RDW CPS

RDW Certification Practice Statement

RDW
Europaweg 205
2711 ER ZOETERMEER
Postbus 777
2700 AT ZOETERMEER

Oktober 2004

RDW CPS

RDW Certification Practice Statement

Titel:	RDW Certification Practice Statement.
Code:	rdw-cps-v3.4.doc
Versie/datum:	3.4 / 14 oktober 2004
Autorisatie:	Directie RDW;
Datum ingang:	1 november 2004;
Onderhoud:	RDW/ICT/BB;
Classificatie:	openbaar;
Aantal pagina's:	39;
Print Datum:	

Inhoudsopgave.

1. Inleiding.

1.1 Algemeen

Dit Certification Practice Statement is opgesteld als raamwerk voor de toepassing van certificaten die worden uitgegeven door de RDW Centrum voor Voertuigtechniek en Informatie. De RDW geeft digitale certificaten uit binnen haar eigen Public Key Infrastructuur (PKI). Hierbij treedt de RDW zelf op als Certification Authority (CA).

De certificaten van eind-entiteiten worden uitgegeven door de RDW Diensten Certification Authority. Dit CPS beschrijft de procedures, technieken en juridische randvoorwaarden die de RDW hanteert bij het beheer de RDW PKI.

De structuur van dit CPS is in overeenstemming met de internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 2527) van de PKIX werkgroep van de IETF.

Een verklarende woordenlijst is opgenomen als bijlage.

1.2 Identificatie

De naamgeving van dit CPS is de "RDW Certification Practice Statement". Prospect aanvragers kunnen bij de RDW een kopie aanvragen van dit CPS. Er is geen object identifier aan dit CPS toegekend of geregistreerd.

1.3 Bij RDW-PKI betrokken partijen en toepasbaarheid

1.3.1 Certification Authority

De RDW PKI bestaat uit verschillende certificaatketens. Elke CA binnen de RDW PKI handelt conform specifieke procedures die in verband staan met hun taak. Binnen de RDW PKI zijn de volgende CA's operationeel:

- RDW Root
- RDW Diensten
- RDW Services

De RDW Root is de CA die het eerste certificaat uitgeeft binnen een certificaatketen.
De Root CA ondertekent de certificaten van de onderliggende CA's binnen de RDW PKI.

De RDW Diensten CA en de RDW Services CA zijn de CA's die certificaten uitgeven aan eind-entiteiten binnen de RDW PKI. Deze CA's worden in de rest van dit document de Issuing CA's genoemd. Waar relevant worden de bepalingen in de rest van dit CPS verbijzonderd naar de verschillende CA's.

1.3.2 Regelingen

De basis voor het verstrekken van een RDW-certificaat kan een wettelijke regeling dan wel beheersregeling zijn. In het vervolg van het CPS wordt slechts gesproken van wettelijke regeling of beheersregeling.

1.3.3 Registration Authority

Binnen de RDW zijn diverse Registration Authorities operationeel.

1 Unit Erkenning en Toezicht
Voor certificaten die worden uitgegeven aan erkenninghouders ten behoeve van de RDW-diensten Online Registratiebedrijfsvoorraad en Tenaamstellen Voertuigen treedt de Unit Erkenning en Toezicht op als Registration Authority.

2 Afdeling Voertuigtechniek
Voor certificaten die worden uitgegeven aan erkenninghouders ten behoeve van het online aanmelden van APK en wijziging constructie (inbouw LPG-installaties, inbouw tachografen, inbouw snelheidsbegrenzers) treedt afdeling Voertuigtechniek op als Registration Authority.

3 Unit Klantenbeheer en Informatie
Voor certificaten die worden uitgegeven aan partijen die niet onder een van de hiervoor genoemde regelingen vallen, treedt de Unit KBI op als Registration Authority.

1.3.4 Eind-entiteiten

Als eind-entiteiten binnen de RDW PKI worden aangemerkt: aanvragers en certificaathouders, die geen RA of CA zijn. De binnen de RDW PKI operationele eind-entiteiten zijn:

1 **Aanvragers**
Alle rechtspersonen die online toegang wensen tot RDW-applicaties, waaronder rechtspersonen en natuurlijke personen, verzekeraars en gevolmachtigden, organisaties zonder registratie in het Handelsregister of de RDW in het kader van regelingen als genoemd onder 1.3.2..

2 **Certificaathouders**
De aanvragers die op basis van de regelingen als genoemd onder 1.3.2. door de RDW geautoriseerd zijn voor toegang tot de RDW-applicaties.

1.3.5 Toepasbaarheid

Bij de uitgifte van een certificaat wordt benadrukt voor welke toepassing het certificaat dient. Er worden de volgende certificaattypen onderscheiden:

1. Certificaten uitgegeven door de RDW Diensten CA
   - 1.1. Productie certificaten t.b.v. eind-entiteiten
     De uitgegeven productiecertificaten ten behoeve van eind-entiteiten binnen de RDW PKI zijn uitsluitend bedoeld voor identificatie en authenticatie van de eind-entiteit ten behoeve van:
     - 1.1.1. toegang tot RDW-applicaties,
     - 1.1.2. het raadplegen en wijzigen van registers die door de RDW bij of krachtens wettelijke taak worden beheerd en waarvoor de RDW verantwoordelijk is,
     - 1.1.3. toegang tot applicaties door eind-entiteiten (al dan niet) beheerd door RDW erkende applicatie communicatieproviders die gerelateerd zijn aan RDW-applicaties of registers zoals genoemd in de vorige twee punten
     - 1.1.4. het beveiligen van gegevensuitwisseling tussen eind-entiteiten en de RDW.
   - 1.2. RDW Server Certificaten
     Server certificaten worden uitsluitend uitgegeven aan de RDW ten behoeve van het opzetten van een beveiligde verbinding tussen communicatieproviders en de RDW en/of, eind-entiteiten en de RDW.
   - 1.3. Productie-Acceptatie certificaten
     Productie-acceptatie certificaten zijn uitsluitend bedoeld voor identificatie en authenticatie van eind-entiteiten voor toegang tot de RDW-acceptatie omgeving ten behoeve van het uitvoeren van ketentesten.

2. Certificaten uitgegeven door de RDW Services CA
   RDW Services zijn uitsluitend bedoeld voor identificatie en authenticatie van eind-entiteiten ten behoeve van toegang tot RDW-applicaties.

1.4 Contact gegevens

1.4.1 Verantwoordelijke organisatie

De RDW is verantwoordelijk voor het beheer van dit CPS

1.4.2 Contactpersoon

De volgende personen zijn bij RDW verantwoordelijk voor het beheer (onderhoud en interpretatie) van dit CPS.

RDW RA	RDW RA
Bureau Erkenningen en Toezicht	Afdeling Voertuigtechniek
Postbus 30000	Postbus 777
9640 RA Veendam	2700 AT Zoetermeer
tel: 0598 – 699815	tel: 0900 - 0739

Zie ook:
http://www.rdw.nl/ned/04_profiel/index_adressen.htm

1.4.3 Persoon die toepasbaarheid CPS bepaalt Certificate Policies (CPs)

De RDW maakt geen gebruik van Certificate Policies. Uitwerking van de voorwaarden die verbonden zijn aan het gebruik van certificaten zijn neergelegd in deze CPS.

2. Algemene Bepalingen.

2.1 Verplichtingen.

Dit hoofdstuk bevat een omschrijving van de verplichtingen van alle entiteiten binnen de RDW PKI.

2.1.1 Verplichtingen van de Root CA

De RDW Root is een entiteit die certificaten uitgeeft aan de onderliggende Certification Authorities. De Root CA ondertekent zelf zijn eigen publieke sleutel.

De RDW Root CA heeft de volgende verplichtingen binnen de RDW PKI:

1. De RDW Root CA handelt in overeenstemming met de bepalingen van dit CPS.
2. De RDW Root CA zorgt voor een adequate bescherming van zijn privé-sleutel zoals beschreven in par 6.2 van dit CPS.
3. Ingeval van verlies of compromittering van zijn privé-sleutel stelt de Root CA alle entiteiten binnen de RDW PKI hiervan op de hoogte.

2.1.2 Verplichtingen van de RDW Issuing CA's

De CA heeft de volgende verplichtingen binnen de RDW PKI:

1. De CA handelt in overeenstemming met de bepalingen van dit CPS.
2. De CA zorgt voor een adequate bescherming van zijn privé-sleutel zoals beschreven in par 6.2 van dit CPS.
3. Ingeval van verlies of compromittering van zijn privé-sleutel stelt de CA alle entiteiten binnen de RDW PKI hiervan op de hoogte.
4. Indien een certificaat ongeldig is geworden zal de CA zorgdragen voor het opnemen van dit certificaat in een Certificate Revocation List (CRL).
5. De CA draagt zorg voor de publicatie van deze CRL.
6. De CA gebruikt zijn privé-sleutel uitsluitend voor het uitgeven van certificaten en het digitaal ondertekenen van CRL's zoals in dit CPS is omschreven.
7. De verwerking van persoonsgegevens door de CA geschiedt conform de Wet bescherming persoonsgegevens.

2.1.3 Verplichtingen van de RA

De RA heeft de volgende verplichtingen binnen de RDW PKI:

1. De RA handelt in overeenstemming met de bepalingen van dit CPS.
2. De RA verricht de noodzakelijke validatie- en authenticatieprocedures en zal hierbij de gegevens in de certificaataanvraag die RA heeft ontvangen van de aanvragers, correct weergeven.
3. De verwerking van persoonsgegevens door de CA geschiedt conform de Wet bescherming persoonsgegevens.

2.1.4 Verplichtingen van de eind-entiteit

De eind-entiteit heeft de volgende verplichtingen binnen de RDW PKI:

1. De certificaathouder zorgt voor een adequate bescherming en beveiliging van de CD-rom of diskette dan wel online voor services certificaten waarop zijn certificaat en privé-sleutel zijn opgeslagen en van de brief met wachtwoord ten behoeve van de installatie van deze CD-rom of diskette.
2. De certificaathouder zorgt voor een adequate bescherming van zijn privé-sleutel en van het wachtwoord die in samenhang met de privé-sleutel toegang geeft tot RDW-applicaties, zoals beschreven in par 6.2. van dit CPS.
3. In geval van verlies of diefstal van de CD-rom of diskette dan wel online voor services certificaten en het wachtwoord ten behoeve van de installatie van de CD-rom of diskette en/of ingeval van compromittering of verlies van de privé-sleutel en/of van het wachtwoord die in samenhang met de privé-sleutel toegang geeft tot de RDW-applicaties, stelt de houder van dat certificaat onmiddellijk de CA hiervan op de hoogte (zie par. 4.4.3).
4. De certificaathouder zal het certificaat en het hierbij behorende sleutelpaar uitsluitend gebruiken voor het doel zoals omschreven in paragraaf 1.3.4 (toepasbaarheid).
5. De eind-entiteit garandeert de juistheid van de gegevens bij de aanvraag van een certificaat.
6. Indien de inhoud van een certificaat en/of voor de inhoud van het certificaat relevante gegevens niet (meer) overeenkomen met de werkelijkheid, zal de eind-entiteit de RA hiervan onverwijld op de hoogte stellen (zie par. 1.4 en par. 7.1).

2.1.5 Verplichtingen van relying party

Binnen de RDW worden als relying party aangemerkt:

- De RDW zelf bij de beveiliging van de datacommunicatie ten behoeve van het wijzigen en raadplegen van registers, die door de RDW bij of krachtens wettelijke taak worden beheerd.

1. Door gebruik te maken van het RDW eind-entiteit certificaat erkent de relying party op de hoogte te zijn van de bepalingen in dit CPS.
2. De relying party en door de RDW erkende providers zijn verplicht na te gaan dat een eind-entiteit certificaat geldig is, door:
   - Verificatie van de digitale handtekening op het eind-certificaat en van de certificaten in het certificatie pad waaronder het eind-certificaat is afgegeven.
   - Verificatie dat het eind-certificaat niet gerevokeerd is door gebruik te maken van een geldige Certificate Recovation List verstrekt door de RDW, zie paragraaf 4.4.
3. De relying party en door de RDW erkende providers accepteren door het gebruik van een RDW eind-entiteit certificaat de limitering van aansprakelijkheid en garanties zoals beschreven in dit CPS, alsmede de bepalingen uit de gebruiksvoorwaarden en de overige bij de uitreiking van het certificaat verstrekte informatie. Indien van toepassing gelden aanvullend de bepalingen uit de aansluitvoorwaarden communicatie- en informatieproviders, voor zover deze van toepassing zijn op de beveiligde datacommunicatie.

2.1.6 Verplichtingen ten aanzien van de repository

De repository met uitgegeven certificaten wordt niet gepubliceerd of beschikbaar gesteld aan partijen buiten de RDW. Per RDW Issuing CA wordt de lijst met ingetrokken certificaten (CRL) gepubliceerd en ter beschikking gesteld ten behoeve van de vaststelling van de geldigheid van een certificaat.

2.2 Aansprakelijkheid

2.2.1 Aansprakelijkheid van de CA

De CA garandeert zijn dienstverlening uit te voeren conform dit CPS.

2.2.2 Uitsluiting van aansprakelijkheid

RDW is niet aansprakelijk voor schade, direct of indirect voortvloeiend uit het gebruik van een RDW certificaat voor andere doeleinden dan waarvoor het is uitgegeven (zie par. 1.3.4).

2.2.3 Aansprakelijkheid van de als RA optredende entiteiten

De RA's en de namens de RA optredende organisatie-onderdelen garanderen hun dienstverlening uit te voeren conform dit CPS.

2.2.4 Aansprakelijkheid van eind-entiteiten

De certificaathouder is aansprakelijk voor schade voortvloeiend uit aan hem toerekenbaar handelen in strijd met zijn verplichtingen zoals beschreven in par. 2.1.4.

2.2.5 Aansprakelijkheid van relying parties

De relying party en door de RDW erkende providers zijn aansprakelijk voor schade voortvloeiend uit aan hem toerekenbaar handelen in strijd met zijn verplichtingen zoals beschreven in par. 2.1.5.

2.3 Financiële verantwoordelijkheden

2.3.1 Vrijwaring door relying parties

Niet van toepassing.

2.3.2 Fiduciare relaties

Niet van toepassing.

2.3.3 Administratieve procedures

Niet van toepassing.

2.4 Interpretatie en handhaving

1. Op de bepalingen in dit CPS en op de RDW-gebruikersvoorwaarden is Nederlands recht van toepassing.
2. Indien een van de bepalingen van dit CPS in strijd met de wet zou blijken te zijn, blijven de overige bepalingen van dit CPS onverminderd van kracht, voor zover deze bepalingen, gelet op de inhoud en de strekking van die bepalingen, niet in onverbrekelijk verband met die bepalingen staan.
3. Alle geschillen voortvloeiend uit of verband houdend met CPS en/of gebruikersvoorwaarden worden beslecht door de bevoegde rechter te Groningen.
4. Alvorens een geschil voor te leggen aan de bevoegde rechter zullen partijen proberen om samen in goed overleg tot een oplossing te komen.

2.5 Kosten

1 Voor de instandhouding van de beveiliging van de on-line aansluiting wordt jaarlijks een beveiligingstarief in rekening gebracht. Dit tarief is te vinden in de Staatscourant onder het tarievenbesluit RDW.

2 Voor onderstaande zaken worden - naast genoemd beveiligingstarief - geen verdere kosten in rekening gebracht:
- 2.1 het feitelijk gebruik van het certificaat,
- 2.2 het aanvragen van de CPS,
- 2.3 periodieke vernieuwing van certificaten,
- 2.4 intrekken van een certificaat op verzoek van de houder,
- 2.5 intrekken en vernieuwen van een certificaat op verzoek van de houder (zoals in situaties beschreven in par. 2.1.4 artikel 3),
- 2.6 het opvragen van Certificate Revocation Lists (CRL's)..

3 Kosten van niet gebruikte certificaten worden niet vergoed.

2.6 Publicatie en repository

1. De lijst met uitgegeven certificaten wordt niet gepubliceerd of beschikbaar gesteld aan partijen buiten de RDW.
2. De Issuing CA's publiceren elk een CRL iedere keer als een eind-entiteit certificaat wordt ingetrokken en minimaal één keer per 24 uur.
3. De CRL heeft een geldigheidsduur van 120 uur.
4. De publicatie van de CPS geschiedt volgens de bepalingen in paragraaf 8.

2.7 Audit

1. Jaarlijks vindt een audit plaats waarbij wordt nagegaan of de bepalingen in dit CPS door de CA en RA worden nageleefd.
2. De audit zal worden uitgevoerd door een onafhankelijke IT-Auditor (RE).
3. De auditor zal volledig onafhankelijk zijn en op geen enkele wijze verbonden zijn aan de partij die het voorwerp is van de audit.
4. De naleving van dit CPS en de bijbehorende procedures en technieken in opzet, bestaan en werking zijn het object van de audit.
5. Indien er naar aanleiding van de audit onvolkomenheden of gebreken worden vastgesteld, zal de RDW zo spoedig mogelijk tot herstel van deze onvolkomenheden of gebreken overgaan.
6. Nadat herstel van de onvolkomenheden of gebreken heeft plaatsgevonden zal er opnieuw een audit plaatsvinden.
7. De resultaten van de audit zijn terug te vinden in het jaarverslag van de RDW.

2.8 Vertrouwelijkheid

1. Onder vertrouwelijke informatie wordt verstaan:
   1.1. persoonsgegevens,
   1.2. correspondentie met eind-entiteiten
   1.3. privé-sleutels en de hierbij behorende wachtwoorden,
   1.4. gegevens over de certificaathouder zoals de RDW die registreert in het kader van de wettelijke regelingen en beheersregeling(en) (indien van toepassing),
   1.5. bedrijfs- of fabricage gegevens,
   1.6. redenen van de intrekking van een certificaat
   1.7. audit logs
   1.8. gedetailleerde documentatie inzake het beheer van de RDW PKI
   1.9. audit rapporten door interne of externe auditors.
2. Als niet vertrouwelijke informatie wordt alle overige informatie aangemerkt.
3. De reden van intrekking van een certificaat wordt niet aan derden verstrekt.
4. Vertrouwelijke informatie wordt niet vrijgegeven, tenzij hiertoe een wettelijke plicht bestaat.
5. Certificaathouders die inzage wensen in hun persoonsgegevens, dienen hiertoe een verzoek in te dienen bij de RDW. Het verzoek dient schriftelijk naar de RA te worden gestuurd (zie par. 1.4).
6. De RDW behoudt zich het recht voor, om tot het vrijgeven van vertrouwelijke informatie over te gaan op grond van andere omstandigheden, die naar haar oordeel daartoe aanleiding kunnen geven. Alvorens tot vrijgeven van informatie wordt overgegaan zullen betrokkenen in de gelegenheid worden gesteld om hun zienswijze kenbaar te maken.

2.9 Intellectuele eigendomsrechten

1. Het auteursrecht met betrekking tot dit CPS berust bij de RDW.
2. De CA is rechthebbende ten aanzien van het openbaren, verveelvoudigen of iedere andere beheersactiviteit met betrekking tot de certificaten die hij heeft uitgegeven.
3. Binnen de RDW PKI berusten alle rechten, die mogelijkerwijs kunnen worden gevestigd op sleutelparen, bij de CA.

3. Identificatie en authenticatie.

3.1 Initiële registratie

3.1.1 Naamgeving

Elke entiteit heeft een Distinguished Name (DN) die is opgenomen in het "certificate subject name" veld, zoals gedefinieerd in de X.500 standaard voor DN's. Het onderscheid tussen RDW-certificaten uitgegeven op basis van de wettelijke regelingen is aangebracht in de Common Name (Cn)* Zie voor de certificaatprofielen paragraaf 7.1.1..

De volgende certificaatnaamgeving wordt gehanteerd:

CA	Root	Issuing	end entity
issuer E			
Issuer CN	SS	RDW Root	RDW Diensten
Issuer O	RDW	RDW	RDW
Issuer L	Groningen	Groningen	Groningen
Issuer C	NL	NL	NL
subject E			
subject CN*	RDW Root	RDW Diensten	RDW Diensten-KvK
subject CN*	RDW Root	RDW Diensten	RDW Diensten-CRWAM-code
subject CN*	RDW Root	RDW Diensten	RDW Acceptatietest-KvK
Subject CN *	RDW Root	RDW Diensten	RDW Diensten-uniek RDW nummer
Subject CN *	RDW Root	RDW Services Certificaten	(De door de certificaathouder gekozen naamgeving)
subject O	RDW	RDW	Relatie ID
subject L	Groningen	Groningen	
Subject C	NL	NL	NL
Descriptive name			SubjectO/subjectCN

3.1.2 Zinvolle naamgeving

De namen die gebruikt worden binnen de RDW PKI komen overeen met de entiteit. De namen zijn door de relying party en door de RDW erkende providers uniek identificeerbaar met de entiteit.

3.1.3 Regels voor het interpreteren van de naamgeving

Zie paragraaf. 3.1.1.

3.1.4 Unieke naamgeving

Alle gecertificeerde namen zijn uniek.

3.1.5 Geschillenbeslechting ten aanzien van de naamgeving

Voor geschillenbeslechting ten aanzien van naamgeving geldt de procedure zoals beschreven in par. 2.4, artikel 3.

3.1.6 Regels ten aanzien van merkenrechten

Voor regels ten aanzien van merkenrechten geldt de procedure zoals beschreven in par. 2.4 artikel 3.

3.1.7 Aantonen bezit van een privé-sleutel

Omdat de privé-sleutel als onderdeel van het certificaat aan de eind-entiteit op aanvraag wordt toegezonden (zie par. 4.2.), wordt vermoed dat de entiteit binnen twee weken na verzending in het bezit is van de privé-sleutel.

3.1.8 Authenticatie door de betrokken RA's

Voor wat betreft de procedure voor het aanvragen van een certificaat bij de betrokken RA zal worden aangesloten bij de reeds bestaande procedures binnen de RDW.

1 Authenticatie van aanvragers op basis van de wettelijke regeling(en)

- De initiële authenticatie van de aanvrager door de RA vindt plaats als onderdeel van de procedure die wordt gehanteerd in het geval een bedrijf in aanmerking wenst te komen voor een erkenning als bedoeld in de artikelen 62, 83 en 100, Wegenverkeerswet 1994 (erkenning bedrijfsvoorraad, APK-keuringen, inbouw LPG-installaties, inbouw tachografen, inbouw snelheidsbegrenzers, en kentekenplaat fabrikant). De vaststelling van de identiteit en de authenticiteit van de aanvrager geschiedt op basis van een uittreksel uit het handelsregister, bedoeld in artikel 2 van de Handelsregisterwet 1996 van de Kamer van Koophandel, dat de aanvrager aan de RA dient te verstrekken.

- De initiële authenticatie van de aanvrager door de RA, op basis van schriftelijke aanmelding door de Pensioen- & Verzekeringskamer, vindt plaats als onderdeel van de procedure tot het invoeren van de betreffende verzekeraar in het WAM register, als bedoeld in artikel 13, lid 2, Wet aansprakelijkheidsverzekering motorrijtuigen. De vaststelling van de identiteit en de authenticiteit van de aanvrager geschiedt op basis van een vergunning die een verzekeringsonderneming ingevolge artikel 24, eerste lid, van de Wet toezicht verzekeringsbedrijf 1993 behoeft voor de uitoefening van de branche Aansprakelijkheid motorrijtuigen, en die wordt afgegeven door de Pensioen- & Verzekeringskamer, als bedoeld in artikel 2, lid1, Wet toezicht verzekeringsbedrijf 1993. Een gevolmachtigde wordt schriftelijk aangemeld bij de RA door de verzekeraar welke op grond van bovenstaande procedure geauthenticeerd is. De NAW-gegevens voor verzending van het certificaat alsmede de CRWAM-code zijn afkomstig uit het WAM register.

2 Authenticatie van aanvragers op basis van de beheersregeling(en)

- De authenticatie van de aanvragers van certificaten welke vallen onder beheersregeling(en) wordt geborgd door interne procedures.

3.1.9 Authenticatie van natuurlijke personen

Er worden certificaten uitgegeven aan natuurlijke personen, mits deze in het bezit zijn van een erkenning (zie bijvoorbeeld artikel 62, lid 1 WVW 1994 voor erkenning bedrijfsvoorraad).

3.2 Routinematige heruitgifte van een certificaat

Heruitgifte van een certificaat betekent het genereren van een nieuw sleutelpaar en certificaat voorafgaand aan het verstrijken van de geldigheidsduur van een certificaat.

De RDW CA draagt zorg voor de tijdige verstrekking van een nieuw certificaat voorafgaand aan het verstrijken van de geldigheidsduur van het bestaande certificaat, dan wel waarschuwt tijdig, zodat de certificaathouder het certificaat kan vervangen via de daarvoor door de CA ter beschikking gestelde middelen (online vervanging)

De CA zal slechts certificaten heruitgeven indien op het moment van heruitgifte de betreffende eind-entiteiten nog steeds voldoen aan de bij of krachtens de Wegenverkeerswet, de Wet aansprakelijkheidsverzekering motorrijtuigen, dan wel de andere wettelijke regelingen ten aanzien van de taken van de RDW aan hen gestelde eisen, zoals beschreven onder § 3.1.8. Het heruitgifte proces voorziet daartoe in een controle procedure daaromtrent.

De CA zal slechts op verzoek van de RDW certificaten heruitgeven welke vallen onder beheersregeling(en).

3.3 Heruitgifte na intrekking van een certificaat

Heruitgifte na de intrekking van een certificaat betekent het genereren van een nieuw sleutelpaar en certificaat nadat het certificaat is ingetrokken.

1. De RDW kan een certificaat intrekken in het kader van het toezicht op de uitvoering van de wettelijke regeling(en), in het kader van de controle op de rechtmatigheid van de toegang tot de bij of krachtens de wet door de RDW beheerde registers of een certificaat intrekken om procedurele en/of technische redenen. Eventuele heruitgifte zal dan plaatsvinden conform de procedure voor initiële registratie (zie paragraaf 3.1).

2. De RDW kan een certificaat intrekken in het kader van de interne procedures als opgesteld voor certificaten welke vallen onder de beheersregeling(en).

3. Intrekking op verzoek van de certificaathouder kan worden gevolgd door een heruitgifte. Deze heruitgifte zal plaatsvinden conform de procedure voor initiële registratie, waarbij afhankelijk van de reden van intrekking bepaalde stappen versneld doorlopen kunnen worden.

3.4 Verzoek tot intrekking

1. De RDW kan in het kader van het toezicht op de uitvoering van de wettelijke regeling(en) een certificaat intrekken.

2. De RDW kan in het kader van het toezicht op de interne procedures van beheersregeling(en) een certificaat intrekken.

3. De RDW kan een certificaat intrekken in het geval een eind-entiteit niet langer voldoet aan de wettelijke regelingen ten aanzien van de taken van de RDW aan hem gestelde eisen en voorwaarden of een certificaat intrekken om procedurele en/of technische redenen.

4. De beëindiging van de relatie tussen verzekeraar en gevolmachtigde wordt schriftelijk gemeld door de verzekeraar of de Pensioen- & Verzekeringskamer bij de RDW, echter leidt niet tot intrekking van het certificaat maar tot intrekking van de autorisatie om het WAM register te raadplegen of te muteren.

5. Een eind-entiteit kan ook zelf een verzoek indienen tot intrekking van zijn certificaat, bijvoorbeeld indien zijn privé-sleutel is gecompromitteerd.

6. Aanvragen voor intrekking kunnen schriftelijk bij de RA worden ingediend. Indien de privé-sleutel is gecompromitteerd, kan intrekking telefonisch bij de CA worden aangevraagd (zie par. 4.4.3).

4. Operationele vereisten.

4.1 Certificaat aanvraag

Indien de aanvrager een verzoek indient voor het verkrijgen van een certificaat dan moet dit gedaan worden bij de verantwoordelijke RA.

4.2 Certificaat uitgifte

Als onderdeel van de certificaat uitgifte voor eind-entiteiten wordt binnen de RDW Issuing CA's een publiek / privaat sleutelpaar gegenereerd, waarna een certificaat wordt geproduceerd op basis van de publieke sleutel en de aanvraag gegevens van de entiteit. Na het genereren van het certificaat geeft de CA het certificaat uit aan de aanvrager. De uitgifte vindt plaats doordat de CA het certificaat en het gegeneerde publiek / privaat sleutelpaar vastlegt op een CD-rom of diskette dan wel online voor services certificaten en deze per post aan de aanvrager toestuurt.

4.3 Certificaat acceptatie

De aanvrager ontvangt het certificaat dat is vastgelegd op een CD-rom of diskette. De aanvrager ontvangt tegelijkertijd de gebruikersvoorwaarden die van toepassing zijn op het gebruik van het certificaat. De privé-sleutel op de CD-rom of diskette is beschermd door een installatiewachtwoord. De aanvrager ontvangt het installatiewachtwoord een dag later middels een wachtwoordbrief.

Door installatie van het certificaat verklaart de certificaathouder aan de voorwaarden voor de verkrijging ervan en aan de gebruikersvoorwaarden te (blijven) voldoen.

4.4 Certificaat intrekking

De CA is verantwoordelijk voor de intrekking van certificaten. Intrekking vindt plaats doordat de CA het ingetrokken certificaat toevoegt aan de CRL.

Na de intrekking van het certificaat wordt de certificaathouder hiervan op de hoogte gesteld.

4.4.1 Redenen voor intrekking

Geldige redenen voor de intrekking van een certificaat zijn:

1. Compromittering of verlies van de privé-sleutel of van het wachtwoord die in samenhang met de privé-sleutel toegang geven tot de RDW-applicaties.
2. Onjuistheid van de inhoud van een certificaat; intrekking vindt in deze situatie slechts plaats nadat de certificaathouder in de gelegenheid is gesteld zijn zienswijze daarover kenbaar te maken.
3. Op verzoek van de certificaathouder.
4. Het door de eind-entiteit niet langer voldoen aan de bij of krachtens de Wegenverkeerswet, de Wet aansprakelijkheidsverzekering motorrijtuigen dan wel de andere wettelijke regelingen ten aanzien van de taken van de RDW aan hem gestelde eisen en voorwaarden.
5. Het door de eind-entiteit niet langer voldoen aan de interne procedures die gelden voor certificaten als uitgegeven voor de beheersregeling(en).
6. De certificaathouder voldoet niet aan zijn verplichtingen zoals beschreven in dit CPS; intrekking vindt in deze situatie slechts plaats nadat de certificaathouderhouder in de gelegenheid is gesteld zijn zienswijze daarover kenbaar te maken.

4.4.2 Entiteiten bevoegd tot het intrekken van een certificaat

De volgende entiteiten zijn bevoegd om een verzoek tot intrekking in te dienen:

1. de CA,
2. de RA,
3. de certificaathouder.

4.4.3 Procedure voor een verzoek tot intrekking

Voor services certificaten geldt in eerste instantie online intrekking dan wel onderstaande zoals voor alle andere typen certificaten. De entiteit die een verzoek tot intrekking van een certificaat indient kan dit alleen doen door middel van:

1.1. Een schriftelijk verzoek aan de betreffende RDW RA indienen.

1.2. Een telefonisch verzoek; indien (mogelijk) sprake is van compromittering van zijn privé-sleutel, waardoor intrekking terstond moet worden uitgevoerd, kan de certificaathouder een telefonisch verzoek tot intrekking doen bij de desbetreffende RDW CA.

1.3. Het telefoonnummer hiervoor is 050-3656197 op werkdagen te bereiken van

1.4. 07.30 – 17.00 uur. De CA zal het telefonische verzoek in beide gevallen verifiëren door de certificaathouder terug te bellen op het bij de CA bekende telefoonnummer.

4.4.4 Geldigheidsperiode van een verzoek tot intrekking

RDW behandelt een verzoek tot intrekking zo spoedig mogelijk maar uiterlijk binnen 10 werkdagen na ontvangst van het verzoek. Bij mogelijke compromittering zal de RDW, na ontvangst van het verzoek, het verzoek tot intrekking terstond afhandelen.

4.4.5 Schorsing van een certificaat

Niet van toepassing.

4.4.6 Uitgifte frequentie CRL

De CRL wordt na iedere intrekking en minimaal één keer per 24 uur ververst.

4.4.7 Vereisten voor het controleren van een CRL

Het certificaat uitgegeven door een RDW Issuing CA's bevat geen CRL Distribution Point (CDP). Controle op de geldigheid van de certificaten moet daarom specifiek op webservers worden geconfigureerd en/of in relevante applicaties worden ingebouwd.

4.4.8 Beschikbaarheid on-line controle van intrekkingsstatus

Deze server is minimaal dubbel uitgevoerd op twee verschillende locaties. Deze server is 7 dagen per week en 24 uur per dag beschikbaar.

4.4.9 Vereisten on-line controle van intrekkingstatus

Zie 4.4.7.

4.4.10 Andere vormen van publiceren intrekkingstatus

Niet van toepassing.

4.4.11 Speciale vereisten in geval van compromittering van de privé-sleutel

1. In geval van compromittering van de privé-sleutel van de RDW Root of de RDW Issuing CA's zal de RDW zich inspannen om zo spoedig mogelijk alle entiteiten binnen de RDW-PKI inlichten.
2. In geval van compromittering of verlies van de privé-sleutel van een eind-entiteit zal deze zo spoedig mogelijk een verzoek tot intrekking van het certificaat indienen bij de RA.

4.5 Security Audit Procedures

4.5.1 Gebeurtenissen die worden gelogd

De volgende gebeurtenissen worden binnen de RDW PKI gelogd, hetzij automatisch hetzij handmatig:

- Rond de certificaat levenscyclus
  - de aanvraag van een certificaat,
  - de gegevens waartegen de eind-entiteit werd geauthenticeerd.
  - de generatie van een publiek / privaat sleutel paar voor een eind-entiteit
  - de generatie van een certificaat,
  - de uitgifte van een certificaat,
  - het intrekken van certificaten
  - de generatie van CRLs
- Rond het beheer van de CA sleutels binnen de RDW PKI
  - Sleutel generatie, backup, recovery en vernietiging
  - Beveiligingsrelevante gebeurtenissen rond de gebruikte Hardware Security Modules (HSMs), zoals initialisatie en vernietiging.
- Beveiligingsrelevante gebeurtenissen bij de CA en RA systemen
  - Fysieke toegang tot CA systemen
  - Succesvolle en niet succesvolle aanlogpogingen
  - PKI of systeem relevante gebeurtenissen
  - Systeem opstart, uitval of shutdown

Gebeurtenissen gaan vergezeld met elementen waaruit het volgende kan worden afgeleid:

- Datum, tijd van de gebeurtenis.
- Identiteit van de bron die de gebeurtenis veroorzaakt.
- Identiteit van de bron die de gebeurtenis logt.

4.5.2 Frequentie van logverwerking

De gebeurtenissen uit par. 4.5.1. worden minimaal wekelijks beoordeeld.

4.5.3 Bewaarperiode van logs

De logs worden twee jaar bewaard.

4.5.4 Beveiliging van de audit logs

Audit logs zijn beschermd tegen ongeautoriseerde inzage, wijziging, verwijdering en vernietiging door gebruik te maken van een combinatie van fysieke en logische toegangbeveiliging.

4.5.5 Audit log back-up procedures

Van de digitale audit logs wordt een back-up gemaakt.

4.5.6 Audit collectie systeem (intern vs extern)

Niet van toepassing.

4.5.7 Kennisgeving van logging gebeurtenis

De RDW verplicht zich niet tot kennisgeving rond gebeurtenissen die gelogd zijn in de richting van de entiteit of de organisatie waar deze toe behoort. Kennisgeving zal slechts plaatsvinden indien de RDW dit noodzakelijk acht.

4.5.8 Kwetsbaarheidanalyses

In het kader van de beoordeling van de audit logs (zie paragraaf 4.5.2) wordt bepaald of er sprake is van zwakheden in de beveiliging in de RDW PKI omgeving. Geconstateerde (mogelijke) zwakheden worden opgevolgd. Deze beoordelingen en de mogelijk geconstateerde zwakheden worden vastgelegd.

4.6 Archivering van documenten

4.6.1 Gebeurtenissen die worden gearchiveerd

Een overzicht van de gebeurtenissen die worden gearchiveerd is beschreven in interne procedures van de RDW en zijn in overeenstemming met relevante wet- en regelgeving, waaronder de Archiefwet 1995.

4.6.2 Bewaarperiode archief

Zie 4.6.1.

4.6.3 Bescherming van archief

Zie 4.6.1

4.6.4 Archief back-up procedures

Er zijn maatregelen genomen die waarborgen dat het archief zodanig wordt bewaard, dat verlies in redelijkheid is uitgesloten. De RDW verplicht zich niet tot kennisgeving rond de archivering in de richting van de entiteit of de organisatie waar deze toe behoort. Kennisgeving zal slechts plaatsvinden indien de RDW dit noodzakelijk acht.

4.6.5 Vereisten voor het tijdstempelen van documenten

Alle gebeurtenissen zoals beschreven in par. 4.6.1 worden voorzien van een tijdsmarkering.

4.6.6 Archief systeem

Alle gearchiveerde gebeurtenissen worden intern opgeslagen.

4.6.7 Procedures ter verkrijging en verificatie van archief informatie

De zaken genoemd in 4.6.1 worden periodiek gecontroleerd op integriteit. Deze controles vinden jaarlijks plaats in het kader van de reguliere EDP-audits.

4.7 Verstrekken van RDW PKI Sleutels

De publieke sleutels die deel uit maken van de RDW PKI worden automatisch mee geïnstalleerd bij de installatie van het eind-entiteit certificaat. Bij een eventuele wijziging van de eind-entiteit publieke sleutels zijn de CPS-artikelen 3.2 en 3.3 van toepassing.

De RDW geeft geen certificaten uit met een levensduur die langer is dan die van één der bovenliggende CA's, te weten de RDW Root CA of RDW Issuing CA's. Dit betekent dat er een tijdstip ontstaat dat de certificaten van de bovenliggende CA's nog wel geldig zijn, maar dat er geen nieuwe eind-entiteit certificaten kunnen worden uitgegeven. Tijdig voor dit tijdstip zal de RDW zorg dragen dat de betreffende CA sleutels worden vervangen. De RDW zal de door de RDW erkende providers hiervan tijdig op de hoogte stellen en zorg dragen dat zij beschikking krijgen over authentieke kopieën van de nieuwe certificaten gebaseerd op deze sleutels. De procedures rond revocatie en de publicatie van CRLs inzake de vervangen CA's blijven van kracht tijdens de resterende levensduur van de certificaten van deze CA's.

4.8 Compromitteren van de privé-sleutel en calamiteitenbeheersing

De back-up- en recoveryprocedures in geval van calamiteiten zijn onderdeel van de interne procedures van de RDW zoals neergelegd in de RDW-calamiteitenplanning. De RDW verplicht zich niet tot kennisgeving rond de genoemde procedures in de richting van de entiteit of de organisatie waar deze toe behoort. Kennisgeving zal slechts plaatsvinden indien de RDW dit noodzakelijk acht.

4.8.1 Computers, software, en/of data zijn gecorrumpeerd

De RDW heeft toereikende maatregelen genomen die in redelijkheid waarborgen dat bij gecorrumpeerde computers, software en/of data de dienstverlening binnen de gemaakte afspraken kan worden hersteld.

4.8.2 Intrekking van een publieke sleutel

In het geval dat de publieke sleutel van de RDW Root of de RDW Issuing CA's dient te worden ingetrokken zal de RDW zich inspannen om alle eind-entiteiten hiervan tijdig te notificeren, waarbij getracht wordt een periode van minimaal 60 dagen voorafgaand aan de geplande intrekking in acht te nemen.

4.8.3 Compromittering van privé-sleutel

Zie 4.4.11.

4.8.4 Uitwijkmogelijkheden

De procedures met betrekking tot uitwijkmogelijkheden zijn beschreven in interne procedures van de RDW. De RDW verplicht zich niet tot kennisgeving rond de genoemde procedures in de richting van de entiteit of de organisatie waar deze toe behoort. Kennisgeving zal slechts plaatsvinden indien de RDW dit noodzakelijk acht.

4.9 CA beëindiging

Bij beëindigen van RDW Issuing CA's activiteiten draagt deze CA zorg voor de volgende handelingen:

1. De CA informeert de root CA van het voornemen om haar activiteiten als CA te staken,
2. De CA stelt alle entiteiten binnen de RDW PKI schriftelijk op de hoogte van haar voornemen om haar activiteiten als CA te staken, minimaal 60 dagen voorafgaand hieraan.
3. Alle niet verlopen certificaten uitgegeven door de CA worden gerevokeerd conform de procedures genoemd in paragraaf 4.4.
4. De CA dient een verzoek in ter intrekking van het CA certificaat bij de root CA.

5. Fysieke, procedurele en personele beveiligingsmaatregelen.

De RDW draagt zorg voor een adequate fysieke, procedurele en personele informatiebeveiliging om de risico's op verlies, beschadiging, en compromittering van essentiële componenten van de CA dienstverlening tot een minimum te beperken. Dit geldt in het bijzonder voor de omgeving van de CA, waar de certificaten worden uitgegeven.

De fysieke, procedurele en personele beveiligingsmaatregelen zijn beschreven in interne procedures van de RDW. Deze worden minimaal één keer per jaar geaudit. Relevante bemerkingen zullen worden gepubliceerd in het RDW jaarverslag.

6. Technische beveiligingsmaatregelen.

6.1 Genereren sleutelpaar en installatie

6.1.1 Genereren sleutelpaar

1. De sleutelparen van de CA's binnen de RDW PKI worden in een Hardware Security Module (HSM) gegenereerd
2. De sleutelparen van de eind-entiteiten worden in een Hardware Security Module (HSM) gegenereerd.

6.1.2 Aflevering van privé-sleutel aan eind-entiteit

De privé-sleutel wordt door de desbetreffende Issuing CA aan de eind-entiteit toegestuurd. De privé-sleutel is beveiligd met een installatiewachtwoord dat middels een brief minimaal een dag later per post aan de eind-entiteit zal worden toegestuurd dan wel online via SSL aan de certificaathouder getoond. Het installatiewachtwoord is voor de RDW niet zichtbaar en niet reproduceerbaar.

6.1.3 Aflevering van publieke sleutel aan de CA

Niet van toepassing. Eind-entiteiten hoeven hun publieke sleutel niet naar de CA te sturen.

6.1.4 Aflevering van de publieke sleutel van de CA aan eind-entiteiten

De publieke-sleutel van de CA wordt op dezelfde wijze afgeleverd als de privé-sleutel van de eind-entiteit. Tijdens de installatieprocedure wordt de publieke-sleutel van de CA bij de eind-entiteit geïnstalleerd.

6.1.5 Sleutellengten

De lengtes van de publieke en privé sleutels binnen de RDW PKI zijn:
2048 bit voor de RDW Root en RDW Diensten
1024 bit voor de RDW eind-entiteiten

6.1.6 Parameters ten behoeve van het genereren van publieke sleutels

De parameterinstelling van publieke sleutels is gebaseerd op RSA.

6.1.7 Controle kwaliteit parameters

Er wordt een Hardware Security Module (HSM) gebruikt voor het genereren, beschermen en eventueel vernietigen van de CA privé-sleutel.

6.1.8 Genereren hardware/software sleutel

De sleutels van de CA's en van eind-entiteiten worden door middel van hardware gegenereerd.

6.1.9 Gebruik publieke sleutels

De publieke sleutel behorende bij het certificaat van een eind-entiteit is uitsluitend bestemd voor doelen zoals beschreven in paragraaf 1.3.4 (toepasbaarheid). In de extensie van het certificaat zijn deze doelen vastgelegd.

6.2 Bescherming van de privé-sleutel

1. Algemeen
   1.1. Het beschermen van CA privé-sleutels vindt plaats door middel van een Hardware Security Module (HSM)
   1.2. De eind-entiteit is exclusief verantwoordelijk voor het beschermen van zijn privé-sleutel.
2. RDW Diensten CA
   2.1. Voordat de privé-sleutel in de browser van de eind-entiteit is geïmporteerd (en zich derhalve op de CD-rom of diskette bevindt) is de privé-sleutel beschermd door middel van een wachtwoord die per aparte brief aan de eind-entiteit per post zal worden toegestuurd.
   2.2. Indien de eind-entiteit de privé-sleutel importeert in zijn browser dient hij deze te beschermen door middel van een zelfgekozen wachtwoord.
   2.3. De installatie van de privé-sleutel dient zodanig te geschieden dat de privé-sleutel niet geëxporteerd kan worden.
3. RDW Services CA
   3.1. Het wachtwoord dat gebruikt wordt om het bestand met de privé-sleutel en het certificaat te openen, moet eenmalig tijdens het opstarten handmatig worden ingevoerd en mag niet in bestanden worden opgeslagen.
   3.2. Het wachtwoord dient willekeurig te zijn, minimaal 10 karakters lang en te worden samengesteld uit 58 karakters. Bijvoorbeeld de karakters {a-z, A-Z en 0-9} waaruit de gelijkvormige karakters '1', 'l', 'O' en '0' zijn weggelaten.
   3.3. De privé-sleutel moet worden opgeslagen als een versleuteld PKCS#12 bestand of een andere wijze met minimaal hetzelfde niveau van beveiliging.
   3.4. De privé-sleutel dient zodanig te worden gebruikt en opgeslagen dat toegang slechts mogelijk is voor een zeer beperkte groep van personen die hiervoor expliciet zijn geautoriseerd door de hoogst verantwoordelijke persoon binnen de organisatie en een geheimhoudingsverklaring hebben ondertekend.
   3.5. De privé-sleutel mag tijdens het gebruik op geen enkele manier vanaf in- of externe netwerken (internet) benaderd kunnen worden.

6.2.1 Standaarden cryptografische module

Er wordt een Hardware Security Module gebruikt voor het genereren, beschermen en eventueel vernietigen van de CA privé-sleutel.

6.2.2 Functiescheiding met betrekking tot beheer privé-sleutel

Beheer van privé-sleutels van CA's is slechts mogelijk in de fysieke aanwezigheid van minimaal drie daartoe geautoriseerde RDW PKI medewerkers.

6.2.3 Escrow privé-sleutel

Er vindt geen escrowing van CA privé-sleutels of eind-entiteiten plaats.

6.2.4 Back up privé-sleutel

1. Van CA privé-sleutels is een backup gemaakt.
2. Van de privé-sleutel van de eind-entiteiten wordt geen backup gemaakt, maar kan vanaf CD-rom of diskette opnieuw worden geïnstalleerd.

6.2.5 Archivering privé-sleutel

Niet van toepassing

6.2.6 Invoer privé-sleutel in cryptografische module

De CA privé-sleutels worden in principe gegenereerd in de cryptografische module (HSM) waarin ze worden gebruikt. Slechts in het geval van recovery is er sprake van invoer van een privé-sleutel. Deze vindt plaats door de versleutelde inhoud van de HSM die hersteld moet worden beschikbaar te stellen aan een nieuwe HSM en deze in te lezen. Hiertoe dienen minimaal drie geautoriseerde personen aanwezig te zijn.

6.2.7 Activeren privé-sleutel

De privé-sleutel van de eind-entiteit kan gebruikt worden op het moment dat het juiste wachtwoord is ingevoerd.

6.2.8 Buiten werking stellen privé- sleutel

Elke eind-entiteit die toegang heeft tot zijn privé-sleutel kan deze buiten werking stellen door deze te de-ïnstalleren.

6.2.9 Vernietiging privé- sleutel

Zie par. 6.2.8. Voor definitieve vernietiging van de privé-sleutel dient deze te worden verwijderd van alle drager(s) dan wel de drager te worden vernietigd.

6.3 Overige aspecten van sleutelbeheer

6.3.1 Archivering publieke sleutels

1. De publieke sleutels van de CA's worden gearchiveerd.
2. De publieke sleutels van de eind-entiteiten worden niet gearchiveerd.

6.3.2 Periode van gebruik sleutels

1. De geldigheidsduur van het Root CA certificaat bedraagt 12 jaar.
2. De geldigheidsduur van het Diensten CA certificaat bedraagt 6 jaar
3. De geldigheidsduur van het certificaat van een eind-entiteit bedraagt 2 jaar.
4. De geldigheidsduur van een certificaat uitgegeven op basis van een beheersregeling varieert van 2,5 – 6 jaar.

6.4 Activeringsdata

6.4.1 Generatie en installatie

De privé-sleutels van eind-entiteiten zijn beveiligd door een wachtwoord dat gegenereerd wordt de RDW Issuing CA's software. Eind-entiteiten dienen bij installatie hun privé-sleutels te beveiligen met een door hen zelf te kiezen wachtwoord.

6.4.2 Bescherming van activeringsdata

Het wachtwoord dat dient ter beveiliging van de privé-sleutel dient uniek en onvoorspelbaar te zijn en van een zodanige lengte zodat deze in verhouding staat met sleutel die beveiligd wordt. Het wachtwoord moet uit minimaal 6 karakters bestaan. Deze karakters kunnen zijn: de letters van het alfabet, de hoofdletters van het alfabet en de cijfers 0 t/m 9.

6.4.3 Overige aspecten

Niet van toepassing.

6.5 Computer beveiligingsmaatregelen

De specifieke technische beveiligmaatregelen zijn beschreven in interne procedures van de RDW.

7. Certificaat en CRL-profiel.

7.1 Certificaatprofiel

Alle certificaten die worden uitgegeven betreffen X.509 versie 3 certificaten.
Deze certificaten bevatten de volgende velden:

7.1.1 Inhoud certificaten

Inhoud Root CA certificaat

Version	3 (is gelijk aan X.509 versie 3)
Serial number	Uniek serienummer
Issuer Distinguished name	
Country (C)	NL
Organization (O)	RDW
Location (L)	Groningen
Common Name (CN)	Self Signed
Validity	
Not before	2002
Not after	2014
Subject	
Country (C)	NL
Organization (O)	RDW
Location (L)	Groningen
Common Name (CN)	RDW Root
Subject Public Key Info	2048 bit
X509v3 extensions	
X509v3 Basic Constraints	Critical; CA: TRUE, pathlen:1
X509v3 Key Usage	Critical; Certificate Sign, CRL Sign
X509v3 Subject Key Identifier	

Inhoud RDW Diensten certificaat

Version	3 (is gelijk aan X.509 versie 3)
Serial number	Uniek serienummer toegekend door de RDW Root CA
Issuer Distinguished name	
Country (C)	NL
Organization (O)	RDW
Location (L)	Groningen
Common Name (CN)	RDW Root CA
Validity	
Not before	2002
Not after	2008
Subject	
Country (C)	NL
Organization (O)	RDW
Location (L)	Groningen
Common Name (CN)	RDW Diensten CA
Subject Public Key Info	2048 bit
X509v3 extensions	
X509v3 Basic Constraints	Critical; CA: TRUE, pathlen:0
X509v3 Key Usage	Critical; Certificate Sign, CRL Sign
X509v3 Subject Key Identifier	

Inhoud RDW Services certificaat

Version	3 (is gelijk aan X.509 versie 3)
Serial number	Uniek serienummer toegekend door de RDW Root CA
Issuer Distinguished name	
Country (C)	NL
Organization (O)	RDW
Location (L)	Groningen
Common Name (CN)	RDW Root CA
Validity	
Not before	2004
Not after	2010
Subject	
Country (C)	NL
Organization (O)	RDW
Location (L)	Groningen
Common Name (CN)	RDW Services CA
Subject Public Key Info	2048 bit
X509v3 extensions	
X509v3 Basic Constraints	Critical; CA: TRUE, pathlen:0
X509v3 Key Usage	Critical; Certificate Sign, CRL Sign
X509v3 Subject Key Identifier	

Inhoud certificaten van eind-entiteiten

- **Erkenninghouders***
- **Verzekeraars en gevolmachtigden****

Version	3 (is gelijk aan X.509 versie 3)
Serial number	Uniek serienummer toegekend door de RDW Diensten CA
Issuer Distinguished name	
Country (C)	NL
Organization (O)	RDW
Location (L)	Groningen
Common Name (CN)*	RDW Diensten
Common Name (CN)**	RDW Diensten-CRWAM code
Validity	
Not before	Jaar, maand en dag van uitgifte
Not after	Jaar, maand en dag van uitgifte plus 730 dagen
Subject	
Organization (O)	Relatie ID
Organizational Unit (OU)	
Common Name (CN)	RDW Diensten-KvK
Subject Public Key Info	1024 bit
X509v3 extensions	
X509v3 Key Usage	Critical; Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment
X509v3 Authority Key Identifier	
Netscape Cert Type	SSL Client, S/MIME

Inhoud certificaten van Productie-Acceptatie certificaten

Version	3 (is gelijk aan X.509 versie 3)
Serial number	Uniek serienummer toegekend door de RDW Diensten CA
Issuer Distinguished name	
Country (C)	NL
Organization (O)	RDW
Location (L)	Groningen
Common Name (CN)	RDW acceptatietest-KvK
Validity	
Not before	Jaar, maand en dag van uitgifte
Not after	Jaar, maand en dag van uitgifte (varieert van 2,5 – 6 jaar)
Subject	
Organization (O)	Relatie ID
Organizational Unit (OU)	
Common Name (CN)	RDW Diensten-KvK
Subject Public Key Info	1024 bit
X509v3 extensions	
X509v3 Key Usage	Critical; Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment
X509v3 Authority Key Identifier	
Netscape Cert Type	SSL Client, S/MIME

Inhoud certificaten van RDW Services

Version	3 (is gelijk aan X.509 versie 3)
Serial number	Uniek serienummer toegekend door de RDW Services CA
Issuer Distinguished name	
Country (C)	NL
Organization (O)	RDW
Location (L)	Groningen
Common Name (CN)	RDW Services CA
Validity	
Not before	Jaar, maand en dag van uitgifte
Not after	Jaar, maand en dag van uitgifte (2 jaar)
Subject	
Organization (O)	Relatie ID
Organizational Unit (OU)	
Common Name (CN)	(Door aanvrager gekozen naamgeving)
Subject Public Key Info	1024 bit
X509v3 extensions	
X509v3 Key Usage	Critical; Digital Signature, Key Encipherment, Data Encipherment
X509v3 Authority Key Identifier	
Netscape Cert Type	SSL Client, S/MIME

Inhoud certificaten van servercertificaten

Version	3 (is gelijk aan X.509 versie 3)
Serial number	Uniek serienummer toegekend door de RDW Diensten CA
Issuer Distinguished name	
Country (C)	NL
Organization (O)	RDW
Location (L)	Groningen
Common Name (CN)	RDW Diensten
Validity	
Not before	Jaar, maand en dag van uitgifte
Not after	Jaar, maand en dag van uitgifte (varieert van 2,5 – 6 jaar)
Subject	
Organization (O)	Relatie ID
Organizational Unit (OU)	
Common Name (CN)	RDW Diensten-KvK
Subject Public Key Info	1024 bit
X509v3 extensions	
X509v3 Key Usage	Critical; Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment
X509v3 Authority Key Identifier	
Netscape Cert Type	SSL Client, S/MIME

7.1.2 ***Versie nummers***
De CA genereert X.509 versie 3 certificaten.

7.1.3 ***Certificaat extensies***
De certificaten binnen de RDW PKI bevatten X.509v3-extensies.
Zie par. 7.1.1
De eind-entiteit certificaten bevatten de volgende PKCS#12 extensies:
1. Bescherming privé sleutel tijdens transport met installatie wachtwoord
2. Publieke sleutels (certificate chain) worden mee geïnstalleerd.

7.1.4 ***Algoritme object identifiers***
Niet van toepassing.

7.1.5 ***Vormen van de naamgeving***
Zie paragraaf 3.1.1 en verder.

7.1.6 ***Beperkingen aan de naamgeving***
Zie par. 3.1.1. en verder.

7.1.7 ***Certificate policy object identifiers***
Worden niet toegepast

7.1.8 ***Gebruik van policy constraints extensie***
Deze extensie wordt niet gebruikt.

7.1.9 ***Policy beperkingen syntaxis en betekenis***
Niet van toepassing.

7.1.10 ***Betekenis voor de afhandeling van critical certificate policy extensie***
Niet van toepassing.

7.2 CRL-profiel

7.2.1 ***Versienummer CRL***
De Certificate Revocation List wordt gepubliceerd in het X.509 v3-formaat.

7.2.2 ***CRL en CRL-entry extensies***
Niet van toepassing.

8. Specificatie administratieve procedures.

8.1 Specifieke wijzigingsprocedures

1. De RDW is bevoegd tot het wijzigen van de bepalingen in dit CPS.
2. Indien er bepalingen uit dit CPS gewijzigd worden waarvan de wijziging van invloed is op de rechten, verplichtingen en bevoegdheden van de entiteiten binnen de PKI zal de RDW deze wijzigingen publiceren en bekendmaken aan deze entiteiten zoals beschreven in par. 8.2.
3. Voor wat betreft wijziging van bepalingen van de CPS die geen materiele gevolgen hebben voor entiteiten binnen de PKI is de RDW niet verplicht om deze wijzigingen kenbaar te maken aan de entiteiten binnen haar PKI. De RDW zal de herziene CPS publiceren op haar website.

8.2 Publicatie- en bekendmakingsbeleid

8.2.1 Onderdelen van de CPS die niet worden gepubliceerd.

Documenten inzake het gedetailleerde beheer van de RDW PKI worden door de RDW als vertrouwelijk bestempeld en zullen niet worden openbaard aan het publiek.

8.2.2 Distributiewijze van CPS

1. Indien de CPS gewijzigd wordt zullen alle entiteiten binnen de RDW PKI, met inachtneming van 8.1 punt 3, hiervan op de hoogte worden gesteld.
2. De entiteiten binnen de PKI zullen op de hoogte worden gebracht door middel van een brief en publicatie van de CPS op de website van de RDW, www.rdw.nl/cps

8.3 Goedkeurings- en wijzigingsprocedure

Dit CPS wordt uitgegeven door en onder verantwoordelijkheid van de Algemeen Directeur van de RDW.

De procedure voor wijzigingen en goedkeuringen van het CPS is als volgt:

1. Voorstellen tot wijziging kunnen worden ingediend door de organisatie-onderdelen van de Dienst Wegverkeer aan wie de uitvoering van de CA of RA taken conform dit CPS is opgedragen dan wel organisatie-onderdelen ten behoeve waarvan de RDW Issuing CA's wordt ingezet;
2. De Algemeen Directeur is verantwoordelijk voor de verwerking van de voorstellen. Hij kan zich hierbij laten adviseren door inhoudelijk experts, onder andere op technisch, procedureel, commercieel en juridisch gebied. Uiteindelijk beslist de Algemeen Directeur of een voorstel tot wijziging wordt doorgevoerd; en
3. Indien het voorstel is goedgekeurd, laat de Algemeen Directeur het CPS aanpassen. Indien op grond van onderdeel 8.1 van dit CPS voor inwerkingtreding voorafgaande inkennisstelling van de certificaathouders noodzakelijk is, draagt de Algemeen Directeur tevens hiervoor de verantwoordelijkheid.

De wijziging treedt in werking vijf werkdagen nadat de nieuwe CPS door de Algemeen Directeur is bekend gemaakt.

9. Formele goedkeuring.

Akkoord algemeen directeur RDW

Datum:

10. Bijlagen.

10.1 Gebruikte afkortingen

CA	Certification Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List
ID	Identifier
IETF	Internet Engineering Task Force
ITU	International Telecommunication Union
HTTPS	Hypertext Transfer Protocol over SSL
HSM	Hardware Security Module
PKCS	Public-Key Cryptography Standards
PKIX	Public-Key Infrastructure X.509
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request for Comment
SSL/TLS	Secure Sockets Layer / Transport Layer Security
WAM	Wet Aansprakelijkheidsverzekering Motorrijtuigen

10.2 Verklarende woordenlijst

Aanvrager
Een entiteit die een certificaat aanvraagt bij een RA.

Audit
Een procedure uitgevoerd door een auditor waarbij wordt nagegaan of de bepalingen in de CPS worden nageleefd.

Authenticatie
Het proces om de identiteit van een eind-entiteit of de integriteit van bepaalde informatie te bevestigen.

Autorisatie
De bevoegdheid die wordt verleend om toegang te krijgen tot de RDW informatiesystemen.

Beheersregeling(en)
Regelingen met een intern karakter in het kader van de uitvoering van wettelijke regelingen.

Certificaat (digitaal certificaat)
Een publieke sleutel certificaat dat de publieke sleutel van een entiteit bindt aan de identiteit van deze entiteit en dat de geldigheid van de corresponderende privé-sleutel aanduidt. Een certificaat biedt waarborgen omtrent de identiteit van eind-entiteiten en diens bevoegdheden bij het langs elektronische weg uitwisselen van berichten en andere vormen van datacommunicatie door het gebruik van een door hem gegenereerd sleutelpaar bestaande uit een privé-sleutel en een publieke sleutel.

Certification Authority (CA)
Een vertrouwde autoriteit die certificaten creëert en uitgeeft.

Certificaat extensie
Extensie-velden in X.509 versie 3 certificaten.

Certificaathouder
De eind-entiteit, CA of RA die in het bezit is van de privé-sleutel die correspondeert met een publieke sleutel.

Certificaat keten
Een geordende lijst van certificaten die nodig zijn om een certificaat te valideren.
Een certificaat keten bestaat uit certificaten van eind-entiteiten, certificaten van CA's die de certificaten van eind-entiteiten hebben ondertekend en certificaten van CA's die de certificaten van onderliggende CA's hebben ondertekend.

Certificaat management
Certificaat management omvat onder andere de opslag, verspreiding, publicatie en intrekking van certificaten.

Certificate Revocation List (CRL)
Een door de CA getekende lijst met ingetrokken certificaten.

Certificate Policy (CP)

Een gedetailleerde beschrijving binnen welke gebruiksgebieden, voor welke toepassingen en voor welke doeleinden certificaten worden uitgegeven.

Certificatie
Het proces van certificaatuitgifte door een CA.

Certification Practice Statement (CPS)
Een gedetailleerde beschrijving van de praktijken die de CA hanteert bij het uitgeven van certificaten.

Client systeem
Dit is het systeem van de eind-entiteit die aanvragen doet bij de webserver.

Compromittering
Het verlies van de vertrouwelijkheid van de privé-sleutel; bijvoorbeeld indien een onbevoegde persoon een kopie van de sleutel verkrijgt.

Distinguished name
Een set van gegevens die een eind-entiteit identificeren.

Eind-entiteit
Een certificaathouder of een aanvrager, die geen CA of RA is.

Gebruikersvoorwaarden
Document met de verplichtingen voor de eind-entiteit die als geaccepteerd wordt beschouwd zodra het certificaat wordt geïnstalleerd.

Genereren van een sleutelpaar
Het proces van het creëren van een publieke en privé-sleutel.

Identificatie
Het proces ter bevestiging van de identiteit van een eind-entiteit.

Object identifier
Een uniek nummer dat gekoppeld is aan dit CPS.

Privé-sleutel
Een door middel van een wiskundig programma gegenereerde code die door de certificaathouder geheim wordt gehouden.

Productie-Acceptatie certificaat
Certificaten uitgegeven aan belanghebbenden voor “ketentest”-doeleinden en het verschaffen van toegang tot de acceptatie-omgeving.

Public Key Infrastructure (PKI)
Het geheel van hardware, software, personen, procedures en beleid die noodzakelijk zijn voor het creëren, managen, opslaan, distribueren en herroepen van certificaten gebaseerd op public key cryptografie.

Publieke-sleutel
Een door middel van een wiskundig programma gegenereerde code die openbaar is en die is opgenomen in het certificaat.

Registration Authority (RA)
Een entiteit die verantwoordelijk is voor de identificatie en authenticatie van eind-entiteiten. Een RA ondertekent geen certificaten en geeft geen certificaten uit.

Relying party
Een persoon of organisatie die handelt op basis van vertrouwen in een certificaat en op basis daarvan toegang verleent tot de online RDW-dienstverlening.

Repository
Een on-line database met relevante informatie met betrekking tot de PKI. In een repository kunnen de CRL of een lijst met uitgegeven certificaten worden gepubliceerd.

Root CA
De CA die het eerste certificaat in een certificaat keten uitgeeft.

Server certificaat
Een RDW-certificaat gekoppeld aan een server of een stukje informatie om zekerheid te geven omtrent de identiteit van de server.

Services certificaat
Een RDW-certificaat gekoppeld aan een server of een stukje informatie om zekerheid te geven omtrent de identiteit van de server van de wederpartij.

Sleutelpaar
Een publieke sleutel en een hierbij behorende privé-sleutel.

Secure Socket Layer (SSL) / TLS
Een cryptografisch protocol dat het mogelijk maakt om op een veilige manier gegevens via het internet te kunnen versturen (HTTPS).

Wachtwoord
Een unieke code die de aanvrager in staat stelt het door hem aangevraagde certificaat te activeren.

Webserver
Een computersysteem dat reageert op verzoek van client systemen.

X.509
De standaard van de ITU-T (International Telecommunications Union-T) voor digitale certificaten. X.509 versie 3 verwijst naar certificaten die extensies bevatten of kunnen bevatten.