration_C)
     T: '80' ( = File size)
     L: '02'
     V: 'LL LL'
SW: '90 00' (=successful processing)
```

j. Lees EF.Registration_C

```
T→C: '00 B0 00 00 00'
C→T: 'XX ...XX 90 00'
```

Response heeft lengte van '01 02' ofwel 258 bytes. Dit is '01 00' ofwel 256 bytes aan data plus de status words '90 00' (successful processing).

Lees commando vanaf offset '01 00'

```
T→C: '00 B0 01 00 00'
C→T: 'XX ...XX 90 00'
```

Response heeft lengte van '01 02' ofwel 258 bytes. Dit is '01 00' ofwel 256 bytes aan data plus de status words '90 00' (successful processing).

Herhaal lees commando's met juiste offset ('00 00', '01 00', '02 00', ...) totdat alle bytes van de file zijn uitgelezen. Lengte van de file volgt uit response op het hiervoor gegeven select commando: 'LL LL'.

Plaats alle data uit de responses op de lees commando's (dus zonder de status bytes '90 00') achter elkaar om de EF.Registration_C data te krijgen. Dit moet een totale lengte hebben van 'LL LL' bytes

k. Controleer authenticiteit EF.Registration_C (Passive Authentication (2e deel))

i. Bereken hash over EF.Registration_C

Gebruik hiervoor het hash algoritme aangegeven in de het RDWIdsSecurityObject. Het hash algoritme bevindt zich in eContent onder:

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

RDW maakt gebruik van sha 256 (OID ::= 2.16.840.1.101.3.4.2.1).
De hash wordt berekend over de data (dus zonder status words) uit EF.Registration_C.

ii. Haal hash waarde uit RDWIdsSecurityObject

De hash waarde van EF.Registration_C bevindt zich in eContent onder:

```
T:'30'(RDWIdsSecurityObject)
     T:'30'(dataGroupHashValues)
            T:'04'(dataGroupFileIdentifier)
                 V: 'D0 21'
            T: '04' (dataGroupHashValue)
```

De file identifier van EF.Registration_C is 'D0 21'.

iii. Vergelijk de hash-waarden

Indien de hash waarde uit RDWIdsSecurityObject overeenkomt met de berekende hash over EF.Registration_C uit i. is de data in EF.Registration_C authentiek en kan aan de gebruiker getoond worden.

l. Toon EF.Registration_C data aan gebruiker

4.3 Lezen en verifiëren van buitenlandse kentekencard chips

Het onderstaande proces geeft aan wat de uitlees- en verificatiesoftware moet doen voor het uitlezen en controleren van de chip van (buitenlandse) kentekencards die voldoen aan de Europese richtlijn [1]. Voor Nederlandse kentekencards die ook voldoen aan [1] dient echter gebruik gemaakt te worden van het proces in paragraaf 4.2. Buitenlandse kentekencards dienen qua commando's te voldoen aan ISO 7816-4 [7]en ISO 7816-8 [8]. Daarbij hoeven niet dezelfde keuzes gemaakt te zijn als voor de commando's die ondersteund worden door de Nederlandse kentekencard chip. App 2 en de hieronder aangegeven exacte commando-opbouw zijn daarom niet leidend voor buitenlandse kentekencards.

1. Selecteer eVRC applicatie (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'
```

```
T: 6F ( = FCI template)
L: 0D
   T: 84 ( = DF name)
   L: 0B
   V: A0 00 00 04 56 45 56 52 2D 30 31 (= AID)
SW: 90 00 (= successful processing)
```

2. Selecteer EF.C.IA_A.DS (File ID = 'C0 01')

```
T→C: '00 A4 02 04 02 C0 01 00'
C→T: '62 08 83 02 C0 01 80 02 LL LL 90 00'
```

```
T:'62'(= FCP template)
L:'08'
   T:'83' (= File ID)
   L:'02'
   V:'C0 01' (= EF.C.IS_A.DS)
   T:'80' ( = File size)
   L:'02'
   V:'LL LL'
SW:'90 00' (=successful processing)
```

3. Lees EF.C.IA_A.DS (lengte = 'LL LL')

Lees commando vanaf offset '00 00'

```
T→C: '00 B0 00 00 00'
C→T: 'XX ...XX 90 00'
```

Response heeft lengte van '01 02' ofwel 258 bytes. Dit is '01 00' ofwel 256 bytes aan data plus de status words '90 00' (successful processing).

Lees commando vanaf offset '01 00'

```
T→C: '00 B0 01 00 00'
C→T: 'XX ...XX 90 00'
```

Response heeft lengte van '01 02' ofwel 258 bytes. Dit is '01 00' ofwel 256 bytes aan data plus de status words '90 00' (successful processing).

Herhaal lees commando's met juiste offset ('00 00', '01 00', '02 00', ...) totdat alle bytes van de file zijn uitgelezen. Lengte van de file volgt uit response op het hiervoor gegeven select commando: 'LL LL'.

Plaats alle data uit de responses op de lees commando's (dus zonder de status bytes '90 00') achter elkaar om de EF.C.IA_A.DS data te krijgen. Dit moet een totale lengte hebben van 'LL LL' bytes

4. **Controleer DS certificaat uit EF.C.IA_A.DS**
   a. **DS certificaat profiel voldoet aan CP/CPS**
      CP/CPS OID is te vinden in de DS certificaat extensie CertificatePolicies
      Meestal zal de uitleessoftware al bekend zijn met het certificaatprofiel.
      De uitleessoftware controleert dat de kritieke extensies aanwezig zijn en dat de aangegeven KeyUsage uitsluitend DigitalSignature is.
   b. **DS certificaat is niet verlopen**
      Certificaat valid to date ligt na huidige datum
   c. **DS certificaat komt niet voor op CRL**
      CRL locatie is te vinden in de DS certificaat extensie CRLDistributionPoints
      Meestal zal de uitleessoftware al de actuele CRL bezitten (zie verder hoofdstuk 6).
   d. **DS certificaat is uitgegeven door CSCA**
      (controle tegen CSCA certificaat indien CSCA certificaat beschikbaar is)[2]
      De CSCA waardoor het DS certificaat is uitgegeven (CSCA private key) is te vinden in het DS certificaat veld Issuer en in de extensie AuthorityKeyIdentifier.
      De uitleessoftware heeft het bijbehorende CSCA public key certificaat nodig voor het controleren van de signature van het DS certificaat (zie hoofdstuk 6).
      De uitleessoftware gebruikt de public key uit het vertrouwde CSCA certificaat voor controle van de handtekening (veld signatureValue) uit het DS certificaat.
      De handtekening is door de CSCA gezet over het TBSCertificate.
      Het gebruikt daartoe het algoritme zoals aangegeven in het veld signatureAlgorithm en in het veld Signature van het TBSCertificate.
   e. **Sla DS public key uit DS certificaat op in geheugen**

5. **Selecteer EF.Signature_A ('E0 01')**

```
T→C: '00 A4 02 04 02 E0 01 00'
C→T: '62 08 83 02 E0 01 80 02 LL LL 90 00'
```

```
T:'62'(= FCP template)
L:'08'
   T:'83' (= File ID)
   L:'02'
   V:'E0 01' (= EF.Signature_A)
   T:'80' ( = File size)
   L:'02'
   V:'LL LL'
SW:'90 00' (=successful processing)
```

6. **Lees EF.Signature_A**

[2] Eventueel zou sprake kunnen zijn van een self-signed DS certificaat. Dan dient gecontroleerd te worden met de public key uit het certificaat zelf.

Lees commando vanaf offset '00 00'

```
T→C: '00 B0 00 00 00'
C→T: 'XX ...XX 90 00'
```

Response heeft lengte van '01 02' ofwel 258 bytes. Dit is '01 00' ofwel 256 bytes aan dataplus de status words '90 00' (successful processing).

Lees commando vanaf offset '01 00'

```
T→C: '00 B0 01 00 00'
C→T: 'XX ...XX 90 00'
```

Response heeft lengte van '01 02' ofwel 258 bytes. Dit is '01 00' ofwel 256 bytes aan data plus de status words '90 00' (successful processing).

Herhaal lees commando's met juiste offset ('00 00', '01 00', '02 00', ...) totdat alle bytes van de file zijn uitgelezen. Lengte van de file volgt uit response op het hiervoor gegeven select commando: 'LL LL'.

Plaats alle data uit de responses op de lees commando's (dus zonder de status bytes '90 00') achter elkaar om de EF.Signature_A data te krijgen. Dit moet een totale lengte hebben van 'LL LL' bytes

7. 'Controleer'/'ontcijfer' handtekening uit EF.Signature_A met public key uit DS certificaat

a. Haal handtekening en algoritme uit EF.Signature_A

De handtekening bevindt zich in de EF.Signature_A data onder:

```
T: '30'(Signature)
     T: '03(SignatureValue)
```

Het gebruikte algoritme is te vinden in de EF.Signature_A data onder:

```
T: '30'(Signature)
     T: '30'(AlgorithmIdentifier)
           T: '06'(Algorithm)
```

b. 'Controleer' / 'Ontcijfer' met DS public key

Door 'controle' / 'ontcijfering' van de SignatureValue met de DS public key uit het DS certificaat volgt de hash over EF.Registration_A.

8. Selecteer 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 LL LL 90 00'
```

```
T:'62'(= FCP template)
L:'08'
   T:'83' (= File ID)
   L:'02'
   V:'D0 01' (= EF.Registration_A)
   T:'80' ( = File size)
```

```
   L:'02'
   V:'LL LL'
SW:'90 00' (=successful processing)
```

9. Lees EF.Registration_A

```
T→C: '00 B0 00 00 00'
C→T: 'XX ...XX 90 00'
```

Response heeft lengte van '01 02' ofwel 258 bytes. Dit is '01 00' ofwel 256 bytes aan data plus de status words '90 00' (successful processing).

Lees commando vanaf offset '01 00'.

```
T→C: '00 B0 01 00 00'
C→T: 'XX ...XX 90 00'
```

Response heeft lengte van '01 02' ofwel 258 bytes. Dit is '01 00' ofwel 256 bytes aan data plus de status words '90 00' (successful processing).

Herhaal lees commando's met juiste offset ('00 00', '01 00', '02 00', ...) totdat alle bytes van de file zijn uitgelezen. Lengte van de file volgt uit response op het hiervoor gegeven select commando: 'LL LL'.

Plaats alle data uit de responses op de lees commando's (dus zonder de status bytes '90 00') achter elkaar om de EF.Registration_A data te krijgen. Dit moet een totale lengte hebben van 'LL LL' bytes

10. Controleer authenticiteit EF.Registration_A

a. Bereken hash over EF.Registration_A
Gebruik hiervoor het digest algoritme aangegeven in EF.Signature_A

b. Vergelijk hash waarden
Vergelijk de berekende hash-waarde met de opgeslagen hash-waarde uit EF.Signature_A

11. Toon EF.Registration_A data aan gebruiker

12. Selecteer EF.C.IA_B.DS (File ID = 'C0 11')

```
T→C: '00 A4 02 04 02 C0 11 00'
C→T: '62 08 83 02 C0 11 80 02 LL LL 90 00'
```

```
T:'62'(= FCP template)
L:'08'
   T:'83' (= File ID)
   L:'02'
   V:'C0 11' (= EF.C.IS_B.DS)
   T:'80' ( = File size)
```

```
   L:'02'
   V:'LL LL'
SW:'90 00' (=successful processing)
```

13. Lees EF.C.IA_B.DS (lengte = 'LL LL')

Lees commando vanaf offset '00 00'

```
T→C: '00 B0 00 00 00'
C→T: 'XX ...XX 90 00'
```

Response heeft lengte van '01 02' ofwel 258 bytes. Dit is '01 00' ofwel 256 bytes aan data plus de status words '90 00' (successful processing).

Lees commando vanaf offset '01 00'

```
T→C: '00 B0 01 00 00'
C→T: 'XX ...XX 90 00'
```

Response heeft lengte van '01 02' ofwel 258 bytes. Dit is '01 00' ofwel 256 bytes aan data plus de status words '90 00' (successful processing).

Herhaal lees commando's met juiste offset ('00 00', '01 00', '02 00', ...) totdat alle bytes van de file zijn uitgelezen. Lengte van de file volgt uit response op het hiervoor gegeven select commando: 'LL LL'.

Plaats alle data uit de responses op de lees commando's (dus zonder de status bytes '90 00') achter elkaar om de EF.C.IA_B.DS data te krijgen. Dit moet een totale lengte hebben van 'LL LL' bytes

14. Controleer DS certificaat uit EF.C.IA_B.DS

a. **DS certificaat profiel voldoet aan CP/CPS**
   CP/CPS OID is te vinden in de DS certificaat extensie CertificatePolicies
   Meestal zal de uitleessoftware al bekend zijn met het certificaatprofiel.
   De uitleessoftware controleert dat de kritieke extensies aanwezig zijn en dat de aangegeven KeyUsage uitsluitend DigitalSignature is.
b. **DS certificaat is niet verlopen**
   Certificaat valid to date ligt na huidige datum
c. **DS certificaat komt niet voor op CRL**
   CRL locatie is te vinden in de DS certificaat extensie CRLDistributionPoints
   Meestal zal de uitleessoftware al de actuele CRL bezitten (zie verder hoofdstuk 6).
d. **DS certificaat is uitgegeven door CSCA**
   (controle tegen CSCA certificaat indien CSCA certificaat beschikbaar is)[3]
   De CSCA waardoor het DS certificaat is uitgegeven (CSCA private key) is te vinden in het DS certificaat veld Issuer en in de extensie AuthorityKeyIdentifier.

[3] Eventueel zou sprake kunnen zijn van een self-signed DS certificaat. Dan dient gecontroleerd te worden met de public key uit het certificaat zelf.

De uitleessoftware heeft het bijbehorende CSCA public key certificaat nodig voor het controleren van de signature van het DS certificaat (zie hoofdstuk 6).
De uitleessoftware gebruikt de public key uit het vertrouwde CSCA certificaat voor controle van de handtekening (veld signatureValue) uit het DS certificaat.
De handtekening is door de CSCA gezet over het TBSCertificate.
Het gebruikt daartoe het algoritme zoals aangegeven in het veld signatureAlgorithm en in het veld Signature van het TBSCertificate.

e. Sla DS public key uit DS certificaat op in geheugen

15. Selecteer EF.Signature_B ('E0 11')

```
T→C: '00 A4 02 04 02 E0 11 00'
C→T: '62 08 83 02 E0 11 80 02 LL LL 90 00'
```

```
T:'62'(= FCP template)
L:'08'
   T:'83' (= File ID)
   L:'02'
   V:'E0 11' (= EF.Signature_B)
   T:'80' ( = File size)
   L:'02'
   V:'LL LL'
SW:'90 00' (=successful processing)
```

16. Lees EF.Signature_B

Lees commando vanaf offset '00 00'

```
T→C: '00 B0 00 00 00'
C→T: 'XX ...XX 90 00'
```

Response heeft lengte van '01 02' ofwel 258 bytes. Dit is '01 00' ofwel 256 bytes aan dataplus de status words '90 00' (successful processing).

Lees commando vanaf offset '01 00'

```
T→C: '00 B0 01 00 00'
C→T: 'XX ...XX 90 00'
```

Response heeft lengte van '01 02' ofwel 258 bytes. Dit is '01 00' ofwel 256 bytes aan data plus de status words '90 00' (successful processing).

Herhaal lees commando's met juiste offset ('00 00', '01 00', '02 00', ...) totdat alle bytes van de file zijn uitgelezen. Lengte van de file volgt uit response op het hiervoor gegeven select commando: 'LL LL'.

Plaats alle data uit de responses op de lees commando's (dus zonder de status bytes '90 00') achter elkaar om de EF.Signature_B data te krijgen. Dit moet een totale lengte hebben van 'LL LL' bytes

17. 'Controleer'/'ontcijfer' handtekening uit EF.Signature_B met public key uit DS certificaat

a. Haal handtekening en algoritme uit EF.Signature_B

De handtekening bevindt zich in de EF.Signature_B data onder:

```
T: '30'(Signature)
     T: '03(SignatureValue)
```

Het gebruikte algoritme inclusief hash algorithme is te vinden in de EF.Signature_B data onder:

```
T: '30'(Signature)
     T: '30'(AlgorithmIdentifier)
          T: '06'(Algorithm)
```

b. 'Controleer' / 'Ontcijfer' met DS public key

Door 'controle' / 'ontcijfering' van de SignatureValue met de DS public key uit het DS certificaat volgt de hash over EF.Registration_B.

18. Selecteer EF.Registration_B ('D0 11')

```
T→C: '00 A4 02 04 02 D0 11 00'
C→T: '62 08 83 02 D0 01 80 02 LL LL 90 00'
```

```
T:'62'(= FCP template)
L:'08'
   T:'83' (= File ID)
   L:'02'
   V:'D0 11' (= EF.Registration_B)
   T:'80' ( = File size)
   L:'02'
   V:'LL LL'
SW:'90 00' (=successful processing)
```

19. Lees EF.Registration_B

```
T→C: '00 B0 00 00 00'
C→T: 'XX ...XX 90 00'
```

Response heeft lengte van '01 02' ofwel 258 bytes. Dit is '01 00' ofwel 256 bytes aan data plus de status words '90 00' (successful processing).

Lees commando vanaf offset '01 00'.

```
T→C: '00 B0 01 00 00'
C→T: 'XX ...XX 90 00'
```

Response heeft lengte van '01 02' ofwel 258 bytes. Dit is '01 00' ofwel 256 bytes aan data plus de status words '90 00' (successful processing).

Herhaal lees commando's met juiste offset ('00 00', '01 00', '02 00', ...) totdat alle bytes van de file zijn uitgelezen. Lengte van de file volgt uit response op het hiervoor gegeven select commando: 'LL LL'.

Plaats alle data uit de responses op de lees commando's (dus zonder de status bytes '90 00') achter elkaar om de EF.Registration_B data te krijgen. Dit moet een totale lengte hebben van 'LL LL' bytes

20. Controleer authenticiteit EF.Registration_B

a. Bereken hash over EF.Registration_B
Gebruik hiervoor het digest algoritme aangegeven in EF.Signature_B

b. Vergelijk hash waarden
Vergelijk de berekende hash-waarde met de opgeslagen hash-waarde uit EF.Signature_B

21. Toon EF.Registration_B data aan gebruiker

OPTIONEEL (het is niet zeker of EF.Registration_C aanwezig zal zijn en of uitlezen gewenst is)

22. Selecteer 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 LL LL 90 00'
```

```
T:'62'(= FCP template)
L:'08'
   T:'83' (= File ID)
   L:'02'
   V:'D0 21' (= EF.Registration_C)
   T:'80' ( = File size)
   L:'02'
   V:'LL LL'
SW:'90 00' (=successful processing)
```

23. Lees EF.Registration_C

```
T→C: '00 B0 00 00 00'
C→T: 'XX ...XX 90 00'
```

Response heeft lengte van '01 02' ofwel 258 bytes. Dit is '01 00' ofwel 256 bytes aan data plus de status words '90 00' (successful processing).

Lees commando vanaf offset '01 00'.

```
T→C: '00 B0 01 00 00'
C→T: 'XX ...XX 90 00'
```

Response heeft lengte van '01 02' ofwel 258 bytes. Dit is '01 00' ofwel 256 bytes aan data plus de status words '90 00' (successful processing).

Herhaal lees commando's met juiste offset ('00 00', '01 00', '02 00', ...) totdat alle bytes van de file zijn uitgelezen. Lengte van de file volgt uit response op het hiervoor gegeven select commando: 'LL LL'.

Plaats alle data uit de responses op de lees commando's (dus zonder de status bytes '90 00') achter elkaar om de EF.Registration_C data te krijgen. Dit moet een totale lengte hebben van 'LL LL' bytes

24. Toon EF.Registration_C data aan gebruiker

5 COMMUNICATIE TUSSEN KAART EN UITLEES- EN VERIFICATIESOFTWARE

De chips van kentekencards die voldoen aan de Europese richtlijn [1] zijn smart cards (ID-1 formaat) met een contact chip die voldoet aan ISO 7816 [7], [8]. De chips ondersteunen in ieder geval het T=1 protocol. Ondersteuning van het T=0 protocol is optioneel. De chips kunnen uitgelezen worden met een reader die werkt volgens ISO 7816.

Voor de Nederlandse kentekencard chips zijn voor de commando's die ondersteund worden de keuzes gemaakt zoals weergegeven in App 2.

De kentekencard applicatie op de chip heeft als Application Identifier
AID = 'A0 00 00 04 56 45 56 52 2D 30 31'.

6 INFORMATIEUITWISSELING MET VERIFICATIESOFTWARE

Voor verificatie van de Nederlandse kentekencard chip dient de verificatiesoftware te beschikken over het CSCA certificaat op basis waarvan de DS certificaten van de chip gecontroleerd kunnen worden. Dit CSCA certificaat is te downloaden van de RDW website, maar om zeker te zijn van de authenticiteit van het certificaat, dient het uitgewisseld te worden via een betrouwbaar kanaal. RDW zal hiervoor een proces opzetten met erkende relying parties. Als door partijen gebruik gemaakt wordt van de RDW uitlees- en verificatiesoftware zal het CSCA certificaat daarin opgenomen zijn (bijgeleverd worden).

Na 10 jaar zal RDW gebruik gaan maken van een nieuw CSCA certificaat. Mogelijk kan dit door omstandigheden al eerder het geval zijn. Ook het nieuwe certificaat zal op de website beschikbaar zijn. Daarnaast zal RDW een CSCA link certificaat genereren en beschikbaar stellen op de website waarin de nieuwe CSCA public key is opgenomen en dat is uitgegeven met het huidige key pair. Relying parties dienen periodiek, maar in ieder geval voor het verlopen van het huidige CSCA certificaat, het nieuwe CSCA (link) certificaat te downloaden van de website, te controleren op authenticiteit met behulp van het huidige certificaat en het nieuwe CSCA certificaat te laden en activeren in de uitlees- en verificatiesoftware. Indien RDW eerder gebruik gaat maken van een nieuw CSCA certificaat zal dit aan erkende relying parties gemeld worden.

Voor verificatie van de Nederlandse kentekencard chip dient de verificatiesoftware ook te beschikken over de meest recente CRL op basis waarvan de revocatie status van een DS certificaat van de chip gecontroleerd kan worden. De CRLs zijn te downloaden van de RDW website. De authenticiteit van een CRL dient gecontroleerd te worden met het CSCA public key certificaat dat gebruikt is voor ondertekening van de CRL. Een CRL is 200 dagen geldig en wordt iedere 180 dagen opnieuw uitgegeven. Relying parties dienen periodiek, minimaal eens in de 200 dagen, een nieuwe CRL van de website te downloaden voor gebruik in de uitlees- en verificatiesoftware. RDW kan ook tussentijds een nieuwe CRL uitgeven als daar aanleiding toe is. Erkende relying parites zullen hiervan op de hoogte gesteld worden. Deze relying parties dienen dan onmiddelijk na de berichtgeving de nieuwe CRL te gaan gebruiken in de uitlees- en verificatiesoftware.

Mogelijk zal RDW op termijn ook CSCA certificaten en CRLs (en eventueel DS certificaten) voor verificatie van buitenlandse kentekencards beschikbaar stellen.

App 1 LOGICAL DATA STRUCTURE

App 1.1 Overzicht van Elementary Files

File ID	File Name	Description
00 0D	EF.AA	Active Authentication Public Key Info
00 1D	EF.SOd	Document Security Object
C0 01	EF.C.IA_A.DS	X.509v3 certificaat van de uitgevende instantie dat gebruikt wordt voor het controleren van de handtekening in EF.Signature_A (zie [1]).
C0 11	EF.C.IA_B.DS	X.509v3 certificate van de uitgevende instantie dat gebruikt wordt voor het controleren van de handtekening in EF.Signature_B (zie[1]).
D0 01	EF.Registration_A	Registratie data volgens hoofdstukken II.4 en II.5 van [1].
D0 11	EF.Registration_B	Registratie data volgens hoofdstuk II.6 van [1].
D0 21	EF.Registration_C	Additionele registratiedata en evt. CVO data.
E0 01	EF.Signature_A	Elektronische handtekening over de volledige data van EF.Registration_A (zie [1]).
E0 11	EF.Signature_B	Eleketronische handtekening over de volledige data van EF.Registration_B (zie [1]).

Tabel 1: File identifiers in de NL-eVRD applicatie

App 1.2 EF.AA

De structuur van EF.AA is identiek aan die van het elektronisch rijbewijs (ISO/IEC 18013-3:2009, section 8.4.2 [2])
Tag=tag, Len=Length, Val=Value. De lengte wordt niet gespecificeerd maar wordt berekend tijdens constructie van het TLV object.

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)	

Tabel 2: Format van EF.AA.

App 1.3 EF.SOd

De twee tabellen hieronder definiëren het Document Security Object (SOd).
De SOd is een CMS Signed Data object (RFC 5652 [6]). De twee tabellen hieronder kunnen gezien worden als het gekozen profiel voor het CMS Signed Data object en geven aan welke specifieke keuzes gemaakt zijn, plus enige additionele informatie: het eerste nummer in iedere rij is de (hexadecimale) tag voor het TLV-veld (tag value '??' geeft aan dat de tag af te leiden is uit de inhoud); waar dat van toepassing is, wordt de waarde voor een veld aangegeven.
De betekenis van de 'Gebruik' kolom is als volgt: m=mandatory (verplicht), x=must not be used (dient niet gebruikt worden), c=conditional (conditioneel).
Merk op dat de structuur van een CMS Signed Data object tamelijk complex is, waaronder verschillende keuzemogelijkheden, sets en reeksen. In geval van twijfel dienst RFC 5652 [6] geraadpleegd te worden.
Merk ook op dat de uiteindelijke handtekening berekend wordt *na* het vervangen van het tag nummer.
Behalve voor de velden Certificate(Choices), Issuer, en rSASSA-PSS-SHA256-Params s, wordt de volledige TLV boomstructuur voor de SOd hieronder aangegeven.
De volledige SOd moet DER geëncodeerd worden (RFC 5652 [6] staat ook oneindige lengte BER encoding toe om compatibel te zijn met verouderde tape drive apparatuur).
De keuze voor sid is issuerAndSerialNumber (volgens de elektronische rijbewijs [2] en paspoort standaarden [3]), maar merkt op dat volgens RFC 5652 [6] de alternatieve optie subjectKeyIdentifier voor sid ook door implementaties ondersteund moet worden.
De huidige voorkeur voor het RSA signature algoritme is PKCS#1v1.5, maar de optie om in plaats daarvan gebruik te maken van RSA-PSS wordt open gelaten. Hetzelfde signature algoritme moet gebruikt worden voor de handtekeningen over het CSCA certificaat, DS certificaat, Signature_A, Signature_B en de SOd.

Veldnaam								Ge-bruik	Referentie sectie (in RFC 5652 [6])	Waarde van het veld	Commentaar
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			Slechts één digest algoritme is nodig
			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		RDWldsSecurityObject	OCTEST STRING, zie volgende tabel (Tabel 4) voor waarden
			A0	Certificates				m	5.1, 10.2.3		
				??	CertificateChoices			m	10.2.2	Certificate	Dit is het DS X.509 certificaat (beginnend met tag '30'), zie RFC 5280 [4]
				--	...			x			Er is slechts één certificaat nodig
			--	Crls				x			CRLs worden niet gebruikt
			31	signerInfos				m	5.1		
				30	SignerInfo			m	5.3		
					02	Version		m	5.3, 10.2.5	1 (sid=issuerAndSerialNumber), or	INTEGER waarde hangt af van de keuze voor

Veldnaam										Ge-bruik	Referentie sectie (in RFC 5652 [6])	Waarde van het veld	Commentaar
												3 (sid=subjectKeyIdentifier)	sid
					…	Sid				-			Formeel dient gekozen te worden tussen OF issuerAndSerialNumber OF subjectKeyIdentifier. In de praktijk wordt issuerAndSerialNumber gebruikt.
					30	…	issuerAndSerialNumber			c			
							??	issuer		m	4.1.2.4 in RFC 5280 [4]		Issuer DN Name van DS X.509 certificaat (beginnend met tag '30')
							02	serialnumber		m	4.1.2.2 in RFC 5280 [4]	CertificateSerialNumber	INTEGER Serial Number van DS X.509 certificaat
					A0	…	subjectKeyIdentifier			c			subjectKeyIdentifier is hier alleen opgenomen om conform te zijn aan RFC 5652 [6], maar wordt in de praktijk niet gebruikt.
							04	SubjectKeyIdentifier		m	4.2.1.2 in RFC 5280 [4]		subjectKeyIdentifier is hier alleen opgenomen om conform te zijn aan RFC 5652 [6], maar wordt in de praktijk niet gebruikt. OCTET STRING subject key identifier uit DS X.509 certificaat 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		

Veldnaam	Ge-bruik	Referentie sectie (in RFC 5652 [6])	Waarde van het veld	Commentaar
06 attrType	m	11.1	id-contentType ::= 1.2.840.113549.1.9.3	OID
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		Slechts één AttributeValue is hier toegestaan
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		Deze OCTET STRING bevat de hash waarde over de *waarde* van het eContent OCTET STRING (bijv. over het RDWldsSecurityObject).
-- …	x	11.2		Slechts één AttributeValue is hier toegestaan
-- …	x			Meer Attributes zijn niet nodig
30 signatureAlgorithm				
06 Algorithm	c	2.1 in RFC 4055 [9]	sha256WithRSAEncryption ::= 1.2.840.113549.1.1.11	Conditioneel: dit veld gebruiken als het signature algoritme PKCS#1v1.5 is.
05 Parameters	c	5 in RFC 4055 [9]	null	Conditioneel: dit veld gebruiken als het signature algoritme PKCS#1v1.5 is. Hier moeten de parameters op NULL gezet worden.
06 Algorithm	c	RFC 4055 [9]	id-RSASSA-PSS ::= 1.2.840.113549.1.1.10	Conditioneel: dit veld gebruiken als het signature algoritme RSA-PSS is.
30 Parameters	c	RFC 4055 [9]	rSASSA-PSS-SHA256-Params structure	Conditioneel: dit veld gebruiken als het signature algoritme RSA-PSS is. RSA PSS parameters moeten gebruikt worden (mgf1, SHA256, saltlength 32).

Veldnaam							Ge-bruik	Referentie sectie (in RFC 5652 [6])	Waarde van het veld	Commentaar
					04	Signature	m	11.2, 5.5		Deze OCTET STRING bevat de signature over het signedAttrs TLV vels *alsof dat geëncodeerd was als EXPLICIETe TAG VAN (d.w.z. vervang de leidende tag 'A0' door '31')*.
					--	unsignedAttrs	x			Er zijn geen ongetekende attributen nodig
				--	…		x			Slechts één signerInfo is nodig.

Tabel 3: Format van EF.SOd.

Veldnaam							Ge-bruik	Waarde van veld	Commentaar
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		Dit is de two-byte OCTET STRING file-identifier
			04	dataGroupHashValue			m		Dit is de 32-byte OCTET STRING SHA-256 hash van een datagroup
		30	…				m		Herhalen voor iedere datagroup, volgorde op basis van file ID

Tabel 4: Format van RDWIdsSecurityObject

App 1.4 EF.C.IA_A.DS

Conform 2003/127/EC is de inhoud van deze data group een X.509v3 geformatteerd DS certificaat gebruikt om de EF.Signature_A handtekening te genereren over de data in EF.Registration_A. Het certificaat profiel voor het DS certificaat is gedefinieerd in de CP/CPS [5].

App 1.5 EF.C.IA_B.DS

Conform 2003/127/EC is de inhoud van deze data group een X.509v3 geformatteerd DS certificaat gebruikt om de EF.Signature_B handtekening te genereren over de data in EF.Registration_B. Het certificaat profiel voor het DS certificaat is gedefinieerd in de CP/CPS [5].

App 1.6 EF.Registration_A

Conform 2003/127/EC is de inhoud van deze data group in BER-TLV structuur geformatteerd volgens het profiel in 2003/127/EC Annex I, III.11, Tabel 2 [1].

tag				code	Beschrijving van veld	EU m/o	NL m/x	Corresponderend DD10 XML element	Typische waarde van veld op de 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	Beschrijving van veld	EU m/o	NL m/x	Corresponderend DD10 XML element	Typische waarde van veld op de 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"

Tabel 5: Format van EF.Registration_A

App 1.7 EF.Registration_B

Conform 2003/127/EC is de inhoud van deze data group in BER-TLV structuur geformatteerd volgens het profiel in 2003/127/EC Annex I, III.11, Tabel 3 [1].

tag				code	Beschrijving van veld	EU m/o	NL m/x	Corresponderend DD10 XML element	Typische waarde van veld op de 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	Beschrijving van veld	EU m/o	NL m/x	Corresponderend DD10 XML element	Typische waarde van veld op de 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"
	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		

Tabel 6: Format van EF.Registration_B

App 1.8 EF.Registration_C

Tag	L	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
	…	…	…	…	…

Tabel 7: Format van EF.Registration_C

App 1.8.1 Registratiedata

EF.Registration_C bevat altijd registratiedata zoals weergegeven in Tabel 8. Dit bevat als toevoeging op de data uit EF.Registration_A de datum van eerste registratie in Nederland.

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

Tabel 8: Format van registratiedata in EF.Registration_C

App 1.8.2 Individual Vehicle Information

EF.Registration_C bevat een willekeurig aantal (0, 1, 2, 3, ...) IndividualVehicleInformation data elementen. Voor iedere van toepassing zijnde COC/CvO zal er een IndividualVehicleInformation data element zijn. Per individueel IndiviualVehicleInformation data element zijn er drie keuzes toegestaan voor formats en slechts een representatie (XML, Compressed XML of TLV) zal aanwezig zijn (per individueel 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

Tabel 9: Format van Individual Vehicle Information

App 1.8.2.1 IndividualVehicleInformation (XML)

XML encoded Vehicle Information zal nog gespecificeerd worden.

App 1.8.2.2 IndividualVehicleInformation (Compressed XML)

Tag	**L**	**Value**		
9F8704	X	Compression Algorithm Identifier (zie Tabel 11)	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

Tabel 10: Format van IndividualVehicleInformation (Compressed XML).

Identifier	**Algorithm**
0	GZIP
*	RFU

Tabel 11: Compression Algorithm Identifiers

App 1.8.2.3 IndividualVehicleInformation (TLV)

L(max) geeft de maximal toegestande lengte (in bytes) aan van het overeenkomende value veld.

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)			

Tabel 12: Format van IndividualVehicleRegistration

App 1.9 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)	

Tabel 13: Format van EF.Signature_A

De huidige voorkeur voor het RSA signature algoritme is PKCS#1v1.5, maar de mogelijkheid wordt open gelaten om in plaats daarvan gebruik te maken van RSA-PSS. Uitlees- en verificatiesoftware moet ook het RSA-PSS signature algoritme ondersteunen.
Hetzelfde signature algoritme wordt gebruikt voor de signatures over het CSCA certificaat, DS certificaat, Signature_A, Signature_B en de EF.SOd.
Merk op dat voor RSA PKCS#1v1.5 de optionele parameters verplicht de NULL value moeten hebben (RFC 4055 [9]).

App 1.10 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)	

Tabel 14: Format van EF.Signature_B

De huidige voorkeur voor het RSA signature algoritme is PKCS#1v1.5, maar de mogelijkheid wordt open gelaten om in plaats daarvan gebruik te maken van RSA-PSS. Uitlees- en verificatiesoftware moet ook het RSA-PSS signature algoritme ondersteunen.
Hetzelfde signature algoritme wordt gebruikt voor de signatures over het CSCA certificaat, DS certificaat, Signature_A, Signature_B en de EF.SOd.
Merk op dat voor RSA PKCS#1v1.5 de optionele parameters verplicht de NULL value moeten hebben (RFC 4055 [9]).

App 2 NL-eVRD Commando's en Responses

For an explanation of the Command and Response APDUs and the abbreviations used see ISO 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	XX	Length of the Data field
Data	XX ... XX	AID of the VR Application
Le	00	

Tabel 15: SELECT APPLICATION Command APDU

App 2.1.2 Response APDU

Field	Value	Description
FCI Template		
Tag	6F	
Length	XX	
DF Name		
Tag	84	
Length	XX	
Value	XX ... XX	AID of the VR Application
SW1 SW2	90 00	Successful processing

Tabel 16: Response on successful processing

Field	Value	Description
SW1 SW2	XX XX *Tabel 17: Response in case of an error condition*	See section App 2.1.3.

App 2.1.3 Status Words

Value	Description	
90 00	Successful processing	
67 00	Error: Wrong Length	Lc is smaller than 5 or bigger than 16.

		Le is not equal to 00
68 81	Error: Logical Channel not supported	CLA not equal to 00
6A 81	Error: Function not supported	The card has been blocked
6A 82	Error: File not found	The AID specified in the Command Data field is not present on the card
6A 86	Error: Incorrect parameters P1-P2	The bytes P1 P2 do not have the value 04 00.

Tabel 18: SELECT APPLICATION Status Words

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	

Tabel 19: SELECT FILE Command APDU

App 2.2.2 Response APDU

Field	Value	Description
FCP Template		
Tag	62	
Length	08	
File ID		
Tag	83	
Length	02	
Value	XX XX	File Identifier of the EF
File Size		
Tag	80	
Length	02	
Value	XX XX	Number of data bytes in the file (set at last UPDATE BINARY command during personalization)
SW1 SW2	90 00	

Tabel 20: Response on successful processing

Field	Value	Description
SW1 SW2	XX XX	See section App 2.2.3.

Tabel 21: Response in case of an error condition

App 2.2.3 Status Words

Value	Description	
90 00	Successful processing	
67 00	Error: Wrong Length	Lc is not equal to 02. Le is not equal to 00
68 81	Error: Logical Channel not supported	CLA not equal to 00
6A 81	Error: Function not supported	The card has been blocked
6A 82	Error: File not found	The EF Identifier specified in the Data field does not match with one of the values specified in App 1.1.
6A 86	Error: Incorrect parameters P1-P2	The bytes P1 P2 do not have the value 02 04.

Tabel 22: SELECT FILE Status Words

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.

Tabel 23: READ BINARY Command APDU

App 2.3.2 Response APDU

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

Tabel 24: Response on successful processing, Le bytes available

Field	Value	Description
Response Data	XX ... XX	Ne data bytes, starting at offset P1P2 Ne = length of the data in the currently selected EF – offset P1P2
SW1 SW2	62 82	Warning: End of file reached before reading Ne bytes

Tabel 25: Response on successful processing, less than Le bytes available

Field	Value	Description
SW1 SW2	XX XX	See section App 2.3.3.

Tabel 26: Response in case of an error condition

App 2.3.3 Status Words

Value	Description	
90 00	Successful processing	
62 82	Warning: End of file reached before reading Ne bytes	Offset + Le > File Size
69 86	Error: Command not allowed	no current EF
6A 81	Error: Function not supported	The card has been blocked
6A 86	Error: Incorrect parameters P1-P2	P1 > 7F
6B 00	Error: Wrong parameters P1-P2	Offset > File Size

Tabel 27: READ BINARY Status Words

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 8-byte random value generated by the off-card entity
Le	00	

Tabel 28: INTERNAL AUTHENTICATE Command APDU

App 2.4.2 Response APDU

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

Tabel 29: Response on successful processing

Field	Value	Description
SW1 SW2	XX XX	See section App 2.4.3

Tabel 30: 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 Lc is not equal to 08
69 85	Error: Conditions of use not satisfied	Active Authentication Session Flag is set or 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.

Tabel 31: INTERNAL AUTHENTICATE Status Words

App 2.5 Status Words Summary

Value	Description
90 00	Succesful processing

Tabel 32: 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)

Tabel 33: 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

Tabel 34: Status Words indicating an error condition

App 3 TRACES COMMUNICATIE UITLEES/VERIFICATIESOFTWARE & CHIP (INFORMATIEF)

De APDU traces zijn gemaakt op basis van een specimen kentekencard. De DS certificaten in de APDU trace kunnen gevalideerd worden met het CSCA certificaat uit App 4.

App 3.1 Lezen en verifieren van de Nederlandse kentekencard chip

APDU trace volgens de inspectieprocedure die gespecificeerd is in 4.2.

1. Selecteer eVRC applicatie (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. Selecteer 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. Lees EF.SOd (lengte = '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
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
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. Selecteer 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. Lees EF.AA

```
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 authenticatie

```
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. Lees en controleer data

a. Selecteer 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. Lees 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
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. Selecteer 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. Lees 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. Selecteer 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. Lees 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
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
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'
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 3.2 Lezen en verifieren van buitenlandse kentekencard chips

APDU trace volgens de inspectieprocedure die gespecificeerd is in 4.3.

Disclaimer: hierbij is aangenomen dat de kentekencard is geimplementeerd volgens de EU richtlijn; het beschrijft en mogelijke uitleesprocedure. Elk land kan een specifieke uitleesprocedure voorschrijven.

1. Selecteer eVRC applicatie (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. Selecteer EF.C.IA_A.DS (File ID = 'C0 01')

```
T→C: '00 A4 02 04 02 C0 01 00'
C→T: '62 08 83 02 C0 01 80 02 05 0B 90 00'
```

3. Lees EF.C.IA_A.DS

```
T→C: '00 B0 00 00 00'
C→T: '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 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 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 90 00'

T→C: '00 B0 01 00 00'
C→T: '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 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 90 00'

T→C: '00 B0 02 00 00'
C→T: '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 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 90 00'

T→C: '00 B0 03 00 00'
C→T: '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 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 F8 64 4A 73 1C 57 0B 95 04 AE 24 E9 24 6E 33
B3 DD 06 AA B3 90 00'

T→C: '00 B0 04 00 00'
C→T: '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 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 90 00'

T→C: '00 B0 05 00 00'
C→T: 'FD 4A 4C 9C 96 56 F0 44 33 18 74 90 00'
```

4. Selecteer EF.Signature_A ('E0 01')

```
T→C: '00 A4 02 04 02 E0 01 00'
C→T: '62 08 83 02 E0 01 80 02 01 18 90 00'
```

5. Lees EF.Signature_A

```
T→C: '00 B0 00 00 00'
C→T: '30 82 01 14 30 0D 06 09 2A 86 48 86 F7 0D 01 01 0B 05 00 03 82
01 01 00 7D B1 A9 21 8E EC 63 95 44 EF FF A2 F0 A3 EB B5 3B CE 1C 31
D2 C4 87 BF 66 CD 3E AD 5F C9 B2 53 5C C7 1A B9 D4 58 8F 63 3A 33 EC
EA 1F 27 8E D5 44 E6 42 E1 78 37 92 3F 3E 78 9C 07 8D 6F AA 3B 05 95
34 49 43 C9 AA F6 FE E1 5C BC 2A E4 24 17 25 C9 46 95 CA 1E C5 F1 EA
B3 CB E1 86 7C 65 24 A7 95 32 A2 7C 65 6C 44 9B 54 4F 23 47 A7 7C C5
41 70 2B 18 27 A2 7D 54 BE A1 19 ED 23 61 17 E7 AF 36 EF 1F BC 8E 72
63 ED 81 7B 34 26 3D 67 0C 78 CE 57 A5 EB A8 E5 99 04 07 A0 47 91 70
13 23 31 4C DF DD 49 99 8B 18 CB D2 7E A3 3C 1F 38 D2 A1 A0 05 95 28
31 46 64 D7 64 F3 19 18 A5 64 07 49 C6 46 5C 2F 59 13 1A 40 F2 51 D7
```


```
10 B5 23 FE 52 E7 1B 43 0E B1 44 D0 DD A5 ED DB FC 07 58 68 94 7D 9B
6D 6F 31 5E 94 90 00'

T→C: '00 B0 01 00 00'
C→T: 'A6 95 A9 0E 45 01 39 4A 65 C4 F6 42 98 6E 68 A7 93 0B B3 BD 64
4A 2E 2B 90 00'
```

6. Selecteer 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'
```

7. Lees 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
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'
```

8. Selecteer EF.C.IA_B.DS (File ID = 'C0 11')

```
T→C: '00 A4 02 04 02 C0 11 00'
C→T: '62 08 83 02 C0 11 80 02 05 0B 90 00'
```

9. Lees EF.C.IA_B.DS

```
T→C: '00 B0 00 00 00'
C→T: '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 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 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 90 00'

T→C: '00 B0 01 00 00'
C→T: '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 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 90 00'

T→C: '00 B0 02 00 00'
C→T: '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 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 90 00'

T→C: '00 B0 03 00 00'
C→T: '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 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 F8 64 4A 73 1C 57 0B 95 04 AE 24 E9 24 6E 33
B3 DD 06 AA B3 90 00'

T→C: '00 B0 04 00 00'
C→T: '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 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 90 00'
```


```
T→C: '00 B0 05 00 00'
C→T: 'FD 4A 4C 9C 96 56 F0 44 33 18 74 90 00'
```

10. Selecteer EF.Signature_B ('E0 11')

```
T→C: '00 A4 02 04 02 E0 11 00'
C→T: '62 08 83 02 E0 11 80 02 01 18 90 00'
```

11. Lees EF.Signature_B

```
T→C: '00 B0 00 00 00'
C→T: '30 82 01 14 30 0D 06 09 2A 86 48 86 F7 0D 01 01 0B 05 00 03 82
01 01 00 3E 6C D6 C1 E0 2A 84 40 84 18 20 56 99 BB 6A EF D0 B6 6B F3
F2 5D 60 AD 53 87 F8 77 66 1B 7D FC E0 AD 15 76 7B 16 6B 21 1E 65 2B
43 5E 55 F8 C3 14 61 4A 3A 0E 20 F6 65 90 24 04 72 56 C9 9D 0E 69 5B
38 A9 34 3A 00 6E 38 AE 81 F9 C8 DE DC E9 E6 23 7A 42 A6 D6 02 45 DB
39 A7 C4 AA 41 3C 88 CE EC D8 7B B4 14 8A D6 B6 5A ED C8 23 FC B6 92
BD 86 9B D6 77 4D A3 6F 2B 12 B1 22 7C CD E0 A1 EA AC 76 4C 94 BF B7
B5 00 74 0F 37 43 B8 A1 AA AE D0 57 C3 97 17 31 44 E8 29 32 8D FC E3
24 39 E5 25 3D F5 12 1B 99 92 41 61 24 05 72 1E CD D4 F9 10 DD 01 3E
CA C6 B0 31 B7 B1 56 F9 13 87 92 58 C1 56 5D EB 8C C5 9D 12 65 F4 F6
AD 4C 15 BF F0 4D 3E 17 CC D7 A4 42 31 BE 0B AF 24 08 C3 55 F6 49 FA
7F 58 0E 18 8A 90 00'

T→C: '00 B0 01 00 00'
C→T: 'C8 C2 2A 48 07 FB 57 C8 0C CF 75 25 5C 8D 99 D4 CF 5D 93 1B FE
2E 27 0C 90 00'
```

12. Selecteer 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'
```

13. Lees 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'
```

14. Selecteer 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'
```

15. Lees 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
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
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'
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 CERTIFICAAT

```
-----BEGIN CERTIFICATE-----
MIIGHjCCBAagAwIBAgIRAKx4L8nRF1m12piT8OIPZ+UwDQYJKoZIhvcNAQELBQAw
ZjEZMBcGA1UEAxMQQ1NDQSBHQVQgTkwgZVZSRDELMAkGA1UEBRMCMDExDDAKBgNV
BAsTA1JEVzEhMB8GA1UEChMYU3RhdGUgb2YgdGhlIE5ldGhlcmxhbmRzMQswCQYD
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-----
```