STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 2965
31 januari
2020

Regeling van de Minister van Infrastructuur en Waterstaat, van 30 januari 2020, nr. IENW/BSK-2020/5375, tot wijziging van de Regeling specificaties en typegoedkeuring boordcomputer taxi in verband met de wijziging van bijlage 4 van de Regeling specificaties en typegoedkeuring boordcomputer taxi

De Minister van Infrastructuur en Waterstaat,

Gelet op de artikelen 22, eerste en vierde lid, en 23, derde lid, van de Wegenverkeerswet 1994;

Besluit:

ARTIKEL I

Bijlage 4 van de Regeling specificaties en typegoedkeuring boordcomputer taxi wordt als volgt gewijzigd:

1. Aan de tabel 'wijzigingshistorie' wordt een nieuwe rij toegevoegd:

2.0	***jan 2020*** 1) 2) 3)	Wijzigingen naar aanleiding van transitie naar een nieuwe BCT-chip: In § 8.5 een tweede variant voor het zetten van een handtekening toegevoegd In § 8.6 een tweede variant voor het zetten van een handtekening toegevoegd In § 8.7 een tweede variant voor het zetten van een handtekening toegevoegd

2. In paragraaf 2.2 wordt na 'uitgegeven conform' ingevoegd 'het vigerende Programma van Eisen (PvE) van '.

3. De paragrafen 8.5 tot en met 8.7 komen te luiden:

8.5 Elektronische handtekening zetten met een chauffeurs- of inspectiekaart

Naam Gebruik	SignDataLegally Chauffeurskaart, Inspectiekaart
Input gegevens	Gegevens waarover handtekening berekend moet worden
Resultaat	Handtekening ll '90 00'H OK 'xx xx'H Foutcode van een van de gebruikte commando's, afhankelijk van de implementatie

Deze functie wordt gebruikt voor het door een natuurlijke persoon zetten van een rechtsgeldige elektronische handtekening met de sleutel-certificaatcombinatie PKI.CH.DS die uitsluitend op chauffeurs- en inspectiekaarten bestaat.

Elke boordcomputerkaart (chip) ondersteunt minimaal een van de twee navolgende procedures voor het uitvoeren van deze functie. De boordcomputer moet op basis van het door de chip geleverde Answer To Reset (ATR) bepalen welke van de twee procedures met de betreffende chip gebruikt moet worden. Bij chips die beide procedures ondersteunen is de boordcomputer vrij om een van beide procedures te kiezen.

Voor deze functie bestaat procedure 1 uit de volgende stappen:

1. Selectie hash template en algoritme: alvorens de digitale handtekening berekend kan worden, moet het hash template geselecteerd worden en het te gebruiken algoritme.
   Dit wordt gedaan met het commando Manage Security Environment, met P1 de waarde '41'H en P2 de waarde 'AA'H. De data bij dit commando is '80 01 40'H ('40'H om de algoritme identifier voor SHA-256 aan te geven).
2. Selectie private key en algoritme: de private key van de BCT Handtekening moet geselecteerd worden met het te gebruiken algoritme.
   Dit wordt gedaan met het commando Manage Security Environment, met P1 de waarde '41'H

en P2 de waarde ‘B6’H. De data bij dit commando is ‘80 01 42 84 01 86’H (‘42’H om ‘PKCS#1 v1.5 – SHA-256’ aan te duiden en ‘86’H om het Security Data Object (SDO) van PKI.CH.DS aan te duiden).
3. PIN valideren: de private key van de BCT Handtekening mag pas gebruikt worden nadat de PIN gevalideerd is. Dit is nodig voor iedere keer dat deze key gebruikt wordt.
   Dit wordt gedaan met het commando Verify, waarbij P2 (de PIN reference) de waarde ‘01’H heeft. Voor de PIN wordt PIN formaat 2 gebruikt (zie onder 8.1).
4. Berekenen van de intermediate hash (SHA256) over de input gegevens door de boordcomputerlogica. Hierbij wordt het laatste gegevensblok niet gehashed, maar wordt de intermediate hash en het aantal gehashte bits onthouden voor de volgende stap.
   NB. Wanneer het totaal aan input gegevens uit maximaal 64 bytes bestaat, wordt er geen intermediate hash berekend en worden alle inputgegevens in de volgende stap gebruikt.
5. Berekenen van de uiteindelijke hash (SHA256) door de boordcomputerkaart. Hiervoor wordt het commando PSO Hash gebruikt. Hierbij worden de ‘intermediate hash value’, het aantal gehashte bits en het laatste (of enige) blok inputdata van minimaal 1 en maximaal 64 bytes opgenomen in het Dataveld van het commando. Bij een succesvol uitgevoerde PSO HASH zal de uiteindelijke hash waarde in het geheugen van de boordcomputerkaart (chip) achterblijven ten behoeve van de volgende en laatste stap.
6. Handtekening berekenen: hierbij wordt met de gekozen private key de handtekening berekend over de in het chipgeheugen aanwezige hashwaarde en geeft de kaart die handtekening terug aan de boordcomputerlogica.
   Dit wordt gedaan met het commando PSO Compute Digital Signature. Le, het verwachte aantal bytes in de response, moet daarbij op ‘00’H staan.

Voor deze functie bestaat procedure 2 uit de volgende stappen (nummering gelijk aan die van procedure 1):

1. Niet van toepassing.
2. Gelijk aan stap 2 van procedure 1.
3. Gelijk aan stap 3 van procedure 1.
4. Berekenen van de volledige hash (SHA256) over de input gegevens door de boordcomputerlogica.
5. Niet van toepassing.
6. Handtekening berekenen: hierbij wordt met de gekozen private key de handtekening berekend over de in stap 4 berekende hashwaarde en geeft de kaart die handtekening terug aan de boordcomputerlogica.
   Dit wordt gedaan met het commando PSO Compute Digital Signature. Daarbij moet Lc, het aantal bytes van de input data, op ‘20’H staan, het DATA veld worden gevuld met de hashwaarde uit stap 4 (32 bytes) en Le, het verwachte aantal bytes in de response, op ‘00’H staan.

Zie ook PSO Hash en PSO Compute Digital Signature in Referentie [7].
Voor de vermelde SDO ID wordt verwezen naar de kaartstructuur documenten in Referenties [9] en [12]. Omdat dit SDO een lokaal object is, moet de in de kaartstructuur documenten gespecificeerde keyReference niet letterlijk worden overgenomen, maar met bit8 hoog (dus ‘86’H in plaats van ‘06’H).

8.6 Elektronische handtekening zetten met een systeemkaart

Naam Gebruik	SignDataSystem Systeemkaart
Input gegevens	Gegevens waarover handtekening berekend moet worden
Resultaat	Handtekening ǁ ‘90 00’H OK ‘xx xx’H Foutcode van een van de gebruikte commando’s, afhankelijk van de implementatie

Deze functie wordt gebruikt voor het door een boordcomputer zetten van een elektronische handtekening met de sleutel-certificaatcombinatie PKI.CH.AUT van de systeemkaart.

Op de systeemkaart mag deze functie alleen uitgevoerd worden onder beveiligde gegevensoverdracht (zie Hoofdstuk 4), gebruikmakend van de sleutelset SM.ICC.

Elke systeemkaart (chip) ondersteunt minimaal een van de twee navolgende procedures voor het uitvoeren van deze functie. De boordcomputer moet op basis van het door de chip geleverde Answer To Reset (ATR) bepalen welke van de twee procedures met de betreffende chip gebruikt

moet worden. Bij chips die beide procedures ondersteunen is de boordcomputer vrij om een van beide procedures te kiezen.

Voor deze functie bestaat procedure 1 uit de volgende stappen:

1. Selectie hash template en algoritme: alvorens de digitale handtekening berekend kan worden, moet het hash template geselecteerd worden en het te gebruiken algoritme.
   Dit wordt gedaan met het commando Manage Security Environment, met P1 de waarde '41'H en P2 de waarde 'AA'H. De data bij dit commando is '80 01 40'H ('40'H om de algoritme identifier voor SHA-256 aan te geven).
2. Selectie private key en algoritme: de private key van de BCT Authenticiteit moet geselecteerd worden met het te gebruiken algoritme.
   Dit wordt gedaan met het commando Manage Security Environment, met P1 de waarde '41'H en P2 de waarde 'B6'H. De data bij dit commando is '80 01 42 84 01 85'H ('42'H om 'PKCS#1 v1.5 – SHA-256' aan te duiden en '85'H om het Security Data Object (SDO) van PKI.CH.AUT aan te duiden).
3. Berekenen van de intermediate hash (SHA256) over de input gegevens door de boordcomputerlogica. Hierbij wordt het laatste gegevensblok niet gehashed, maar wordt de intermediate hash en het aantal gehashte bits onthouden voor de volgende stap.
   NB. Wanneer het totaal aan input gegevens uit maximaal 64 bytes bestaat, wordt er geen intermediate hash berekend en worden alle inputgegevens in de volgende stap gebruikt.
4. Berekenen van de uiteindelijke hash (SHA256) door de systeemkaart. Hiervoor wordt het commando PSO Hash gebruikt. Hierbij worden de 'intermediate hash value', het aantal gehashte bits en het laatste (of enige) blok inputdata van minimaal 1 en maximaal 64 bytes opgenomen in het Dataveld van het commando. Bij een succesvol uitgevoerde PSO HASH zal de uiteindelijke hash waarde in het geheugen van de systeemkaart (chip) achterblijven ten behoeve van de volgende en laatste stap.
5. Handtekening berekenen: hierbij wordt met de gekozen private key de handtekening berekend over de in het chipgeheugen aanwezige hashwaarde en geeft de kaart die handtekening terug aan de boordcomputerlogica.
   Dit wordt gedaan met het commando PSO Compute Digital Signature. Le, het verwachte aantal bytes in de response, moet daarbij op '00'H staan.

Voor deze functie bestaat procedure 2 uit de volgende stappen (nummering gelijk aan die van procedure 1):

1. Niet van toepassing.
2. Gelijk aan stap 2 van procedure 1.
3. Berekenen van de volledige hash (SHA256) over de input gegevens door de boordcomputerlogica.
4. Niet van toepassing.
5. Handtekening berekenen: hierbij wordt met de gekozen private key de handtekening berekend over de in stap 3 berekende hashwaarde en geeft de kaart die handtekening terug aan de boordcomputerlogica.
   Dit wordt gedaan met het commando PSO Compute Digital Signature. Daarbij moet Lc, het aantal bytes van de input data, op '20'H staan, het DATA veld worden gevuld met de hashwaarde uit stap 3 (32 bytes) en Le, het verwachte aantal bytes in de response, op '00'H staan.

Zie ook PSO Hash en PSO Compute Digital Signature in Referentie [7]).
Voor de vermelde SDO ID wordt verwezen naar het kaartstructuur documenten in Referentie [8]. Omdat dit SDO een lokaal object is, moet de in het kaartstructuur document gespecificeerde keyReference niet letterlijk worden overgenomen, maar met bit8 hoog (dus '85'H in plaats van '05'H).

Noot: Zie ook 5.4 (digitale handtekening).

8.7 Authenticiteit handtekening zetten met een boordcomputerkaart

Naam Gebruik	SignDataForAuthenticity Chauffeurskaart, Ondernemerskaart, Keuringskaart, Inspectiekaart
Input gegevens	Gegevens waarover handtekening berekend moet worden
Resultaat	Handtekening ll '90 00'H OK 'xx xx'H Foutcode van een van de gebruikte commando's, afhankelijk van de implementatie

Deze functie wordt gebruikt voor het door een boordcomputerkaarthouder zetten van een elektronische handtekening met de sleutel-certificaatcombinatie PKI.CH.AUT die op elke boordcomputerkaart bestaat.

Elke boordcomputerkaart (chip) ondersteunt minimaal een van de twee navolgende procedures voor het uitvoeren van deze functie. De boordcomputer moet op basis van het door de chip geleverde Answer To Reset (ATR) bepalen welke van de twee procedures met de betreffende chip gebruikt moet worden. Bij chips die beide procedures ondersteunen is de boordcomputer vrij om een van beide procedures te kiezen.

Voor deze functie bestaat procedure 1 uit de volgende stappen:

1. Selectie hash template en algoritme: alvorens de digitale handtekening berekend kan worden, moet het hash template geselecteerd worden en het te gebruiken algoritme.
   Dit wordt gedaan met het commando Manage Security Environment, met P1 de waarde '41'H en P2 de waarde 'AA'H. De data bij dit commando is '80 01 40'H ('40'H om de algoritme identifier voor SHA-256 aan te geven).
2. Selectie private key en algoritme: de private key van de BCT Authenticiteit moet geselecteerd worden met het te gebruiken algoritme.
   Dit wordt gedaan met het commando Manage Security Environment, met P1 de waarde '41'H en P2 de waarde 'B6'H. De data bij dit commando is '80 01 42 84 01 85'H ('42'H om 'PKCS#1 v1.5 – SHA-256' aan te duiden en '85'H om het Security Data Object (SDO) van PKI.CH.AUT aan te duiden).
3. PIN valideren: de private key van de BCT Authenticiteit mag pas gebruikt worden nadat de PIN gevalideerd is. Een eenmaal uitgevoerde PIN validatie mag – zo lang de kaart in de boordcomputer aanwezig blijft – worden 'herbruikt' bij elke volgende keer dat deze key gebruikt wordt.
   Dit wordt gedaan met het commando Verify, waarbij P2 (de PIN reference) de waarde '01'H heeft. Voor de PIN wordt PIN formaat 2 gebruikt (zie onder 8.1).
4. Berekenen van de intermediate hash (SHA256) over de input gegevens door de boordcomputerlogica. Hierbij wordt het laatste gegevensblok niet gehashed, maar wordt de intermediate hash en het aantal gehashte bits onthouden voor de volgende stap.
   NB. Wanneer het totaal aan input gegevens uit maximaal 64 bytes bestaat, wordt er geen intermediate hash berekend en worden alle inputgegevens in de volgende stap gebruikt.
5. Berekenen van de uiteindelijke hash (SHA256) door de boordcomputerkaart. Hiervoor wordt het commando PSO Hash gebruikt. Hierbij worden de 'intermediate hash value', het aantal gehashte bits en het laatste (of enige) blok inputdata van minimaal 1 en maximaal 64 bytes opgenomen in het Dataveld van het commando. Bij een succesvol uitgevoerde PSO HASH zal de uiteindelijke hash waarde in het geheugen van de boordcomputerkaart (chip) achterblijven ten behoeve van de volgende en laatste stap.
6. Handtekening berekenen: hierbij wordt met de gekozen private key de handtekening berekend over de in het chipgeheugen aanwezige hashwaarde en geeft de kaart die handtekening terug aan de boordcomputerlogica.
   Dit wordt gedaan met het commando PSO Compute Digital Signature. Le, het verwachte aantal bytes in de response, moet daarbij op '00'H staan.

Voor deze functie bestaat procedure 2 uit de volgende stappen (nummering gelijk aan die van procedure 1):

1. Niet van toepassing.
2. Gelijk aan stap 2 van procedure 1.
3. Gelijk aan stap 3 van procedure 1.
4. Berekenen van de volledige hash (SHA256) over de input gegevens door de boordcomputerlogica.
5. Niet van toepassing.
6. Handtekening berekenen: hierbij wordt met de gekozen private key de handtekening berekend over de in stap 4 berekende hashwaarde en geeft de kaart die handtekening terug aan de boordcomputerlogica.
   Dit wordt gedaan met het commando PSO Compute Digital Signature. Daarbij moet Lc, het aantal bytes van de input data, op '20'H staan, het DATA veld worden gevuld met de hashwaarde uit stap 4 (32 bytes) en Le, het verwachte aantal bytes in de response, op '00'H staan.

Zie ook PSO Hash en PSO Compute Digital Signature in Referentie [7].
Voor de vermelde SDO ID wordt verwezen naar de kaartstructuur documenten in Referenties [9] t/m [12]. Omdat dit SDO een lokaal object is, moet de in de kaartstructuur documenten gespecifi-

ceerde keyReference niet letterlijk worden overgenomen, maar met bit8 hoog (dus ‘85’H in plaats van ‘05’H).

ARTIKEL II

Deze regeling treedt in werking met ingang van de dag na de datum van uitgifte van de Staatscourant waarin zij wordt geplaatst.

Deze regeling zal met de toelichting in de Staatscourant worden geplaatst.

De Minister van Infrastructuur en Waterstaat,
C. van Nieuwenhuizen Wijbenga

TOELICHTING

Algemeen

Inleiding

In 2019 is er een nieuwe generatie van chips ontwikkeld voor de kaarten van de boordcomputer taxi (BCT). Geconstateerd is dat deze nieuwe generatie een van de bestaande chips afwijkende wijze van genereren van digitale handtekening heeft. Met deze regeling is daarom een wijziging aangebracht in de paragrafen 8.5 tot en met 8.7 van bijlage 4 van de Regeling specificaties en typegoedkeuring boordcomputer taxi. Met voornoemde wijziging is de specificatie van de wijze waarop de boordcomputer handtekeningen genereert als bedoeld in artikel 17, eerste lid, onder l, m en u, van de Regeling specificaties en typegoedkeuring boordcomputer taxi, aangevuld met de (nieuwe) wijze waarop de nieuwe generatie chips digitale handtekeningen genereert.

Handhaafbaarheids- en uitvoerbaarheidstoetsen

De onderhavige wijzigingsregeling is door de ILT en de RDW getoetst op handhaafbaarheid en uitvoerbaarheid, en door beide instanties handhaafbaar en uitvoerbaar bevonden. De toets door de RDW heeft geleid tot enkele tekstuele aanpassingen in de tekst.

Consultatie

De wijziging is geconsulteerd bij de betrokken partijen. De consultatie heeft niet tot reacties geleid. Om de reden dat de wijziging raakt aan de technische eisen waaraan BCT's moeten voldoen, is de ontwerpregeling tevens ingevolge richtlijn 98/34/EG ter notificatie voorgelegd. Hierop zijn evenmin reacties ontvangen.

Administratieve lasten

Deze regeling leidt niet tot administratieve lasten voor burgers en bedrijven. De groep van belanghebbenden is klein, waardoor zij snel op de hoogte zullen zijn van aanstaande wijzigingen. Het Adviescollege toetsing regeldruk (ATR) deelt de analyse dat er geen omvangrijke negatieve gevolgen zijn voor de regeldruk. Om die reden heeft het ATR geen formeel advies uitgebracht.

Inwerkingtreding

Deze regeling treedt in werking met ingang van de dag na de datum van uitgifte van de Staatscourant waarin zij wordt geplaatst. Van het besluit van het kabinet inzake vaste verandermomenten van regelgeving wordt afgeweken omdat het wenselijk is dat de specificatie van de wijze waarop de boordcomputer handtekeningen genereert, zo spoedig mogelijk wordt aangevuld met de wijze waarop de nieuwe generatie chips digitale handtekeningen genereert.

De Minister van Infrastructuur en Waterstaat,
C. van Nieuwenhuizen Wijbenga